Documentação de backup e recuperação do BlueXP

BlueXP backup and recovery

NetApp
December 13, 2024

Índice

Documentação de backup e recuperação do BlueXP

Notas de lançamento

Novidades do backup e recuperação do BlueXP

Saiba o que há de novo no backup e recuperação do BlueXP .

22 de novembro de 2024

Esta versão de backup e recuperação do BlueXP inclui as seguintes atualizações.

Modos de proteção SnapLock Compliance e SnapLock Enterprise

Agora, o backup e a recuperação do BlueXP podem fazer backup de volumes no local do FlexVol e do FlexGroup configurados com os modos de proteção SnapLock Compliance ou SnapLock Enterprise. Os clusters precisam estar executando o ONTAP 9.14 ou superior para esse suporte. O backup de volumes do FlexVol usando o modo SnapLock Enterprise tem sido suportado desde a versão 9.11.1 do ONTAP. As versões anteriores do ONTAP não oferecem suporte para fazer backup de volumes de proteção SnapLock.

Consulte a lista completa de volumes suportados no "Saiba mais sobre o backup e a recuperação do BlueXP ".

Indexação para processo de pesquisa e restauração na página volumes

Antes de poder utilizar a Pesquisa e Restauro, tem de ativar a "Indexação" em cada ambiente de trabalho de origem a partir do qual pretende restaurar os dados de volume. Isso permite que o Catálogo indexado acompanhe os arquivos de backup para cada volume. A página volumes agora mostra o status da indexação:

- Indexado: Os volumes foram indexados.
- Em curso
- Não indexado
- Indexação em pausa
- Erro
- Não ativado

27 de setembro de 2024

Esta versão de backup e recuperação do BlueXP inclui as seguintes atualizações.

Suporte a Podman no RHEL 8 ou 9 com Browse and Restore

O backup e a recuperação do BlueXP agora suportam restaurações de arquivos e pastas no Red Hat Enterprise Linux (RHEL) versões 8 e 9 usando o mecanismo Podman. Isso se aplica ao método de pesquisa e restauração de backup e recuperação do BlueXP .

O BlueXP Connector versão 3.9.40 suporta determinadas versões do Red Hat Enterprise Linux versões 8 e 9 para qualquer instalação manual do software Connector em um host RHEL 8 ou 9, independentemente do local, além dos sistemas operacionais mencionados no "requisitos de host" . Essas novas versões RHEL requerem o mecanismo Podman em vez do mecanismo Docker. Anteriormente, o backup e a recuperação do BlueXP tinham duas limitações ao usar o motor Podman. Estas limitações foram removidas.

"Saiba mais sobre como restaurar dados do ONTAP a partir de arquivos de backup".

A indexação mais rápida do catálogo melhora a Pesquisa e a Restauração

Esta versão inclui um índice de catálogo melhorado que completa a indexação da linha de base muito mais rápido. A indexação mais rápida permite que você use o recurso Pesquisa e Restauração mais rapidamente.

"Saiba mais sobre como restaurar dados do ONTAP a partir de arquivos de backup".

22 de julho de 2024

Restaure volumes com menos de 1 GB

Com esta versão, agora você pode restaurar volumes criados no ONTAP com menos de 1 GB. O tamanho mínimo de volume que você pode criar usando o ONTAP é de 20 MB.

Dicas sobre como mitigar os custos do DataLock

O recurso DataLock protege seus arquivos de backup de serem modificados ou excluídos por um período de tempo especificado. Isso é útil para proteger seus arquivos contra ataques de ransomware.

Para obter detalhes sobre o DataLock e dicas sobre como mitigar os custos associados, "Configurações de política de backup para objeto" consulte .

Integração com o AWS IAM em qualquer lugar

O serviço Amazon Web Services (AWS) Identity and Access Management (IAM) Role Anywhere permite que você use funções do IAM e credenciais de curto prazo para suas cargas de trabalho *fora* da AWS para acessar APIs da AWS com segurança, da mesma forma que você usa funções do IAM para cargas de trabalho *on* AWS. Quando você usa funções do IAM em qualquer infraestrutura de chave privada e tokens da AWS, não precisa de chaves de acesso e chaves secretas de longo prazo da AWS. Isso permite que você gire as credenciais com mais frequência, melhorando a segurança.

Com esta versão, o suporte para o serviço AWS IAM Roles Anywhere é uma prévia da tecnologia.

Consulte a "Blog de lançamento de backup e recuperação do BlueXP em julho de 2024".

Pasta FlexGroup ou restauração de diretório agora disponível

Anteriormente, os volumes do FlexVol podiam ser restaurados, mas não era possível restaurar pastas ou diretórios do FlexGroup. Com o ONTAP 9.15,1 P2, você pode restaurar pastas do FlexGroup usando a opção Procurar e restaurar.

Com esta versão, o suporte para a restauração de pastas FlexGroup é uma prévia da tecnologia.

Para obter detalhes, "Restaure pastas e ficheiros utilizando Procurar Restaurar" consulte .

Para obter detalhes para ativá-lo manualmente, "Blog de lançamento de backup e recuperação do BlueXP em julho de 2024" consulte .

17 de maio de 2024

Limitações ao usar RHEL 8 e RHEL 9 para seu conetor no local

O BlueXP Connector versão 3.9.40 suporta determinadas versões do Red Hat Enterprise Linux versões 8 e 9 para qualquer instalação manual do software Connector em um host RHEL 8 ou 9, independentemente do local, além dos sistemas operacionais mencionados no "requisitos de host" . Essas novas versões RHEL requerem o mecanismo Podman em vez do mecanismo Docker. Neste momento, o backup e recuperação do BlueXP tem duas limitações ao usar o motor Podman.

```
https://docs.netapp.com/us-en/bluexp-backup-recovery/reference-
limitations.html["Limitações de backup e restauração"]Consulte para obter
detalhes.
```

Os procedimentos a seguir incluem novas instruções do Podman:

- "Reinicie o backup e a recuperação do BlueXP "
- "Restaure os dados de recuperação e backup do BlueXP em um local escuro"

30 de abril de 2024

Capacidade de ativar ou desativar varreduras programadas de ransomware

Anteriormente, você poderia ativar ou desativar varreduras de ransomware, mas não poderia fazer isso para varreduras agendadas.

Com esta versão, agora você pode ativar ou desativar varreduras de ransomware agendadas na cópia Snapshot mais recente usando a opção na página Configurações avançadas. Se você ativá-lo, as verificações são realizadas semanalmente por padrão. Você pode alterar esse horário para dias ou semanas ou desativá-lo, economizando custos.

Consulte as seguintes informações para obter detalhes:

- "Gerir as definições de cópia de segurança"
- "Gerenciar políticas para ONTAP volumes"
- "Configurações de política de backup para objeto"

04 de abril de 2024

Capacidade de ativar ou desativar varreduras de ransomware

Anteriormente, quando você ativou a detecção de ransomware em uma política de backup, as verificações ocorreram automaticamente quando o primeiro backup foi criado e quando você restaurou um backup. Anteriormente, o serviço digitalizava todas as cópias Snapshot e não era possível desativar as digitalizações.

Com esta versão, agora você pode ativar ou desativar varreduras de ransomware na cópia Snapshot mais recente usando a opção na página Configurações avançadas. Se você ativá-lo, as verificações são realizadas semanalmente por padrão.

Consulte as seguintes informações para obter detalhes:

- "Gerir as definições de cópia de segurança"

- "Gerenciar políticas para ONTAP volumes"
- "Configurações de política de backup para objeto"

```
https://docs.netapp.com/us-en/bluexp-backup-recovery/task-backup-to-
s3.html["Fazer backup de dados do Cloud Volumes ONTAP para o Amazon
S3"]Consulte e https://docs.netapp.com/us-en/bluexp-backup-
recovery/task-backup-to-azure.html["Fazer backup de dados do Cloud
Volumes ONTAP para o Azure Blob"].
```

12 de março de 2024

Possibilidade de fazer "restaurações rápidas" de backups na nuvem para volumes ONTAP no local

Agora você pode executar uma *restauração rápida* de um volume do storage de nuvem para um volume de destino ONTAP no local. Anteriormente, você poderia executar uma restauração rápida apenas para um sistema Cloud Volumes ONTAP. A restauração rápida é ideal para situações de recuperação de desastres em que você precisa fornecer acesso a um volume o mais rápido possível. Uma restauração rápida é muito mais rápida do que a restauração de volume total. Ela restaura os metadados de um snapshot de nuvem para um volume de destino do ONTAP. A fonte poderia ser AWS S3, Azure Blob, Google Cloud Services ou NetApp StorageGRID.

O sistema de destino ONTAP local deve estar executando o ONTAP versão 9.14.1 ou superior.

Você pode fazer isso usando o processo Procurar e restaurar, não o processo de pesquisa e restauração.

Para obter detalhes, "Restaure dados do ONTAP a partir de arquivos de backup" consulte .

Capacidade de restaurar arquivos e pastas de cópias Snapshot e replicação

Anteriormente, você poderia restaurar arquivos e pastas apenas de cópias de backup na AWS, Azure e Google Cloud Services. Agora, você pode restaurar arquivos e pastas de cópias Snapshot locais e de cópias de replicação.

Você pode executar esse recurso usando o processo de pesquisa e restauração, e não usando o processo Procurar e restaurar.

01 de fevereiro de 2024

Melhorias no backup e recuperação do BlueXP para máquinas virtuais

- Suporte a restaurar máquinas virtuais para um local alternativo
- Suporte para desproteger datastores

15 de dezembro de 2023

Relatórios disponíveis para cópias Snapshot locais e cópias Snapshot de replicação

Anteriormente, você poderia gerar relatórios apenas sobre cópias de backup. Agora, você também pode criar relatórios sobre cópias Snapshot locais e cópias Snapshot de replicação.

Com esses relatórios, você pode fazer o seguinte:

- Garantir que os dados críticos estejam protegidos de acordo com sua política organizacional.
- Garantir que os backups sejam executados sem problemas para um grupo de volumes.
- Fornecer uma prova de proteção sobre seus dados de produção.

Consulte a "Relatório sobre a cobertura de proteção de dados".

Marcação personalizada disponível em volumes para classificação e filtragem

Agora você pode adicionar tags personalizadas a volumes a partir do ONTAP 9.13,1 para que você possa agrupar volumes dentro e entre ambientes de trabalho. Isso permite classificar volumes nas páginas da IU de backup e recuperação do BlueXP e filtrar em relatórios.

Backups do catálogo mantidos por 30 dias

Anteriormente, Catalog.zip backups foram retidos por 7 dias. Agora, eles são retidos por 30 dias.

Consulte a "Restaure os dados de recuperação e backup do BlueXP em locais escuros".

23 de outubro de 2023

3-2-1 criação de política de backup durante a ativação do backup

Anteriormente, políticas personalizadas precisavam ser criadas antes de iniciar um Snapshot, replicação ou backup. Agora você pode criar uma política durante o processo de ativação do backup usando a IU de backup e recuperação do BlueXP .

"Saiba mais sobre políticas".

Suporte para restauração rápida sob demanda de volumes ONTAP

O backup e a recuperação do BlueXP agora permitem executar uma "restauração rápida" de um volume do storage de nuvem para um sistema Cloud Volumes ONTAP. A restauração rápida é ideal para situações de recuperação de desastres em que você precisa fornecer acesso a um volume o mais rápido possível. Uma restauração rápida restaura os metadados do arquivo de backup para um volume em vez de restaurar todo o arquivo de backup.

O sistema de destino do Cloud Volumes ONTAP deve estar executando o ONTAP versão 9.13.0 ou superior. "Saiba mais sobre como restaurar dados".

O Monitor de trabalhos de cópia de segurança e recuperação do BlueXP também mostra informações sobre o progresso dos trabalhos de restauro rápido.

Suporte para trabalhos agendados no Monitor de trabalhos

O Monitor de tarefas de backup e recuperação do BlueXP monitorou anteriormente tarefas de backup e restauração agendadas de volume para armazenamento de objetos, mas não tarefas de Snapshot local, replicação, backup e restauração que foram agendadas por meio da IU ou API.

O Monitor de tarefas de backup e recuperação do BlueXP agora inclui tarefas agendadas para snapshots locais, replicações e backups para o storage de objetos.

"Saiba mais sobre o Monitor de trabalhos atualizado".

13 de outubro de 2023

Melhorias no backup e recuperação do BlueXP para aplicações (nativo da nuvem)

- Base de dados Microsoft SQL Server
  - Suporta backup, restauração e recuperação de bancos de dados Microsoft SQL Server residentes no Amazon FSX for NetApp ONTAP
  - Todas as operações são suportadas apenas por APIs REST.
- Sistemas SAP HANA
  - Durante a atualização do sistema, a montagem automática e a desmontagem dos volumes são realizadas usando fluxos de trabalho em vez de scripts
  - Suporta a adição, remoção, edição, exclusão, manutenção e atualização do host do plug-in usando UI

Melhorias no backup e recuperação do BlueXP para aplicativos (híbridos)

- É compatível com bloqueio de dados e proteção contra ransomware
- Compatível com a migração de backups do StorageGRID para a camada de arquivamento
- É compatível com o backup de dados de aplicações MongoDB, MySQL e PostgreSQL de sistemas ONTAP locais para Amazon Web Services, Microsoft Azure, Google Cloud Platform e StorageGRID. Você pode restaurar os dados quando necessário.

Melhorias no backup e recuperação do BlueXP para máquinas virtuais

- Suporte para modelo de implantação de proxy de conetor

11 de setembro de 2023

Gerenciamento de novas políticas para dados do ONTAP

Esta versão inclui a capacidade da IU criar políticas Snapshot personalizadas, políticas de replicação e políticas para backups para storage de objetos para dados do ONTAP.

"Saiba mais sobre políticas".

Suporte para restaurar arquivos e pastas de volumes no armazenamento de objetos do ONTAP S3

Anteriormente, não era possível restaurar arquivos e pastas usando o recurso "Procurar e Restaurar" quando os volumes foram copiados para o armazenamento de objetos do ONTAP S3. Esta versão remove essa restrição.

"Saiba mais sobre como restaurar dados".

Capacidade de arquivar dados de backup imediatamente em vez de gravar primeiro no storage padrão

Agora você pode enviar seus arquivos de backup imediatamente para o armazenamento de arquivamento, em vez de gravar os dados no storage de nuvem padrão. Isso pode ser especialmente útil para usuários que raramente precisam acessar dados de backups na nuvem ou usuários que estão substituindo um ambiente de backup em fita.

Suporte adicional para backup e restauração de volumes SnapLock

Agora, o backup e a recuperação podem fazer backup de volumes FlexVol e FlexGroup configurados usando o modo de proteção SnapLock Enterprise. Os clusters precisam estar executando o ONTAP 9.14 ou superior para esse suporte. O backup de volumes do FlexVol usando o modo SnapLock Enterprise tem sido suportado desde a versão 9.11.1 do ONTAP. As versões anteriores do ONTAP não oferecem suporte para fazer backup de volumes de proteção SnapLock.

"Saiba mais sobre como proteger dados do ONTAP".

1 de agosto de 2023

- Devido a um importante aprimoramento de segurança, seu conetor agora requer acesso de saída à Internet a um endpoint adicional para gerenciar recursos de backup e recuperação em seu ambiente de nuvem pública. Se este endpoint não tiver sido adicionado à lista "permitido" no firewall, verá um erro na IU sobre "Serviço indisponível" ou "Falha ao determinar o estado do serviço":

  https://NetApp-cloud-account.auth0.com

- Uma assinatura PAYGO de backup e recuperação agora é necessária quando você estiver usando o pacote "CVO Professional" que permite agrupar backup e recuperação do Cloud Volumes ONTAP e do BlueXP . Isso não era necessário no passado. Nenhuma cobrança será cobrada na assinatura de backup e recuperação de sistemas Cloud Volumes ONTAP qualificados, mas ela será necessária ao configurar o backup em novos volumes.

Foi adicionado suporte para fazer backup de volumes em buckets em sistemas ONTAP configurados com S3

Agora você pode usar um sistema ONTAP que foi configurado para o Simple Storage Service (S3) para fazer backup de volumes no storage de objetos. Isso é compatível com sistemas ONTAP no local e sistemas Cloud Volumes ONTAP. Essa configuração é suportada em implantações de nuvem e em locais locais locais sem acesso à Internet (uma implantação em modo "privada").

"Saiba mais".

Agora você pode incluir snapshots existentes de um volume protegido em seus arquivos de backup

No passado, você conseguiu incluir cópias Snapshot existentes de volumes de leitura e gravação em seu arquivo de backup inicial para storage de objetos (em vez de começar com a cópia Snapshot mais recente). As cópias Snapshot existentes de volumes somente leitura (volumes de proteção de dados) não foram incluídas no arquivo de backup. Agora você pode optar por incluir cópias Snapshot mais antigas no arquivo de backup para volumes "DP".

O assistente de backup exibe um prompt no final das etapas de backup, onde você pode selecionar esses "instantâneos existentes".

O backup e a recuperação do BlueXP não são mais compatíveis com o backup automático de volumes adicionados no futuro

Anteriormente, você poderia marcar uma caixa no assistente de backup para aplicar a política de backup selecionada a todos os volumes futuros adicionados ao cluster. Esta funcionalidade foi removida com base no feedback do utilizador e na falta de utilização desta funcionalidade. Você precisará ativar manualmente os backups de quaisquer novos volumes adicionados ao cluster.

A página monitorização de trabalhos foi atualizada com novas funcionalidades

A página Monitoramento de tarefas agora fornece mais informações relacionadas à estratégia de backup 3-2-1. O serviço também fornece notificações de alerta adicionais relacionadas à estratégia de backup.

O filtro tipo "Backup Lifecycle" foi renomeado para "retenção". Use esse filtro para controlar o ciclo de vida do backup e identificar a expiração de todas as cópias de backup. O tipo de tarefa "retenção" captura todos os trabalhos de exclusão Instantânea iniciados em um volume protegido pelo backup e recuperação do BlueXP .

"Saiba mais sobre o Monitor de trabalhos atualizado".

6 de julho de 2023

O backup e a recuperação do BlueXP agora incluem a capacidade de agendar e criar cópias Snapshot e volumes replicados

Agora, o backup e a recuperação do BlueXP permitem que você implemente uma estratégia 3-2-1 em que você possa ter 3 cópias dos dados de origem em 2 sistemas de storage diferentes, juntamente com a cópia 1 na nuvem. Após a ativação, você terá:

- Cópia Snapshot do volume no sistema de origem
- Volume replicado em um sistema de storage diferente
- Backup do volume no armazenamento de objetos

"Saiba mais sobre os novos recursos de backup e restauração de espetro completo".

Essa nova funcionalidade também se aplica às operações de recuperação. É possível executar operações de restauração a partir de uma cópia Snapshot, de um volume replicado ou de um arquivo de backup na nuvem. Assim, você tem flexibilidade para escolher o arquivo de backup que atenda aos requisitos de recuperação, incluindo custo e velocidade de recuperação.

Observe que essa nova funcionalidade e interface de usuário são compatíveis apenas com clusters executando o ONTAP 9.8 ou superior. Se o cluster tiver uma versão anterior do software, você poderá continuar usando a versão anterior do backup e recuperação do BlueXP . No entanto, recomendamos que você atualize para uma versão suportada do ONTAP para obter os recursos e funcionalidades mais recentes. Para continuar usando a versão mais antiga do software, siga estas etapas:

1. Na guia **volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, clique no botão de opção **Exibir a versão anterior de backup e recuperação do BlueXP** .

   Depois, você pode gerenciar os clusters mais antigos usando a versão anterior do software.

Capacidade de criar seu contêiner de storage para backup em storage de objetos

Quando você cria arquivos de backup no armazenamento de objetos, por padrão, o serviço de backup e recuperação criará os buckets no armazenamento de objetos para você. Você mesmo pode criar os buckets se quiser usar um determinado nome ou atribuir propriedades especiais. Se você quiser criar seu próprio bucket, você deve criá-lo antes de iniciar o assistente de ativação. "Saiba como criar seus buckets de armazenamento de objetos".

Esta funcionalidade não é atualmente suportada ao criar ficheiros de cópia de segurança para sistemas StorageGRID.

04 de julho de 2023

Melhorias no backup e recuperação do BlueXP para aplicações (nativo da nuvem)

- Sistemas SAP HANA
  - É compatível com a restauração de volumes que não são de dados e volumes que não são de dados globais com proteção secundária Azure NetApp Files
- Bancos de dados Oracle
  - Suporta restauração de bancos de dados Oracle no Azure NetApp Files para local alternativo
  - Suporta a catalogação de backups de bancos de dados Oracle no Azure NetApp Files
  - Permite colocar o host do banco de dados no modo de manutenção para executar tarefas de manutenção

Melhorias no backup e recuperação do BlueXP para aplicativos (híbridos)

- Suporta restauração para local alternativo
- Permite montar backups de banco de dados Oracle
- Compatível com a migração de backups do GCP para a camada de arquivamento

Melhorias no backup e recuperação do BlueXP para máquinas virtuais (híbridas)

- Dá suporte à proteção dos tipos de datastores NFS e VMFS
- Permite cancelar o Registro do plug-in do SnapCenter para o host VMware vSphere
- Suporta atualização e descoberta de armazenamentos de dados e backups mais recentes

5 de junho de 2023

É possível fazer backup e proteger os volumes do FlexGroup usando a proteção DataLock e ransomware

As políticas de backup para volumes FlexGroup agora podem usar a proteção DataLock e ransomware quando o cluster estiver executando o ONTAP 9.13,1 ou superior.

Novos recursos de relatórios

Agora há uma guia relatórios onde você pode gerar um relatório de inventário de backup, que inclui todos os backups de uma conta específica, ambiente de trabalho ou inventário de SVM. Você também pode criar um relatório de atividade de trabalho de proteção de dados, que fornece informações sobre operações de Snapshot, backup, clone e restauração que podem ajudá-lo com o monitoramento de contrato de nível de serviço. Consulte a "Relatório sobre a cobertura de proteção de dados".

Melhorias no Monitor de trabalho

Agora você pode rever *backup Lifecycle* como um tipo de tarefa na página Monitor de tarefas, ajudando você a acompanhar todo o ciclo de vida do backup. Você também pode ver detalhes de todas as operações na linha do tempo do BlueXP . Consulte a "Monitore o status dos trabalhos de backup e restauração".

Alerta de notificação adicional para rótulos de política não correlacionados

Foi adicionado um novo alerta de cópia de segurança: "Os ficheiros de cópia de segurança não foram criados porque os rótulos de política de instantâneo não correspondem". Se o *label* definido em uma política de backup não tiver um *label* correspondente na política Snapshot, nenhum arquivo de backup será criado. Você precisará usar o Gerenciador do sistema ou a CLI do ONTAP para adicionar o rótulo ausente à política de snapshot de volume.

"Revise todos os alertas que o backup e a recuperação do BlueXP podem enviar".

Backup automático de arquivos críticos de backup e recuperação do BlueXP em locais escuros

Quando você estiver usando backup e recuperação do BlueXP em um site sem acesso à Internet, conhecido como implantação de "modo privado", as informações de backup e recuperação do BlueXP são armazenadas somente no sistema de conetores locais. Essa nova funcionalidade faz o backup automático de dados críticos de backup e recuperação do BlueXP para um bucket no sistema StorageGRID conectado, para que você possa restaurar esses dados em um novo conector, se necessário. "Saiba mais"

8 de maio de 2023

As operações de restauração em nível de pasta agora são suportadas a partir de armazenamento de arquivo e de backups bloqueados

Se um arquivo de backup tiver sido configurado com proteção DataLock & ransomware ou se o arquivo de backup residir no armazenamento de arquivamento, agora as operações de restauração em nível de pasta serão suportadas se o cluster estiver executando o ONTAP 9.13,1 ou superior.

Chaves gerenciadas por clientes entre regiões e entre projetos são compatíveis ao fazer backup de volumes no Google Cloud

Agora você pode escolher um bucket que está em um projeto diferente do projeto de suas chaves de criptografia gerenciadas pelo cliente (CMEK).

"Saiba mais sobre como configurar suas próprias chaves de criptografia gerenciadas pelo cliente".

As regiões da AWS China agora são compatíveis com arquivos de backup

As regiões AWS China Beijing (CN-North-1) e Ningxia (cn-Northwest-1) agora são suportadas como destinos para seus arquivos de backup se o cluster estiver executando o ONTAP 9.12,1 ou superior.

Observe que as políticas do IAM atribuídas ao BlueXP Connector precisam alterar o nome de recurso da AWS "arn" em todas as seções *recurso* de "AWS" para "AWS-cn"; por exemplo, "ARN:aws-cn:S3:::NetApp-backup-*".

```
https://docs.netapp.com/us-en/bluexp-backup-recovery/task-backup-to-s3.html["Faça backup dos dados do Cloud Volumes ONTAP para o Amazon S3"]Consulte e https://docs.netapp.com/us-en/bluexp-backup-recovery/task-backup-onprem-to-aws.html["Fazer backup de dados do ONTAP no local para o Amazon S3"] para obter detalhes.
```

Melhorias no Monitor de trabalhos

As tarefas iniciadas pelo sistema, tais operações de backup em curso, estão agora disponíveis na guia **Monitoramento de tarefas** para sistemas ONTAP locais que executam o ONTAP 9.13,1 ou superior. As versões anteriores do ONTAP irão apresentar apenas trabalhos iniciados pelo utilizador.

14 de abril de 2023

Melhorias no backup e recuperação do BlueXP para aplicações (nativo da nuvem)

- Bancos de dados SAP HANA
  - Suporta atualização de sistema baseada em script
  - Suporta cópia de segurança do ficheiro único-instantâneo-restauro se a cópia de segurança do Azure NetApp Files estiver configurada
  - Suporta atualização de plug-in
- Bancos de dados Oracle
  - Melhorias na implantação do plug-in simplificando a configuração do usuário sudo não-raiz
  - Suporta atualização de plug-in
  - Oferece suporte a descoberta automática e proteção orientada por políticas de bancos de dados Oracle no Azure NetApp Files
  - Compatível com a restauração do banco de dados Oracle para o local original com recuperação granular

Melhorias no backup e recuperação do BlueXP para aplicativos (híbridos)

- O backup e a recuperação do BlueXP para aplicações (híbridas) são baseados no plano de controle SaaS
- Modificou as APIS REST híbridas para se alinhar às APIs nativas da nuvem.
- Suporta notificação por e-mail

4 de abril de 2023

Capacidade de fazer backup de dados para a nuvem a partir de sistemas Cloud Volumes ONTAP no modo "restrito"

Agora você pode fazer backup dos dados de sistemas Cloud Volumes ONTAP instalados nas regiões comerciais da AWS, Azure e GCP no "modo restrito". Isso requer que você instale primeiro o conetor na região comercial "restrita". "Saiba mais sobre os modos de implantação do BlueXP ".

Consulte "Fazer backup de dados do Cloud Volumes ONTAP para o Amazon S3"

```
https://docs.netapp.com/us-en/bluexp-backup-recovery/task-backup-to-
azure.html["Fazer backup de dados do Cloud Volumes ONTAP para o Azure
Blob"]Consulte .
```

Capacidade de fazer backup de volumes do ONTAP no local para o ONTAP S3 usando a API

A nova funcionalidade nas APIs permite fazer backup de seus snapshots de volume para o ONTAP S3 usando

o backup e a recuperação do BlueXP . Essa funcionalidade está disponível apenas para sistemas ONTAP no local no momento. Para obter instruções detalhadas, consulte o Blog "Integração com o ONTAP S3 como destino".

Capacidade de alterar o aspeto de redundância de zona da sua conta de armazenamento Azure de LRS para ZRS

Ao criar backups de sistemas Cloud Volumes ONTAP para o storage Azure, por padrão, o backup e a recuperação do BlueXP provisionam o contêiner de Blob com redundância local (LRS) para otimização de custos. Você pode alterar essa configuração para redundância de zona (ZRS) se desejar que seus dados sejam replicados entre diferentes zonas. Consulte as instruções da Microsoft para "alterar a forma como a sua conta de armazenamento é replicada".

Melhorias no Monitor de trabalhos

- As operações de backup e restauração iniciadas pelo usuário a partir da API e UI de recuperação do BlueXP , e as tarefas iniciadas pelo sistema, tais operações de backup contínuas, estão agora disponíveis na guia **Monitoramento de tarefas** para sistemas Cloud Volumes ONTAP que executam o ONTAP 9.13,0 ou superior. As versões anteriores do ONTAP irão apresentar apenas trabalhos iniciados pelo utilizador.
- Além de poder baixar um arquivo CSV para gerar relatórios em todos os trabalhos, agora você pode baixar um arquivo JSON para uma única tarefa e ver seus detalhes. "Saiba mais".
- Foram adicionados dois novos alertas de tarefa de cópia de segurança: "Falha de tarefa agendada" e "Restaurar tarefa concluída, mas com avisos". "Revise todos os alertas que o backup e a recuperação do BlueXP podem enviar".

9 de março de 2023

As operações de restauração em nível de pasta agora incluem todas as subpastas e arquivos

No passado, quando você restaurou uma pasta, apenas os arquivos dessa pasta foram restaurados - nenhuma subpastas ou arquivos em subpastas foram restaurados. Agora, se você estiver usando o ONTAP 9.13,0 ou superior, todas as subpastas e arquivos na pasta selecionada serão restaurados. Isso pode economizar muito tempo e dinheiro nos casos em que você tem várias pastas aninhadas em uma pasta de nível superior.

Capacidade de fazer backup de dados de sistemas Cloud Volumes ONTAP em locais com conectividade de saída limitada

Agora você pode fazer backup de dados de sistemas Cloud Volumes ONTAP instalados nas regiões comerciais da AWS e do Azure para o Amazon S3 ou Azure Blob. Isso requer que você instale o conetor em "modo restrito" em um host Linux na região comercial, e que você implante o sistema Cloud Volumes ONTAP lá também.

```
https://docs.netapp.com/us-en/bluexp-backup-recovery/task-backup-to-
s3.html["Fazer backup de dados do Cloud Volumes ONTAP para o Amazon
S3"]Consulte .
```

```
https://docs.netapp.com/us-en/bluexp-backup-recovery/task-backup-to-
azure.html["Fazer backup de dados do Cloud Volumes ONTAP para o Azure
Blob"]Consulte .
```

Várias melhorias no Monitor de trabalhos

- A página Monitoramento de tarefas adicionou filtragem avançada para que você possa procurar tarefas de backup e restauração por tempo, carga de trabalho (volumes, aplicativos ou máquinas virtuais), tipo de tarefa, status, ambiente de trabalho e VM de armazenamento. Você também pode inserir texto livre para procurar qualquer recurso, por exemplo, "Application_3". "Veja como usar os filtros avançados".
- As operações de backup e restauração iniciadas pelo usuário a partir da API e UI de recuperação do BlueXP , e as tarefas iniciadas pelo sistema, tais operações de backup contínuas, estão agora disponíveis na guia **Monitoramento de tarefas** para sistemas Cloud Volumes ONTAP que executam o ONTAP 9.13,0 ou superior. As versões anteriores dos sistemas Cloud Volumes ONTAP e sistemas ONTAP locais irão apresentar apenas trabalhos iniciados pelo utilizador neste momento.

6 de fevereiro de 2023

Capacidade de mover arquivos de backup mais antigos para o storage de arquivamento do Azure a partir de sistemas StorageGRID

Agora você pode categorizar arquivos de backup mais antigos de sistemas StorageGRID para storage de arquivamento no Azure. Isso permite que você libere espaço em seus sistemas StorageGRID e economize dinheiro usando uma classe de armazenamento barata para arquivos de backup antigos.

Essa funcionalidade estará disponível se o cluster no local estiver usando o ONTAP 9.12,1 ou superior e o sistema StorageGRID estiver usando o 11,4 ou superior. "Saiba mais aqui".

A proteção DataLock e ransomware pode ser configurada para arquivos de backup no Azure Blob

DataLock e ransomware Protection agora são compatíveis com arquivos de backup armazenados no Azure Blob. Se o seu sistema Cloud Volumes ONTAP ou ONTAP no local estiver executando o ONTAP 9.12,1 ou superior, agora você pode bloquear seus arquivos de backup e digitalizá-los para detectar possíveis ransomware. "Saiba mais sobre como proteger seus backups usando a proteção DataLock e ransomware".

Aprimoramentos de volume do FlexGroup de backup e restauração

- Agora você pode escolher vários agregados ao restaurar um volume FlexGroup. Na última versão, você só pode selecionar um único agregado.
- A restauração de volume do FlexGroup agora é compatível com sistemas Cloud Volumes ONTAP. Na última versão, você só podia restaurar para sistemas ONTAP locais.

Os sistemas Cloud Volumes ONTAP podem mover backups mais antigos para o armazenamento do Google Archival

Os arquivos de backup são criados inicialmente na classe de armazenamento padrão do Google. Agora você pode usar o backup e a recuperação do BlueXP para categorizar backups mais antigos no storage do Google Archive para otimizar ainda mais os custos. A última versão suportava apenas essa funcionalidade com clusters ONTAP locais. Agora, os sistemas Cloud Volumes ONTAP implantados no Google Cloud são compatíveis.

As operações de Restauração de volume agora permitem que você selecione o SVM onde você deseja restaurar dados de volume

Agora você restaura os dados de volume para diferentes VMs de storage nos clusters do ONTAP. No passado, não era possível escolher a VM de storage.

Suporte aprimorado para volumes nas configurações do MetroCluster

Ao utilizar o ONTAP 9.12,1 GA ou superior, a cópia de segurança é agora suportada quando ligada ao sistema principal numa configuração MetroCluster. Toda a configuração de backup é transferida para o sistema secundário para que os backups para a nuvem continuem automaticamente após o switchover.

"Consulte limitações de backup para obter mais informações".

9 de janeiro de 2023

Capacidade de mover arquivos de backup mais antigos para o storage de arquivamento do AWS S3 a partir de sistemas StorageGRID

Agora você pode categorizar arquivos de backup mais antigos de sistemas StorageGRID para storage de arquivamento no AWS S3. Isso permite que você libere espaço em seus sistemas StorageGRID e economize dinheiro usando uma classe de armazenamento barata para arquivos de backup antigos. Você pode optar por categorizar backups no storage do AWS S3 Glacier ou do S3 Glacier Deep Archive.

Esse recurso estará disponível se o cluster no local estiver usando o ONTAP 9.12,1 ou superior e o sistema StorageGRID estiver usando o 11,3 ou superior. "Saiba mais aqui".

Capacidade de selecionar suas próprias chaves gerenciadas pelo cliente para criptografia de dados no Google Cloud

Ao fazer backup de dados de seus sistemas ONTAP para o Google Cloud Storage, agora você pode selecionar suas próprias chaves gerenciadas pelo cliente para criptografia de dados no assistente de ativação em vez de usar as chaves de criptografia gerenciadas pelo Google padrão. Basta configurar primeiro as chaves de criptografia gerenciadas pelo cliente no Google e, em seguida, inserir os detalhes ao ativar o backup e a recuperação do BlueXP .

A função "Administrador de armazenamento" não é mais necessária para que a conta de serviço crie backups no Google Cloud Storage

Em versões anteriores, a função "Administrador do storage" era necessária para a conta de serviço que permite o backup e a recuperação do BlueXP acessar buckets do Google Cloud Storage. Agora você pode criar uma função personalizada com um conjunto reduzido de permissões a serem atribuídas à conta de serviço.

"Veja como preparar seu Google Cloud Storage para backups".

Foi adicionado suporte para restaurar dados utilizando a Pesquisa e Restauração em sites sem acesso à Internet

Se você estiver fazendo backup de dados de um cluster do ONTAP local para o StorageGRID em um site sem acesso à Internet, também conhecido como site escuro ou site off-line, agora você pode usar a opção pesquisar e Restaurar para restaurar dados quando necessário. Esta funcionalidade requer que o conetor BlueXP (versão 3.9.25 ou superior) seja implantado no site offline.

"Consulte como restaurar dados do ONTAP usando pesquisar Restaurar". "Veja como instalar o conetor no

seu site offline".

Capacidade de transferir a página de resultados da monitorização de trabalhos como um relatório .csv

Depois de filtrar a página Monitoramento de tarefas para exibir os trabalhos e ações em que você está interessado, agora você pode gerar e baixar um arquivo .csv desses dados. Em seguida, você pode analisar as informações ou enviar o relatório para outras pessoas em sua organização. "Consulte como gerar um relatório de monitorização de trabalhos".

19 de dezembro de 2022

Melhorias no Cloud Backup para aplicações

- Bancos de dados SAP HANA
  - É compatível com backup e restauração baseados em políticas de bancos de dados SAP HANA que residem no Azure NetApp Files
  - Suporta políticas personalizadas
- Bancos de dados Oracle
  - Adicione hosts e implante plug-in automaticamente
  - Suporta políticas personalizadas
  - É compatível com backup, restauração e clone baseados em políticas de bancos de dados Oracle residentes no Cloud Volumes ONTAP
  - Suporta backup e restauração baseados em políticas de bancos de dados Oracle residentes no Amazon FSX for NetApp ONTAP
  - Suporta a restauração de bancos de dados Oracle usando o método de conexão e cópia
  - Compatível com Oracle 21c
  - Compatível com clonagem de banco de dados Oracle nativo da nuvem

Melhorias no Cloud Backup para máquinas virtuais

- Máquinas virtuais
  - Fazer backup de máquinas virtuais a partir do storage secundário no local
  - Suporta políticas personalizadas
  - É compatível com o Google Cloud Platform (GCP) para fazer backup de um ou mais datastores
  - Oferece suporte a storage de nuvem de baixo custo, como Glacier, Deep Glacier e Azure Archive

6 de dezembro de 2022

Alterações de ponto de extremidade de acesso à Internet de saída de conetor necessárias

Devido a uma mudança no Cloud Backup, você precisa alterar os seguintes pontos de extremidade de conetor para uma operação bem-sucedida do Cloud Backup:

Endpoint antigo	Novo endpoint
https://cloudmanager.cloud.NetApp.com	https://api.BlueXP .NetApp.com
https://*.cloudmanager.cloud.NetApp.com	https://*.api.BlueXP .NetApp.com

Consulte a lista completa de pontos de extremidade do seu "AWS" "Google Cloud" ambiente de nuvem , ou "Azure" .

Suporte para selecionar a classe de armazenamento do Google Archival na IU

Os arquivos de backup são criados inicialmente na classe de armazenamento padrão do Google. Agora você pode usar a IU do Cloud Backup para categorizar backups mais antigos no storage do Google Archive após um determinado número de dias para otimização adicional de custos.

Esse recurso atualmente é compatível com clusters ONTAP on-premise que usam o ONTAP 9.12,1 ou superior. Atualmente, não está disponível para sistemas Cloud Volumes ONTAP.

Suporte para FlexGroup volumes

O Cloud Backup agora é compatível com o backup e a restauração de volumes do FlexGroup. Ao usar o ONTAP 9.12,1 ou superior, você pode fazer backup do FlexGroup volumes em storage de nuvem pública e privada. Se você tiver ambientes de trabalho que incluem o FlexVol e o FlexGroup volumes, depois de atualizar o software ONTAP, poderá fazer backup de qualquer um dos volumes do FlexGroup nesses sistemas.

"Consulte a lista completa dos tipos de volume suportados".

Capacidade de restaurar dados de backups para um agregado específico em sistemas Cloud Volumes ONTAP

Em versões anteriores, você poderia selecionar o agregado somente ao restaurar dados para sistemas ONTAP locais. Esta funcionalidade agora funciona ao restaurar dados para sistemas Cloud Volumes ONTAP.

2 de novembro de 2022

Capacidade de exportar cópias Snapshot mais antigas para seus arquivos de backup de linha de base

Se houver cópias Snapshot locais para volumes no ambiente de trabalho que correspondam aos rótulos de agendamento de backup (por exemplo, diariamente, semanalmente, etc.), você poderá exportar esses snapshots históricos para o storage de objetos como arquivos de backup. Isso permite inicializar seus backups na nuvem movendo cópias snapshot mais antigas para a cópia de backup da linha de base.

Essa opção está disponível ao ativar o Cloud Backup para seus ambientes de trabalho. Também pode alterar esta definição mais tarde no "Página Configurações avançadas".

Agora, o Cloud Backup pode ser usado para arquivar volumes que não precisam mais no sistema de origem

Agora você pode excluir o relacionamento de backup de um volume. Isso fornece um mecanismo de arquivamento se você quiser interromper a criação de novos arquivos de backup e excluir o volume de origem, mas manter todos os arquivos de backup existentes. Isso permite que você restaure o volume do arquivo de backup no futuro, se necessário, enquanto limpa espaço do sistema de armazenamento de origem. "Saiba como".

O suporte foi adicionado para receber alertas do Cloud Backup por e-mail e no Centro de notificações

O Cloud Backup foi integrado ao serviço de notificação do BlueXP . Você pode exibir as notificações do Cloud Backup clicando no sino de notificação na barra de menu do BlueXP . Você também pode configurar o BlueXP para enviar notificações por e-mail como alertas para que você possa ser informado sobre atividades

importantes do sistema, mesmo quando não estiver conetado ao sistema. O e-mail pode ser enviado para qualquer destinatário que precise estar ciente da atividade de backup e restauração. "Saiba como".

A nova página Configurações avançadas permite alterar as configurações de backup no nível do cluster

Esta nova página permite alterar muitas configurações de backup em nível de cluster definidas ao ativar o Cloud Backup para cada sistema ONTAP. Você também pode modificar algumas configurações que são aplicadas como configurações de backup "padrão". O conjunto completo de configurações de backup que você pode alterar inclui:

- As chaves de storage que dão permissão ao sistema ONTAP para acessar o storage de objetos
- A largura de banda de rede alocada para carregar backups para armazenamento de objetos
- A configuração de backup automático (e política) para volumes futuros
- A classe de storage de arquivamento (somente AWS)
- Se as cópias Snapshot históricas estão incluídas nos arquivos de backup da linha de base inicial
- Se os instantâneos "anuais" são removidos do sistema de origem
- O espaço IPspace ONTAP que está conetado ao armazenamento de objetos (em caso de seleção incorreta durante a ativação)

"Saiba mais sobre como gerenciar configurações de backup em nível de cluster".

Agora você pode restaurar arquivos de backup usando a Pesquisa e Restauração ao usar um conetor no local

Na versão anterior, foi adicionado suporte para a criação de arquivos de backup na nuvem pública quando o conetor é implantado em suas instalações. Nesta versão, o suporte continuou a permitir o uso da Pesquisa e Restauração para restaurar backups do Amazon S3 ou do Azure Blob quando o conetor é implantado em suas instalações. A pesquisa e restauração também oferece suporte à restauração de backups de sistemas StorageGRID para sistemas ONTAP locais agora.

Neste momento, o conetor deve ser implantado na Google Cloud Platform ao usar a Pesquisa e Restauração para restaurar backups do Google Cloud Storage.

A página monitorização de trabalhos foi atualizada

As seguintes atualizações foram feitas ao "Página monitorização de trabalhos" :

- Uma coluna para "carga de trabalho" está disponível para que você possa filtrar a página para exibir trabalhos para os seguintes serviços de backup: Volumes, aplicativos e máquinas virtuais.
- Você pode adicionar novas colunas para "Nome de usuário" e "tipo de tarefa" se quiser exibir esses detalhes para um trabalho de backup específico.
- A página Detalhes do trabalho apresenta todos os subtrabalhos que estão a ser executados para concluir o trabalho principal.
- A página é atualizada automaticamente a cada 15 minutos para que você sempre veja os resultados mais recentes do status do trabalho. E você pode clicar no botão **Refresh** para atualizar a página imediatamente.

Aprimoramentos de backup entre contas da AWS

Se você quiser usar uma conta AWS diferente para seus backups do Cloud Volumes ONTAP do que está usando para os volumes de origem, adicione as credenciais da conta AWS de destino no BlueXP e adicione as permissões "S3:PutBucketPolicy" e "S3:PutBucketOwnershipControls" à função do IAM que fornece permissões ao BlueXP . No passado, você precisava configurar muitas configurações no Console da AWS - você não precisa mais fazer isso.

28 de setembro de 2022

Melhorias no Cloud Backup para aplicações

- É compatível com o Google Cloud Platform (GCP) e o StorageGRID para fazer backup de snapshots consistentes com aplicações
- Crie políticas personalizadas
- Suporta armazenamento de arquivamento
- Fazer backup de aplicações SAP HANA
- Faça backup das aplicações Oracle e SQL que estão no ambiente VMware
- Fazer backup de aplicações de storage secundário no local
- Desativar cópias de segurança
- Anular o registo do servidor SnapCenter

Melhorias no Cloud Backup para máquinas virtuais

- Suporta o StorageGRID para fazer backup de um ou mais datastores
- Crie políticas personalizadas

19 de setembro de 2022

A proteção DataLock e ransomware pode ser configurada para arquivos de backup em sistemas StorageGRID

A última versão introduziu *DataLock e ransomware Protection* para backups armazenados em buckets do Amazon S3. Esta versão expande o suporte a arquivos de backup armazenados em sistemas StorageGRID. Se o cluster estiver usando o ONTAP 9.11,1 ou superior e o sistema StorageGRID estiver executando a versão 11.6.0.3 ou superior, essa nova opção de política de backup estará disponível. "Saiba mais sobre como você pode usar a proteção DataLock e ransomware para proteger seus backups".

Observe que você precisará estar executando um conetor com a versão 3.9.22 ou superior do software. O conetor deve ser instalado em suas instalações, e pode ser instalado em um site com ou sem acesso à Internet.

A restauração em nível de pasta está agora disponível a partir dos seus ficheiros de cópia de segurança

Agora você pode restaurar uma pasta de um arquivo de backup se precisar de acesso a todos os arquivos nessa pasta (diretório ou compartilhamento). Restaurar uma pasta é muito mais eficiente do que restaurar um volume inteiro. Esta funcionalidade está disponível para operações de restauro utilizando o método de procura e restauro e o método de pesquisa e restauro ao utilizar o ONTAP 9.11,1 ou superior. Neste momento, você pode selecionar e restaurar apenas uma única pasta, e apenas os arquivos dessa pasta são restaurados - nenhuma sub-pastas ou arquivos em subpastas são restaurados.

A restauração em nível de arquivo agora está disponível a partir de backups que foram movidos para armazenamento de arquivamento

No passado, você só podia restaurar volumes de arquivos de backup movidos para storage de arquivamento (somente AWS e Azure). Agora você pode restaurar arquivos individuais desses arquivos de backup arquivados. Esta funcionalidade está disponível para operações de restauro utilizando o método de procura e restauro e o método de pesquisa e restauro ao utilizar o ONTAP 9.11,1 ou superior.

A restauração em nível de arquivo agora fornece a opção de substituir o arquivo de origem original

No passado, um arquivo restaurado para o volume original foi sempre restaurado como um novo arquivo com o prefixo "Restore_<file_name>". Agora você pode optar por substituir o arquivo de origem original ao restaurar o arquivo para o local original no volume. Esta funcionalidade está disponível para operações de restauro utilizando o método de pesquisa e restauro e o método de pesquisa e restauro.

Arraste e solte para habilitar o backup em nuvem para sistemas StorageGRID

Se o "StorageGRID" destino dos backups existir como um ambiente de trabalho no Canvas, você poderá arrastar seu ambiente de trabalho no ONTAP local para o destino para iniciar o assistente de configuração do backup em nuvem.

Limitações conhecidas

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

Limitações de backup e restauração para volumes ONTAP

Limitações de replicação

- Você pode selecionar apenas um volume FlexGroup de cada vez para replicação. Você precisará ativar os backups separadamente para cada volume do FlexGroup.

  Não há limitação para o FlexVol volumes - você pode selecionar todos os volumes do FlexVol em seu ambiente de trabalho e atribuir as mesmas políticas de backup.

- A funcionalidade a seguir é suportada no "Serviço de replicação BlueXP ", mas não ao usar o recurso de replicação do backup e recuperação do BlueXP :
  - Não há suporte para uma configuração em cascata em que a replicação ocorra do volume A para o volume B e do volume B para o volume C. o suporte inclui replicação do volume A para o volume B.
  - Não há suporte para replicar dados de e para os sistemas FSX for ONTAP.
  - Não há suporte para criar uma replicação única de um volume.
- Ao criar replicações a partir de sistemas ONTAP locais, se a versão ONTAP no sistema Cloud Volumes ONTAP de destino for 9,8, 9,9 ou 9,11, somente políticas de espelhamento-cofre serão permitidas.

Limitações de backup para objeto

- Quando você cria ou edita uma política de backup quando nenhum volume é atribuído à política, o número de backups retidos pode ser no máximo 1018. Depois de atribuir volumes à política, você pode editar a política para criar até 4000 backups.

- Ao fazer backup de volumes de proteção de dados (DP):
  - Relacionamentos com os rótulos do SnapMirror `app_consistent` e `all_source_snapshot` não serão feitos backup na nuvem.
  - Se você criar cópias locais de snapshots no volume de destino do SnapMirror (independentemente dos rótulos do SnapMirror usados), esses snapshots não serão movidos para a nuvem como backups. Neste momento, você precisará criar uma política de snapshot com os rótulos desejados para o volume DP de origem para que o backup e a recuperação do BlueXP os façam.
- Os backups de volume do FlexGroup não podem ser movidos para armazenamento de arquivamento.
- Os backups de volume do FlexGroup podem usar a proteção DataLock e ransomware se o cluster estiver executando o ONTAP 9.13,1 ou superior.
- O backup em volume SVM-DR é compatível com as seguintes restrições:
  - Os backups são suportados apenas a partir do secundário do ONTAP.
  - A política Snapshot aplicada ao volume deve ser uma das políticas reconhecidas pelo backup e recuperação do BlueXP , incluindo diária, semanal, mensal, etc. a política padrão "SM_created" (usada para **espelhar todos os snapshots**) não é reconhecida e o volume DP não será exibido na lista de volumes que podem ser copiados.
- Suporte ao MetroCluster:
  - Quando utiliza o ONTAP 9.12,1 GA ou superior, é suportada a cópia de segurança quando está ligado ao sistema principal. Toda a configuração de backup é transferida para o sistema secundário para que os backups para a nuvem continuem automaticamente após o switchover. Você não precisa configurar o backup no sistema secundário (na verdade, você está impedido de fazê-lo).
  - Quando você usa o ONTAP 9.12,0 e versões anteriores, o backup é suportado apenas pelo sistema secundário do ONTAP.
  - No momento, não há suporte para backups de volumes FlexGroup.
- Backup de volume ad hoc usando o botão **Backup Now** não é suportado em volumes de proteção de dados.
- Configurações SM-BC não são suportadas.
- O ONTAP não suporta fan-out de relacionamentos SnapMirror de um único volume para vários armazenamentos de objetos; portanto, essa configuração não é suportada pelo backup e recuperação do BlueXP .
- O modo WORM/conformidade em um armazenamento de objetos é suportado no Amazon S3, Azure e StorageGRID no momento. Isso é conhecido como o recurso DataLock e deve ser gerenciado usando configurações de backup e recuperação do BlueXP , não usando a interface do provedor de nuvem.

Limitações de restauração

Estas limitações aplicam-se tanto aos métodos de Pesquisa e Restauro como Procurar e Restaurar para restaurar ficheiros e pastas; a menos que seja especificamente chamado.

- O recurso Procurar e Restaurar pode restaurar até 100 arquivos individuais de cada vez.
- A Pesquisa e Restauração pode restaurar o arquivo 1 de cada vez.
- Ao utilizar o ONTAP 9.13,0 ou superior, Procurar e Restaurar e pesquisar e Restaurar pode restaurar uma pasta juntamente com todos os ficheiros e subpastas dentro da mesma.

  Ao utilizar uma versão do ONTAP superior a 9.11.1 mas antes de 9.13.0, a operação de restauro pode restaurar apenas a pasta selecionada e os ficheiros nessa pasta - não são restauradas subpastas ou ficheiros em subpastas.

Ao usar uma versão do ONTAP antes de 9.11.1, a restauração de pastas não é suportada.

- A restauração de diretório/pasta é suportada para dados que residem no armazenamento de arquivamento somente quando o cluster está executando o ONTAP 9.13,1 e superior.
- A restauração de diretório/pasta é suportada para dados protegidos usando o DataLock somente quando o cluster estiver executando o ONTAP 9.13,1 e superior.
- Atualmente, a restauração de diretório/pasta não é suportada nos backups de volume do FlexGroup.
- Atualmente, a restauração de diretório/pasta não é suportada a partir de replicações e/ou instantâneos locais.
- A restauração do FlexGroup volumes para o FlexVol volumes ou do FlexVol volumes para o FlexGroup volumes não é compatível.
- O arquivo que está sendo restaurado deve estar usando o mesmo idioma que o idioma no volume de destino. Você receberá uma mensagem de erro se os idiomas não forem os mesmos.
- A prioridade de restauração *alta* não é suportada ao restaurar dados do armazenamento de arquivamento do Azure para sistemas StorageGRID.
- Se você fizer o backup de um volume DP e decidir quebrar a relação do SnapMirror para esse volume, não será possível restaurar arquivos para esse volume, a menos que você também exclua a relação do SnapMirror ou inverta a direção do SnapMirror.
- Limitações de restauração rápida:
  - A localização de destino tem de ser um sistema Cloud Volumes ONTAP que utilize o ONTAP 9.13,0 ou superior.
  - Ele não é compatível com backups localizados em armazenamento arquivado.
  - Os volumes do FlexGroup são suportados apenas se o sistema de origem a partir do qual o backup na nuvem foi criado estiver executando o ONTAP 9.12,1 ou superior.
  - Os volumes do SnapLock são suportados apenas se o sistema de origem a partir do qual o backup na nuvem foi criado estiver executando o ONTAP 9.11,0 ou superior.

Limitações ao usar RHEL 8 com Podman

Suporte para restauração de arquivo único

A partir da versão de 30 de setembro de 2024, essa limitação foi removida.

A funcionalidade Procurar e Restaurar para restauração de um único arquivo e restauração de diretório não é suportada ao usar conetores BlueXP em execução no Podman (conetores BlueXP criados manualmente quando executados no RHEL 8 ou 9). Todos os outros tipos de operações de restauração são suportados ao usar o Podman, para que você possa restaurar seus dados usando esses outros métodos até que esse problema seja resolvido:

- Restaure os arquivos ou pastas de um volume replicado, se existir um volume replicado.
- Restaure os arquivos ou pastas de um backup na nuvem usando o recurso pesquisar e restaurar.
- Restaure o volume a partir de uma cópia de segurança na nuvem utilizando Procurar e Restaurar e aceda aos ficheiros ou pastas de que necessita.

Comece agora

Saiba mais sobre o backup e a recuperação do BlueXP

O serviço de backup e recuperação do BlueXP fornece proteção de dados eficiente, segura e econômica para dados, bancos de dados e máquinas virtuais do NetApp ONTAP, tanto no local quanto na nuvem. Os backups são gerados e armazenados automaticamente em um armazenamento de objetos em sua conta de nuvem pública ou privada.

O serviço executa replicação incremental e em nível de bloco e preserva todas as eficiências de storage, o que reduz significativamente a quantidade de dados replicados e armazenados. Além disso, você paga apenas pelo que é protegido e usa as categorias de storage mais baratas disponíveis, o que torna o backup e a recuperação do BlueXP muito econômicos.

Quando necessário, você pode restaurar um *volume* inteiro de um backup para o mesmo ambiente de trabalho ou diferente. Ao fazer backup de dados do ONTAP, você também pode optar por restaurar uma pasta ou um ou mais *arquivos* de um backup para o mesmo ambiente de trabalho ou diferente.

"Saiba mais sobre backup e recuperação do BlueXP".

Backup e recuperação podem ser usados para:

- Faça backup e restauração de dados de volume ONTAP a partir de sistemas Cloud Volumes ONTAP e ONTAP no local. "Veja os recursos detalhados aqui".
- Fazer backup dos snapshots consistentes com aplicações a partir de sistemas ONTAP locais que usam o backup e a recuperação do BlueXP para aplicações. "Veja os recursos detalhados aqui".
- Faça backup de armazenamentos de dados na nuvem e restaure máquinas virtuais de volta ao vCenter no local usando o backup e a recuperação do BlueXP para VMware. "Veja os recursos detalhados aqui".

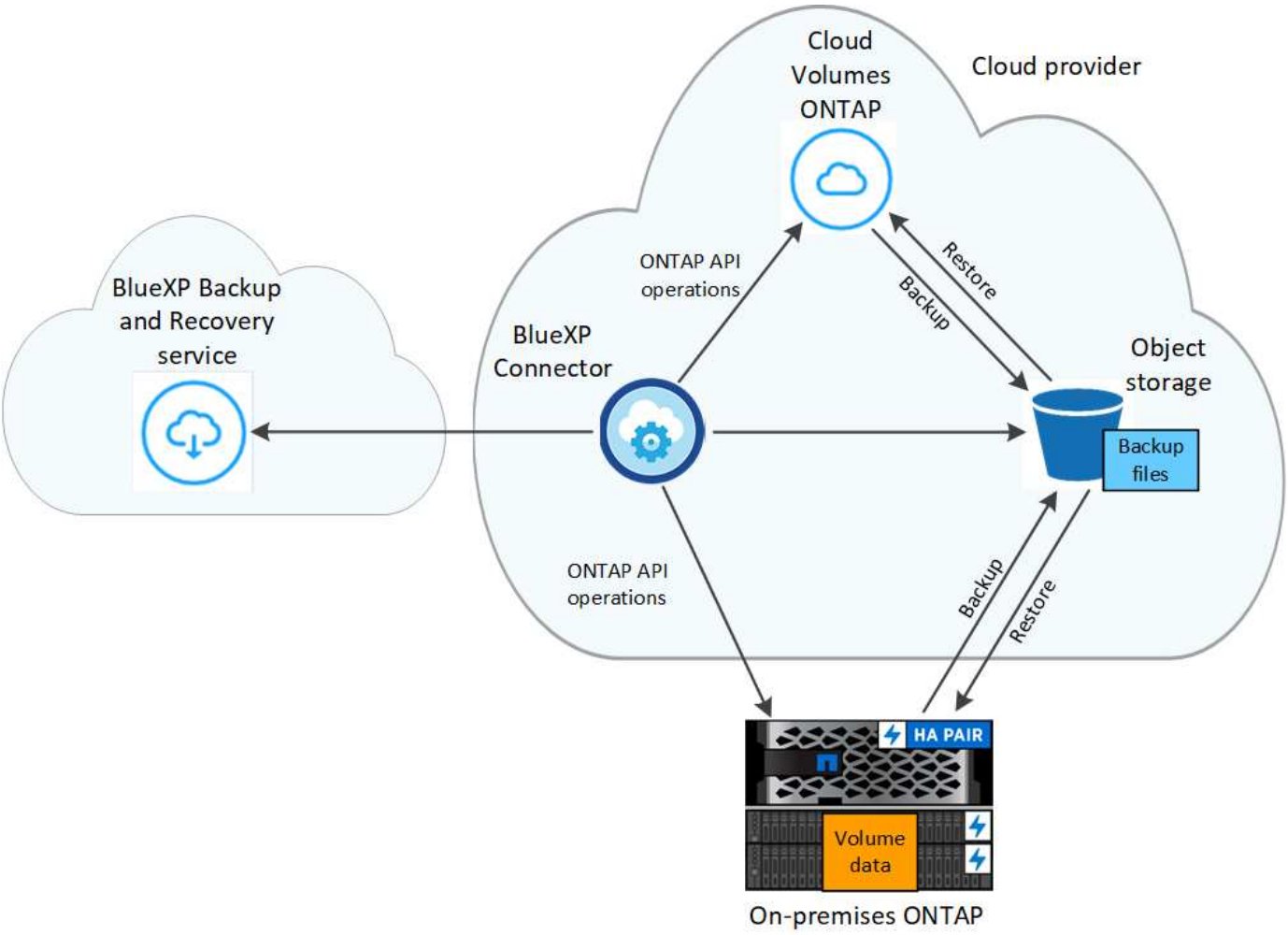
"Assista a uma demonstração rápida"

Quando o BlueXP Connector é implantado em uma região governamental na nuvem ou em um local sem acesso à Internet (um local escuro), o backup e a recuperação do BlueXP só oferecem suporte a operações de backup e restauração de sistemas ONTAP. Ao usar esses tipos de métodos de implantação, o backup e a recuperação do BlueXP não oferecem suporte a operações de backup e restauração de aplicativos ou máquinas virtuais.

Como funciona o backup e a recuperação do BlueXP

Ao habilitar o backup e a recuperação do BlueXP 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. Isso mantém o tráfego de rede no mínimo.

A imagem a seguir mostra a relação entre os componentes:



Onde os backups residem

As cópias de backup são armazenadas em um armazenamento de objetos que o BlueXP cria na sua conta de nuvem. Há um armazenamento de objetos por cluster/ambiente de trabalho e o BlueXP nomeia o armazenamento de objetos da seguinte forma: `netapp-backup-clusteruuid`. Certifique-se de não excluir este armazenamento de objetos.

- Na AWS, o BlueXP ativa o "Recurso de acesso público do Amazon S3 Block" bucket do no S3.
- No Azure, o BlueXP usa um grupo de recursos novo ou existente com uma conta de storage para o contêiner de Blob. BlueXP "bloqueia o acesso público aos seus dados de blob" por padrão.
- No GCP, o BlueXP usa um projeto novo ou existente com uma conta de storage para o bucket do Google Cloud Storage.
- No StorageGRID, o BlueXP usa uma conta de storage existente para o bucket do armazenamento de objetos.
- No ONTAP S3, o BlueXP usa uma conta de usuário existente para o bucket do S3.

Quando os backups são feitos

- Os backups por hora começam 5 minutos depois da hora, a cada hora.
- 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 no primeiro dia de cada mês.
- Os backups anuais começam logo após a meia-noite no primeiro dia do ano.

A hora de início baseia-se no fuso horário definido em cada sistema ONTAP de origem. Não é possível agendar operações de backup em um horário especificado pelo usuário a partir da IU. Para obter mais informações, contacte o seu engenheiro de sistemas.

As cópias de backup estão associadas à sua conta do NetApp

As cópias de backup estão associadas ao "Conta NetApp" no qual reside o BlueXP Connector.

Se você tiver vários conetores na mesma conta do NetApp, cada conetor exibirá a mesma lista de backups. Isso inclui os backups associados a instâncias do Cloud Volumes ONTAP e ONTAP locais de outros conetores.

Configure o licenciamento para backup e recuperação do BlueXP

Você pode licenciar o backup e a recuperação do BlueXP comprando uma assinatura anual de mercado ou pagamento conforme o uso do seu fornecedor de nuvem, ou comprando uma "traga sua própria licença" (BYOL) da NetApp. É necessária uma licença válida para ativar o backup e a recuperação do BlueXP em um ambiente de trabalho, para criar backups de seus dados de produção e para restaurar os dados de backup em um sistema de produção.

Algumas notas antes de ler mais:

- Se você já se inscreveu na assinatura de pagamento conforme o uso (PAYGO) no mercado do seu provedor de nuvem para um sistema Cloud Volumes ONTAP, então você está automaticamente inscrito no backup e recuperação do BlueXP também. Você não precisará se inscrever novamente.
- O bring-your-own-license (BYOL) de backup e recuperação do BlueXP é uma licença flutuante que você pode usar em todos os sistemas associados à sua organização ou conta do BlueXP . Portanto, se você tiver capacidade de backup suficiente disponível em uma licença BYOL existente, não precisará comprar outra licença BYOL.
- Se você estiver usando uma licença BYOL, é recomendável que você também assine uma assinatura PAYGO. Se você fizer backup de mais dados do que o permitido pela sua licença BYOL ou se o prazo da sua licença expirar, o backup continuará por meio da sua assinatura paga conforme o uso - não haverá interrupção do serviço.
- Ao fazer backup de dados ONTAP locais para o StorageGRID, você precisa de uma licença BYOL, mas não há custo para o espaço de storage do fornecedor de nuvem.

"Saiba mais sobre os custos relacionados ao uso do backup e recuperação do BlueXP ."

teste gratuito de 30 dias

Um teste gratuito de 30 dias de backup e recuperação do BlueXP está disponível se você se inscrever para uma assinatura paga conforme o uso no mercado do seu provedor de nuvem. O teste gratuito começa no momento em que você se inscrever na lista do mercado. Observe que se você pagar pela assinatura do marketplace ao implantar um sistema Cloud Volumes ONTAP e iniciar o teste gratuito de backup e recuperação do BlueXP 10 dias depois, você terá 20 dias restantes para usar a avaliação gratuita.

Quando a avaliação gratuita terminar, você será automaticamente transferido para a assinatura PAYGO sem interrupção. Se você decidir não continuar usando o backup e a recuperação do BlueXP , "Anular o registo da cópia de segurança e recuperação do BlueXP a partir do ambiente de trabalho"pouco antes do final da avaliação e você não será cobrado.

Use uma assinatura PAYGO de backup e recuperação do BlueXP

Para pagamento conforme o uso, você pagará ao seu fornecedor de nuvem pelos custos de storage de objetos e pelos custos de licenciamento do backup do NetApp por hora em uma única assinatura. 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 por hora de acordo com a quantidade de dados que você faz backup.
- Se você fizer backup de mais dados do que o permitido pela sua licença BYOL, as operações de backup e restauração de dados continuarão usando sua assinatura paga conforme o uso. Por exemplo, se você tiver uma licença BYOL TIB de 10 TB, toda a capacidade além do TIB de 10 TB será cobrada por meio da assinatura PAYGO.

Você não será cobrado da sua assinatura paga conforme o uso durante a avaliação gratuita ou se não tiver excedido a sua licença BYOL.

Existem alguns planos PAYGO para backup e recuperação do BlueXP :

- Um pacote "backup em nuvem" que permite fazer backup dos dados do Cloud Volumes ONTAP e dos dados do ONTAP no local.
- Um pacote "CVO Professional" que permite agrupar o backup e a recuperação do Cloud Volumes ONTAP e do BlueXP . Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a capacidade de backup não é contada em relação à capacidade licenciada). Essa opção não permite que você faça backup de dados ONTAP on-premises.

  Observe que essa opção também requer uma assinatura PAYGO de backup e recuperação, mas não haverá cobrança para sistemas Cloud Volumes ONTAP qualificados.

"Saiba mais sobre esses pacotes de licença baseados em capacidade".

Use esses links para assinar o backup e a recuperação do BlueXP no mercado do seu fornecedor de nuvem:

- AWS: "Acesse a oferta do mercado BlueXP para obter detalhes sobre preços".
- Azure: "Acesse a oferta do mercado BlueXP para obter detalhes sobre preços".
- Google Cloud: "Acesse a oferta do mercado BlueXP para obter detalhes sobre preços".

Use um contrato anual

Pague pelo backup e recuperação do BlueXP anualmente comprando um contrato anual. Eles estão disponíveis em termos de 1, 2 ou 3 anos.

Se você tiver um contrato anual de um mercado, todo o consumo de backup e recuperação do BlueXP será cobrado em relação a esse contrato. Você não pode misturar e combinar um contrato de mercado anual com um BYOL.

Ao usar a AWS, há dois contratos anuais disponíveis nos "Página do AWS Marketplace" sistemas ONTAP para Cloud Volumes ONTAP e no local:

- Um plano de "backup em nuvem" que permite fazer backup dos dados do Cloud Volumes ONTAP e dos dados do ONTAP no local.

  Se você quiser usar essa opção, configure sua assinatura na página do Marketplace e, em seguida "Associe a assinatura às suas credenciais da AWS", . Observe que você também precisará pagar pelos sistemas Cloud Volumes ONTAP usando essa assinatura anual de contrato, já que você pode atribuir apenas uma assinatura ativa às credenciais da AWS no BlueXP .

- Um plano "CVO Professional" que permite agrupar o backup e a recuperação do Cloud Volumes ONTAP e do BlueXP . Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a capacidade de backup não é contada em relação à capacidade licenciada). Essa opção não permite que você faça backup de dados ONTAP on-premises.

  Consulte "Tópico de licenciamento do Cloud Volumes ONTAP" para saber mais sobre esta opção de licenciamento.

  Se você quiser usar essa opção, você pode configurar o contrato anual quando criar um ambiente de trabalho do Cloud Volumes ONTAP e o BlueXP solicita que você assine o AWS Marketplace.

Ao usar o Azure, há dois contratos anuais disponíveis nos "Página do Azure Marketplace" sistemas ONTAP para Cloud Volumes ONTAP e no local:

- Um plano de "backup em nuvem" que permite fazer backup dos dados do Cloud Volumes ONTAP e dos dados do ONTAP no local.

  Se você quiser usar essa opção, configure sua assinatura na página do Marketplace e, em seguida "Associe a assinatura às suas credenciais do Azure", . Observe que você também precisará pagar pelos seus sistemas Cloud Volumes ONTAP usando essa assinatura de contrato anual, já que você pode atribuir apenas uma assinatura ativa às suas credenciais do Azure no BlueXP .

- Um plano "CVO Professional" que permite agrupar o backup e a recuperação do Cloud Volumes ONTAP e do BlueXP . Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a capacidade de backup não é contada em relação à capacidade licenciada). Essa opção não permite que você faça backup de dados ONTAP on-premises.

  Consulte "Tópico de licenciamento do Cloud Volumes ONTAP" para saber mais sobre esta opção de licenciamento.

  Se você quiser usar essa opção, você pode configurar o contrato anual ao criar um ambiente de trabalho do Cloud Volumes ONTAP e o BlueXP solicita que você se inscreva no mercado do Azure.

Ao usar o GCP, entre em Contato com seu representante de vendas da NetApp para adquirir um contrato anual. O contrato está disponível como uma oferta privada no Google Cloud Marketplace.

Depois que o NetApp compartilhar a oferta privada com você, você poderá selecionar o plano anual ao se inscrever no Google Cloud Marketplace durante a ativação de backup e recuperação do BlueXP .

Use uma licença BYOL de backup e recuperação do BlueXP

As licenças bring-your-own da NetApp fornecem termos de 1, 2 ou 3 anos. Você paga apenas pelos dados que protege, calculados pela capacidade lógica usada (*antes* quaisquer eficiências) dos volumes ONTAP de origem que estão sendo copiados. Essa capacidade também é conhecida como Front-End Terabytes (FETB).

A licença de backup e recuperação do BYOL BlueXP é uma licença flutuante em que a capacidade total é

compartilhada em todos os sistemas associados à sua organização ou conta do BlueXP . Para sistemas ONTAP, você pode obter uma estimativa aproximada da capacidade de que precisará executando o comando CLI `volume show -fields logical-used-by-afs` para os volumes que planeja fazer backup.

Se você não tiver uma licença BYOL de backup e recuperação do BlueXP , clique no ícone de bate-papo no canto inferior direito do BlueXP para comprar uma.

Opcionalmente, se você tiver uma licença não atribuída baseada em nó para o Cloud Volumes ONTAP que você não usará, poderá convertê-la em uma licença de backup e recuperação do BlueXP com a mesma equivalência em dólar e a mesma data de expiração. "Acesse aqui para obter detalhes".

Você usa a carteira digital BlueXP para gerenciar licenças BYOL. Pode adicionar novas licenças, atualizar licenças existentes e ver o estado da licença a partir da carteira digital BlueXP .

Obtenha seu arquivo de licença de backup e recuperação do BlueXP

Depois de adquirir sua licença de backup e recuperação do BlueXP (backup em nuvem), você ativa a licença no BlueXP inserindo o número de série de backup e recuperação do BlueXP e a conta do site de suporte da NetApp (NSS) ou carregando o arquivo de licença do NetApp (NLF). As etapas abaixo mostram como obter o arquivo de licença NLF se você planeja usar esse método.

Se você estiver executando o backup e a recuperação do BlueXP em um site local que não tenha acesso à Internet, o que significa que você implantou o conetor BlueXP no "modo privado", você precisará obter o arquivo de licença de um sistema conetado à Internet. A ativação da licença usando o número de série e a conta do site de suporte da NetApp não está disponível para instalações em modo privado.

Antes de começar

Você precisará do número de série de backup e recuperação do BlueXP . Localize esse número no seu pedido de vendas ou entre em Contato com a equipe da conta para obter essas informações.

Passos

1. Encontre o ID da sua conta BlueXP :
   a. No canto superior direito do console BlueXP , selecione > **Gerenciamento de identidade e acesso**.
   b. Na página Organização, procure o ID da sua conta e copie-o.

      Se não houver um ID de conta listado e você tiver apenas um ID de organização, precisará copiar os primeiros oito carateres do ID da organização e anexá-lo a *conta-*

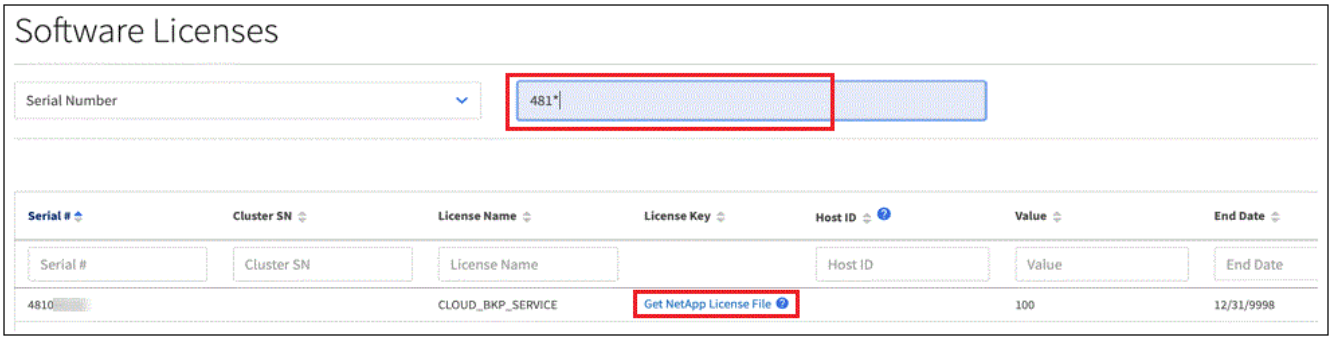
      Por exemplo, digamos que este é o ID da sua organização:

      ea10e1c6-80cc-4219-8e99-3c3e6b161ba5

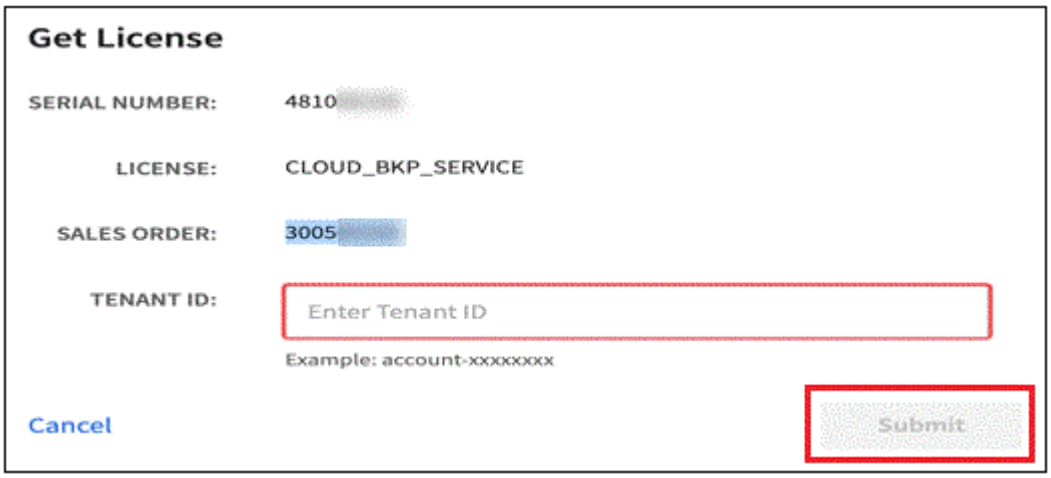
      O seu ID de conta seria o seguinte:

      conta-ea10e1c6

      Para um site de modo privado sem acesso à Internet, use **Account-DARKSITE1**.
2. Inicie sessão no "Site de suporte da NetApp" e clique em **sistemas > licenças de software**.
3. Introduza o número de série da licença de cópia de segurança e recuperação do BlueXP .



4. Na coluna **chave de licença**, clique em **obter ficheiro de licença NetApp**.
5. Introduza a sua ID de conta do BlueXP (chamada ID do locatário no site de suporte) e clique em **Enviar** para transferir o ficheiro de licença.



Adicione licenças BYOL de backup e recuperação do BlueXP à sua conta

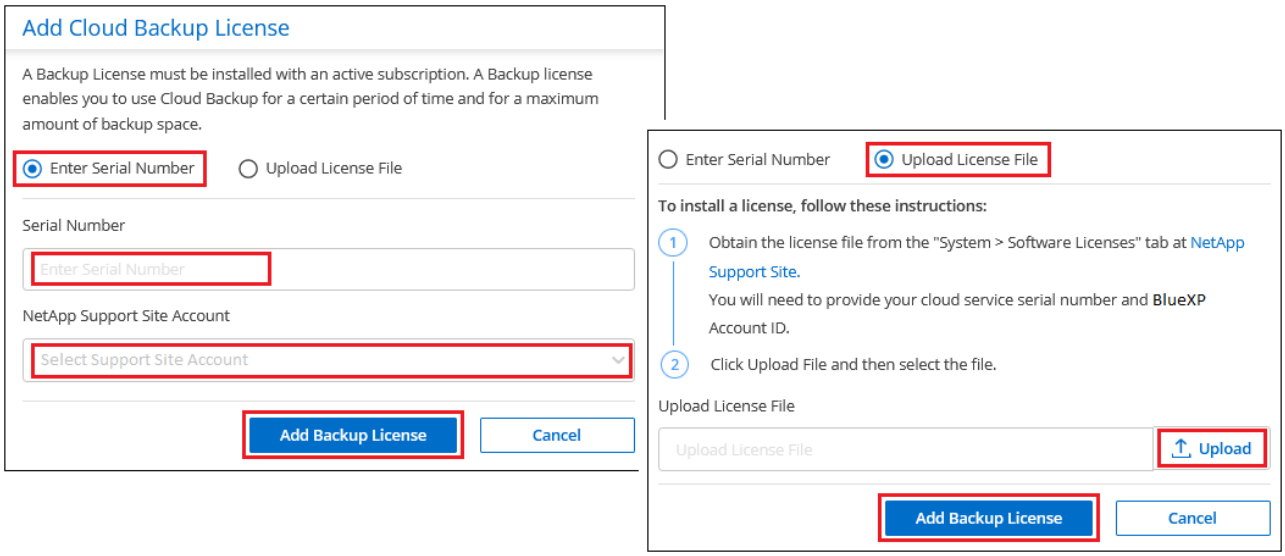
Depois de adquirir uma licença de backup e recuperação do BlueXP para sua conta do NetApp, você precisa adicionar a licença ao BlueXP .

Passos

1. No menu BlueXP , clique em **Governança > carteira digital** e selecione a guia **licenças de serviços de dados**.
2. Clique em **Adicionar licença**.
3. Na caixa de diálogo *Adicionar licença*, insira as informações da licença e clique em **Adicionar licença**:
   - Se tiver o número de série da licença de cópia de segurança e souber a sua conta NSS, selecione a opção **introduzir número de série** e introduza essas informações.

     Se a conta do site de suporte da NetApp não estiver disponível na lista suspensa, "Adicione a conta NSS ao BlueXP".

   - Se você tiver o arquivo de licença de backup (necessário quando instalado em um site escuro), selecione a opção **Upload License File** e siga as instruções para anexar o arquivo.

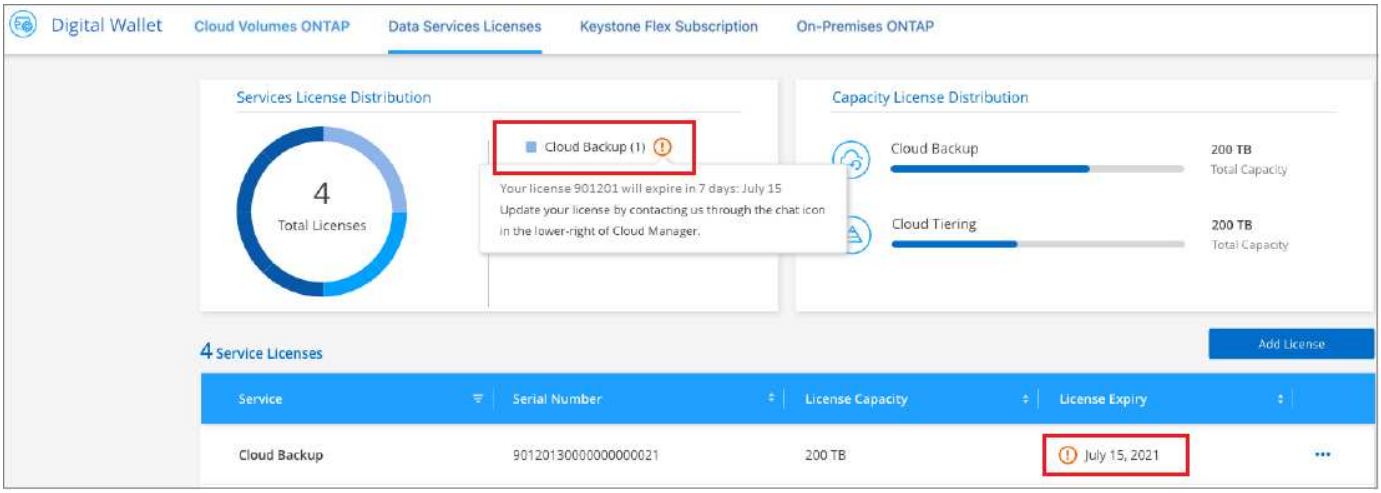


Resultado

O BlueXP adiciona a licença para que o backup e a recuperação do BlueXP estejam ativos.

Atualize uma licença BYOL de backup e recuperação do BlueXP

Se o prazo licenciado estiver próximo da data de expiração ou se a capacidade licenciada estiver atingindo o limite, você será notificado na IU de backup. Esse status também aparece na página da carteira digital do BlueXP e em "Notificações".



Você pode atualizar sua licença de backup e recuperação do BlueXP antes que ela expire, para que não haja interrupção na capacidade de fazer backup e restaurar seus dados.

Passos

1. Clique no ícone de bate-papo no canto inferior direito do BlueXP ou entre em Contato com o suporte para solicitar uma extensão do seu prazo ou capacidade adicional para sua licença de backup e recuperação do BlueXP para o número de série específico.

   Depois de pagar a licença e esta ser registada no Site de suporte da NetApp, a BlueXP atualiza automaticamente a licença na carteira digital da BlueXP e a página licenças dos Serviços de dados refletirá a alteração em 5 a 10 minutos.

2. Se o BlueXP não puder atualizar automaticamente a licença (por exemplo, quando instalado em um site escuro), você precisará fazer o upload manual do arquivo de licença.
   a. Você pode Obtenha o arquivo de licença no site de suporte da NetApp.
   b. Na página da carteira digital do BlueXP *licenças de serviços de dados*, clique ••• para obter o número de série do serviço que está a atualizar e clique em **Atualizar licença**.

   c. Na página *Atualizar Licença*, carregue o arquivo de licença e clique em **Atualizar Licença**.

Resultado

O BlueXP atualiza a licença para que o backup e a recuperação do BlueXP continuem ativos.

Considerações sobre a licença BYOL

Ao usar uma licença BYOL de backup e recuperação do BlueXP , o BlueXP exibe um aviso na interface do usuário quando o tamanho de todos os dados que você está fazendo backup está próximo ao limite de capacidade ou se aproximando da data de expiração da licença. Você receberá estes avisos:

- 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 BlueXP para renovar sua licença quando você vir esses avisos.

Duas coisas podem acontecer quando sua licença BYOL expirar:

- Se a conta que você está usando tiver uma conta PAYGO marketplace, o serviço de backup continuará sendo executado, mas você será transferido para um modelo de licenciamento PAYGO. Você será cobrado pela capacidade que seus backups estão usando.
- Se a conta que você está usando não tiver uma conta de mercado, o serviço de backup continuará sendo executado, mas você continuará a ver os avisos.

Depois de renovar sua assinatura BYOL, o BlueXP atualiza automaticamente a licença. Se o BlueXP não puder acessar o arquivo de licença pela conexão segura à Internet (por exemplo, quando instalado em um site escuro), você poderá obter o arquivo sozinho e enviá-lo manualmente para o BlueXP . Para obter instruções, "Como atualizar uma licença de backup e recuperação do BlueXP "consulte .

Os sistemas que foram transferidos para uma licença PAYGO são devolvidos à licença BYOL automaticamente. E os sistemas que estavam funcionando sem uma licença pararão de ver os avisos.

Monitorar a proteção de dados

Relatório sobre a cobertura de proteção de dados

Com os relatórios de backup e recuperação do BlueXP , você garante a proteção dos dados essenciais de acordo com as políticas definidas pela sua organização e realiza auditorias de necessidades de conformidade.

Os relatórios de backup e recuperação do BlueXP ajudam você a realizar o seguinte:

- **Visibilidade das operações**: Monitore seus contratos de nível de serviço com relação à proteção de dados, taxa de sucesso de backup e alinhamento de janelas de backup às necessidades de negócios.
- * Conformidade e auditoria*: Use relatórios operacionais e de inventário em seus processos de auditoria interna e externa para monitoramento contínuo da conformidade.

As atividades de relatório são monitorizadas no registo de monitorização de trabalhos para que possa auditar todas as atividades. "Saiba mais sobre Monitoramento de trabalhos".

Escopo dos relatórios

Os relatórios de backup e recuperação do BlueXP fornecem informações sobre os seguintes aspetos:

- **Localização do conetor**: No local ou na nuvem
- **Origem**: Volumes Cloud Volumes ONTAP, volumes ONTAP locais ou aplicações
- **Destino**: Qualquer um dos provedores de nuvem, NetApp StorageGRID ou ONTAP S3
- **Versões ONTAP**: 9.13.0

Criar um relatório de inventário de backup

Na guia relatórios de backup e recuperação do BlueXP , você pode criar o relatório de inventário de backup e filtrar seu conteúdo. Com o relatório Backup Inventory, você pode ver todos os backups de uma conta específica, ambiente de trabalho ou inventário de SVM.

O relatório Backup Inventory mostra as seguintes informações e muito mais:

- Conta, ambiente de trabalho e SVM
- Volumes protegidos e não protegidos
- Destino de backup
- Política de backup aplicada
- Estilo de criptografia (chave gerenciada pelo provedor ou chave gerenciada pelo usuário)
- Status de proteção DataLock e ransomware (governança, conformidade ou nenhuma)
- Estado de arquivamento ativado
- Contagem de cópias de backup
- Tipo de cópia de segurança (cópia de segurança ad-hoc agendada ou iniciada pelo utilizador)
- Classe de armazenamento

- Etiqueta do instantâneo

O relatório Backup Inventory não inclui informações de backup expiradas ou com falha.

A parte superior do relatório inclui um gráfico que mostra as seguintes informações:

- Contagem de volumes no escopo com pelo menos um backup
- Total de volumes inativos mais volumes ativos

O relatório Backup Inventory mostra os seguintes gráficos:

- **Status do backup de volume**: Mostra protegido em comparação com volumes não protegidos para o escopo selecionado.
- **Volumes por contagem de backup**: Agrupa volumes pelo número de cópias de backup disponíveis para esse volume.

Passos

1. No menu superior, selecione **relatórios**.
2. Selecione **Backup de inventário**.
3. Selecione **criar relatório**.
4. Selecione a conta, o ambiente de trabalho e o SVM.

   Você pode selecionar vários ambientes de trabalho e SVMs.

5. Selecione o período de tempo: Últimas 24 horas, semana ou mês.
6. Revise as seções do relatório (políticas Snapshot, políticas de replicação ou políticas de backup), dependendo das seleções de relatório.
7. (Opcional) Filtrar os resultados por status do trabalho.
8. (Opcional) Exporte o conteúdo do relatório no formato .CSV selecionando **Download CSV**.

Criar um relatório de atividade de trabalho de proteção de dados

O monitoramento proativo pode reduzir o esforço necessário para monitorar todos os recursos em seu ecossistema. A partir do ONTAP 9.13,0, o relatório atividade de trabalho de proteção de dados fornece informações sobre operações de snapshot, backup, clone e restauração que você pode usar com o monitoramento de SLA e rastrear taxas de backup e recuperação.

O relatório se aplica às operações de backup e recuperação do BlueXP para dados de Cloud Volumes ONTAP, on-premises e aplicações.

O relatório atividade trabalho proteção de dados mostra as seguintes informações e muito mais:

- Conta, ambiente de trabalho e SVM
- Tipo de tarefa (backup ou restauração)
- Nome do recurso (volume ou aplicativo)
- Estado do trabalho
- Horários de início e fim e duração

- Nome da política para trabalhos de cópia de segurança
- Etiqueta Snapshot para trabalhos de cópia de segurança

Os gráficos na parte superior da página mostram as seguintes informações:

- Trabalhos por tipo
  - Contagem de tarefas de backup e restauração do ONTAP volumes
  - Contagem dos trabalhos de cópia de segurança e restauro de aplicações
  - Contagem de tarefas de backup e restauração de máquinas virtuais
- Atividade de trabalho diária

Passos

1. No menu superior, selecione **relatórios**.
2. Selecione **atividade do trabalho de proteção de dados**.
3. Selecione **criar relatório**.
4. Selecione a conta, o ambiente de trabalho e o SVM.
5. Selecione o período de tempo: Últimas 24 horas, semana ou mês.
6. (Opcional) Filtrar os resultados por status da tarefa, tipos de tarefa (backup ou restauração) e recurso.
7. (Opcional) Exporte o conteúdo do relatório no formato .CSV selecionando **Download CSV**.

Monitore o status dos trabalhos de backup e restauração

Você pode monitorar o status de snapshots locais, replicações e tarefas de backup para armazenamento de objetos iniciadas e restaurar tarefas iniciadas por você. Você pode ver os trabalhos que foram concluídos, estão em andamento ou falharam para que você possa diagnosticar e corrigir problemas. Usando a Central de notificações do BlueXP , você pode habilitar notificações para serem enviadas por e-mail para que você possa ser informado sobre atividades importantes do sistema, mesmo quando não estiver conetado ao sistema. Usando a linha do tempo do BlueXP , você pode ver detalhes de todas as ações iniciadas por meio da interface do usuário ou da API.

Ver o estado do trabalho no Monitor de trabalhos

Você pode exibir uma lista de todas as operações de captura instantânea, replicação, backup para armazenamento de objetos e restauração e seu status atual na guia **Monitoramento de tarefas**. Isso inclui operações do Cloud Volumes ONTAP, ONTAP no local, aplicativos e máquinas virtuais. Cada operação, ou trabalho, tem um ID exclusivo e um status.

O estado pode ser:

- Sucesso
- Em curso
- Em fila de espera
- Aviso

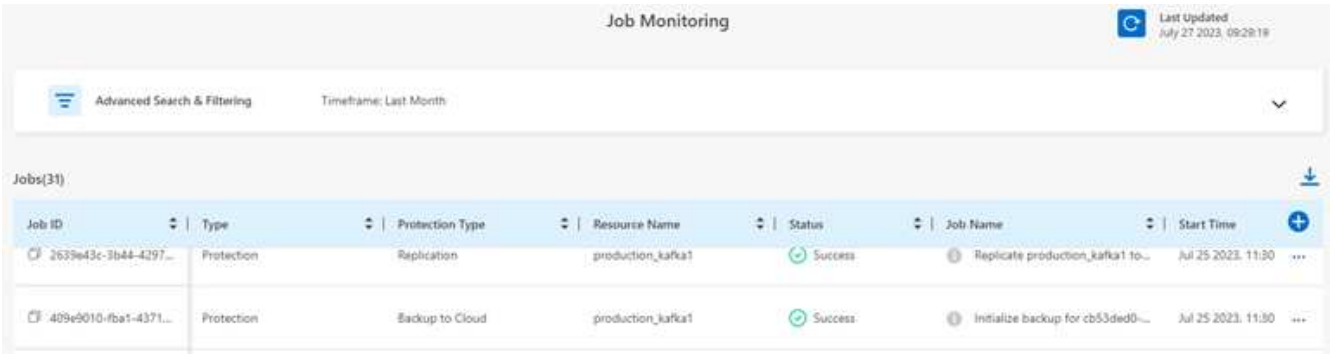
- Falha

Snapshots, replicações, backups para armazenamento de objetos e operações de restauração iniciadas a partir da API e IU de recuperação do BlueXP estão disponíveis na guia Monitoramento de tarefas.

Se você atualizou seus sistemas ONTAP para 9,13.x e não vê as operações de backup agendadas em andamento no Monitor de trabalho, precisará reiniciar o serviço de backup e recuperação do BlueXP . "Saiba como reiniciar o backup e a recuperação do BlueXP ".

Passos

1. No menu BlueXP , selecione **proteção > Backup e recuperação**.
2. Selecione a guia **Monitoramento de trabalho**.



Esta captura de tela mostra os cabeçalhos de coluna padrão.

3. Para mostrar colunas adicionais (ambiente de trabalho, SVM, Nome de usuário, carga de trabalho, Nome da diretiva, Etiqueta Snapshot), selecione .

PESQUISE e filtre a lista de trabalhos

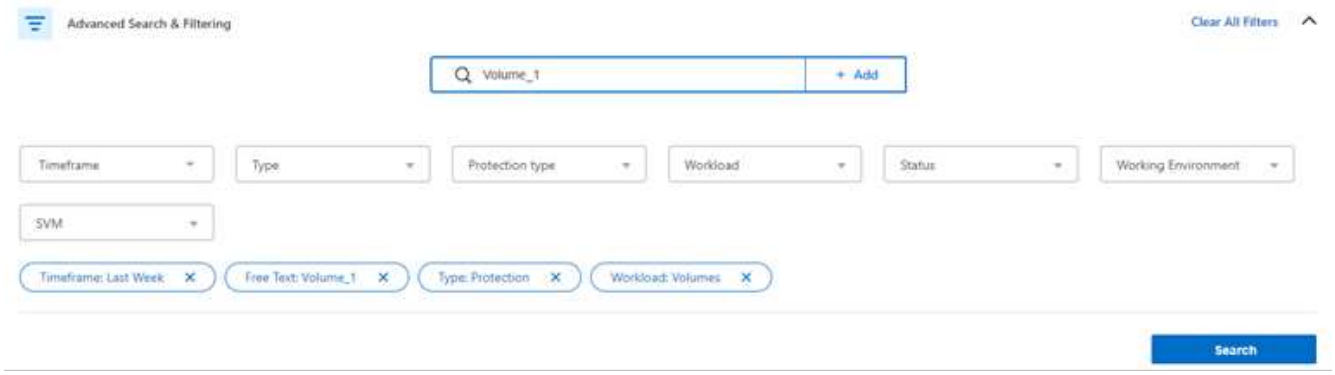
Você pode filtrar as operações na página Monitoramento de tarefas usando vários filtros, como política, etiqueta Snapshot, tipo de operação (proteção, restauração, retenção ou outro) e tipo de proteção (Snapshot local, replicação ou backup na nuvem).

Por predefinição, a página monitorização de trabalhos mostra os trabalhos de proteçãoão e recuperação das últimas 24 horas. Você pode alterar o período de tempo usando o filtro de período de tempo.

Passos

1. Selecione a guia **Monitoramento de trabalho**.
2. Para classificar os resultados de forma diferente, selecione cada cabeçalho de coluna para classificar por Status, hora de Início, Nome do recurso e muito mais.
3. Se você estiver procurando trabalhos específicos, selecione a área **Pesquisa avançada & filtragem** para abrir o painel Pesquisa.

   Utilize este painel para introduzir uma pesquisa de texto livre para qualquer recurso; por exemplo, "volume 1" ou "aplicação 3". Também pode filtrar a lista de trabalhos de acordo com os itens nos menus pendentes.



Esta captura de tela mostra como você pesquisaria todos os trabalhos "volume" "Backup" para volumes nomeados "volume_1" na "semana passada".

A maioria dos filtros são auto-explicativos. O filtro para "carga de trabalho" permite visualizar trabalhos nas seguintes categorias:

- Volumes (Cloud Volumes ONTAP e ONTAP volumes no local)
- Aplicações
- Máquinas virtuais

- Você pode pesquisar dados em um "SVM" específico somente se você tiver selecionado primeiro um ambiente de trabalho.
- Pode pesquisar utilizando o filtro "tipo de proteção" apenas quando tiver selecionado o "tipo" de "proteção".

4. Para atualizar a página imediatamente, selecione o botão. Caso contrário, esta página é atualizada a cada 15 minutos para que você sempre veja os resultados mais recentes do status do trabalho.

Ver detalhes do trabalho

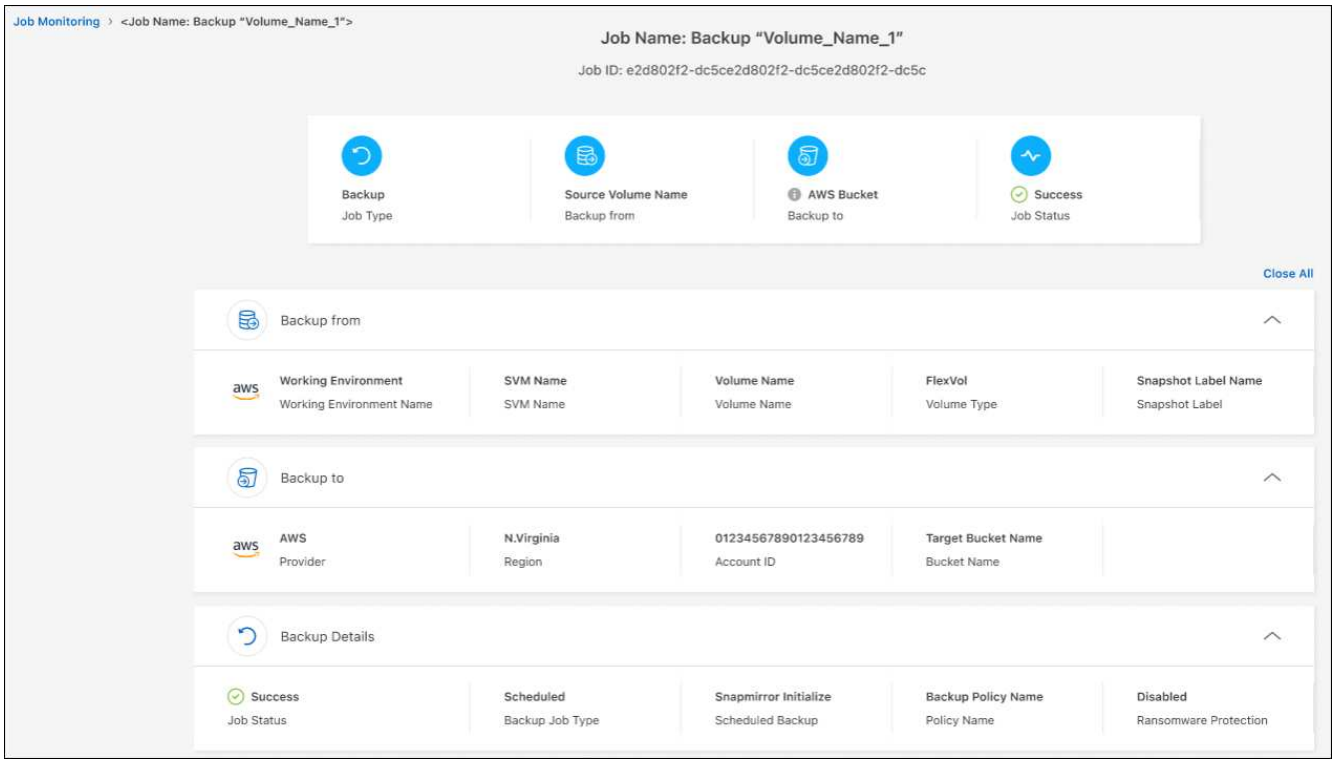
Pode ver detalhes correspondentes a um trabalho concluído específico. Você pode exportar detalhes de uma tarefa específica em um formato JSON.

Você pode exibir detalhes como tipo de tarefa (agendada ou sob demanda), tipo de backup do SnapMirror (inicial ou periódica) horários de início e término, duração, quantidade de dados transferidos do ambiente de trabalho para o armazenamento de objetos, taxa de transferência média, nome da política, bloqueio de retenção ativado, verificação de ransomware realizada, detalhes da fonte de proteção e detalhes do destino de proteção.

As tarefas de restauração mostram detalhes como provedor de destino de backup (Amazon Web Services, Microsoft Azure, Google Cloud, no local), nome do bucket S3, nome do SVM, nome do volume de origem, volume de destino, etiqueta Snapshot, contagem de objetos recuperados, nomes de arquivos, tamanhos de arquivo, data da última modificação e caminho completo do arquivo.

Passos

1. Selecione a guia **Monitoramento de trabalho**.
2. Selecione o nome do trabalho.
3. Selecione o menu ações ••• e selecione **Exibir detalhes**.



4. Expanda cada seção para ver os detalhes.

Faça o download dos resultados da monitorização de trabalhos como um relatório

Pode transferir o conteúdo da página principal de monitorização de trabalhos como um relatório depois de o ter refinado. O backup e a recuperação do BlueXP geram e fazem o download de um arquivo .CSV que você pode revisar e enviar para outros grupos conforme necessário. O arquivo .CSV inclui até 10.000 linhas de dados.

A partir das informações de Detalhes de Monitoramento de tarefa, você pode baixar um arquivo JSON contendo detalhes de uma única tarefa.

Passos

1. Selecione a guia **Monitoramento de trabalho**.
2. Para transferir um ficheiro CSV para todos os trabalhos, selecione o botão e localize o ficheiro no diretório de transferências.
3. Para baixar um arquivo JSON para uma única tarefa, selecione o menu ações para a tarefa, selecione **Baixar arquivo JSON** e localize o arquivo no diretório de download.

Rever trabalhos de retenção (ciclo de vida de cópia de segurança)

O monitoramento de fluxos de retenção (ou *ciclo de vida de backup*) ajuda você com integridade de auditoria, responsabilidade e segurança de backup. Para ajudá-lo a controlar o ciclo de vida do backup, talvez você queira identificar a expiração de todas as cópias de backup.

Uma tarefa de ciclo de vida de backup controla todas as cópias Snapshot que são excluídas ou na fila a serem excluídas. A partir do ONTAP 9.13, você pode olhar para todos os tipos de tarefa chamados "retenção" na página Monitoramento de tarefa.

O tipo de tarefa "retenção" captura todos os trabalhos de exclusão Instantânea iniciados em um volume

protegido pelo backup e recuperação do BlueXP .

Passos

1. Selecione a guia **Monitoramento de trabalho**.
2. Selecione a área **Pesquisa avançada & filtragem** para abrir o painel Pesquisa.
3. Selecione "retenção" como o tipo de tarefa.

Revise alertas de backup e restauração no Centro de notificações do BlueXP

O Centro de notificações do BlueXP rastreia o progresso dos trabalhos de backup e restauração iniciados para que você possa verificar se a operação foi bem-sucedida ou não.

Além de visualizar os alertas na Central de notificações, você pode configurar o BlueXP para enviar determinados tipos de notificações por e-mail como alertas para que você possa ser informado sobre atividades importantes do sistema, mesmo quando não estiver conetado ao sistema. "Saiba mais sobre a Central de notificações e como enviar e-mails de alerta para tarefas de backup e restauração".

O Centro de notificações exibe vários eventos de Snapshot, replicação, backup na nuvem e restauração, mas apenas certos eventos acionam alertas de e-mail:

Tipo de operação	Evento	Nível de alerta	E-mail enviado
Ativação	Falha na ativação de backup e recuperação para o ambiente de trabalho	Erro	Sim
Ativação	Falha na edição de backup e recuperação para o ambiente de trabalho	Erro	Sim
Instantâneo local	Falha de tarefa ad-hoc de criação de snapshot de backup e recuperação do BlueXP	Erro	Sim
Replicação	Falha de trabalho de replicação ad-hoc de backup e recuperação do BlueXP	Erro	Sim
Replicação	Falha do trabalho de pausa de replicação de backup e recuperação do BlueXP	Erro	Não
Replicação	Falha na tarefa de interrupção da replicação de backup e recuperação do BlueXP	Erro	Não
Replicação	Falha de tarefa ressincronizada de replicação de backup e recuperação do BlueXP	Erro	Não
Replicação	Falha na tarefa de interrupção da replicação de backup e recuperação do BlueXP	Erro	Não
Replicação	Falha de tarefa ressincronizada reversa da replicação de backup e recuperação do BlueXP	Erro	Sim
Replicação	Falha na tarefa de eliminação da replicação de recuperação e cópia de segurança do BlueXP	Erro	Sim

A partir do ONTAP 9.13,0, todos os alertas são exibidos para sistemas Cloud Volumes ONTAP e ONTAP locais. Para sistemas com Cloud Volumes ONTAP 9.13.0 e ONTAP no local, apenas o alerta relacionado com "Restaurar trabalho concluído, mas com avisos" é apresentado.

Por padrão, os administradores de contas e organizações do BlueXP recebem e-mails para todos os alertas "críticos" e "Recomendação". Todos os outros usuários e destinatários estão configurados, por padrão, para não receber nenhum e-mail de notificação. Os e-mails podem ser enviados para qualquer usuário do BlueXP que faça parte da sua conta do NetApp Cloud ou para qualquer outro destinatário que precise estar ciente da atividade de backup e restauração.

Para receber os alertas de backup e recuperação do BlueXP , você precisará selecionar os tipos de gravidade de notificação "crítico", "Aviso" e "erro" na página Configurações de alertas e notificações.

"Saiba como enviar e-mails de alerta para tarefas de backup e restauração".

Passos

1. Na barra de menu BlueXP (Menu do sistema), selecione ( ).
2. Reveja as notificações.

Reveja a atividade de operação na linha do tempo do BlueXP

Você pode exibir detalhes das operações de backup e restauração para mais investigações na linha do tempo do BlueXP . A linha do tempo do BlueXP fornece detalhes de cada evento, seja iniciado pelo usuário ou iniciado pelo sistema, e mostra ações iniciadas na IU ou pela API.

"Saiba mais sobre as diferenças entre a linha do tempo e o Centro de notificações".

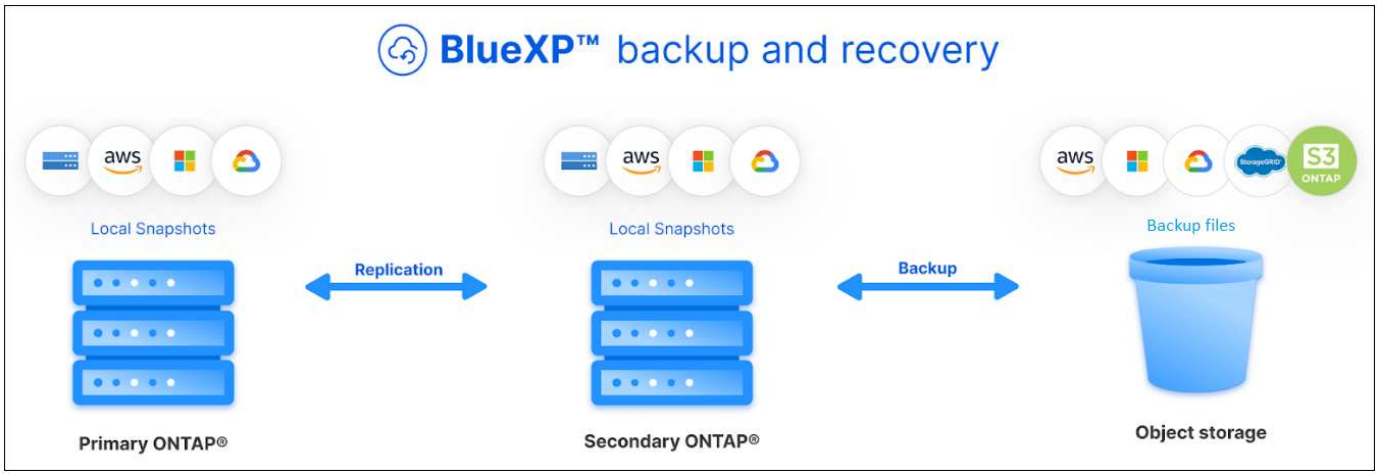
Faça backup e restaure dados do ONTAP

Proteja os dados de volume do ONTAP usando o backup e a recuperação do BlueXP

O serviço de backup e recuperação do BlueXP oferece recursos de backup e restauração para proteção e arquivamento a longo prazo de seus dados de volume do ONTAP. Você pode implementar uma estratégia 3-2-1 em que tenha 3 cópias dos dados de origem em 2 sistemas de storage diferentes e 1 cópias na nuvem.

Após a ativação, o backup e a recuperação criam backups incrementais para sempre em nível de bloco que são armazenados em outro cluster ONTAP e no storage de objetos na nuvem. Além do volume de origem, você terá:

- Cópia Snapshot do volume no sistema de origem
- Volume replicado em um sistema de storage diferente
- Backup do volume no armazenamento de objetos



O backup e a recuperação do BlueXP utilizam a tecnologia de replicação de dados SnapMirror da NetApp para garantir que todos os backups sejam totalmente sincronizados criando cópias Snapshot e transferindo-as para os locais de backup.

Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados fornecem proteção em várias camadas contra ameaças internas (internas) e externas à segurança cibernética.
- Vários tipos de Mídia garantem a viabilidade do failover em caso de falha física ou lógica de um tipo de Mídia.
- A cópia no local facilita restaurações rápidas, com as cópias externas prontas, caso a cópia no local seja comprometida.

Quando necessário, você pode restaurar um *volume* inteiro, uma *pasta* ou um ou mais *arquivos*, de qualquer uma das cópias de backup para o mesmo ou diferente ambiente de trabalho.

Caraterísticas

Recursos de replicação:

- Replique dados entre sistemas de storage ONTAP para dar suporte a backup e recuperação de desastres.
- Garanta a confiabilidade do seu ambiente de recuperação de desastres com alta disponibilidade.
- Criptografia nativa ONTAP em trânsito configurada via chave pré-compartilhada (PSK) entre os dois sistemas.
- Os dados copiados são imutáveis até que você os torne graváveis e prontos para uso.
- A replicação é de autorrecuperação no caso de uma falha de transferência.
- Em comparação com o "Serviço de replicação BlueXP ", a replicação no backup e recuperação do BlueXP inclui os seguintes recursos:
  - Replique vários volumes FlexVol de cada vez para um sistema secundário.
  - Restaure um volume replicado para o sistema de origem ou para um sistema diferente usando a IU.
  - Gerenciar políticas de replicação

Consulte "Limitações de replicação" para obter uma lista de recursos de replicação que não estão disponíveis com backup e recuperação do BlueXP .

Recursos de backup para objeto:

- Faça backup de cópias independentes de seus volumes de dados para storage de objetos de baixo custo.
- Aplique uma única política de backup a todos os volumes em um cluster ou atribua diferentes políticas de backup a volumes que tenham objetivos únicos de ponto de recuperação.
- Crie uma política de backup a ser aplicada a todos os volumes futuros criados no cluster.
- Faça arquivos de backup imutáveis para que eles sejam bloqueados e protegidos durante o período de retenção.
- Verifique os arquivos de backup para possíveis ataques de ransomware e remova/substitua os backups infetados automaticamente.
- Disponha arquivos de backup mais antigos em storage de arquivamento para economizar custos.
- Exclua o relacionamento de backup para que você possa arquivar volumes de origem desnecessários e reter backups de volume.
- Fazer backup da nuvem para a nuvem e dos sistemas no local para a nuvem pública ou privada.
- Os dados de backup são protegidos com criptografia AES-256 bits em repouso e conexões HTTPS TLS 1,2 em trânsito.
- Use suas próprias chaves gerenciadas pelo cliente para criptografia de dados em vez de usar as chaves de criptografia padrão do seu provedor de nuvem.
- Suporte para até 4.000 backups de um único volume.
- Restaurar recursos: *
- Restaure os dados de um ponto específico no tempo a partir de cópias Snapshot locais, volumes replicados ou volumes de backup no storage de objetos.
- Restaure um volume, uma pasta ou arquivos individuais para o sistema de origem ou para um sistema diferente.
- Restaure dados para um ambiente de trabalho usando uma assinatura/conta diferente ou que esteja em

uma região diferente.

- Execute uma *restauração rápida* de um volume de armazenamento em nuvem para um sistema Cloud Volumes ONTAP ou para um sistema local; perfeito para situações de recuperação de desastres em que você precisa fornecer acesso a um volume o mais rápido possível.
- Restaure dados em um nível de bloco, colocando os dados diretamente no local especificado, tudo preservando as ACLs originais.
- Navegue e pesquise catálogos de arquivos para fácil seleção de pastas e arquivos individuais para restauração de arquivos único.

Ambientes de trabalho compatíveis para operações de backup e restauração

O backup e a recuperação do BlueXP são compatíveis com ambientes de trabalho do ONTAP e fornecedores de nuvem pública e privada.

Regiões suportadas

O backup e a recuperação do BlueXP são compatíveis com o Cloud Volumes ONTAP em muitas regiões da Amazon Web Services, Microsoft Azure e Google Cloud.

"Saiba mais usando o mapa das Regiões globais"

Destinos de cópia de segurança suportados

Com o backup e a recuperação do BlueXP , você faz backup de volumes do ONTAP dos seguintes ambientes de trabalho de origem para os seguintes ambientes de trabalho secundários e storage de objetos em fornecedores de nuvem pública e privada. As cópias Snapshot residem no ambiente de trabalho de origem.

Fonte ambiente de trabalho	Ambiente de trabalho secundário (replicação)	Armazenamento de objetos de destino (Backup) ifdef::aws[]
Cloud Volumes ONTAP na AWS	Cloud Volumes ONTAP no sistema ONTAP on-premises da AWS	Amazon S3 endif::aws[] ifdef::azul[]
Cloud Volumes ONTAP no Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Azure Blob endif::azure[] ifdef::gcp[]
Cloud Volumes ONTAP no Google	Cloud Volumes ONTAP no sistema ONTAP local do Google	Google Cloud Storage endif::gcp[]
Sistema ONTAP no local	Sistema ONTAP no local da Cloud Volumes ONTAP	Ifdef::aws[] Amazon S3 endif::aws[] ifdef::azure[] Azure Blob endif::azure[] ifdef::gcp[] Google Cloud Storage endif::gcp[] NetApp StorageGRID ONTAP S3

Destinos de restauração suportados

É possível restaurar os dados do ONTAP a partir de um arquivo de backup que reside em um ambiente de trabalho secundário (um volume replicado) ou no storage de objetos (um arquivo de backup) para os seguintes ambientes de trabalho. As cópias Snapshot residem no ambiente de trabalho de origem e podem ser restauradas somente nesse mesmo sistema.

Localização do ficheiro de cópia de segurança		Ambiente de trabalho de destino
Object Store (Backup)	**Sistema secundário (replicação)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP on-premises da AWS	Cloud Volumes ONTAP no AWS on-premises ONTAP system endif::aws[] ifdef::azure[]
Blob do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP in Azure on-premises ONTAP system endif::azul[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP no sistema ONTAP local do Google	Cloud Volumes ONTAP no Google on-premises ONTAP system endif::gcp[]
NetApp StorageGRID	ONTAP System Cloud Volumes ONTAP no local	Sistema ONTAP no local
ONTAP S3	ONTAP System Cloud Volumes ONTAP no local	Sistema ONTAP no local

Observe que as referências a "sistemas ONTAP on-premises" incluem sistemas FAS, AFF e ONTAP Select.

Volumes compatíveis

O backup e a recuperação do BlueXP são compatíveis com os seguintes tipos de volumes:

- Volumes de leitura-gravação do FlexVol
- Volumes FlexGroup (requer ONTAP 9.12,1 ou posterior)
- Volumes SnapLock Enterprise (requer ONTAP 9.11,1 ou posterior)
- SnapLock Compliance para volumes no local (requer ONTAP 9.14 ou posterior)
- Volumes de destino da proteção de dados da SnapMirror (DP)

Consulte as secções em "Limitações de backup e restauração" para obter requisitos e limitações adicionais.

Custo

Há dois tipos de custos associados ao uso de backup e recuperação do BlueXP com sistemas ONTAP: Taxas de recursos e taxas de serviço. Ambos os encargos são para a parte de backup para objeto do serviço.

Não há cobrança para criar cópias Snapshot ou volumes replicados - além do espaço em disco necessário para armazenar as cópias Snapshot e volumes replicados.

Cobranças de recursos

As cobranças de recursos são pagas ao provedor de nuvem pela capacidade de armazenamento de objetos e pela gravação e leitura de arquivos de backup na nuvem.

- No caso de backup para storage de objetos, você paga seu fornecedor de nuvem pelos custos de storage de objetos.

  Como o backup e a recuperação do BlueXP preservam as eficiências de storage do volume de origem, você paga os custos de storage de objetos do fornecedor de nuvem pelas eficiências de dados *após* ONTAP (para o menor volume de dados após a aplicação de deduplicação e compactação).

- Para restaurar dados usando Pesquisa e Restauração, certos recursos são provisionados pelo provedor de nuvem e há custo por TIB associado à quantidade de dados que é verificada por suas solicitações de pesquisa. (Esses recursos não são necessários para navegar e restaurar.)
  - Na AWS "Amazon Athena", e "Cola da AWS" os recursos são implantados em um novo bucket do S3.
  - No Azure, os "Espaço de trabalho do Azure Synapse" e "Storage do Azure Data Lake" são provisionados na sua conta de storage para armazenar e analisar seus dados.
- No Google, um novo bucket é implantado e o "Serviços do Google Cloud BigQuery" é provisionado em um nível de conta/projeto.
- Se você planeja restaurar dados de volume de um arquivo de backup que foi movido para o armazenamento de objetos de arquivamento, então há uma taxa de recuperação por GiB adicional e uma taxa por solicitação do provedor de nuvem.
- Se você planeja verificar um arquivo de backup para ransomware durante o processo de restauração de dados de volume (se você ativou a proteção DataLock e ransomware para seus backups na nuvem), você também terá custos extras de saída do seu provedor de nuvem.

Taxas de serviço

As cobranças de serviço são pagas ao NetApp e cobrem tanto o custo de *criar* backups para armazenamento de objetos quanto de *restaurar* volumes ou arquivos desses backups. Você paga apenas pelos dados que protege no storage de objetos, calculados pela capacidade lógica de origem usada (*before* eficiências de ONTAP) de volumes do ONTAP com backup no storage de objetos. Essa capacidade também é conhecida como Front-End Terabytes (FETB).

Há três maneiras de pagar pelo serviço de backup. A primeira opção é se inscrever no seu provedor de nuvem, o que permite que você pague por mês. A segunda opção é obter um contrato anual. A terceira opção é comprar licenças diretamente da NetApp. Leia Licenciamentoa seção para obter detalhes.

Licenciamento

O backup e a recuperação do BlueXP estão disponíveis nos seguintes modelos de consumo:

- **BYOL**: Uma licença adquirida na NetApp que pode ser usada com qualquer provedor de nuvem.
- **PAYGO**: Uma assinatura por hora do mercado do seu provedor de nuvem.
- **Anual**: Um contrato anual do mercado do seu provedor de nuvem.

Uma licença de backup é necessária apenas para backup e restauração a partir do storage de objetos. A criação de cópias Snapshot e volumes replicados não exige licença.

Traga sua própria licença

O BYOL é baseado no termo (1, 2 ou 3 anos) *e* baseado na capacidade em incrementos de 1 TIB. Você paga a NetApp para usar o serviço por um período de tempo, digamos 1 ano, e por um valor máximo de capacidade, digamos 10 TIB.

Receberá um número de série introduzido na página da carteira digital da BlueXP para ativar o serviço. Quando um dos limites for atingido, você precisará renovar a licença. A licença BYOL de backup se aplica a todos os sistemas de origem associados à sua organização ou conta do BlueXP .

"Saiba como gerenciar suas licenças BYOL".

Subscrição com pagamento conforme o uso

O backup e a recuperação do BlueXP oferecem 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 GiB pelos dados que são copiados – não há pagamento inicial. Você é cobrado pelo seu provedor de nuvem por meio da sua fatura mensal.

"Saiba como configurar uma assinatura paga conforme o uso".

Observe que uma avaliação gratuita de 30 dias está disponível quando você se inscrever inicialmente com uma assinatura PAYGO.

Contrato anual

Quando você usa a AWS, dois contratos anuais estão disponíveis para prazos de 1, 2 ou 3 anos:

- Um plano de "backup em nuvem" que permite fazer backup dos dados do Cloud Volumes ONTAP e dos dados do ONTAP no local.
- Um plano "CVO Professional" que permite agrupar o backup e a recuperação do Cloud Volumes ONTAP e do BlueXP . Isso inclui backups ilimitados para volumes Cloud Volumes ONTAP cobrados com essa licença (a capacidade de backup não é contada com a licença).

Quando você usa o Azure, dois contratos anuais estão disponíveis para prazos de 1, 2 ou 3 anos:

- Um plano de "backup em nuvem" que permite fazer backup dos dados do Cloud Volumes ONTAP e dos dados do ONTAP no local.
- Um plano "CVO Professional" que permite agrupar o backup e a recuperação do Cloud Volumes ONTAP e do BlueXP . Isso inclui backups ilimitados para volumes Cloud Volumes ONTAP cobrados com essa licença (a capacidade de backup não é contada com a licença).

Ao usar o GCP, é possível solicitar uma oferta privada do NetApp e selecionar o plano ao se inscrever no Google Cloud Marketplace durante a ativação de backup e recuperação do BlueXP .

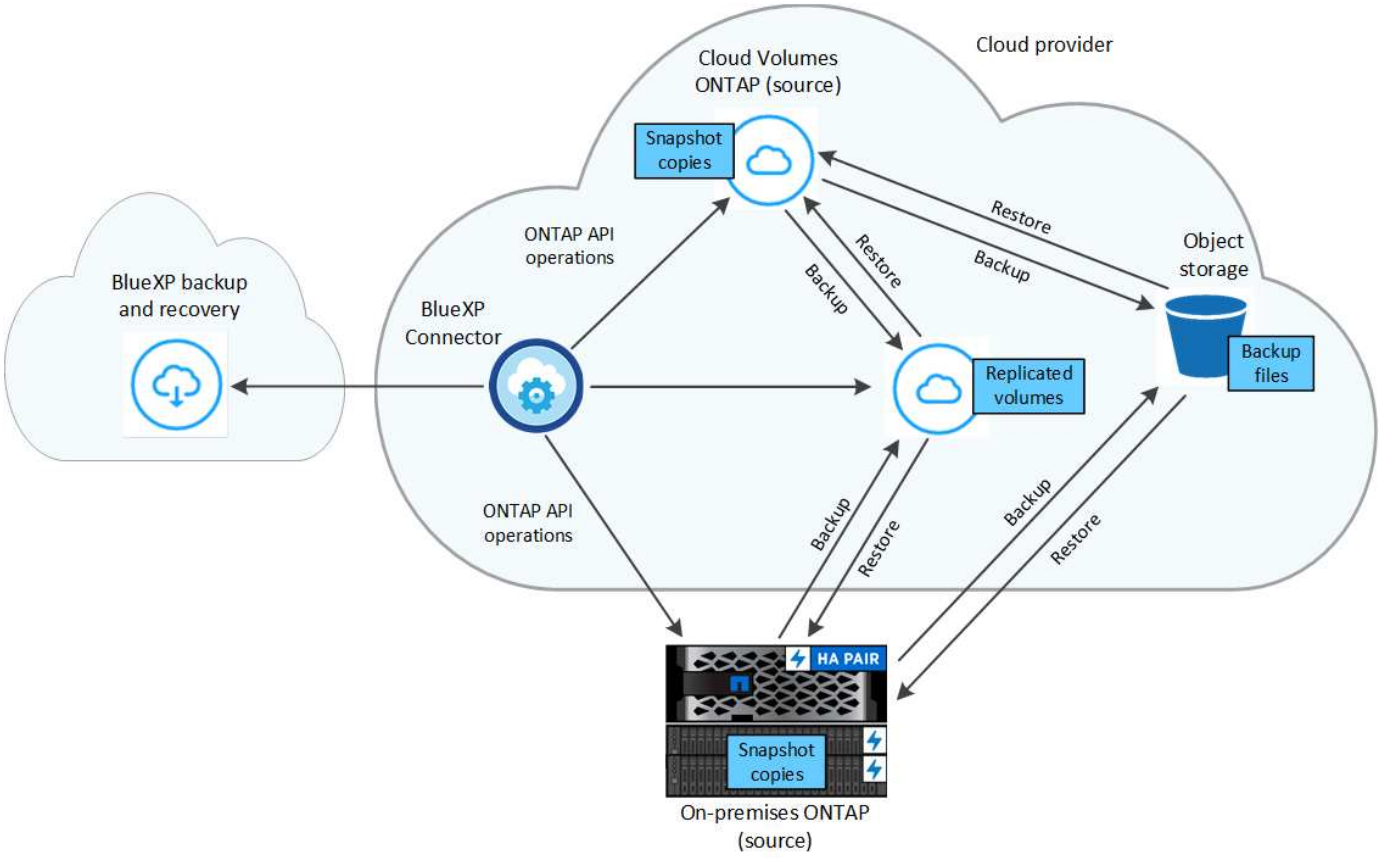
"Saiba como configurar contratos anuais".

Como funciona o backup e a recuperação do BlueXP

Ao habilitar o backup e a recuperação do BlueXP em um sistema Cloud Volumes ONTAP ou ONTAP no local, o serviço realiza um backup completo dos dados. Após o backup inicial, todos os backups adicionais são incrementais, o que significa que somente blocos alterados e novos blocos são copiados. Isso mantém o tráfego de rede no mínimo. O armazenamento de backup para objetos é construído sobre o "Tecnologia de nuvem da NetApp SnapMirror".

> Quaisquer ações tomadas diretamente do ambiente do seu provedor de nuvem para gerenciar ou alterar arquivos de backup na nuvem podem corromper os arquivos e resultará em uma configuração não suportada.

A imagem a seguir mostra a relação entre cada componente:



Esse diagrama mostra os volumes sendo replicados para um sistema Cloud Volumes ONTAP, mas os volumes também podem ser replicados para um sistema ONTAP no local.

Onde os backups residem

Os backups residem em diferentes locais com base no tipo de backup:

- *Cópias Snapshot* residem no volume de origem no ambiente de trabalho de origem.
- *Volumes replicados* residem no sistema de storage secundário: Um sistema Cloud Volumes ONTAP ou ONTAP no local.
- *Cópias de backup* são armazenadas em um armazenamento de objetos que o BlueXP cria em sua conta na nuvem. Há um armazenamento de objetos por cluster/ambiente de trabalho, e o BlueXP nomeia o armazenamento de objetos da seguinte forma: "NetApp-backup-clusteruuid". Certifique-se de não excluir este armazenamento de objetos.
  - Na AWS, o BlueXP ativa o "Recurso de acesso público do Amazon S3 Block" bucket do no S3.
  - No Azure, o BlueXP usa um grupo de recursos novo ou existente com uma conta de armazenamento para o contentor Blob. BlueXP "bloqueia o acesso público aos seus dados de blob" por padrão.
  - No GCP, o BlueXP usa um projeto novo ou existente com uma conta de armazenamento para o bucket do Google Cloud Storage.
  - No StorageGRID, o BlueXP usa uma conta de locatário existente para o bucket do S3.
  - No ONTAP S3, o BlueXP usa uma conta de usuário existente para o bucket do S3.

Se desejar alterar o armazenamento de objetos de destino para um cluster no futuro, será necessário "Anular o registo da cópia de segurança e recuperação do BlueXP para o ambiente de trabalho"e, em seguida, ativar o backup e a recuperação do BlueXP usando as novas informações do provedor de nuvem.

Agendamento de backup personalizável e configurações de retenção

Quando você ativa o backup e a recuperação do BlueXP em um ambiente de trabalho, todos os volumes selecionados inicialmente são copiados usando as políticas selecionadas. Você pode selecionar políticas separadas para cópias Snapshot, volumes replicados e arquivos de backup. Se você quiser atribuir políticas de backup diferentes a determinados volumes com objetivos de ponto de restauração (RPO) diferentes, crie políticas adicionais para esse cluster e atribua essas políticas aos outros volumes após a ativação do backup e da recuperação do BlueXP .

Você pode escolher uma combinação de backups horários, diários, semanais, mensais e anuais de todos os volumes. No caso de backup para objeto, você também pode selecionar uma das políticas definidas pelo sistema que fornece backups e retenção por 3 meses, 1 ano e 7 anos. As políticas de proteção de backup criadas no cluster usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP também aparecerão como seleções. Isso inclui políticas criadas usando rótulos personalizados do SnapMirror.

> A política Snapshot aplicada ao volume deve ter um dos rótulos que você está usando na política de replicação e na política de backup para objeto. Se os rótulos correspondentes não forem encontrados, nenhum arquivo de backup será criado. Por exemplo, se você quiser criar volumes replicados "semanais" e arquivos de backup, use uma política Snapshot que crie cópias Snapshot "semanais".

Depois de atingir o número máximo de backups para uma categoria ou intervalo, backups mais antigos são removidos para que você sempre tenha os backups mais atuais (e assim backups obsoletos não continuem ocupando espaço).

Consulte "Fazer backup de programações" para obter mais detalhes sobre como as opções de agendamento disponíveis.

Observe que você pode "crie um backup sob demanda de um volume" no Painel de backup a qualquer momento, além dos arquivos de backup criados a partir dos backups programados.

> O período de retenção para backups de volumes de proteção de dados é o mesmo que definido na relação de origem do SnapMirror. Você pode alterar isso se quiser usando a API.

Configurações de proteção de arquivo de backup

Se o cluster estiver usando o ONTAP 9.11,1 ou superior, você poderá proteger seus backups no storage de objetos contra exclusões e ataques de ransomware. Cada política de backup fornece uma seção para *DataLock e ransomware Protection* que pode ser aplicada aos seus arquivos de backup por um período específico de tempo - o *período de retenção*.

- *DataLock* protege seus arquivos de backup de serem modificados ou excluídos.
- *Ransomware protection* verifica seus arquivos de backup para procurar evidências de um ataque de ransomware quando um arquivo de backup é criado e quando os dados de um arquivo de backup estão sendo restaurados.

As varreduras de proteção programadas contra ransomware são ativadas por padrão. A predefinição para a frequência de digitalização é de 7 dias. A digitalização ocorre apenas na cópia Snapshot mais recente. As digitalizações programadas podem ser desativadas para reduzir os custos. Você pode ativar ou desativar varreduras de ransomware agendadas na cópia Snapshot mais recente usando a opção na página Configurações avançadas. Se você ativá-lo, as verificações são realizadas semanalmente por padrão. Você pode alterar esse horário para dias ou semanas ou desativá-lo, economizando custos.

O período de retenção do backup é o mesmo que o período de retenção do agendamento do backup, além de

um buffer máximo de 31 dias. Por exemplo, backups *semanais* com cópias *5* retidos bloquearão cada arquivo de backup por 5 semanas. *Backups mensais* com *6* cópias retidas bloquearão cada arquivo de backup por 6 meses.

Atualmente, o suporte está disponível quando o destino do backup é Amazon S3, Azure Blob ou NetApp StorageGRID. Outros destinos de provedores de armazenamento serão adicionados em versões futuras.

Para obter mais detalhes, consulte esta informação:

- "Como funciona a proteção DataLock e ransomware".
- "Como atualizar as opções de proteção contra ransomware na página Configurações avançadas".

O DataLock não pode ser ativado se você estiver categorizando backups em armazenamento de arquivamento.

Armazenamento de arquivos para arquivos de backup mais antigos

Ao usar determinado storage de nuvem, você pode mover arquivos de backup mais antigos para uma classe de storage/categoria de acesso mais barata após um determinado número de dias. Você também pode optar por enviar seus arquivos de backup para o armazenamento de arquivamento imediatamente sem ser gravado no armazenamento padrão na nuvem. Observe que o armazenamento de arquivamento não pode ser usado se você tiver ativado o DataLock.

- Na AWS, os backups são iniciados na classe de armazenamento *Standard* e passam para a classe de armazenamento *Standard-unusual Access* após 30 dias.

  Se o cluster estiver usando o ONTAP 9.10,1 ou superior, você poderá optar por categorizar backups mais antigos no storage *S3 Glacier* ou *S3 Glacier Deep Archive* na IU de backup e recuperação do BlueXP após um determinado número de dias para otimização adicional de custos. "Saiba mais sobre o armazenamento de arquivamento da AWS".

- No Azure, os backups estão associados ao nível de acesso *Cool*.

  Se o cluster estiver usando o ONTAP 9.10,1 ou superior, você poderá optar por categorizar backups mais antigos no storage *Azure Archive* na IU de backup e recuperação do BlueXP após um determinado número de dias para otimização adicional de custos. "Saiba mais sobre o armazenamento de arquivamento do Azure".

- No GCP, os backups estão associados à classe de armazenamento *Standard*.

  Se o cluster estiver usando o ONTAP 9.12,1 ou superior, você poderá optar por categorizar backups mais antigos no storage *Archive* na IU de backup e recuperação do BlueXP após um determinado número de dias para otimização adicional de custos. "Saiba mais sobre o armazenamento de arquivos do Google".

- No StorageGRID, os backups estão associados à classe de armazenamento *Standard*.

  Se o cluster no local estiver usando o ONTAP 9.12,1 ou superior e o sistema StorageGRID estiver usando 11,4 ou mais, você poderá arquivar arquivos de backup mais antigos para storage de arquivamento em nuvem pública após um determinado número de dias. O suporte atual é para camadas de storage do AWS S3 Glacier/S3 Glacier Deep Archive ou do Azure Archive. "Saiba mais sobre o arquivamento de arquivos de backup do StorageGRID".

Consulte "Definições de armazenamento de arquivo" para obter mais detalhes sobre o arquivamento de arquivos de backup mais antigos.

Considerações sobre a política de disposição em camadas do FabricPool

Há certas coisas que você precisa saber quando o volume que você está fazendo backup reside em um agregado do FabricPool e tem uma política de disposição em camadas atribuída que não seja `none`:

- O primeiro backup de um volume em camadas de FabricPool requer a leitura de todos os dados locais e de todos os níveis (do armazenamento de objetos). Uma operação de backup não "reaquece" os dados frios dispostos em camadas no armazenamento de objetos.

  Essa operação pode fazer com que o custo da leitura dos dados do seu provedor de nuvem aumente uma vez.

  - Backups subsequentes são incrementais e não têm esse efeito.
  - Se a política de disposição em camadas for atribuída ao volume quando ela for criada inicialmente, você não verá esse problema.
- Considere o impacto dos backups antes de atribuir a `all` política de disposição em categorias a volumes. Como os dados são categorizados imediatamente, o backup e a recuperação do BlueXP leem os dados da camada de nuvem em vez de da camada local. Como as operações de backup simultâneas compartilham o link de rede para o armazenamento de objetos na nuvem, pode ocorrer degradação do desempenho se os recursos da rede ficarem saturados. Nesse caso, você pode querer configurar proativamente várias interfaces de rede (LIFs) para diminuir esse tipo de saturação de rede.

Planeje sua jornada de proteção

O serviço de backup e recuperação do BlueXP permite que você crie até três cópias dos volumes de origem para proteger os dados. Há muitas opções que você pode selecionar ao ativar este serviço em seus volumes, então você deve revisar suas escolhas para que esteja preparado.

Vamos analisar as seguintes opções:

- Quais recursos de proteção você usará: Cópias snapshot, volumes replicados e/ou backup na nuvem
- Qual arquitetura de backup você usará: Um backup em cascata ou fan-out de seus volumes
- Você usará as políticas de backup padrão ou precisará criar políticas personalizadas
- Você quer que o serviço crie buckets em nuvem para você ou faça seus contêineres de storage de objetos antes de começar
- Que modo de implantação do BlueXP Connector você está usando (modo padrão, restrito ou privado)

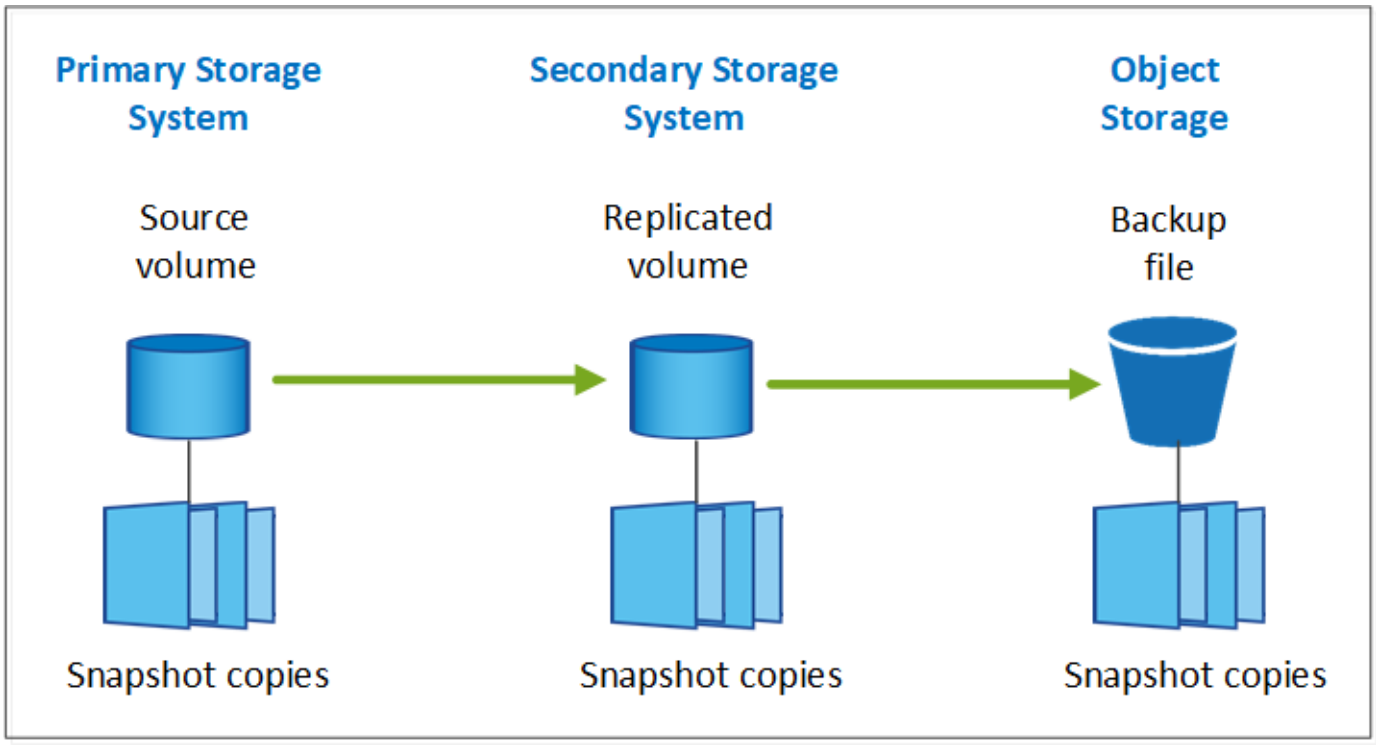
Quais recursos de proteção você usará

Antes de selecionar os recursos que você usará, aqui está uma explicação rápida do que cada recurso faz e que tipo de proteção ele fornece.

Tipo de cópia de segurança	Descrição
Snapshot	Cria uma imagem pontual e somente leitura de um volume dentro do volume de origem como uma cópia Snapshot. Você pode usar a cópia Snapshot para recuperar arquivos individuais ou restaurar todo o conteúdo de um volume.

Tipo de cópia de segurança	Descrição
Replicação	Cria uma cópia secundária de seus dados em outro sistema de storage da ONTAP e atualiza os dados secundários continuamente. Seus dados são mantidos atualizados e permanecem disponíveis sempre que você precisar.
Backup de nuvem	Cria backups dos seus dados na nuvem para fins de proteção e arquivamento de longo prazo. Se necessário, você pode restaurar um volume, pasta ou arquivos individuais do backup para o mesmo ambiente de trabalho ou diferente.

Os instantâneos são a base de todos os métodos de backup e são necessários para usar o serviço de backup e recuperação. Uma cópia Snapshot é uma imagem pontual e somente leitura de um volume. A imagem consome espaço de armazenamento mínimo e incorre em sobrecarga de desempenho insignificante, pois Registra apenas alterações nos arquivos desde que a última cópia Snapshot foi feita. A cópia Snapshot criada no volume é usada para manter o volume replicado e o arquivo de backup sincronizados com as alterações feitas no volume de origem, conforme mostrado na figura.



Você pode optar por criar volumes replicados em outro sistema de storage ONTAP e arquivos de backup na nuvem. Ou você pode escolher apenas criar volumes replicados ou arquivos de backup - é sua escolha.

Em resumo, esses são os fluxos de proteção válidos que você pode criar para volumes no ambiente de trabalho do ONTAP:

- Volume de origem → cópia Snapshot → volume replicado → ficheiro de cópia de segurança
- Volume de origem → cópia Snapshot → ficheiro de cópia de segurança
- Volume de origem → cópia Snapshot → volume replicado

A criação inicial de um volume replicado ou arquivo de backup inclui uma cópia completa dos dados de origem - isso é chamado de *transferência de linha de base*. As transferências subsequentes contêm apenas cópias diferenciais dos dados de origem (Snapshot).

Comparação dos diferentes métodos de backup

A tabela a seguir mostra uma comparação generalizada dos três métodos de backup. Embora o espaço de storage de objetos seja normalmente mais barato do que o storage em disco local, se você acha que pode restaurar dados da nuvem com frequência, as taxas de saída dos provedores de nuvem podem reduzir algumas de suas economias. Você precisará identificar com que frequência precisa restaurar dados dos arquivos de backup na nuvem.

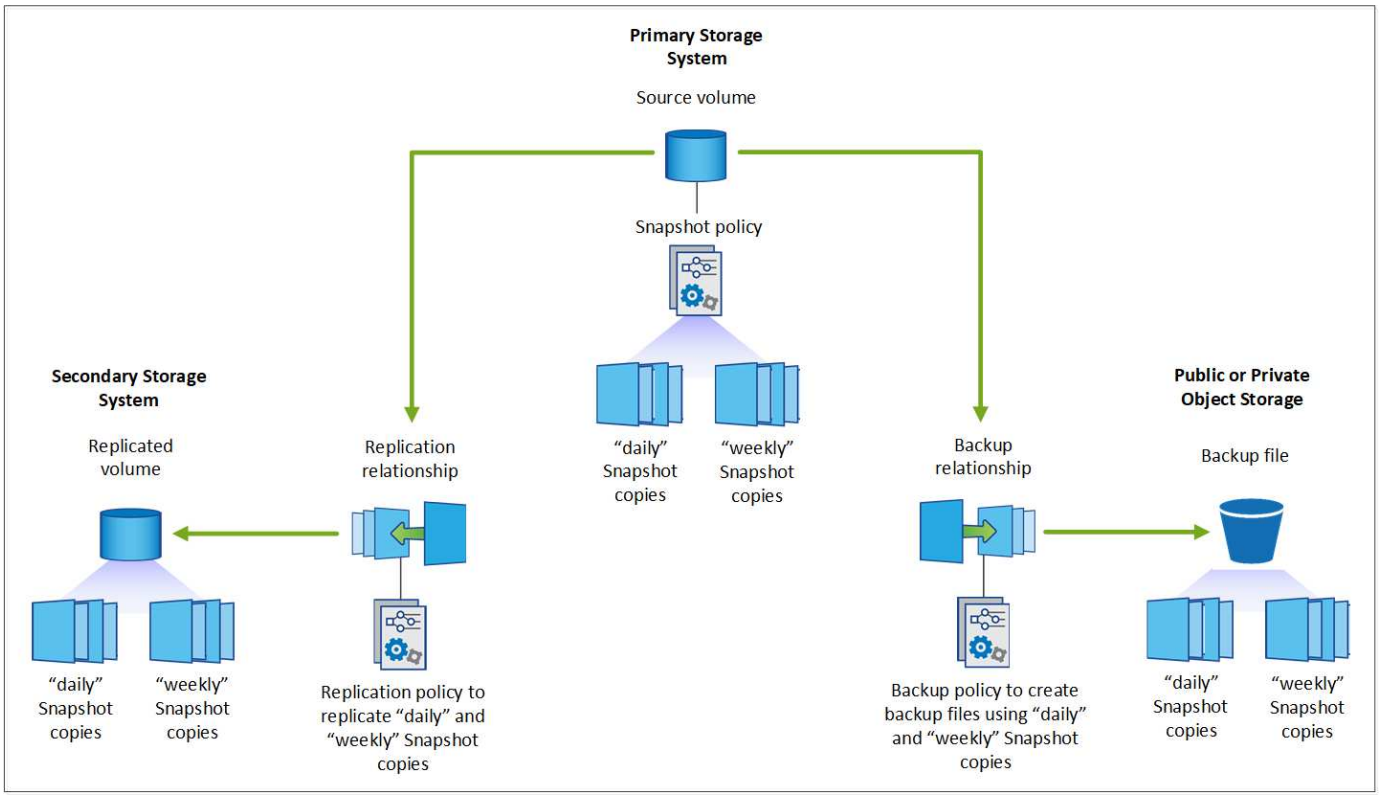
Além desses critérios, o armazenamento em nuvem oferece opções de segurança adicionais se você usar o recurso DataLock and ransomware Protection e economia de custos adicionais selecionando classes de armazenamento de arquivamento para arquivos de backup mais antigos. "Saiba mais sobre a proteção DataLock e ransomware" e "definições de armazenamento de arquivo".

Tipo de cópia de segurança	Velocidade de backup	Custo de backup	Restaure a velocidade	Custo de restauração
Snapshot	Alta	Baixo (espaço em disco)	Alta	Baixo
Replicação	Média	Médio (espaço em disco)	Média	Média (rede)
Backup em nuvem	Baixo	Baixo (espaço do objeto)	Baixo	Alta (taxas do provedor)

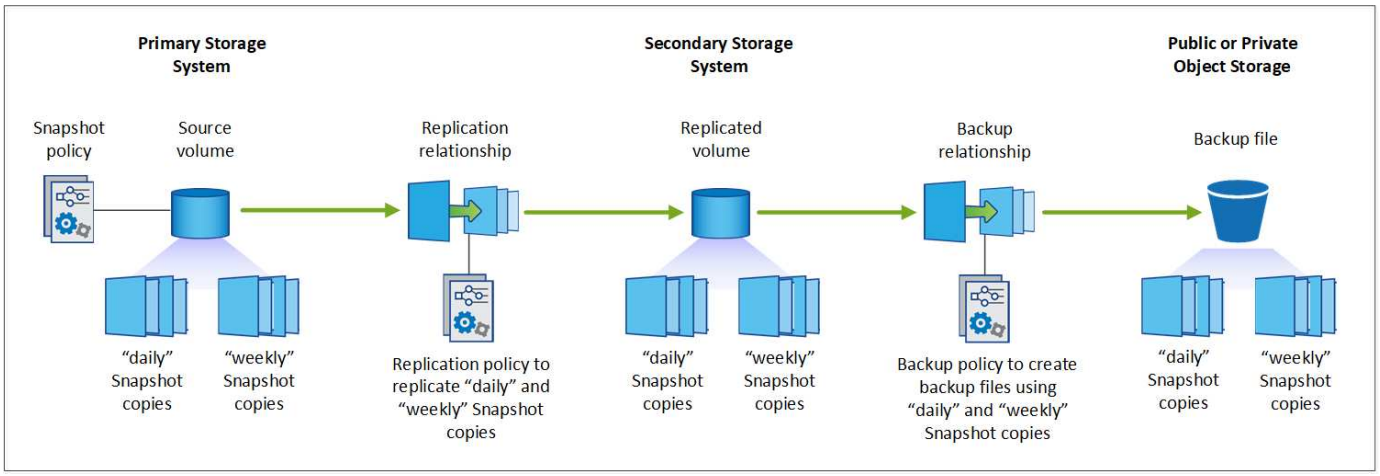
Qual arquitetura de backup você usará

Ao criar volumes replicados e arquivos de backup, você pode escolher uma arquitetura de fan-out ou cascata para fazer backup de seus volumes.

Uma arquitetura * fan-out* transfere a cópia Snapshot de forma independente para o sistema de armazenamento de destino e para o objeto de backup na nuvem.



Uma arquitetura **cascata** transfere a cópia Snapshot primeiro para o sistema de armazenamento de destino e, em seguida, esse sistema transfere a cópia para o objeto de backup na nuvem.



Comparação das diferentes opções de arquitetura

Esta tabela fornece uma comparação das arquiteturas fan-out e cascata.

De fan-out	Cascata
Impacto pequeno na performance no sistema de origem porque ele está enviando cópias Snapshot para 2 sistemas distintos	Menos efeito no desempenho do sistema de storage de origem porque ele envia a cópia Snapshot apenas uma vez
Mais fácil de configurar porque todas as políticas, redes e configurações ONTAP são feitas no sistema de origem	Requer que algumas configurações de rede e ONTAP sejam feitas a partir do sistema secundário também.

Você usará as políticas padrão para cópias Snapshot, replicações e backups

Você pode usar as políticas padrão fornecidas pelo NetApp para criar seus backups ou criar políticas personalizadas. Ao usar o assistente de ativação para habilitar o serviço de backup e recuperação para seus volumes, você pode selecionar entre as políticas padrão e quaisquer outras políticas que já existam no ambiente de trabalho (Cloud Volumes ONTAP ou sistema ONTAP no local). Se você quiser usar uma política diferente das políticas existentes, você pode criar a política antes de iniciar ou durante o uso do assistente de ativação.

- A política padrão do Snapshot cria cópias Snapshot por hora, diárias e semanais, retendo 6 cópias por hora, 2 cópias por dia e 2 cópias por semana.
- A política de replicação padrão replica cópias Snapshot diárias e semanais, retendo 7 cópias Snapshot diárias e 52 cópias Snapshot semanais.
- A política de backup padrão replica cópias Snapshot diárias e semanais, retendo 7 cópias snapshot diárias e 52 cópias Snapshot semanais.

Se você criar políticas personalizadas para replicação ou backup, os rótulos de política (por exemplo, "diário" ou "semanal") devem corresponder aos rótulos que existem em suas políticas Snapshot ou volumes replicados e arquivos de backup não serão criados.

Você pode criar políticas de Snapshot, replicação e backup para storage de objetos na IU de backup e recuperação do BlueXP . Consulte a secção para "adicionando uma nova política de backup"obter detalhes.

Além de usar a recuperação de backup do BlueXP para criar políticas personalizadas, você pode usar o Gerenciador do sistema ou a interface de linha de comando (CLI) do ONTAP.

"Crie uma política Snapshot usando o System Manager" "Crie uma política de snapshot usando a CLI do ONTAP" "Crie uma política de replicação usando o System Manager" "Crie uma política de replicação usando a CLI do ONTAP" "Crie uma política de backup usando o System Manager" "Crie uma política de backup usando a CLI do ONTAP"

Observação: ao usar o System Manager, selecione **assíncrono** como o tipo de política para políticas de replicação e selecione **assíncrono** e **Backup na nuvem** para fazer backup em políticas de objetos.

Aqui estão alguns exemplos de comandos CLI do ONTAP que podem ser úteis se você estiver criando políticas personalizadas. Observe que você deve usar o *admin* vserver (VM de armazenamento) como o `<vserver_name>` nestes comandos.

Descrição da política	Comando
Política do Snapshot simples	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
Backup simples na nuvem	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Descrição da política	Comando
Backup na nuvem com proteção DataLock e ransomware	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
Backup na nuvem com classe de storage de arquivamento	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Replicação simples para outro sistema de storage	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Somente políticas de Vault podem ser usadas para fazer backup em relacionamentos de nuvem.

Onde residem minhas políticas?

As políticas de backup residem em locais diferentes, dependendo da arquitetura de backup que você planeja usar: Fan-out ou Cascading. As políticas de replicação e de backup não são projetadas da mesma maneira porque as replicações emparelham dois sistemas de storage ONTAP e o backup para objeto usam um fornecedor de storage como destino.

- As políticas do Snapshot sempre residem no sistema de storage primário.
- As políticas de replicação sempre residem no sistema de storage secundário.
- As políticas de backup para objeto são criadas no sistema em que o volume de origem reside - este é o cluster principal para configurações de fan-out e o cluster secundário para configurações em cascata.

Essas diferenças são mostradas na tabela.

Arquitetura	Política do Snapshot	Política de replicação	Política de backup
Saída de ventilador	Primário	Secundário	Primário
Cascata	Primário	Secundário	Secundário

Portanto, se você estiver planejando criar políticas personalizadas ao usar a arquitetura em cascata, será necessário criar a replicação e o backup para políticas de objetos no sistema secundário onde os volumes replicados serão criados. Se você estiver planejando criar políticas personalizadas ao usar a arquitetura de fan-out, será necessário criar as políticas de replicação no sistema secundário onde os volumes replicados serão criados e fazer backup para políticas de objeto no sistema primário.

Se você estiver usando as políticas padrão que existem em todos os sistemas ONTAP, então você está tudo definido.

Você deseja criar seu próprio contêiner de storage de objetos

Quando você cria arquivos de backup no storage de objetos para um ambiente de trabalho, por padrão, o serviço de backup e recuperação cria o contentor (bucket ou conta de armazenamento) para os arquivos de backup na conta de armazenamento de objetos que você configurou. O bucket da AWS ou do GCP é chamado de "NetApp-backup-<uuid>" por padrão. A conta de armazenamento Blob do Azure é chamada "netappbackup<uuid>".

Você pode criar o contentor sozinho na conta do provedor de objetos se quiser usar um determinado prefixo ou atribuir propriedades especiais. Se você quiser criar seu próprio contentor, você deve criá-lo antes de iniciar o assistente de ativação. O backup e a recuperação do BlueXP podem usar qualquer bucket e compartilhar buckets. O assistente de ativação de backup detetará automaticamente os contentores provisionados para a conta e as credenciais selecionadas para que você possa selecionar o que deseja usar.

Você pode criar o bucket do BlueXP ou do seu fornecedor de nuvem.

- "Crie buckets do Amazon S3 no BlueXP "
- "Crie contas de storage do Azure Blob no BlueXP "
- "Crie buckets do Google Cloud Storage no BlueXP "

Observação: neste momento, você não pode usar seus próprios buckets do S3 ao criar backups em sistemas StorageGRID ou para o ONTAP S3.

Se você planeja usar um prefixo de bucket diferente do "NetApp-backup-xxxxxx", será necessário modificar as permissões S3 para a função do IAM do conetor. Para obter detalhes, consulte como criar backups no AWS S3.

- Configurações avançadas do balde*

Se você planeja mover arquivos de backup mais antigos para armazenamento de arquivamento, ou se planeja habilitar a proteção DataLock e ransomware para bloquear seus arquivos de backup e digitalizá-los para possíveis ransomware, você precisará criar o contentor com certas configurações:

- O storage de arquivamento em seus próprios buckets é compatível com o storage AWS S3 no momento em que você usa o software ONTAP 9.10,1 ou superior nos clusters. Por padrão, os backups começam na classe de armazenamento S3 *Standard*. Certifique-se de criar o bucket com as regras de ciclo de vida apropriadas:
  - Mova os objetos em todo o escopo do bucket para S3 *Standard-IA* após 30 dias.
  - Mova os objetos com a tag "smc_push_to_archive: True" para *Glacier Flexible Retrieval* (anteriormente S3 Glacier)
- A proteção DataLock e ransomware é suportada no armazenamento da AWS ao usar o software ONTAP 9.11,1 ou superior nos clusters e o armazenamento do Azure ao usar o software ONTAP 9.12,1 ou superior.
  - Para a AWS, você deve habilitar o bloqueio de objetos no bucket usando um período de retenção de 30 dias.
  - Para o Azure, você precisa criar a Classe de armazenamento com suporte à imutabilidade no nível da versão.

Que modo de implantação do BlueXP Connector você está usando

Se você já estiver usando o BlueXP para gerenciar seu storage, um BlueXP Connector já foi instalado. Se você pretende usar o mesmo conetor com backup e recuperação do BlueXP , então você está tudo pronto. Se

você precisar usar um conetor diferente, precisará instalá-lo antes de iniciar sua implementação de backup e recuperação.

O BlueXP oferece vários modos de implantação que permitem que você use o BlueXP de uma forma que atenda aos requisitos de negócios e segurança. O *modo padrão* aproveita a camada SaaS do BlueXP para fornecer funcionalidade completa, enquanto o *modo restrito* e o *modo privado* estão disponíveis para organizações que têm restrições de conetividade.

"Saiba mais sobre os modos de implantação do BlueXP ".

Suporte para sites com conetividade total à Internet

Quando o backup e a recuperação do BlueXP são usados em um site com conetividade total à Internet (também conhecido como *modo padrão* ou *modo SaaS*), você pode criar volumes replicados em qualquer sistema ONTAP ou Cloud Volumes ONTAP no local gerenciado pelo BlueXP e criar arquivos de backup no storage de objetos em qualquer um dos provedores de nuvem compatíveis. "Consulte a lista completa dos destinos de backup suportados".

Para obter uma lista de locais de conetores válidos, consulte um dos procedimentos de backup a seguir para o provedor de nuvem onde você planeja criar arquivos de backup. Existem algumas restrições em que o conetor deve ser instalado manualmente em uma máquina Linux ou implantado em um provedor de nuvem específico.

- "Faça backup dos dados do Cloud Volumes ONTAP para o Amazon S3"
- "Fazer backup de dados ONTAP on-premises para o Amazon S3"
- "Fazer backup de dados do Cloud Volumes ONTAP para o Azure Blob"
- "Fazer backup de dados do ONTAP no local para o Azure Blob"
- "Faça backup dos dados do Cloud Volumes ONTAP para o Google Cloud"
- "Fazer backup dos dados do ONTAP no local para o Google Cloud"
- "Fazer backup de dados ONTAP on-premises para o StorageGRID"
- "Fazer backup do ONTAP no local para o ONTAP S3"

Suporte para sites com conetividade limitada à Internet

O backup e a recuperação do BlueXP podem ser usados em um site com conetividade limitada à Internet (também conhecido como *modo restrito*) para fazer backup dos dados de volume. Nesse caso, você precisará implantar o BlueXP Connector na região da nuvem de destino.

- É possível fazer backup dos dados de sistemas ONTAP locais ou de sistemas Cloud Volumes ONTAP instalados em regiões comerciais da AWS para o Amazon S3. "Faça backup dos dados do Cloud Volumes ONTAP para o Amazon S3".
- É possível fazer backup de dados de sistemas ONTAP locais ou sistemas Cloud Volumes ONTAP instalados em regiões comerciais do Azure para o Azure Blob. "Fazer backup de dados do Cloud Volumes ONTAP para o Azure Blob".

Suporte para sites sem conetividade com a Internet

Backup e recuperação do BlueXP podem ser usados em um site sem conetividade à Internet (também conhecido como sites *private mode* ou *dark*) para fazer backup de dados de volume. Nesse caso, você precisará implantar o BlueXP Connector em um host Linux no mesmo site.

- É possível fazer backup dos dados de sistemas ONTAP locais no local para sistemas NetApp StorageGRID locais. "Fazer backup de dados ONTAP on-premises para o StorageGRID".
- É possível fazer backup dos dados de sistemas ONTAP locais no local para sistemas ONTAP locais ou sistemas Cloud Volumes ONTAP configurados para storage de objetos S3. "Fazer backup de dados ONTAP on-premises para o ONTAP S3". ifdef::aws[]

Gerenciar políticas de backup para ONTAP volumes

Você pode usar as políticas de backup padrão fornecidas pelo NetApp para criar seus backups ou criar políticas personalizadas. As políticas governam a frequência de backup, o tempo em que o backup é feito e o número de arquivos de backup que são retidos.

Ao usar o assistente de ativação para habilitar o serviço de backup e recuperação para seus volumes, você pode selecionar entre as políticas padrão e quaisquer outras políticas que já existam no ambiente de trabalho (Cloud Volumes ONTAP ou sistema ONTAP no local). Se você quiser usar uma política diferente das políticas existentes, você pode criar a política antes ou durante o uso do assistente de ativação.

Para saber mais sobre as políticas de backup padrão fornecidas, "Planeje sua jornada de proteção"consulte .

O backup e a recuperação do BlueXP oferecem três tipos de backups de dados ONTAP: Snapshots, replicações e backups no storage de objetos. Suas políticas residem em locais diferentes com base na arquitetura que você usa e no tipo de backup:

Arquitetura	Local de armazenamento da política do Snapshot	Local de armazenamento da política de replicação	Local de armazenamento da política de backup para objeto
Saída de ventilador	Primário	Secundário	Primário
Cascata	Primário	Secundário	Secundário

Crie políticas de backup usando as seguintes ferramentas, dependendo do ambiente, das preferências e do tipo de proteção:

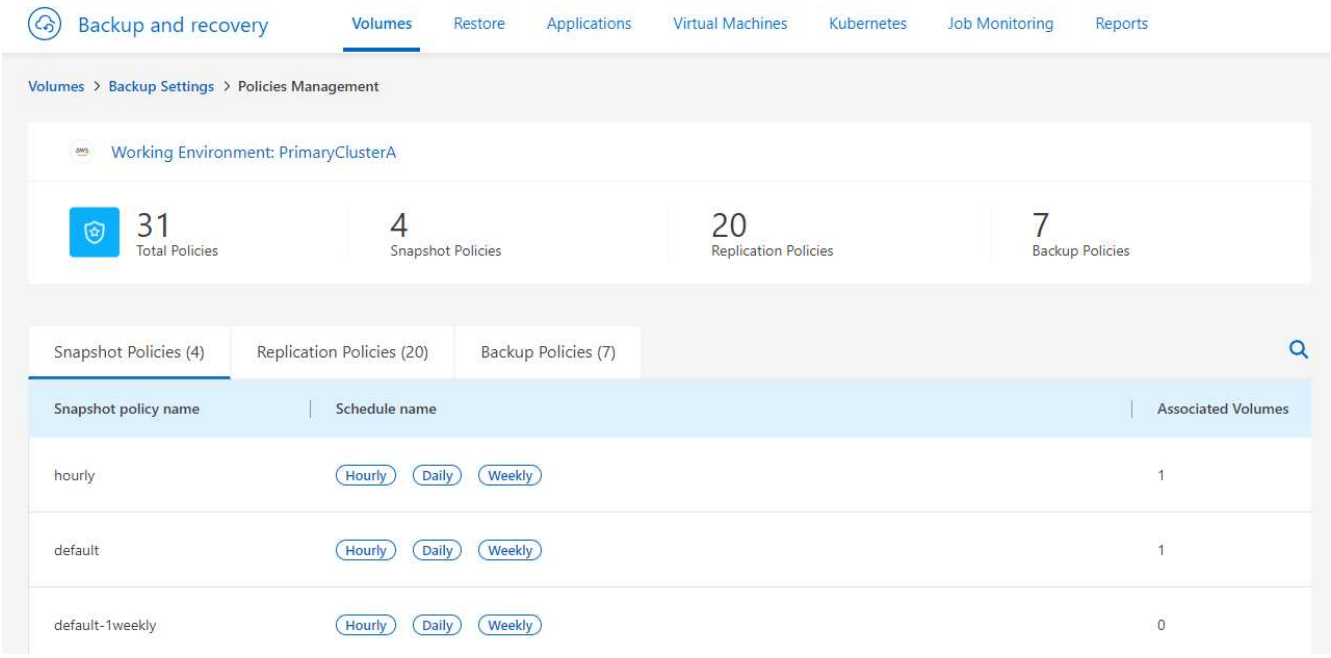
- UI BlueXP
- IU do System Manager
- CLI do ONTAP

Ao usar o System Manager, selecione **assíncrono** como o tipo de política para políticas de replicação e selecione **assíncrono** e **fazer backup na nuvem** para fazer backup em políticas de objetos.

Ver políticas para um ambiente de trabalho

1. Na IU do BlueXP , selecione **volumes** > **Configurações de backup**.
2. Na página Configurações de backup, selecione o ambiente de trabalho, selecione o ícone **ações** ••• e selecione **Gerenciamento de políticas**.

   A página de gerenciamento de políticas é exibida.



As políticas de instantâneos são apresentadas por predefinição.

3. Para exibir outras políticas que existem no ambiente de trabalho, selecione **políticas de replicação** ou **políticas de backup**. Se as políticas existentes puderem ser usadas para seus planos de backup, você estará pronto. Se você precisa ter uma política com caraterísticas diferentes, você pode criar novas políticas a partir desta página.

Criar políticas

Você pode criar políticas que governam cópias Snapshot, replicações e backups para o storage de objetos:

- Crie uma política de instantâneo antes de iniciar o instantâneo
- Crie uma política de replicação antes de iniciar a replicação
- Crie uma política de backup para armazenamento de objetos antes de iniciar o backup

Crie uma política de instantâneo antes de iniciar o instantâneo

Parte da sua estratégia 3-2-1 envolve a criação de uma cópia Snapshot do volume no sistema de armazenamento **Primary**.

Parte do processo de criação de políticas envolve a identificação de rótulos Snapshot e SnapMirror que denotam o agendamento e a retenção. Você pode usar rótulos predefinidos ou criar seus próprios.

Passos

1. Na IU do BlueXP , selecione **volumes** > **Configurações de backup**.
2. Na página Configurações de backup, selecione o ambiente de trabalho, selecione o ícone **ações** ••• e selecione **Gerenciamento de políticas**.

   A página de gerenciamento de políticas é exibida.

3. Na página políticas, selecione **criar política** > **criar política de instantâneo**.
4. Especifique o nome da política.

5. Selecione a agenda ou as programações do instantâneo. Pode ter um máximo de 5 etiquetas. Ou crie uma agenda.
6. Se você optar por criar uma agenda:
    a. Selecione a frequência de hora em hora, dia, semanal, mensal ou anual.
    b. Especifique as etiquetas Snapshot que denotam o agendamento e a retenção.
    c. Introduza quando e com que frequência o instantâneo será tirado.
    d. Retenção: Insira o número de instantâneos a serem mantidos.
7. Selecione **criar**.

Exemplo de política de instantâneo usando arquitetura em cascata

Este exemplo cria uma política de Snapshot com dois clusters:

1. Cluster 1:
    a. Selecione Cluster 1 na página de política.
    b. Ignore as seções de política replicação e backup para objeto.
    c. Crie a política Snapshot.
2. Cluster 2:
    a. Selecione Cluster 2 na página Política.
    b. Ignore a seção de política Snapshot.
    c. Configure as políticas de replicação e backup para objeto.

Crie uma política de replicação antes de iniciar a replicação

Sua estratégia 3-2-1 pode incluir a replicação de um volume em um sistema de storage diferente. A política de replicação reside no sistema de armazenamento **secundário**.

Passos

1. Na página políticas, selecione **criar política** > **criar política de replicação**.
2. Na seção Detalhes da política, especifique o nome da política.
3. Especifique as etiquetas SnapMirror (máximo de 5) indicando a retenção para cada etiqueta.
4. Especifique o agendamento de transferência.
5. Selecione **criar**.

Crie uma política de backup para armazenamento de objetos antes de iniciar o backup

Sua estratégia 3-2-1 pode incluir o backup de um volume para o armazenamento de objetos.

Essa política de storage reside em diferentes locais do sistema de storage, dependendo da arquitetura de backup:

- Fan-out: Sistema de storage primário
- Em cascata: Sistema de storage secundário

Passos

1. Na página Gerenciamento de políticas, selecione **criar política** > **criar política de backup**.

2. Na seção Detalhes da política, especifique o nome da política.
3. Especifique as etiquetas SnapMirror (máximo de 5) indicando a retenção para cada etiqueta.
4. Especifique as configurações, incluindo o agendamento de transferência e quando arquivar backups.
5. (Opcional) para mover arquivos de backup mais antigos para uma classe de armazenamento ou nível de acesso mais barato após um determinado número de dias, selecione a opção **Archive** e indique o número de dias que devem decorrer antes que os dados sejam arquivados. Digite **0** como "Arquivo após dias" para enviar seu arquivo de backup diretamente para o armazenamento de arquivos.

   "Saiba mais sobre as configurações de armazenamento de arquivos".

6. (Opcional) para proteger seus backups de serem modificados ou excluídos, selecione a opção **proteção DataLock & ransomware**.

   Se o cluster estiver usando o ONTAP 9.11,1 ou superior, você pode optar por proteger seus backups contra exclusão configurando *DataLock* e *ransomware Protection*.

   "Saiba mais sobre as configurações do DataLock disponíveis".

7. Selecione **criar**.

Editar uma política

Você pode editar uma política de Snapshot, replicação ou backup personalizada.

A alteração da política de backup afeta todos os volumes que estão usando essa política.

Passos

1. Na página de gerenciamento de políticas, selecione a política, selecione o ícone **ações** ••• e selecione **Editar política**.

   O processo é o mesmo para políticas de replicação e backup.

2. Na página Editar política, faça as alterações.
3. Selecione **Guardar**.

Eliminar uma política

Você pode excluir políticas que não estão associadas a nenhum volume.

Se uma política estiver associada a um volume e pretender eliminar a política, tem de remover a política do volume primeiro.

Passos

1. Na página de gerenciamento de políticas, selecione a política, selecione o ícone **ações** ••• e selecione **Excluir política de instantâneos**.
2. Selecione **Eliminar**.

Encontre mais informações

Para obter instruções sobre como criar políticas usando o Gerenciador do sistema ou a CLI do ONTAP, consulte o seguinte:

"Crie uma política Snapshot usando o System Manager" "Crie uma política de snapshot usando a CLI do ONTAP" "Crie uma política de replicação usando o System Manager" "Crie uma política de replicação usando a CLI do ONTAP" "Crie uma política de backup para armazenamento de objetos usando o System Manager" "Crie uma política de backup para storage de objetos usando a CLI do ONTAP"

Opções de política de backup para objeto

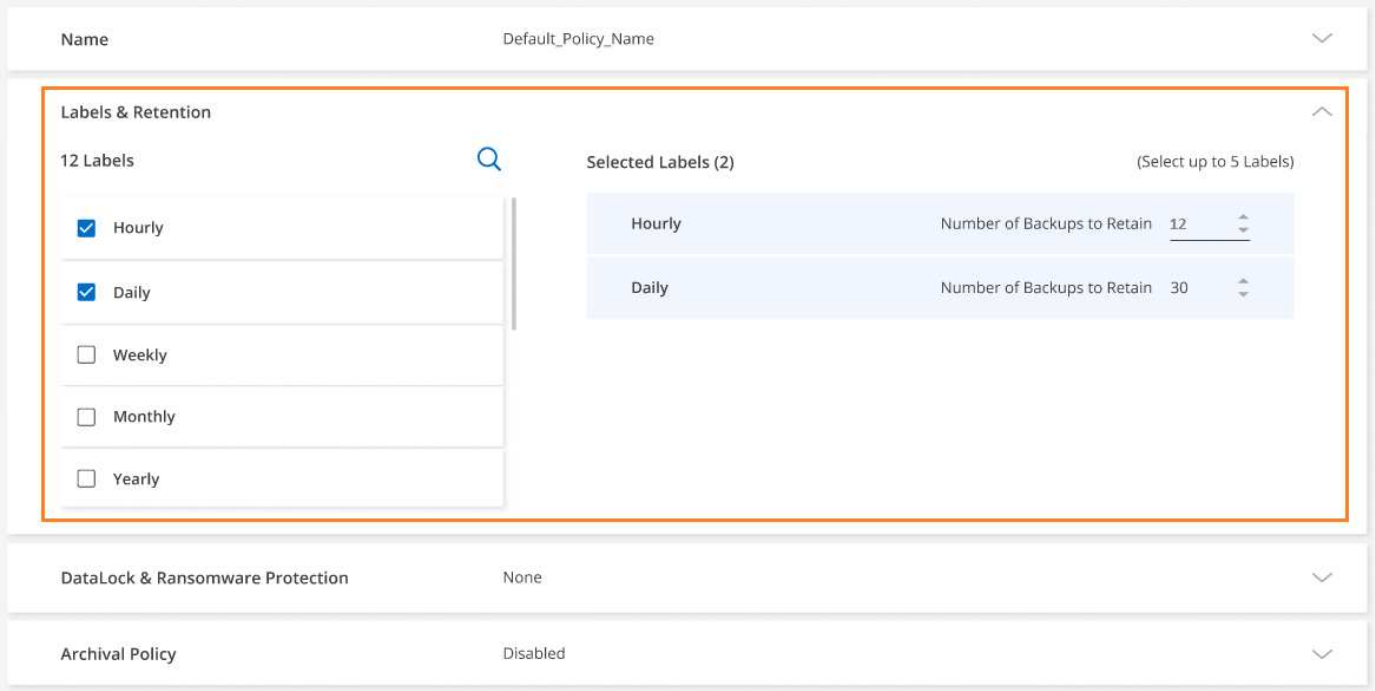
O backup e a recuperação do BlueXP permitem que você crie políticas de backup com várias configurações para seus sistemas ONTAP e Cloud Volumes ONTAP locais.

Essas configurações de política são relevantes somente para o armazenamento de backup para objeto. Nenhuma dessas configurações afeta suas políticas de Snapshot ou replicação. Configurações de política semelhantes para snapshots e replicações serão adicionadas no futuro.

Opções de agendamento de backup

O backup e a recuperação do BlueXP permitem que você crie várias políticas de backup com programações exclusivas para cada ambiente de trabalho (cluster). É possível atribuir diferentes políticas de backup a volumes com objetivos de ponto de restauração (RPO) diferentes.

Cada política de backup fornece uma seção para *rótulos e retenção* que você pode aplicar aos arquivos de backup. Observe que a política Snapshot aplicada ao volume deve ser uma das políticas reconhecidas pelo backup do BlueXP e os arquivos de backup ou recuperação não serão criados.



Existem duas partes do programa: O rótulo e o valor de retenção:

- O **label** define com que frequência um arquivo de backup é criado (ou atualizado) a partir do volume. Você pode selecionar entre os seguintes tipos de rótulos:
  - Você pode escolher um, ou uma combinação de prazos **hora**, **diária**, **semanal**, **mensal** e **anual**.

    - Você pode selecionar uma das políticas definidas pelo sistema que forneça backup e retenção por 3 meses, 1 ano ou 7 anos.
    - Se você criou políticas de proteção de backup personalizadas no cluster usando o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP, selecione uma dessas políticas.
- O valor **retension** define quantos arquivos de backup para cada rótulo (período de tempo) são retidos. Uma vez atingido o número máximo de backups em uma categoria ou intervalo, os backups mais antigos são removidos para que você tenha sempre os backups mais atuais. Isso também economiza custos de armazenamento porque backups obsoletos não continuam ocupando espaço na nuvem.

Por exemplo, digamos que você crie uma política de backup que crie backups 7 * semanais* e 12 **mensais**:

- cada semana e cada mês, um arquivo de backup é criado para o volume
- na semana 8th, o primeiro backup semanal é removido e o novo backup semanal para a semana 8th é adicionado (mantendo um máximo de 7 backups semanais)
- no 13th mês, o primeiro backup mensal é removido e o novo backup mensal para o 13th mês é adicionado (mantendo um máximo de 12 backups mensais)

Observe que backups anuais serão excluídos automaticamente do sistema de origem após serem transferidos para o armazenamento de objetos. Este comportamento predefinido pode ser alterado "Na página Configurações avançadas" para o ambiente de trabalho.

Opções de proteção DataLock e ransomware

O backup e a recuperação do BlueXP oferecem suporte à proteção DataLock e ransomware para seus backups de volume. Esses recursos permitem que você bloqueie seus arquivos de backup e digitalize-os para detetar possíveis ransomware nos arquivos de backup. Esta é uma configuração opcional que você pode definir em suas políticas de backup quando quiser proteção extra para seus backups de volume de um cluster.

Ambos esses recursos protegem seus arquivos de backup para que você sempre tenha um arquivo de backup válido para recuperar dados em caso de uma tentativa de ataque de ransomware em seus backups. Também é útil atender a certos requisitos regulatórios em que os backups precisam ser bloqueados e retidos por um determinado período de tempo. Quando a opção proteção DataLock e ransomware estiver ativada, o bucket da nuvem que é provisionado como parte da ativação de backup e recuperação do BlueXP terá o bloqueio de objetos e o controle de versão de objetos ativados.

"Consulte o blog de proteção DataLock e ransomware para obter mais detalhes".

Esse recurso não fornece proteção para os volumes de origem, apenas para os backups desses volumes de origem. Use o NetApp "Insights da infraestrutura de dados e Cloud Secure" ou alguns dos "Proteções anti-ransomware fornecidas pela ONTAP" para proteger os volumes de origem.

- Se você planeja usar a proteção DataLock e ransomware, poderá habilitá-la ao criar sua primeira política de backup e ativar o backup e a recuperação do BlueXP para esse cluster. Mais tarde, você pode ativar ou desativar a verificação de ransomware usando o backup e recuperação do BlueXP Configurações avançadas.
- Quando o BlueXP verifica um arquivo de backup em busca de ransomware ao restaurar dados de volume, você incorrerá em custos extras de saída do seu provedor de nuvem para acessar o conteúdo do arquivo de backup.

O que é DataLock

O DataLock protege seus arquivos de backup de serem modificados ou excluídos por um determinado período de tempo - também chamado de *armazenamento imutável*. Esta funcionalidade utiliza a tecnologia do fornecedor de armazenamento de objetos para "bloqueio de objetos". O período de tempo em que o arquivo de backup é bloqueado (e retido) é chamado de período de retenção DataLock. Ele é baseado no agendamento e na configuração de retenção da política de backup que você definiu, além de um buffer máximo de 31 dias. Qualquer política de retenção do DataLock que seja inferior a 31 dias é arredondada para um mínimo de 31 dias.

Esteja ciente de que backups antigos são excluídos após o período de retenção do DataLock expirar, não depois que o período de retenção da política de backup expirar.

Vejamos alguns exemplos de como isso funciona:

- Se você criar uma agenda de backup mensal com 12 retenções, cada backup será bloqueado por 12 meses (mais um buffer máximo de 31 dias) antes de ser excluído.
- Se você criar uma política de backup que crie 30 backups diários, 7 semanais e 12 mensais, haverá três períodos de retenção bloqueados. Os backups "30 diários" seriam retidos por 44 dias (30 dias mais um buffer máximo de 31 dias), os backups "7 semanais" seriam mantidos por 9 semanas (7 semanas mais um buffer máximo de 31 dias) e os backups "12 mensais" seriam mantidos por 12 meses (mais um buffer máximo de 31 dias).
- Se você criar um agendamento de backup por hora com retenções 24, talvez pense que os backups estão bloqueados por 24 horas. No entanto, uma vez que isso é inferior ao mínimo de 30 dias, cada backup será bloqueado e retido por 44 dias (30 dias mais um buffer máximo de 31 dias).

  Neste último caso, você pode ver que, se cada arquivo de backup estiver bloqueado por 30 dias (mais um buffer máximo de 31 dias), você acabará com muitos mais arquivos de backup do que normalmente seriam retidos com uma política de retenções horárias/24. Normalmente, quando o backup e a recuperação do BlueXP criam o arquivo de backup 25th, ele excluiria o backup mais antigo para manter as retenções máximas em 24 (com base na política). A configuração retenção DataLock substitui a configuração de retenção de política da política de backup, neste caso. Isso pode afetar seus custos de armazenamento, pois seus arquivos de backup serão salvos no armazenamento de objetos por um período de tempo maior.

O que é proteção contra ransomware

A proteção contra ransomware verifica seus arquivos de backup para procurar evidências de um ataque de ransomware. A detecção de ataques de ransomware é realizada usando uma comparação de checksum. Se um possível ransomware for identificado em um novo arquivo de backup em comparação com o arquivo de backup anterior, esse arquivo de backup mais recente será substituído pelo arquivo de backup mais recente que não mostra sinais de um ataque de ransomware. (O arquivo identificado como tendo um ataque de ransomware é excluído 1 dia após ele ter sido substituído.)

As verificações de ransomware acontecem nos seguintes pontos do processo de backup e restauração:

- Quando um arquivo de backup é criado.

  Opcionalmente, você pode ativar ou desativar varreduras de ransomware.

  A verificação não é realizada no arquivo de backup quando é gravado pela primeira vez no armazenamento em nuvem, mas quando o arquivo de backup **Next** é gravado. Por exemplo, se você tiver um agendamento de backup semanal definido para terça-feira, na terça-feira, o 14th um backup é criado. Então, na terça-feira dia 21st outro backup é criado. A verificação de ransomware é executada no arquivo

de backup do 14th neste momento.

- Quando você tenta restaurar dados de um arquivo de backup

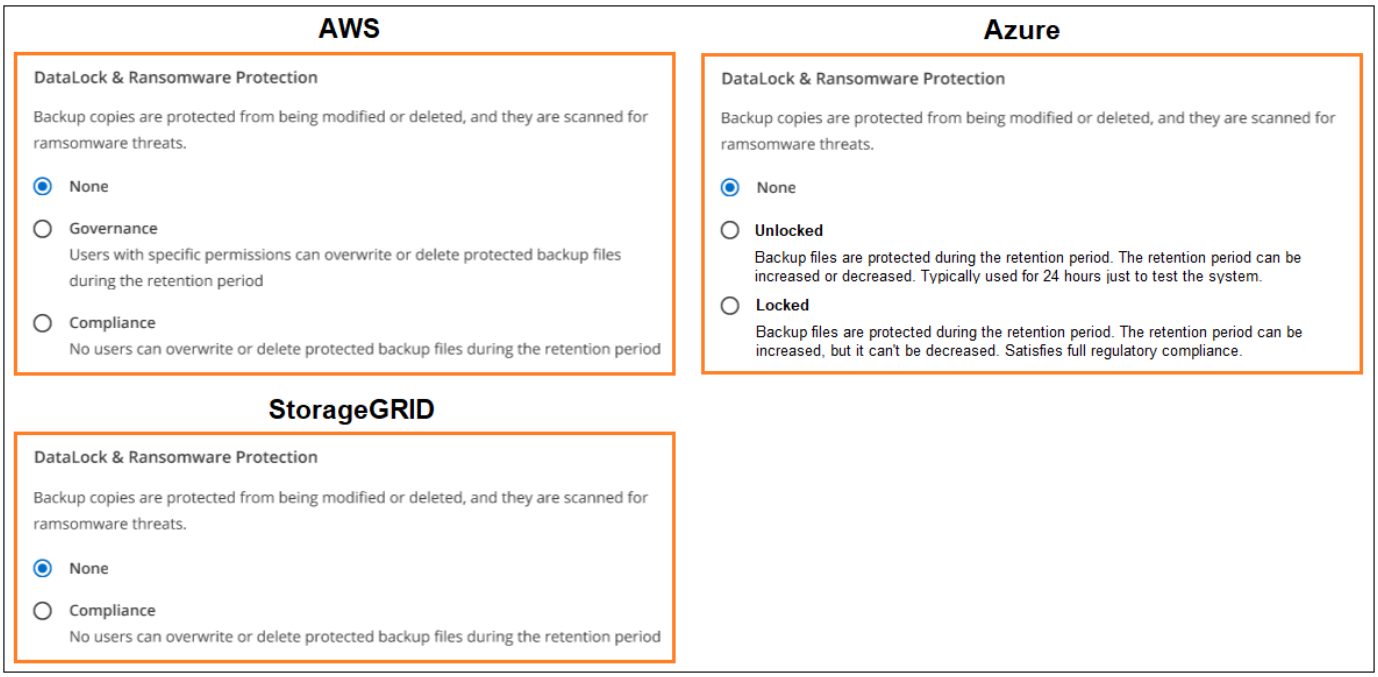
  Pode optar por executar uma verificação antes de restaurar dados de um ficheiro de cópia de segurança ou ignorar esta verificação.

- Manualmente

  Você pode executar uma verificação de proteção contra ransomware sob demanda a qualquer momento para verificar a integridade de um arquivo de backup específico. Isso pode ser útil se você tiver um problema de ransomware em um determinado volume e quiser verificar se os backups desse volume não são afetados.

Opções de proteção DataLock e ransomware

Cada política de backup fornece uma seção para *DataLock e ransomware Protection* que você pode aplicar aos seus arquivos de backup.



As verificações de proteção contra ransomware são ativadas por padrão. A predefinição para a frequência de digitalização é de 7 dias. A digitalização ocorre apenas na cópia Snapshot mais recente. Você pode ativar ou desativar varreduras de ransomware na cópia Snapshot mais recente usando a opção na página Configurações avançadas. Se você ativá-lo, as verificações são realizadas a cada 7 dias por padrão.

Você pode alterar esse horário para dias ou semanas ou desativá-lo, economizando custos.

"Como atualizar as opções de proteção contra ransomware na página Configurações avançadas"Consulte a .

Você pode escolher entre as seguintes configurações para cada política de backup:

AWS

- **Nenhum** (padrão)

  A proteção DataLock e a proteção contra ransomware estão desativadas.

- **Governança**

  O DataLock é definido para o modo *Governance*, onde os usuários com `s3:BypassGovernanceRetention` permissão ("veja abaixo") podem substituir ou excluir arquivos de backup durante o período de retenção. A proteção contra ransomware está ativada.

- **Conformidade**

  DataLock é definido para o modo *Compliance* onde nenhum usuário pode substituir ou excluir arquivos de backup durante o período de retenção. A proteção contra ransomware está ativada.

Azure

- **Nenhum** (padrão)

  A proteção DataLock e a proteção contra ransomware estão desativadas.

- **Desbloqueado**

  Os arquivos de backup são protegidos durante o período de retenção. O período de retenção pode ser aumentado ou diminuído. Normalmente utilizado durante 24 horas para testar o sistema. A proteção contra ransomware está ativada.

- **Bloqueado**

  Os arquivos de backup são protegidos durante o período de retenção. O período de retenção pode ser aumentado, mas não pode ser diminuído. Satisfaz a conformidade regulamentar total. A proteção contra ransomware está ativada.

StorageGRID

- **Nenhum** (padrão)

  A proteção DataLock e a proteção contra ransomware estão desativadas.

- **Conformidade**

  DataLock é definido para o modo *Compliance* onde nenhum usuário pode substituir ou excluir arquivos de backup durante o período de retenção. A proteção contra ransomware está ativada.

Ambientes de trabalho compatíveis e provedores de storage de objetos

Você pode habilitar a proteção DataLock e ransomware no ONTAP volumes dos seguintes ambientes de trabalho ao usar o storage de objetos nos seguintes provedores de nuvem pública e privada. Outros fornecedores de nuvem serão adicionados em versões futuras.

Fonte ambiente de trabalho	Destino do arquivo de backup ifdef::aws[]
Cloud Volumes ONTAP na AWS	Amazon S3 endif::aws[] ifdef::azul[]
Cloud Volumes ONTAP no Azure	Azure Blob endif::azure[] ifdef::gcp[] endif::gcp[]
Sistema ONTAP no local	Ifdef::aws[] Amazon S3 endif::aws[] ifdef::azure[] Azure Blob endif::azure[] ifdef::gcp[] endif::gcp[] NetApp StorageGRID

Requisitos

- Para AWS:
  - Os clusters precisam executar o ONTAP 9.11,1 ou superior
  - O conetor pode ser implantado na nuvem ou no local
  - As seguintes permissões do S3 devem fazer parte da função do IAM que fornece permissões ao conetor. Eles residem na seção "backupS3Policy" do recurso "ARN:aws:S3:::NetApp-backup-*":

Permissões do AWS S3

- S3:GetObjectVersionTagging
- S3:GetBucketObjectLockConfiguration
- S3:GetObjectVersionAcl
- S3:PutObjectTagging
- S3:DeleteObject
- S3:DeleteObjectTagging
- S3:GetObjectRetention
- S3:DeleteObjectVersionTagging
- S3:PutObject
- S3:GetObject
- S3:PutBucketObjectLockConfiguration
- S3:GetLifecycleConfiguration
- S3:GetBucketTagging
- S3:DeleteObjectVersion
- S3:ListBucketVersions
- S3: ListBucket
- S3:PutBucketTagging
- S3:GetObjectTagging
- S3:PutBucketControle de versão
- S3:PutObjectVersionTagging
- S3:GetBucketControle de versão
- S3:GetBucketAcl
- S3:BypassGovernanceretenção
- S3:retenção de objetos Put
- S3:GetBucketLocation
- S3:GetObjectVersion

"Veja o formato JSON completo da política onde você pode copiar e colar as permissões necessárias".

- Para o Azure:
  - Os clusters precisam executar o ONTAP 9.12,1 ou superior
  - O conetor pode ser implantado na nuvem ou no local
- Para o StorageGRID:
  - Os clusters precisam executar o ONTAP 9.11,1 ou superior
  - Seus sistemas StorageGRID devem estar executando 11.6.0.3 ou mais
  - O conetor deve ser implantado em suas instalações (ele pode ser instalado em um site com ou sem acesso à Internet)

◦ As seguintes permissões do S3 devem fazer parte da função do IAM que fornece permissões ao conetor:

Permissões do StorageGRID S3

- S3:GetObjectVersionTagging
- S3:GetBucketObjectLockConfiguration
- S3:GetObjectVersionAcl
- S3:PutObjectTagging
- S3:DeleteObject
- S3:DeleteObjectTagging
- S3:GetObjectRetention
- S3:DeleteObjectVersionTagging
- S3:PutObject
- S3:GetObject
- S3:PutBucketObjectLockConfiguration
- S3:GetLifecycleConfiguration
- S3:GetBucketTagging
- S3:DeleteObjectVersion
- S3:ListBucketVersions
- S3: ListBucket
- S3:PutBucketTagging
- S3:GetObjectTagging
- S3:PutBucketControle de versão
- S3:PutObjectVersionTagging
- S3:GetBucketControle de versão
- S3:GetBucketAcl
- S3:retenção de objetos Put
- S3:GetBucketLocation
- S3:GetObjectVersion

Restrições

- O recurso de proteção DataLock e ransomware não estará disponível se você tiver configurado o armazenamento de arquivamento na política de backup.
- A opção DataLock selecionada ao ativar o backup e a recuperação do BlueXP deve ser usada para todas as políticas de backup desse cluster.
- Não é possível usar vários modos DataLock em um único cluster.
- Se você ativar o DataLock, todos os backups de volume serão bloqueados. Não é possível misturar backups de volume bloqueados e não bloqueados para um único cluster.

- A proteção DataLock and ransomware é aplicável para novos backups de volume usando uma política de backup com a proteção DataLock e ransomware ativada. Mais tarde, você pode ativar ou desativar esses recursos usando a opção Configurações avançadas.
- Os volumes do FlexGroup podem usar a proteção DataLock e ransomware somente ao usar o ONTAP 9.13,1 ou superior.

Dicas sobre como mitigar os custos do DataLock

Você pode ativar ou desativar o recurso ransomware Scan enquanto mantém o recurso DataLock ativo. Para evitar cobranças extras, você pode desativar varreduras de ransomware agendadas. Isso permite que você personalize suas configurações de segurança e evite incorrer em custos do provedor de nuvem.

Mesmo que as varreduras programadas de ransomware estejam desativadas, você ainda pode executar varreduras sob demanda quando necessário.

Você pode escolher diferentes níveis de proteção:

- **DataLock *without* ransomware scans**: Fornece proteção para dados de backup no armazenamento de destino que podem estar no modo Governança ou conformidade.
  - **Modo de governança**: Oferece flexibilidade aos administradores para substituir ou excluir dados protegidos.
  - **Modo de conformidade**: Fornece total indelébilidade até o período de retenção expirar. Isso ajuda a atender aos requisitos mais rigorosos de segurança de dados de ambientes altamente regulamentados. Os dados não podem ser sobrescritos ou modificados durante seu ciclo de vida, fornecendo o nível mais forte de proteção para suas cópias de backup.

    Em vez disso, o Microsoft Azure usa um modo de bloqueio e desbloqueio.

- **DataLock *with* ransomware scans**: Fornece uma camada adicional de segurança para seus dados. Esse recurso ajuda a detetar qualquer tentativa de alterar cópias de backup. Se qualquer tentativa for feita, uma nova versão dos dados é criada discretamente. A frequência de digitalização pode ser alterada para 1, 2, 3, 4, 5, 6 ou 7 dias. Se as digitalizações forem definidas para cada 7 dias, os custos diminuem significativamente.

Para obter mais dicas para mitigar os custos do DataLock, consulte https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-BlueXP-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475

Além disso, você pode obter estimativas para o custo associado ao DataLock visitando o "Calculadora de custo total de propriedade (TCO) de recuperação e backup do BlueXP ".

Opções de armazenamento de arquivamento

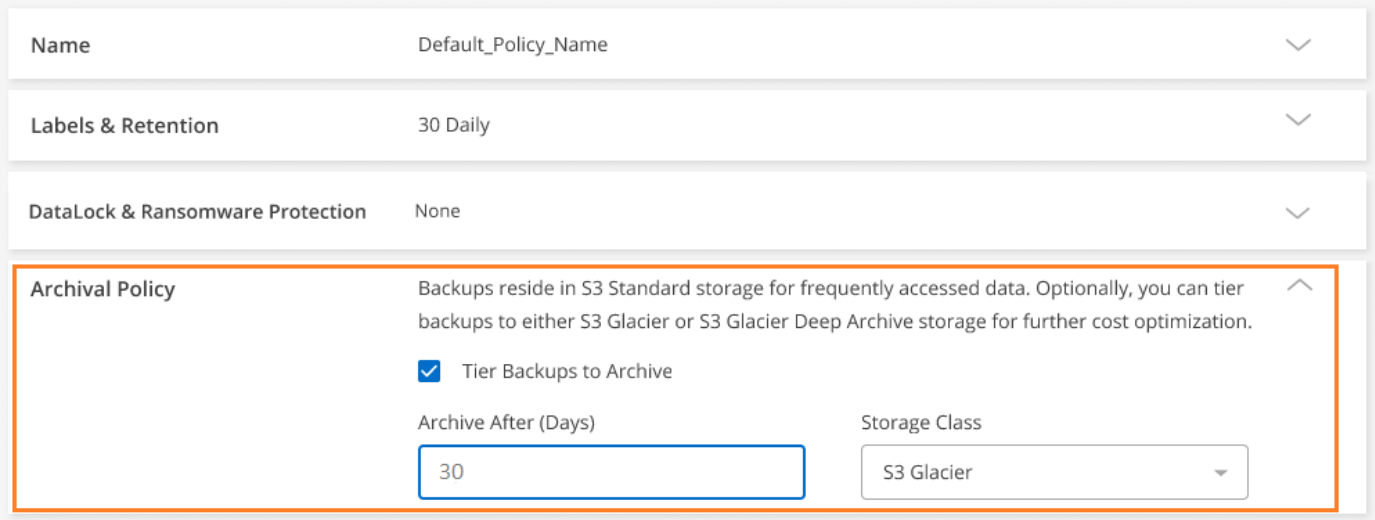
Ao usar o storage de nuvem AWS, Azure ou Google, você pode mover arquivos de backup mais antigos para uma classe de storage de arquivamento ou categoria de acesso mais barata após um determinado número de dias. Você também pode optar por enviar seus arquivos de backup para o armazenamento de arquivamento imediatamente sem ser gravado no armazenamento padrão na nuvem. Basta digitar **0** como "Arquivo depois de dias" para enviar seu arquivo de backup diretamente para o armazenamento de arquivamento. Isso pode ser especialmente útil para usuários que raramente precisam acessar dados de backups na nuvem ou usuários que estão substituindo uma solução de backup em fita.

Os dados em camadas de arquivamento não podem ser acessados imediatamente quando necessário e exigirão um custo de recuperação mais alto, portanto, você precisará considerar com que frequência você

pode precisar restaurar dados de arquivos de backup antes de decidir arquivar seus arquivos de backup.

- Mesmo que você selecione "0" para enviar todos os blocos de dados para o storage de nuvem de arquivamento, os blocos de metadados sempre são gravados no storage de nuvem padrão.
- O armazenamento de arquivamento não pode ser usado se você tiver ativado o DataLock.
- Não é possível alterar a política de arquivamento depois de selecionar **0** dias (arquivar imediatamente).

Cada política de backup fornece uma seção para *Política de arquivamento* que você pode aplicar aos arquivos de backup.



- Na AWS, os backups são iniciados na classe de armazenamento *Standard* e passam para a classe de armazenamento *Standard-unusual Access* após 30 dias.

  Se o cluster estiver usando o ONTAP 9.10,1 ou superior, você poderá categorizar backups mais antigos para o armazenamento *S3 Glacier* ou *S3 Glacier Deep Archive*. "Saiba mais sobre o armazenamento de arquivamento da AWS".

  - Se você selecionar nenhum nível de arquivamento na primeira política de backup ao ativar o backup e a recuperação do BlueXP , o *S3 Glacier* será a única opção de arquivamento para políticas futuras.
  - Se você selecionar *S3 Glacier* em sua primeira política de backup, poderá alterar para o nível *S3 Glacier Deep Archive* para futuras políticas de backup para esse cluster.
  - Se você selecionar *S3 Glacier Deep Archive* em sua primeira política de backup, esse nível será o único nível de arquivamento disponível para políticas futuras de backup para esse cluster.
- No Azure, os backups estão associados ao nível de acesso *Cool*.

  Se o cluster estiver usando o ONTAP 9.10,1 ou superior, você poderá categorizar backups mais antigos no storage *Azure Archive*. "Saiba mais sobre o armazenamento de arquivamento do Azure".
- No GCP, os backups estão associados à classe de armazenamento *Standard*.

  Se o cluster no local estiver usando o ONTAP 9.12,1 ou superior, você poderá optar por categorizar backups mais antigos para o storage *Archive* na IU de backup e recuperação do BlueXP após um determinado número de dias para otimização adicional de custos. "Saiba mais sobre o armazenamento de arquivos do Google".

- No StorageGRID, os backups estão associados à classe de armazenamento *Standard*.

  Se o cluster no local estiver usando o ONTAP 9.12,1 ou superior e o sistema StorageGRID estiver usando o 11,4 ou superior, você poderá arquivar arquivos de backup mais antigos para storage de arquivamento em nuvem pública.

  - Para a AWS, você pode categorizar backups no armazenamento AWS *S3 Glacier* ou *S3 Glacier Deep Archive*. "Saiba mais sobre o armazenamento de arquivamento da AWS".
  - Para o Azure, você pode categorizar backups mais antigos para o armazenamento *Azure Archive*. "Saiba mais sobre o armazenamento de arquivamento do Azure".

E "Saiba mais sobre o arquivamento de arquivos de backup do StorageGRID".

Gerencie as opções de armazenamento de backup para objeto na página Configurações avançadas

Você pode alterar as configurações de armazenamento de backup para objeto no nível do cluster que você definir ao ativar o backup e a recuperação do BlueXP para cada sistema ONTAP usando a página Configurações avançadas. Você também pode modificar algumas configurações que são aplicadas como configurações de backup "padrão". Isso inclui alterar a taxa de transferência de backups para o armazenamento de objetos, se as cópias Snapshot históricas são exportadas como arquivos de backup e ativar ou desativar verificações de ransomware para um ambiente de trabalho.

> Essas configurações estão disponíveis apenas para armazenamento de backup para objeto. Nenhuma dessas configurações afeta suas configurações de Snapshot ou replicação. Configurações semelhantes de replicações em nível de cluster para snapshots e replicações serão adicionadas no futuro.

Você pode alterar as seguintes opções na página Configurações avançadas:

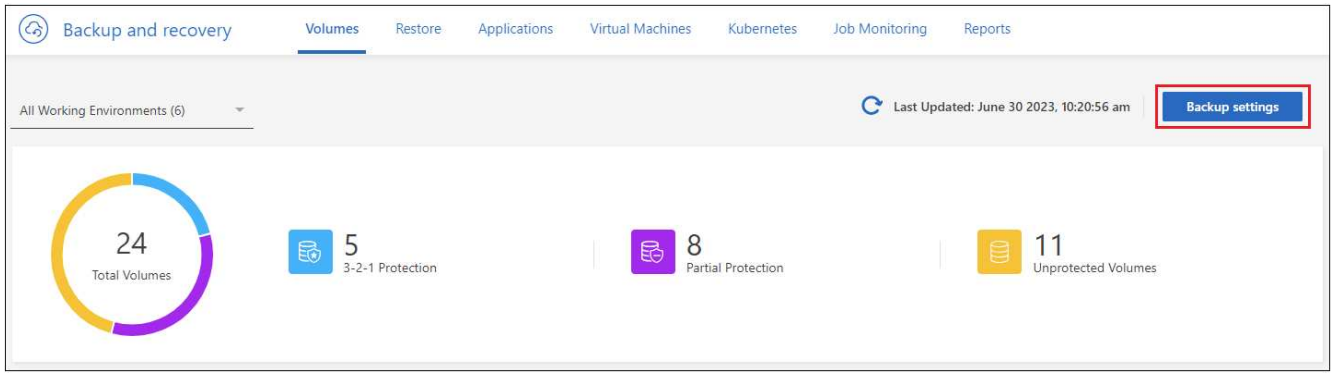
- Alterar a largura de banda da rede alocada para fazer upload de backups para armazenamento de objetos usando a opção taxa de transferência máxima ifdef::aws[]
- Alterar se as cópias Snapshot históricas são exportadas como arquivos de backup e incluídas nos arquivos de backup da linha de base inicial para volumes futuros
- Alterar se os instantâneos "anuais" são removidos do sistema de origem
- Ativar ou desativar varreduras de ransomware para um ambiente de trabalho, incluindo varreduras agendadas

Veja as configurações de backup no nível do cluster

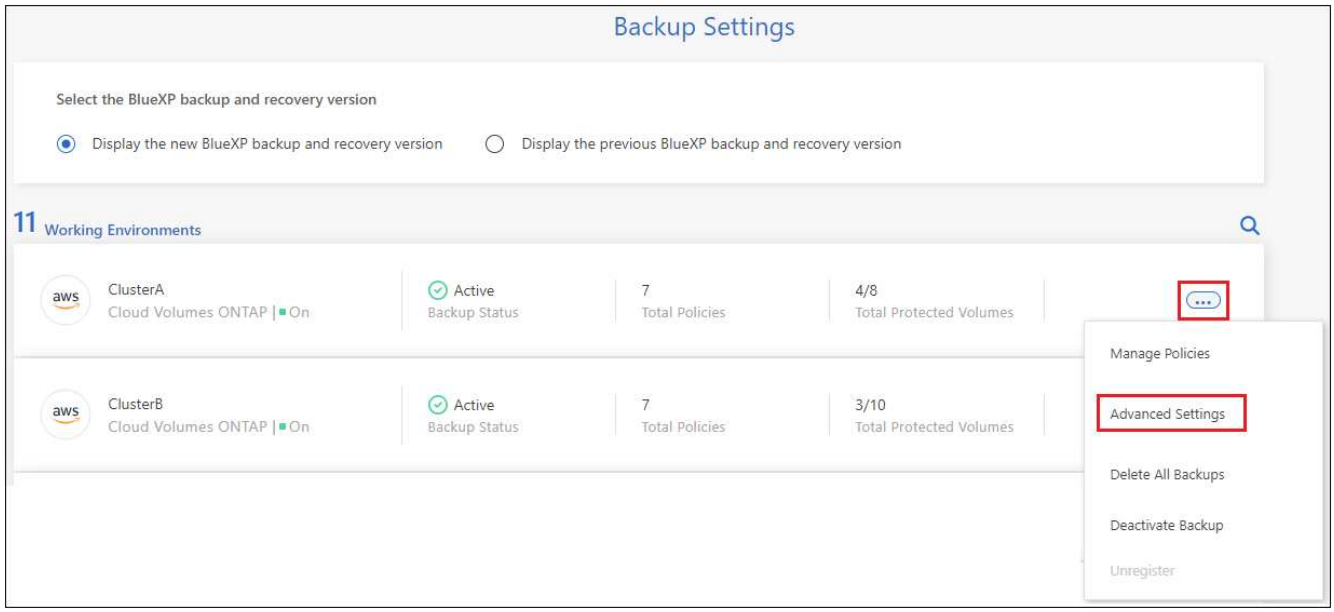
Pode visualizar as definições de cópia de segurança no nível do cluster para cada ambiente de trabalho.

Passos

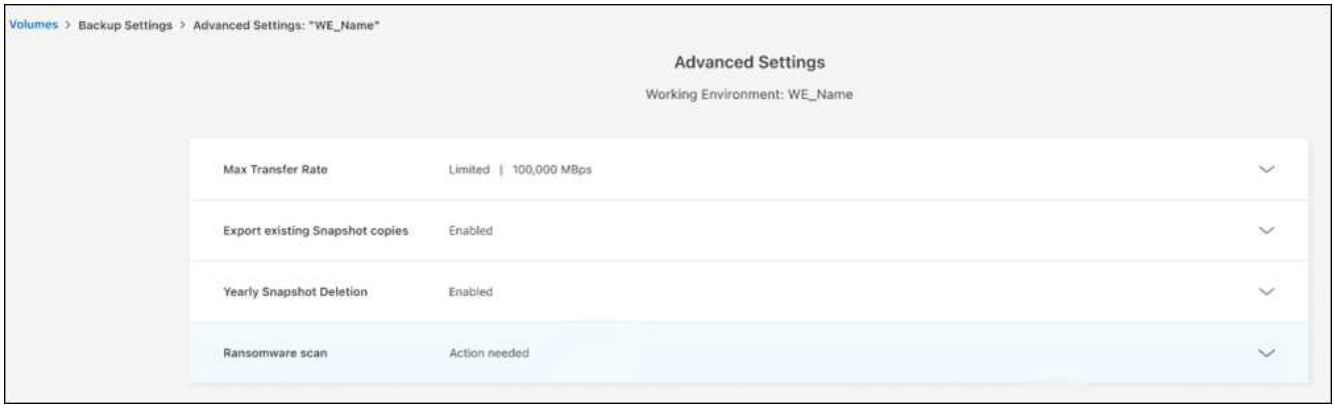
1. No menu BlueXP , selecione **proteção > Backup e recuperação**.
2. Na guia **volumes**, selecione **Configurações de backup**.



3. Na página *Backup Settings*, clique ••• em para o ambiente de trabalho e selecione **Advanced Settings**.



A página *Configurações avançadas* exibe as configurações atuais para esse ambiente de trabalho.



4. Expanda a opção e faça a alteração.

Todas as operações de backup após a alteração usarão os novos valores.

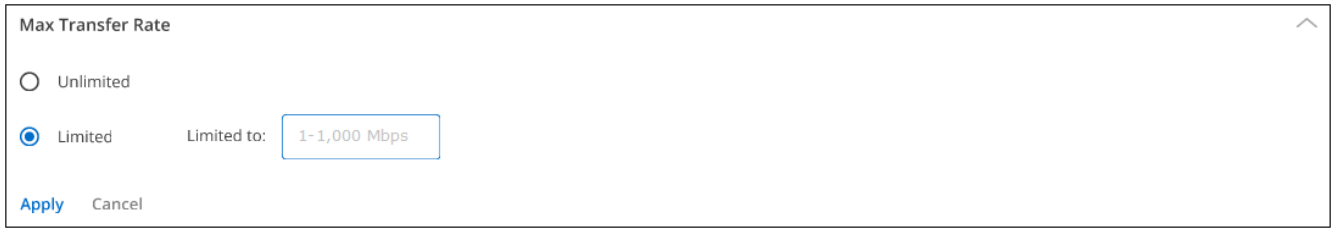
Observe que algumas opções não estão disponíveis com base na versão do ONTAP no cluster de origem e com base no destino do provedor de nuvem onde os backups residem.

Altere a largura de banda de rede disponível para carregar backups para o armazenamento de objetos

Quando você ativa o backup e a recuperação do BlueXP em um ambiente de trabalho, por padrão, o ONTAP pode usar uma quantidade ilimitada de largura de banda para transferir os dados de backup de volumes no ambiente de trabalho para o storage de objetos. Se você notar que o tráfego de backup está afetando as cargas de trabalho normais do usuário, você pode controlar a quantidade de largura de banda da rede usada durante a transferência usando a opção Max Transfer Rate (taxa de transferência máxima) na página Advanced Settings (Configurações avançadas).

Passos

1. Na guia **volumes**, selecione **Configurações de backup**.
2. Na página *Backup Settings*, clique ••• em para o ambiente de trabalho e selecione **Advanced Settings**.
3. Na página Configurações avançadas, expanda a seção **Max Transfer Rate**.



4. Escolha um valor entre 1 e 1.000 Mbps como a taxa de transferência máxima.
5. Selecione o botão de opção **Limited** e insira a largura de banda máxima que pode ser usada ou selecione **Unlimited** para indicar que não há limite.
6. Selecione **aplicar**.

Esta configuração não afeta a largura de banda alocada a quaisquer outras relações de replicação que possam ser configuradas para volumes no ambiente de trabalho.

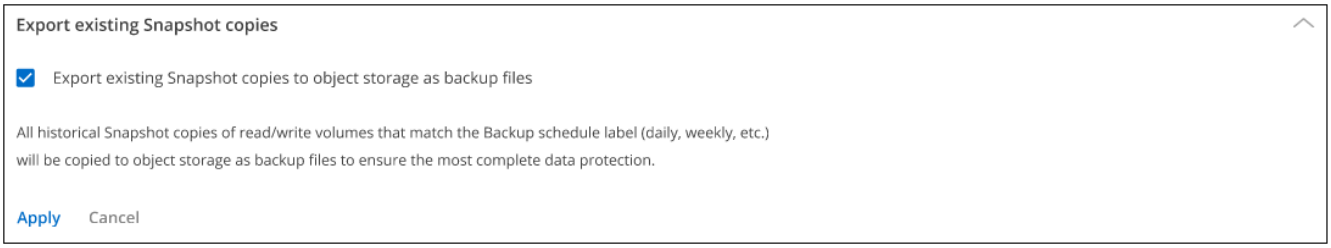
Alterar se as cópias Snapshot históricas são exportadas como arquivos de backup

Se houver cópias Snapshot locais para volumes que correspondam à etiqueta de agendamento de backup que você está usando nesse ambiente de trabalho (por exemplo, diário, semanal, etc.), você poderá exportar esses snapshots históricos para o armazenamento de objetos como arquivos de backup. Isso permite inicializar seus backups na nuvem movendo cópias snapshot mais antigas para a cópia de backup da linha de base.

Observe que essa opção se aplica somente a novos arquivos de backup para novos volumes de leitura/gravação e não é compatível com volumes de proteção de dados (DP).

Passos

1. Na guia **volumes**, selecione **Configurações de backup**.
2. Na página *Backup Settings*, clique ••• em para o ambiente de trabalho e selecione **Advanced Settings**.
3. Na página Configurações avançadas, expanda a seção **Exportar cópias Snapshot existentes**.



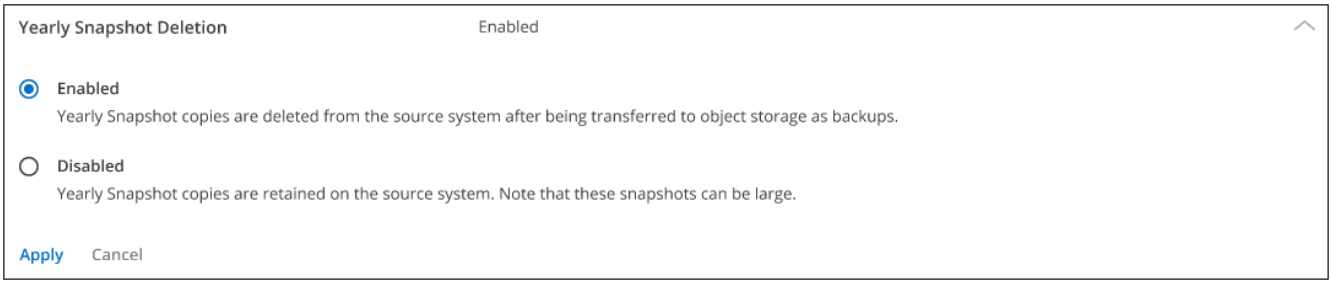
4. Selecione se deseja que as cópias Snapshot existentes sejam exportadas.
5. Selecione **aplicar**.

Altere se os instantâneos "anuais" são removidos do sistema de origem

Quando você seleciona o rótulo de backup "anual" para uma política de backup para qualquer um de seus volumes, a cópia Snapshot criada é muito grande. Por padrão, esses snapshots anuais são excluídos automaticamente do sistema de origem após serem transferidos para o armazenamento de objetos. Você pode alterar esse comportamento padrão na seção exclusão de instantâneo anual.

Passos

1. Na guia **volumes**, selecione **Configurações de backup**.
2. Na página *Backup Settings*, clique ••• em para o ambiente de trabalho e selecione **Advanced Settings**.
3. Na página Configurações avançadas, expanda a seção **eliminação anual de instantâneo**.



4. Selecione **Disabled** (Desativado) para reter os instantâneos anuais no sistema de origem.
5. Selecione **aplicar**.

Ative ou desative varreduras de ransomware

As verificações de proteção contra ransomware são ativadas por padrão. A predefinição para a frequência de digitalização é de 7 dias. A digitalização ocorre apenas na cópia Snapshot mais recente. Você pode ativar ou desativar varreduras de ransomware na cópia Snapshot mais recente usando a opção na página Configurações avançadas. Se você ativá-lo, as verificações são realizadas a cada 7 dias por padrão.

Você pode alterar esse horário para dias ou semanas ou desativá-lo, economizando custos.

A ativação das varreduras de ransomware incorrerá em cobranças extras, dependendo do provedor de nuvem.

As varreduras programadas de ransomware são executadas somente na cópia Snapshot mais recente.

Se as varreduras de ransomware agendadas estiverem desativadas, você ainda poderá executar varreduras sob demanda e a varredura durante uma operação de restauração ainda ocorrerá.

Consulte a "Gerenciar políticas" para obter detalhes sobre o gerenciamento de políticas que implementam a detecção de ransomware.

Passos

1. Na guia **volumes**, selecione **Configurações de backup**.
2. Na página *Backup Settings*, clique ••• em para o ambiente de trabalho e selecione **Advanced Settings**.
3. Na página Configurações avançadas, expanda a seção **ransomware scan**.
4. Ative ou desative o **ransomware Scan**.
5. Selecione **varredura programada de ransomware**.
6. Opcionalmente, altere a verificação padrão de cada semana para dias ou semanas.
7. Defina a frequência em dias ou semanas que a digitalização deve ser executada.
8. Selecione **aplicar**.

Faça backup dos dados do Cloud Volumes ONTAP para o Amazon S3

Execute algumas etapas para começar a fazer backup de dados de volume de seus sistemas 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.

1 Verifique o suporte para sua configuração

- Você está executando o Cloud Volumes ONTAP 9,8 ou posterior na AWS (recomenda-se o ONTAP 9.8P13 e posterior).
- 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 no mercado do BlueXP ", um "Contrato anual da AWS" ou adquiriu "e ativado" uma licença BYOL de backup e recuperação do BlueXP da NetApp.
- Você tem um conetor instalado na AWS:
  - O conetor pode ser instalado em um site com acesso total à Internet ("modo padrão") ou com conetividade limitada à Internet ("modo restrito").
  - A função do IAM que fornece permissões ao BlueXP Connector inclui permissões S3 do último "Política de BlueXP ".

2 Prepare o conetor BlueXP

Se você já tiver um conetor implantado em uma região da AWS, tudo estará definido. Caso contrário, você precisará instalar um BlueXP Connector na AWS para fazer backup dos dados do Cloud Volumes ONTAP na AWS. O conetor pode ser instalado em um site com acesso total à Internet ("modo padrão") ou com conetividade limitada à Internet ("modo restrito").

3 **Verifique os requisitos de licença**

Você precisará verificar os requisitos de licença para AWS e BlueXP .

4 **Verificar os requisitos de rede do ONTAP para replicação de volumes**

Garantir que os sistemas de storage primário e secundário atendam aos requisitos de rede e versão do ONTAP.

5 **Ative o backup e a recuperação do BlueXP**

Selecione o ambiente de trabalho e clique em **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.

6 **Ative backups no ONTAP volumes**

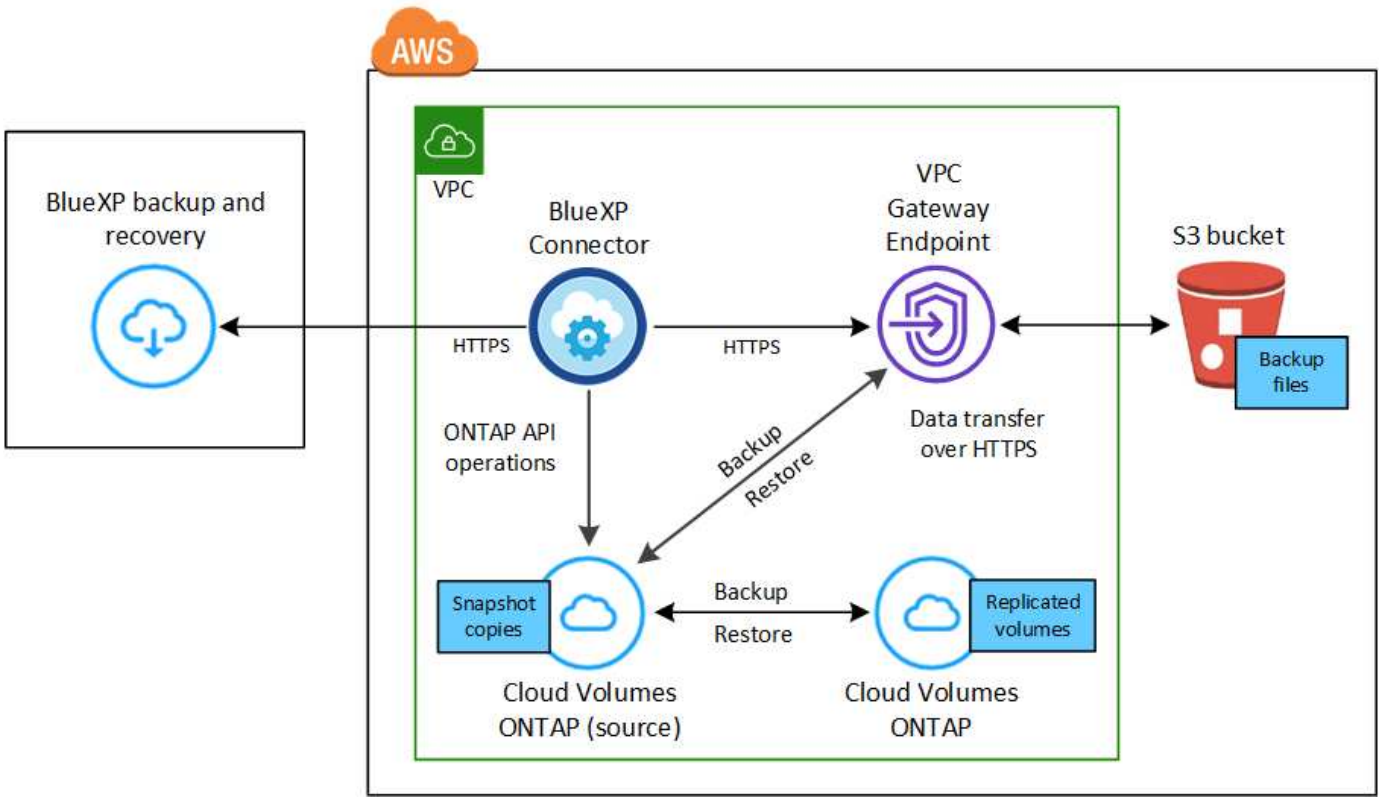
Siga o assistente de configuração para selecionar as políticas de replicação e backup que você usará e os volumes que deseja fazer backup.

Verifique o suporte para sua configuração

Leia os requisitos a seguir para garantir que você tenha uma configuração compatível antes de iniciar o backup de volumes para S3.

A imagem a seguir mostra cada componente e as conexões que você precisa preparar entre eles.

Opcionalmente, você pode se conectar a um sistema ONTAP secundário para volumes replicados usando a conexão pública ou privada.



O endpoint do gateway VPC já deve existir na VPC. "Saiba mais sobre endpoints de gateway".

Versões de ONTAP compatíveis

É recomendado um mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior.

Informações necessárias para usar chaves gerenciadas pelo cliente para criptografia de dados

Você pode escolher suas próprias chaves gerenciadas pelo cliente para criptografia de dados no assistente de ativação em vez de usar as chaves de criptografia padrão do Amazon S3. Nesse caso, você precisará ter as chaves gerenciadas de criptografia já configuradas. "Veja como usar suas próprias chaves".

Verifique os requisitos de licença

Para o licenciamento PAYGO de backup e recuperação do BlueXP , uma assinatura do BlueXP está disponível no AWS Marketplace que permite implantações de backup e recuperação do Cloud Volumes ONTAP e do BlueXP . Você precisa "Assine esta assinatura do BlueXP " antes de ativar o backup e a recuperação do BlueXP . A cobrança do backup e recuperação do BlueXP é feita por meio dessa assinatura.

Para um contrato anual que permita fazer backup dos dados do Cloud Volumes ONTAP e dos dados do ONTAP no local, é necessário fazer a assinatura do "Página do AWS Marketplace" e depois "Associe a assinatura às suas credenciais da AWS"do .

Para um contrato anual que permita agrupar o backup e a recuperação do Cloud Volumes ONTAP e do BlueXP , você precisa configurar o contrato anual ao criar um ambiente de trabalho do Cloud Volumes ONTAP. Essa opção não permite que você faça backup dos dados no local.

Para o licenciamento BYOL de backup e recuperação do BlueXP , você precisa do número de série do NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Saiba como gerenciar suas licenças BYOL". Você deve usar uma licença BYOL quando o conetor e o sistema Cloud Volumes ONTAP forem implantados em um local escuro.

E você precisa ter uma conta da AWS para o espaço de armazenamento onde seus backups estarão localizados.

Prepare o conetor BlueXP

O conetor deve ser instalado em uma região da AWS com acesso total ou limitado à Internet (modo "padrão" ou "restrito"). "Consulte modos de implantação do BlueXP para obter detalhes".

- "Saiba mais sobre conetores"
- "Implantar um conetor na AWS no modo padrão (acesso total à Internet)"
- "Instale o conetor no modo restrito (acesso de saída limitado)"

Verifique ou adicione permissões ao conetor

A função do IAM que fornece permissões ao BlueXP deve incluir permissões S3 do último "Política de BlueXP ". Se a política não contiver todas essas permissões, consulte "Documentação da AWS: Editando políticas do IAM" .

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:DeleteObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
                "s3:PutBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectVersionAcl",
                "s3:PutObjectTagging",
                "s3:DeleteObjectTagging",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersionTagging",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObjectVersion",
                "s3:GetObjectTagging",
                "s3:PutBucketVersioning",
                "s3:PutObjectVersionTagging",
                "s3:GetBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
```

```
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Ao criar backups nas regiões da AWS China, você precisa alterar o Nome de recurso da AWS "ARN" em todas as seções *Resource* nas políticas do IAM de "aws" para "aws-cn"; por exemplo `arn:aws-cn:s3:::netapp-backup-*`.

Permissões necessárias do AWS Cloud Volumes ONTAP

Quando o sistema Cloud Volumes ONTAP está executando o software ONTAP 9.12,1 ou superior, a função IAM que fornece permissões ao ambiente de trabalho deve incluir um novo conjunto de permissões S3 especificamente para backup e recuperação do BlueXP a partir do último "Política de Cloud Volumes ONTAP".

Se você criou o ambiente de trabalho do Cloud Volumes ONTAP usando o BlueXP versão 3.9.23 ou superior, essas permissões já devem fazer parte da função do IAM. Caso contrário, você precisará adicionar as permissões ausentes.

Regiões AWS compatíveis

O backup e a recuperação do BlueXP são compatíveis em todas as regiões da "Onde o Cloud Volumes ONTAP é suportado" AWS, incluindo regiões do AWS GovCloud.

Configuração necessária para criar backups em uma conta AWS diferente

Por padrão, os backups são criados usando a mesma conta usada para o sistema Cloud Volumes ONTAP. Se você quiser usar uma conta AWS diferente para seus backups, você deve:

- Verifique se as permissões "S3:PutBucketPolicy" e "S3:PutBucketOwnershipControls" fazem parte da função do IAM que fornece permissões ao BlueXP Connector.
- Adicione as credenciais da conta AWS de destino no BlueXP . "Veja como fazer isso".
- Adicione as seguintes permissões nas credenciais do usuário na segunda conta:

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

Crie seus próprios baldes

Por padrão, o serviço cria buckets para você. Se você quiser usar seus próprios buckets, você pode criá-los antes de iniciar o assistente de ativação de backup e, em seguida, selecionar esses buckets no assistente.

"Saiba mais sobre como criar seus próprios buckets".

Verificar os requisitos de rede do ONTAP para replicação de volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o backup e a recuperação do BlueXP , certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede da ONTAP no local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da rede corporativa à rede virtual no provedor de nuvem. Normalmente, esta é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou sistemas locais, revise os requisitos de peering para sistemas ONTAP locais. "Veja os pré-requisitos para peering de cluster na documentação do ONTAP".

Requisitos de rede da 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).

Ative o backup e a recuperação do BlueXP no Cloud Volumes ONTAP

É fácil habilitar o backup e a recuperação do BlueXP . As etapas diferem ligeiramente dependendo se você tem um sistema Cloud Volumes ONTAP existente ou um novo.

Ativar backup e recuperação do BlueXP em um novo sistema

O backup e a recuperação do BlueXP são ativados por padrão no assistente do ambiente de trabalho. Certifique-se de que mantém a opção ativada.

```
https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-deploying-otc-aws.html["Iniciando o Cloud Volumes ONTAP na AWS"^]Consulte para obter os requisitos e detalhes para criar seu sistema Cloud Volumes ONTAP.
```

Passos

1. No BlueXP Canvas, selecione **Adicionar ambiente de trabalho**, escolha o provedor de nuvem e selecione **Adicionar novo**. Selecione **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 selecione **continuar**.

5. Complete as páginas no assistente para implantar o sistema.

Resultado

O backup e a recuperação do BlueXP estão ativados no sistema. Depois de criar volumes nesses sistemas Cloud Volumes ONTAP, inicie o backup e a recuperação do BlueXP e "ative o backup em cada volume que você deseja proteger"o .

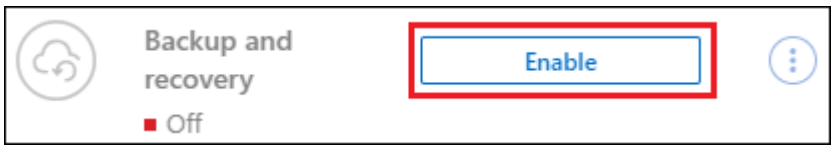
Ativar backup e recuperação do BlueXP em um sistema existente

Habilite o backup e a recuperação do BlueXP em um sistema existente a qualquer momento diretamente do ambiente de trabalho.

Passos

1. No BlueXP Canvas, selecione o ambiente de trabalho e selecione **Enable** ao lado do serviço de backup e recuperação no painel direito.

   Se o destino do Amazon S3 para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster para o ambiente de trabalho do Amazon S3 para iniciar o assistente de configuração.



Para modificar as configurações de backup ou adicionar replicação, "Gerenciar backups do ONTAP"consulte .

Ative backups no ONTAP volumes

Ative os backups a qualquer momento diretamente do seu ambiente de trabalho no local.

Um assistente leva você através dos seguintes passos principais:

- Selecione os volumes que deseja fazer backup
- Defina a estratégia de backup
- Reveja as suas seleções

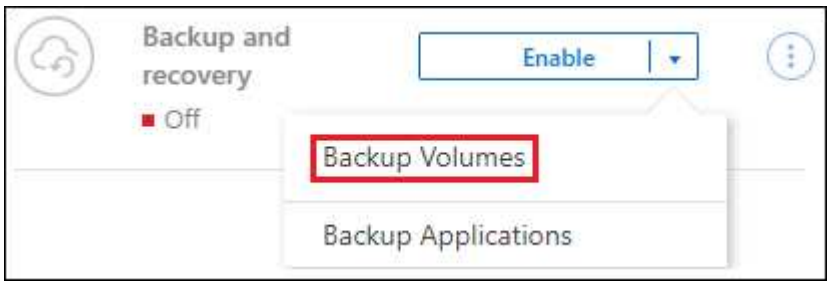
Você também pode Mostrar os comandos APIna etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para futuros ambientes de trabalho.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:

   - Na tela BlueXP , selecione o ambiente de trabalho e selecione **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.

     Se o destino da AWS para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster do ONTAP para o armazenamento de objetos da AWS.

   - Selecione **volumes** na barra de backup e recuperação. Na guia volumes, selecione a opção de ícone **ações** ••• e selecione **Ativar Backup** para um único volume (que ainda não tem replicação ou backup para armazenamento de objetos já ativado).

   A página Introdução do assistente mostra as opções de proteção, incluindo snapshots locais, replicação e backups. Se você fez a segunda opção nesta etapa, a página Definir estratégia de backup será exibida com um volume selecionado.

2. Continue com as seguintes opções:

   - Se já tiver um conetor BlueXP , está tudo definido. Basta selecionar **seguinte**.
   - Se você ainda não tiver um conetor BlueXP , a opção **Adicionar um conetor** será exibida. Prepare o conetor BlueXP Consulte a .

Selecione os volumes que deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem uma ou mais das seguintes opções: Política de snapshot, política de replicação, política de backup para objeto.

Você pode optar por proteger o FlexVol ou o FlexGroup volumes. No entanto, não é possível selecionar uma combinação desses volumes ao ativar o backup para um ambiente de trabalho. Veja como "ative o backup

para volumes adicionais no ambiente de trabalho"(FlexVol ou FlexGroup) depois de configurar o backup para os volumes iniciais.

- Você pode ativar um backup apenas em um único volume FlexGroup de cada vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock. Todos os volumes devem ter o SnapLock Enterprise ativado ou o SnapLock desativado.

Passos

Observe que se os volumes escolhidos já tiverem políticas Snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que deseja proteger.
   - Opcionalmente, filtre as linhas para mostrar apenas volumes com determinados tipos de volume, estilos e muito mais para facilitar a seleção.
   - Depois de selecionar o primeiro volume, você pode selecionar todos os volumes FlexVol (volumes FlexGroup podem ser selecionados um de cada vez somente). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e marque a caixa na linha de título. (

).
   - Para fazer backup de volumes individuais, marque a caixa para cada volume (

).
2. Selecione **seguinte**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Quer você queira uma ou todas as opções de backup: Snapshots locais, replicação e backup no storage de objetos
- Arquitetura
- Política de instantâneo local
- Destino e política de replicação

Se os volumes escolhidos tiverem políticas de Snapshot e replicação diferentes das políticas selecionadas nesta etapa, as políticas existentes serão sobrescritas.

- Backup para informações de armazenamento de objetos (provedor, criptografia, rede, política de backup e opções de exportação).

Passos

1. Na página Definir estratégia de backup, escolha uma ou todas as opções a seguir. Todos os três são selecionados por padrão:
   - **Instantâneos locais**: Se você estiver executando replicação ou fazendo backup em armazenamento de objetos, os snapshots locais devem ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP.
   - **Backup**: Faz backup de volumes para armazenamento de objetos.
2. **Arquitetura**: Se você escolheu replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascading**: As informações fluem do sistema de armazenamento primário para o secundário e do armazenamento secundário para o armazenamento de objetos.

- **Fan out**: As informações fluem do sistema de armazenamento primário para o secundário *e* do armazenamento primário para o armazenamento de objetos.

  Para obter detalhes sobre essas arquiteturas, "Planeje sua jornada de proteção"consulte .

3. **Snapshot local**: Escolha uma política Snapshot existente ou crie uma nova.

   Para criar uma política personalizada antes de ativar a captura Instantânea, "Crie uma política"consulte .

   Para criar uma política, selecione **criar nova política** e faça o seguinte:

   - Introduza o nome da política.
   - Selecione até 5 programações, normalmente de frequências diferentes.
   - Selecione **criar**.

4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o ambiente de trabalho de destino e SVM. Opcionalmente, selecione o agregado de destino ou agregados e o prefixo ou sufixo que será adicionado ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma.

     Para criar uma política personalizada, "Crie uma política"consulte ..

     Para criar uma política, selecione **criar nova política** e faça o seguinte:

     - Introduza o nome da política.
     - Selecione até 5 programações, normalmente de frequências diferentes.
     - Selecione **criar**.

5. **Fazer backup para Objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Fornecedor**: Selecione **Amazon Web Services**.
   - **Configurações do provedor**: Insira os detalhes do provedor e a região onde os backups serão armazenados.

     Insira a conta da AWS usada para armazenar os backups. Esta pode ser uma conta diferente da onde reside o sistema Cloud Volumes ONTAP.

     Se você quiser usar uma conta AWS diferente para seus backups, adicione as credenciais da conta AWS de destino no BlueXP e adicione as permissões "S3:PutBucketPolicy" e "S3:PutBucketOwnershipControls" à função do IAM que fornece permissões ao BlueXP .

     Selecione a região onde os backups serão armazenados. Esta pode ser uma região diferente da onde reside o sistema Cloud Volumes ONTAP.

     Crie um novo bucket ou selecione um existente.

   - **Chave de criptografia**: Se você criou um novo intervalo, insira as informações da chave de criptografia fornecidas pelo provedor. Escolha se você usará as chaves de criptografia padrão da AWS ou escolha suas próprias chaves gerenciadas pelo cliente na sua conta da AWS para gerenciar a criptografia de seus dados. ("Veja como usar suas próprias chaves de criptografia").

Se você optar por usar suas próprias chaves gerenciadas pelo cliente, insira o cofre de chaves e as informações da chave.

> Se você escolheu um bucket existente, as informações de criptografia já estão disponíveis, para que você não precise inseri-lo agora.

- **Política de backup**: Selecione uma política de armazenamento de backup para objeto existente ou crie uma.

> Para criar uma política personalizada antes de ativar a cópia de segurança, "Crie uma política"consulte .

Para criar uma política, selecione **criar nova política** e faça o seguinte:

- Introduza o nome da política.
- Selecione até 5 programações, normalmente de frequências diferentes.
- Para políticas de backup para objeto, defina as configurações DataLock e proteção contra ransomware. Para obter detalhes sobre DataLock e proteção contra ransomware, "Configurações de política de backup para objeto"consulte .
- Selecione **criar**.

- **Exportar cópias Snapshot existentes para o armazenamento de objetos como cópias de backup**: Se houver cópias Snapshot locais para volumes neste ambiente de trabalho que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este ambiente de trabalho (por exemplo, diário, semanal, etc.), esse prompt adicional será exibido. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup para garantir a proteção mais completa para seus volumes.

6. Selecione **seguinte**.

Reveja as suas seleções

Esta é a oportunidade de rever as suas seleções e fazer ajustes, se necessário.

Passos

1. Na página Review (Revisão), reveja as suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos de política Snapshot com os rótulos de política de replicação e backup**. Isso cria snapshots com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O backup e a recuperação do BlueXP começam a fazer os backups iniciais dos seus volumes. A transferência de linha de base do volume replicado e do arquivo de backup inclui uma cópia completa dos dados do sistema de storage primário. As transferências subsequentes contêm cópias diferenciais dos dados do sistema de storage primário contidos nas cópias Snapshot.

Um volume replicado é criado no cluster de destino que será sincronizado com o volume de armazenamento primário.

Um bucket S3 é criado na conta de serviço indicada pela chave de acesso S3 e chave secreta que você inseriu e os arquivos de backup são armazenados lá.

O Painel de backup de volume é exibido para que você possa monitorar o estado dos backups.

Também pode monitorizar o estado dos trabalhos de cópia de segurança e restauro utilizando o "Painel monitorização de trabalhos".

Mostrar os comandos API

Você pode querer exibir e, opcionalmente, copiar os comandos API usados no assistente Ativar backup e recuperação. Você pode querer fazer isso para automatizar a ativação de backup em futuros ambientes de trabalho.

Passos

1. No assistente Ativar backup e recuperação, selecione **Exibir solicitação de API**.
2. Para copiar os comandos para a área de transferência, selecione o ícone **Copiar**.

O que se segue?

- Você pode "gerencie seus arquivos de backup e políticas de backup". Isso inclui iniciar e parar backups, excluir backups, adicionar e alterar o agendamento de backup e muito mais.
- Você pode "gerencie as configurações de backup no nível do cluster". Isso inclui a alteração das chaves de armazenamento que o ONTAP usa para acessar o armazenamento na nuvem, alterar a largura de banda da rede disponível para carregar backups para o armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Você também pode "restaure volumes, pastas ou arquivos individuais a partir de um arquivo de backup"acessar um sistema Cloud Volumes ONTAP na AWS ou um sistema ONTAP no local.

Fazer backup de dados do Cloud Volumes ONTAP para o armazenamento de Blobs do Azure

Conclua algumas etapas para começar a fazer backup de dados de volume de seus sistemas 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 9,8 ou posterior no Azure (recomenda-se o ONTAP 9.8P13 e posterior).
- 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 no mercado do BlueXP ", ou comprou "e ativado" uma licença BYOL de backup e recuperação do BlueXP da NetApp.

Prepare o conetor BlueXP

Se você já tiver um conetor implantado em uma região do Azure, tudo estará definido. Caso contrário, você precisará instalar um BlueXP Connector no Azure para fazer backup dos dados do Cloud Volumes ONTAP para o armazenamento de Blobs do Azure. O conetor pode ser instalado em um site com acesso total à Internet ("modo padrão") ou com conetividade limitada à Internet ("modo restrito").

Prepare o conetor BlueXP

Verifique os requisitos de licença

Você precisará verificar os requisitos de licença para o Azure e o BlueXP .

Verifique os requisitos de licençaConsulte a .

Verificar os requisitos de rede do ONTAP para replicação de volumes

Certifique-se de que os sistemas de origem e destino cumprem os requisitos de rede e versão do ONTAP.

Verificar os requisitos de rede do ONTAP para replicação de volumes.

Ative o backup e a recuperação do BlueXP

Selecione o ambiente de trabalho e clique em **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.

Ative o backup e a recuperação do BlueXP no Cloud Volumes ONTAP.

Ative backups no ONTAP volumes

Siga o assistente de configuração para selecionar as políticas de replicação e backup que você usará e os volumes que deseja fazer backup.

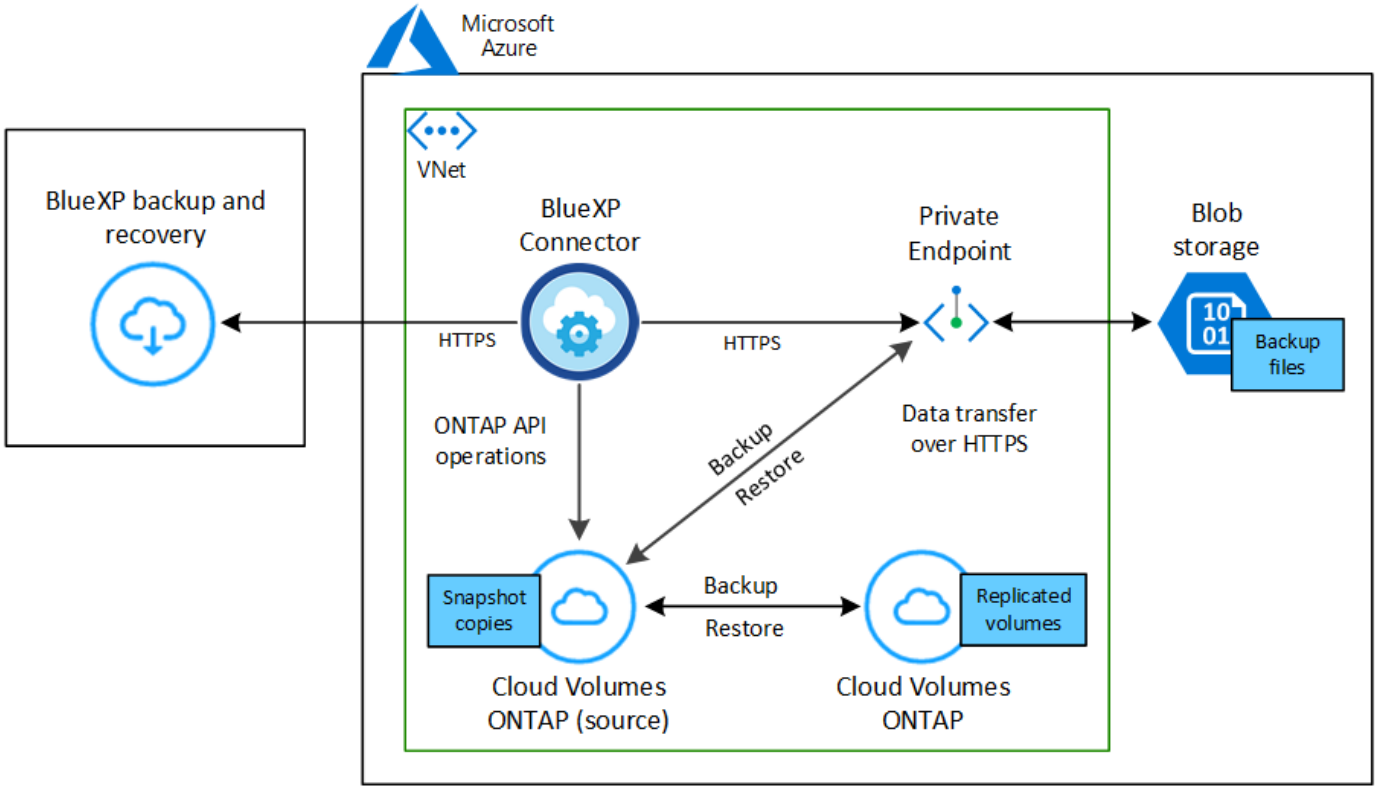
Ative backups no ONTAP volumes.

Verifique o suporte para sua configuração

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.

A imagem a seguir mostra cada componente e as conexões que você precisa preparar entre eles.

Opcionalmente, você pode se conectar a um sistema ONTAP secundário para volumes replicados usando a conexão pública ou privada.



Versões de ONTAP compatíveis

É recomendado um mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior.

Regiões Azure compatíveis

O backup e a recuperação do BlueXP são compatíveis em todas as regiões do Azure "Onde o Cloud Volumes ONTAP é suportado" , incluindo regiões do governo do Azure.

Por padrão, o backup e a recuperação do BlueXP provisiona o contentor Blob com redundância local (LRS) para otimização de custos. Você pode alterar essa configuração para redundância de zona (ZRS) depois que o backup e a recuperação do BlueXP tiverem sido ativados se desejar garantir que seus dados sejam replicados entre diferentes zonas. Consulte as instruções da Microsoft para "alterar a forma como a sua conta de armazenamento é replicada".

Configuração necessária para criar backups em uma assinatura diferente do Azure

Por padrão, os backups são criados usando a mesma assinatura usada para o sistema Cloud Volumes ONTAP. Para usar uma assinatura diferente do Azure para seus backups, você deve "Faça login no portal do Azure e vincule as duas assinaturas".

Verifique os requisitos de licença

Para o licenciamento PAYGO de recuperação e backup do BlueXP , é necessária uma assinatura pelo Azure Marketplace antes de ativar o backup e a recuperação do BlueXP . A cobrança do backup e recuperação do BlueXP é feita por meio dessa assinatura. "Pode subscrever a partir da página Detalhes credenciais do assistente do ambiente de trabalho".

Para o licenciamento BYOL de backup e recuperação do BlueXP , você precisa do número de série do NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Saiba como gerenciar suas licenças BYOL". Você deve usar uma licença BYOL quando o conetor e o sistema Cloud Volumes ONTAP forem implantados em um site escuro ("modo privado").

E você precisa ter uma assinatura do Microsoft Azure para o espaço de armazenamento onde seus backups estarão localizados.

Prepare o conetor BlueXP

O conetor pode ser instalado em uma região do Azure com acesso total ou limitado à Internet (modo "padrão" ou "restrito"). "Consulte modos de implantação do BlueXP para obter detalhes".

- "Saiba mais sobre conetores"
- "Implante um conetor no Azure no modo padrão (acesso total à Internet)"
- "Instale o conetor no modo restrito (acesso de saída limitado)"

Verifique ou adicione permissões ao conetor

Para usar a funcionalidade de pesquisa e restauração de backup e recuperação do BlueXP , você precisa ter permissões específicas na função do conetor para que ele possa acessar a conta de armazenamento de dados e espaço de trabalho do Synapse do Azure. Consulte as permissões abaixo e siga as etapas se precisar modificar a política.

Antes de começar

- Você deve Registrar o Fornecedor de recursos do Azure Synapse Analytics (chamado "Microsoft.Synapse") com sua assinatura. "Veja como registar este fornecedor de recursos para a sua subscrição". Você deve ser a assinatura **proprietário** ou **Colaborador** para Registrar o provedor de recursos.
- A porta 1433 deve estar aberta para comunicação entre o conetor e os serviços SQL do Azure Synapse.

Passos

1. Identifique a função atribuída à máquina virtual do conetor:
   a. No portal do Azure, abra o serviço de máquinas virtuais.
   b. Selecione a máquina virtual do conetor.
   c. Em Configurações, selecione **identidade**.
   d. Selecione **atribuições de função do Azure**.
   e. Anote a função personalizada atribuída à máquina virtual do conetor.
2. Atualize a função personalizada:
   a. No portal do Azure, abra sua assinatura do Azure.
   b. Selecione **Access Control (IAM) > Roles**.
   c. Selecione a elipse (**…**) para a função personalizada e, em seguida, selecione **Edit**.
   d. Selecione **JSON** e adicione as seguintes permissões:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Veja o formato JSON completo da política"

e. Clique em **Revisão e atualização** e, em seguida, clique em **Atualização**.

Informações necessárias para usar chaves gerenciadas pelo cliente para criptografia de dados

Você pode usar suas próprias chaves gerenciadas pelo cliente para criptografia de dados no assistente de ativação em vez de usar as chaves de criptografia gerenciadas pela Microsoft padrão. Nesse caso, você precisará ter a assinatura do Azure, o nome do Cofre-chave e a chave. "Veja como usar suas próprias chaves".

O backup e a recuperação do BlueXP são compatíveis com *políticas de acesso do Azure*, o modelo de permissão de controle de acesso baseado em função do Azure_ (Azure RBAC) e o *modelo de segurança de hardware gerenciado* (HSM) (consulte a "O que é o HSM gerenciado do Azure Key Vault?").

Crie sua conta de armazenamento Azure Blob

Por padrão, o serviço cria contas de armazenamento para você. Se quiser usar suas próprias contas de armazenamento, você pode criá-las antes de iniciar o assistente de ativação de backup e, em seguida, selecionar essas contas de armazenamento no assistente.

"Saiba mais sobre como criar suas próprias contas de armazenamento".

Verificar os requisitos de rede do ONTAP para replicação de volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o backup e a recuperação do BlueXP , certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede da ONTAP no local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da rede corporativa à rede virtual no provedor de nuvem. Normalmente, esta é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou sistemas locais, revise os requisitos de peering para sistemas ONTAP locais. "Veja os pré-requisitos para peering de cluster na documentação do ONTAP".

Requisitos de rede da 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).

Ative o backup e a recuperação do BlueXP no Cloud Volumes ONTAP

É fácil habilitar o backup e a recuperação do BlueXP . As etapas diferem ligeiramente dependendo se você tem um sistema Cloud Volumes ONTAP existente ou um novo.

Ativar backup e recuperação do BlueXP em um novo sistema

O backup e a recuperação do BlueXP são ativados por padrão no assistente do ambiente de trabalho. Certifique-se de que mantém a opção ativada.

```
https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-deploying-otc-azure.html["Iniciar o Cloud Volumes ONTAP no Azure"^]Consulte para obter os requisitos e detalhes para criar seu sistema Cloud Volumes ONTAP.
```

Se você quiser escolher o nome do grupo de recursos, **Disable** backup e recuperação do BlueXP ao implantar o Cloud Volumes ONTAP. Siga as etapas para Ativar o backup e a recuperação do BlueXP em um sistema existentehabilitar o backup e a recuperação do BlueXP e escolher o grupo de recursos.

Passos

1. No BlueXP Canvas, selecione **Adicionar ambiente de trabalho**, escolha o provedor de nuvem e selecione **Adicionar novo**. Selecione **Create Cloud Volumes ONTAP**.
2. Selecione **Microsoft Azure** como provedor de nuvem e escolha um único nó ou sistema de HA.
3. Na página Definir credenciais do Azure, insira o nome das credenciais, o ID do cliente, o segredo do cliente e o ID do diretório e clique em **continuar**.
4. Preencha a página Detalhes e credenciais e certifique-se de que uma assinatura do Azure Marketplace está em vigor e clique em **continuar**.
5. Na página Serviços, deixe o serviço ativado e clique em **continuar**.

6. Complete as páginas no assistente para implantar o sistema.

Resultado

O backup e a recuperação do BlueXP estão ativados no sistema. Depois de criar volumes nesses sistemas Cloud Volumes ONTAP, inicie o backup e a recuperação do BlueXP e "ative o backup em cada volume que você deseja proteger"o .

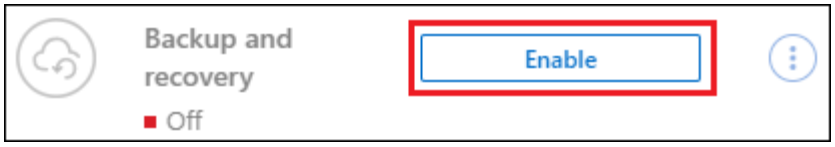
Ativar backup e recuperação do BlueXP em um sistema existente

Ative o backup e a recuperação do BlueXP a qualquer momento diretamente do ambiente de trabalho.

Passos

1. No BlueXP Canvas, selecione o ambiente de trabalho e selecione **Enable** ao lado do serviço de backup e recuperação no painel direito.

   Se o destino do Blob do Azure para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster para o ambiente de trabalho do Blob do Azure para iniciar o assistente de configuração.



2. Conclua as páginas no assistente para implantar o backup e a recuperação do BlueXP .
3. Quando pretender iniciar cópias de segurança, avance para Ative backups no ONTAP volumeso .

Ative backups no ONTAP volumes

Ative os backups a qualquer momento diretamente do seu ambiente de trabalho no local.

Um assistente leva você através dos seguintes passos principais:

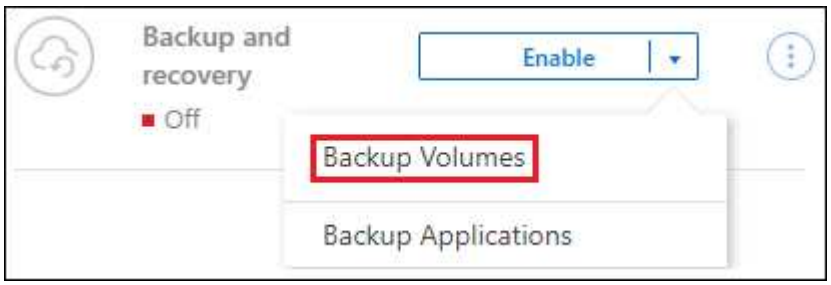
- Selecione os volumes que deseja fazer backup
- Defina a estratégia de backup
- Reveja as suas seleções

Você também pode Mostrar os comandos APIna etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para futuros ambientes de trabalho.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:
   - Na tela BlueXP , selecione o ambiente de trabalho e selecione **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.

     Se o destino do Azure para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster do ONTAP para o armazenamento de objetos Blob do Azure.
   - Selecione **volumes** na barra de backup e recuperação. Na guia volumes, selecione o ícone **ações** ••• e selecione **Ativar Backup** para um único volume (que ainda não tem replicação ou backup para armazenamento de objetos já ativado).

   A página Introdução do assistente mostra as opções de proteção, incluindo snapshots locais, replicação e backups. Se você fez a segunda opção nesta etapa, a página Definir estratégia de backup será exibida com um volume selecionado.
2. Continue com as seguintes opções:
   - Se já tiver um conetor BlueXP , está tudo definido. Basta selecionar **seguinte**.
   - Se você ainda não tiver um conetor BlueXP , a opção **Adicionar um conetor** será exibida. Prepare o

conetor BlueXP Consulte a .

Selecione os volumes que deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem uma ou mais das seguintes opções: Política de snapshot, política de replicação, política de backup para objeto.

Você pode optar por proteger o FlexVol ou o FlexGroup volumes. No entanto, não é possível selecionar uma combinação desses volumes ao ativar o backup para um ambiente de trabalho. Veja como "ative o backup para volumes adicionais no ambiente de trabalho"(FlexVol ou FlexGroup) depois de configurar o backup para os volumes iniciais.

- Você pode ativar um backup apenas em um único volume FlexGroup de cada vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock. Todos os volumes devem ter o SnapLock Enterprise ativado ou o SnapLock desativado.

Passos

Observe que se os volumes escolhidos já tiverem políticas Snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que deseja proteger.
   - Opcionalmente, filtre as linhas para mostrar apenas volumes com determinados tipos de volume, estilos e muito mais para facilitar a seleção.
   - Depois de selecionar o primeiro volume, você pode selecionar todos os volumes FlexVol. (Os volumes FlexGroup só podem ser selecionados um de cada vez.) Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e marque a caixa na linha de título. (

).
   - Para fazer backup de volumes individuais, marque a caixa para cada volume (

).
2. Selecione **seguinte**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Quer você queira uma ou todas as opções de backup: Snapshots locais, replicação e backup no storage de objetos
- Arquitetura
- Política de instantâneo local
- Destino e política de replicação

Se os volumes escolhidos tiverem políticas de Snapshot e replicação diferentes das políticas selecionadas nesta etapa, as políticas existentes serão sobrescritas.

- Backup para informações de armazenamento de objetos (provedor, criptografia, rede, política de backup e opções de exportação).

Passos

1. Na página Definir estratégia de backup, escolha uma ou todas as opções a seguir. Todos os três são selecionados por padrão:

- **Instantâneos locais**: Se você estiver executando replicação ou fazendo backup em armazenamento de objetos, os snapshots locais devem ser criados.
- **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP.
- **Backup**: Faz backup de volumes para armazenamento de objetos.

2. **Arquitetura**: Se você escolheu replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascading**: As informações fluem do sistema de armazenamento primário para o secundário e do armazenamento secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do sistema de armazenamento primário para o secundário *e* do armazenamento primário para o armazenamento de objetos.

     Para obter detalhes sobre essas arquiteturas, "Planeje sua jornada de proteção"consulte .

3. **Snapshot local**: Escolha uma política Snapshot existente ou crie uma.

   Para criar uma política personalizada antes de ativar a captura Instantânea, "Crie uma política"consulte .

   Para criar uma política, selecione **criar nova política** e faça o seguinte:
   - Introduza o nome da política.
   - Selecione até 5 programações, normalmente de frequências diferentes.
   - Selecione **criar**.

4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o ambiente de trabalho de destino e SVM. Opcionalmente, selecione o agregado de destino ou agregados e o prefixo ou sufixo que será adicionado ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma.

     Para criar uma política personalizada antes de ativar a replicação, "Crie uma política"consulte .

     Para criar uma política, selecione **criar nova política** e faça o seguinte:
     - Introduza o nome da política.
     - Selecione até 5 programações, normalmente de frequências diferentes.
     - Selecione **criar**.

5. **Fazer backup para Objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Fornecedor**: Selecione **Microsoft Azure**.
   - **Configurações do provedor**: Insira os detalhes do provedor.

     Introduza a região onde os backups serão armazenados. Esta pode ser uma região diferente da onde reside o sistema Cloud Volumes ONTAP.

     Crie uma nova conta de armazenamento ou selecione uma existente.

     Insira a assinatura do Azure usada para armazenar os backups. Essa pode ser uma assinatura diferente de onde o sistema Cloud Volumes ONTAP reside. Para usar uma assinatura diferente do

Azure para seus backups, você deve "Faça login no portal do Azure e vincule as duas assinaturas".

Crie seu próprio grupo de recursos que gerencia o contentor Blob ou selecione o tipo e o grupo do grupo de recursos.

> Se você quiser proteger seus arquivos de backup de serem modificados ou excluídos, verifique se a conta de armazenamento foi criada com armazenamento imutável habilitado usando um período de retenção de 30 dias.

> Se você quiser categorizar arquivos de backup mais antigos no Azure Archive Storage para otimização de custo adicional, verifique se a conta de storage tem a regra de ciclo de vida apropriada.

- **Chave de criptografia**: Se você criou uma nova conta de armazenamento do Azure, insira as informações da chave de criptografia fornecidas pelo provedor. Escolha se irá utilizar as chaves de encriptação padrão do Azure ou escolher as suas próprias chaves geridas pelo cliente na sua conta Azure para gerir a encriptação dos seus dados.

  Se você optar por usar suas próprias chaves gerenciadas pelo cliente, insira o cofre de chaves e as informações da chave. "Saiba como usar suas próprias chaves".

  > Se você escolheu uma conta de armazenamento Microsoft existente, as informações de criptografia já estão disponíveis, para que você não precise inseri-la agora.

- **Rede**: Escolha o IPspace e se você usará um endpoint privado. O endpoint privado está desativado por predefinição.
  i. O espaço de IPspace no cluster do ONTAP onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.
  ii. Opcionalmente, escolha se você usará um endpoint privado do Azure que você configurou anteriormente. "Saiba mais sobre como usar um endpoint privado do Azure".
- **Política de backup**: Selecione uma política de armazenamento de backup para objeto existente.

  > Para criar uma política personalizada antes de ativar a cópia de segurança, "Crie uma política"consulte .

  Para criar uma política, selecione **criar nova política** e faça o seguinte:

  - Introduza o nome da política.
  - Para políticas de backup para objeto, defina as configurações DataLock e proteção contra ransomware. Para obter detalhes sobre DataLock e proteção contra ransomware, "Configurações de política de backup para objeto"consulte .
  - Selecione até 5 programações, normalmente de frequências diferentes.
  - Selecione **criar**.
- **Exportar cópias Snapshot existentes para o armazenamento de objetos como cópias de backup**: Se houver cópias Snapshot locais para volumes neste ambiente de trabalho que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este ambiente de trabalho (por exemplo, diário, semanal, etc.), esse prompt adicional será exibido. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup para garantir a proteção mais completa para seus volumes.

6. Selecione **seguinte**.

Reveja as suas seleções

Esta é a oportunidade de rever as suas seleções e fazer ajustes, se necessário.

Passos

1. Na página Review (Revisão), reveja as suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos de política Snapshot com os rótulos de política de replicação e backup**. Isso cria snapshots com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O backup e a recuperação do BlueXP começam a fazer os backups iniciais dos seus volumes. A transferência de linha de base do volume replicado e do arquivo de backup inclui uma cópia completa dos dados do sistema de storage primário. As transferências subsequentes contêm cópias diferenciais dos dados de storage primário contidos nas cópias Snapshot.

Um volume replicado é criado no cluster de destino que será sincronizado com o volume primário.

Um contentor de armazenamento de Blob é criado no grupo de recursos que você inseriu e os arquivos de backup são armazenados lá.

Por padrão, o backup e a recuperação do BlueXP provisiona o contentor Blob com redundância local (LRS) para otimização de custos. Você pode alterar essa configuração para redundância de zona (ZRS) se quiser garantir que seus dados sejam replicados entre diferentes zonas. Consulte as instruções da Microsoft para "alterar a forma como a sua conta de armazenamento é replicada".

O Painel de backup de volume é exibido para que você possa monitorar o estado dos backups.

Também pode monitorizar o estado dos trabalhos de cópia de segurança e restauro utilizando o "Painel monitorização de trabalhos".

Mostrar os comandos API

Você pode querer exibir e, opcionalmente, copiar os comandos API usados no assistente Ativar backup e recuperação. Você pode querer fazer isso para automatizar a ativação de backup em futuros ambientes de trabalho.

Passos

1. No assistente Ativar backup e recuperação, selecione **Exibir solicitação de API**.
2. Para copiar os comandos para a área de transferência, selecione o ícone **Copiar**.

O que se segue?

- Você pode "gerencie seus arquivos de backup e políticas de backup". Isso inclui iniciar e parar backups, excluir backups, adicionar e alterar o agendamento de backup e muito mais.
- Você pode "gerencie as configurações de backup no nível do cluster". Isso inclui alterar a largura de banda da rede disponível para fazer upload de backups para o armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.

- Você também pode "restaure volumes, pastas ou arquivos individuais a partir de um arquivo de backup"acessar um sistema Cloud Volumes ONTAP no Azure ou um sistema ONTAP no local.

Faça backup dos dados do Cloud Volumes ONTAP no Google Cloud Storage

Execute algumas etapas para começar a fazer backup de dados de volume de seus sistemas Cloud Volumes ONTAP para o Google Cloud Storage.

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 9,8 ou posterior no GCP (recomenda-se o ONTAP 9.8P13 e posterior).
- Você tem uma assinatura válida do GCP para o espaço de armazenamento onde os backups estarão localizados.
- Você tem uma conta de serviço no Google Cloud Project que tem uma função personalizada com um conjunto reduzido de permissões.

A função de administrador de storage não é mais necessária para a conta de serviço que permite o backup e a recuperação do BlueXP acessar buckets do Google Cloud Storage.

- Você se inscreveu no "Oferta de backup no mercado do BlueXP ", ou comprou "e ativado" uma licença BYOL de backup e recuperação do BlueXP da NetApp.

Prepare o conetor BlueXP

Se você já tiver um conetor implantado em uma região do GCP, tudo estará pronto. Caso contrário, você precisará instalar um BlueXP Connector no GCP para fazer backup dos dados do Cloud Volumes ONTAP no Google Cloud Storage. O conetor pode ser instalado em um site com acesso total à Internet ("modo padrão") ou com conetividade limitada à Internet ("modo restrito").

Verifique os requisitos de licença

Você precisará verificar os requisitos de licença do Google Cloud e do BlueXP .

Verificar os requisitos de rede do ONTAP para replicação de volumes

Certifique-se de que os sistemas de origem e destino cumprem os requisitos de rede e versão do ONTAP.

Ative o backup e a recuperação do BlueXP

Selecione o ambiente de trabalho e clique em **Ativar > volumes de backup** ao lado do serviço de backup e

recuperação no painel direito.

6 Prepare o Google Cloud como destino de backup

Configure permissões para que o conetor crie e gerencie o bucket do Google Cloud.

Opcionalmente, você pode configurar suas próprias chaves gerenciadas personalizadas para criptografia de dados em vez de usar as chaves de criptografia padrão do Google Cloud. Saiba como preparar seu ambiente do Google Cloud para receber backups do ONTAP.

7 Ative backups no ONTAP volumes

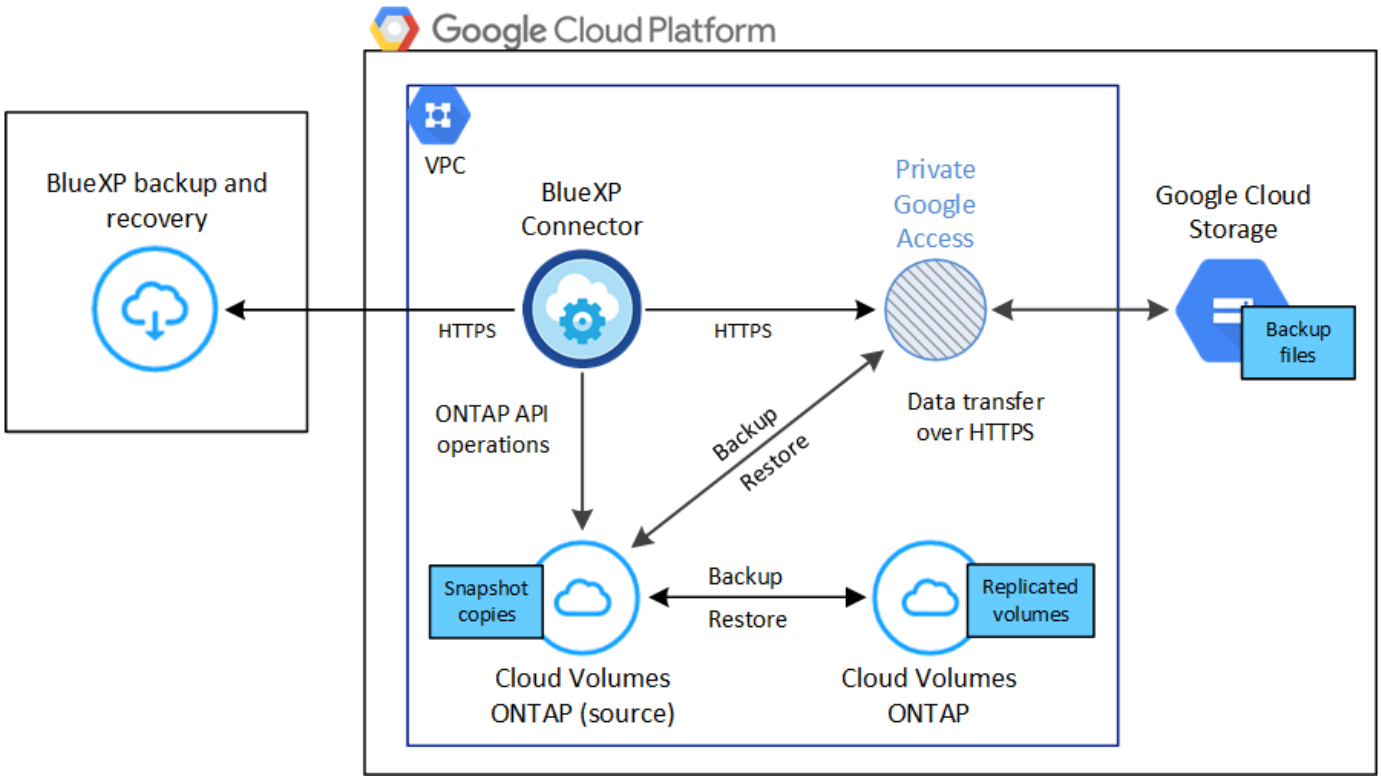
Siga o assistente de configuração para selecionar as políticas de replicação e backup que você usará e os volumes que deseja fazer backup.

Verifique o suporte para sua configuração

Leia os requisitos a seguir para garantir que você tenha uma configuração compatível antes de iniciar o backup de volumes no Google Cloud Storage.

A imagem a seguir mostra cada componente e as conexões que você precisa preparar entre eles.

Opcionalmente, você pode se conectar a um sistema ONTAP secundário para volumes replicados usando a conexão pública ou privada.



Versões de ONTAP compatíveis

É recomendado um mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior.

Regiões GCP compatíveis

O backup e a recuperação do BlueXP são compatíveis em todas as regiões do GCP "Onde o Cloud Volumes ONTAP é suportado" .

Conta de serviço do GCP

Você precisa ter uma conta de serviço no Google Cloud Project que tenha a função personalizada. "Saiba como criar uma conta de serviço".

> A função de administrador de storage não é mais necessária para a conta de serviço que permite o backup e a recuperação do BlueXP acessar buckets do Google Cloud Storage.

Verifique os requisitos de licença

Para o licenciamento PAYGO de backup e recuperação do BlueXP , uma assinatura do BlueXP está disponível no Google Marketplace que permite implantações de backup e recuperação do Cloud Volumes ONTAP e do BlueXP . Você precisa "Assine esta assinatura do BlueXP " antes de ativar o backup e a recuperação do BlueXP . A cobrança do backup e recuperação do BlueXP é feita por meio dessa assinatura. "Pode subscrever a partir da página Detalhes credenciais do assistente do ambiente de trabalho".

Para o licenciamento BYOL de backup e recuperação do BlueXP , você precisa do número de série do NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Saiba como gerenciar suas licenças BYOL".

E você precisa ter uma assinatura do Google para o espaço de armazenamento onde seus backups estarão localizados.

Prepare o conetor BlueXP

O conetor deve ser instalado em uma região do Google com acesso à Internet.

- "Saiba mais sobre conetores"
- "Implante um conetor no Google Cloud"

Verifique ou adicione permissões ao conetor

Para usar a funcionalidade "pesquisar e restaurar" de backup e recuperação do BlueXP , você precisa ter permissões específicas na função do conetor para que ele possa acessar o serviço do Google Cloud BigQuery. Consulte as permissões abaixo e siga as etapas se precisar modificar a política.

Passos

1. No "Google Cloud Console", vá para a página **Roles**.
2. Usando a lista suspensa na parte superior da página, selecione o projeto ou organização que contém a função que deseja editar.
3. Selecione uma função personalizada.
4. Selecione **Editar função** para atualizar as permissões da função.
5. Selecione **Adicionar permissões** para adicionar as seguintes novas permissões à função.

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. Selecione **Atualizar** para salvar a função editada.

Informações necessárias para usar chaves de criptografia gerenciadas pelo cliente (CMEK)

Você pode usar suas próprias chaves gerenciadas pelo cliente para criptografia de dados em vez de usar as chaves de criptografia gerenciadas pelo Google padrão. As chaves entre regiões e entre projetos são suportadas, para que você possa escolher um projeto para um bucket diferente do projeto da chave CMEK. Se você está planejando usar suas próprias chaves gerenciadas pelo cliente:

- Você precisará ter o Key Ring e o Key Name para poder adicionar essas informações no assistente de ativação. "Saiba mais sobre chaves de criptografia gerenciadas pelo cliente".
- Você precisará verificar se essas permissões necessárias estão incluídas na função do conetor:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Você precisará verificar se a API "Cloud Key Management Service (KMS)" do Google está habilitada em seu projeto. Consulte "Documentação do Google Cloud: Habilitando APIs" para obter detalhes.

Considerações CMEK:

- Tanto o HSM (suportado por hardware) quanto as chaves geradas por software são suportados.
- As chaves do Cloud KMS recém-criadas ou importadas são suportadas.
- Apenas chaves regionais são suportadas; chaves globais não são suportadas.
- Atualmente, apenas o propósito "Symmetric encriptar/desencriptar" é suportado.
- Ao agente de serviço associado à conta de armazenamento é atribuída a função do IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" pelo backup e recuperação do BlueXP .

Crie seus próprios baldes

Por padrão, o serviço cria buckets para você. Se você quiser usar seus próprios buckets, você pode criá-los antes de iniciar o assistente de ativação de backup e, em seguida, selecionar esses buckets no assistente.

"Saiba mais sobre como criar seus próprios buckets".

Verificar os requisitos de rede do ONTAP para replicação de volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o backup e a recuperação do BlueXP , certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede da ONTAP no local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da rede corporativa à rede virtual no provedor de nuvem. Normalmente, esta é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou sistemas locais, revise os requisitos de peering para sistemas ONTAP locais. "Veja os pré-requisitos para peering de cluster na documentação do ONTAP".

Requisitos de rede da 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).

Ative o backup e a recuperação do BlueXP no Cloud Volumes ONTAP

É fácil habilitar o backup e a recuperação do BlueXP . As etapas diferem ligeiramente dependendo se você tem um sistema Cloud Volumes ONTAP existente ou um novo.

Ativar backup e recuperação do BlueXP em um novo sistema

O backup e a recuperação do BlueXP podem ser ativados quando você concluir o assistente de ambiente de trabalho para criar um novo sistema Cloud Volumes ONTAP.

Você deve ter uma conta de serviço já configurada. Se você não 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.

```
https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-deploying-
gcp.html["Iniciando o Cloud Volumes ONTAP na GCP"^]Consulte para obter os
requisitos e detalhes para criar seu sistema Cloud Volumes ONTAP.
```

Passos

1. No BlueXP Canvas, selecione **Adicionar ambiente de trabalho**, escolha o provedor de nuvem e

selecione **Adicionar novo**. Selecione **Create Cloud Volumes ONTAP**.

2. **Escolha um local**: Selecione **Google Cloud Platform**.
3. **Escolha tipo**: Selecione **Cloud Volumes ONTAP** (nó único ou alta disponibilidade).
4. **Detalhes e credenciais**: Insira as seguintes informações:

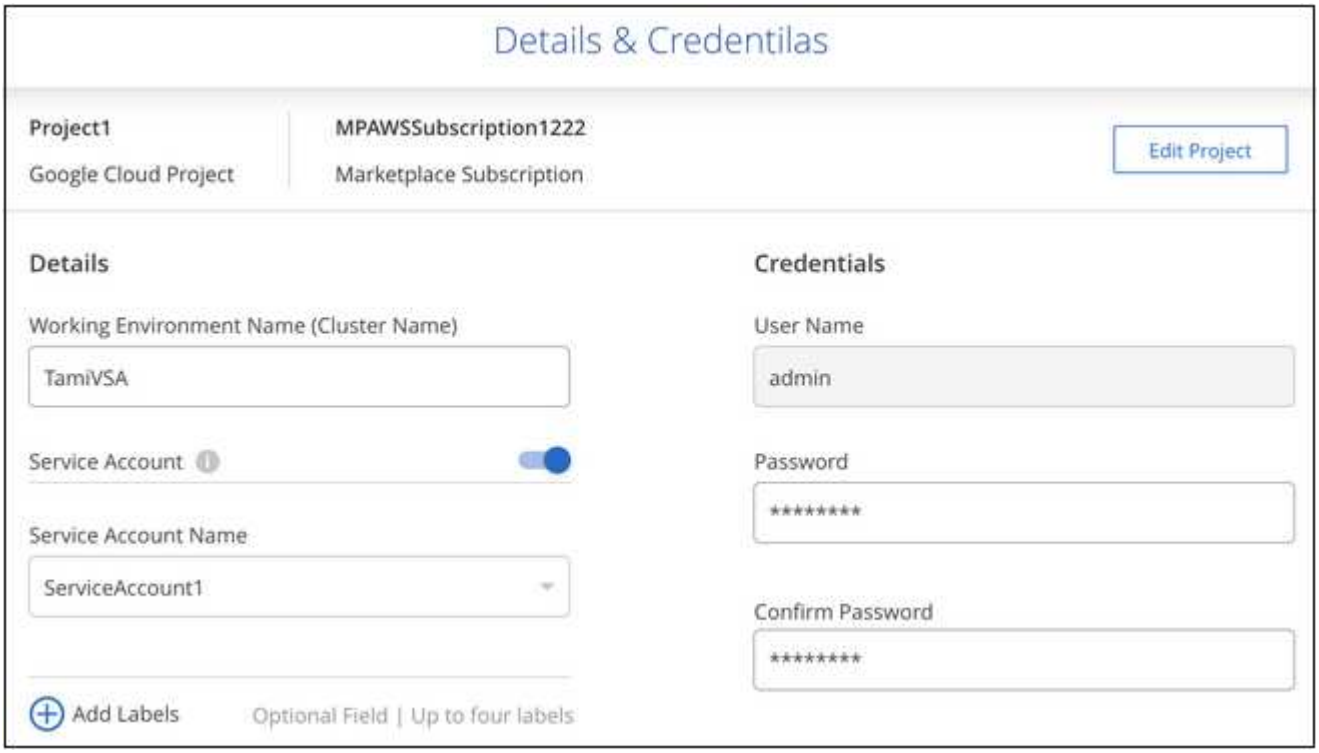
   a. Clique em **Editar Projeto** e selecione um novo projeto se o que você deseja usar for diferente do Projeto padrão (onde o conetor reside).

   b. Especifique o nome do cluster.

   c. Ative a opção **conta de serviço** e selecione a conta de serviço que tem a função Administrador de armazenamento predefinida. Isso é necessário para habilitar backups e disposição em camadas.

   d. Especifique as credenciais.

      Verifique se há uma assinatura do GCP Marketplace.



5. **Serviços**: Deixe o serviço de backup e recuperação do BlueXP ativado e clique em **continuar**.

6. Preencha as páginas do assistente para implantar o sistema conforme descrito em "Iniciando o Cloud Volumes ONTAP na GCP".

Para modificar as configurações de backup ou adicionar replicação, "Gerenciar backups do ONTAP"consulte .

Resultado

O backup e a recuperação do BlueXP estão ativados no sistema. Depois de criar volumes nesses sistemas Cloud Volumes ONTAP, inicie o backup e a recuperação do BlueXP e "ative o backup em cada volume que você deseja proteger"o .

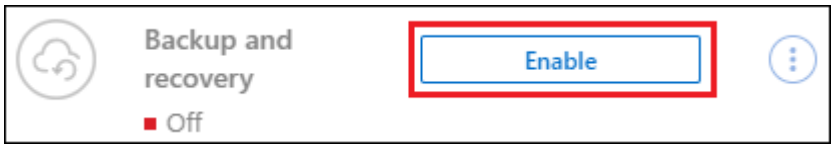
Ativar backup e recuperação do BlueXP em um sistema existente

Você pode habilitar o backup e a recuperação do BlueXP a qualquer momento diretamente do ambiente de trabalho.

Passos

1. No BlueXP Canvas, selecione o ambiente de trabalho e selecione **Enable** ao lado do serviço de backup e recuperação no painel direito.

   Se o destino do Google Cloud Storage para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster para o ambiente de trabalho do Google Cloud Storage para iniciar o assistente de configuração.



Para modificar as configurações de backup ou adicionar replicação, "Gerenciar backups do ONTAP"consulte .

Prepare o Google Cloud Storage como destino de backup

Preparar o Google Cloud Storage como destino de backup envolve as seguintes etapas:

- Configurar permissões.
- (Opcional) Crie seus próprios buckets. (O serviço criará buckets para você, se você quiser.)
- (Opcional) Configurar chaves gerenciadas pelo cliente para criptografia de dados

Configurar permissões

Você precisa fornecer chaves de acesso ao armazenamento para uma conta de serviço que tenha permissões específicas usando uma função personalizada. Uma conta de serviço permite que o backup e a recuperação do BlueXP autentiquem e acessem os buckets do Cloud Storage usados para armazenar backups. As chaves são necessárias para que o Google Cloud Storage saiba quem está fazendo a solicitação.

Passos

1. No "Google Cloud Console", vá para a página **Roles**.
2. "Crie uma nova função" com as seguintes permissões:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. No console do Google Cloud, "Vá para a página Contas de Serviço".
4. Selecione seu projeto Cloud.
5. Selecione **criar conta de serviço** e forneça as informações necessárias:
   a. **Detalhes da conta de serviço**: Insira um nome e uma descrição.
   b. **Conceder acesso a essa conta de serviço ao projeto**: Selecione a função personalizada que você acabou de criar.
   c. Selecione **Concluído**.
6. Vá para "Configurações de armazenamento do GCP" e crie chaves de acesso para a conta de serviço:
   a. Selecione um projeto e selecione **interoperabilidade**. Se ainda não o tiver feito, selecione **Ativar acesso à interoperabilidade**.
   b. Em **chaves de acesso para contas de serviço**, selecione **criar uma chave para uma conta de serviço**, selecione a conta de serviço que acabou de criar e clique em **criar chave**.

      Você precisará inserir as chaves no backup e recuperação do BlueXP mais tarde quando configurar o serviço de backup.

Crie seus próprios baldes

Por padrão, o serviço cria buckets para você. Ou, se você quiser usar seus próprios buckets, você pode criá-los antes de iniciar o assistente de ativação de backup e, em seguida, selecionar esses buckets no assistente.

"Saiba mais sobre como criar seus próprios buckets".

Configurar chaves de criptografia gerenciadas pelo cliente (CMEK) para criptografia de dados

Você pode usar suas próprias chaves gerenciadas pelo cliente para criptografia de dados em vez de usar as chaves de criptografia gerenciadas pelo Google padrão. As chaves entre regiões e entre projetos são suportadas, para que você possa escolher um projeto para um bucket diferente do projeto da chave CMEK.

Se você está planejando usar suas próprias chaves gerenciadas pelo cliente:

- Você precisará ter o Key Ring e o Key Name para poder adicionar essas informações no assistente de ativação. "Saiba mais sobre chaves de criptografia gerenciadas pelo cliente".

- Você precisará verificar se essas permissões necessárias estão incluídas na função do conetor:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Você precisará verificar se a API "Cloud Key Management Service (KMS)" do Google está habilitada em seu projeto. Consulte "Documentação do Google Cloud: Habilitando APIs" para obter detalhes.

Considerações CMEK:

- Tanto as chaves HSM (suportadas por hardware) como as chaves geradas por software são suportadas.
- As chaves do Cloud KMS recém-criadas ou importadas são suportadas.
- Apenas são suportadas chaves regionais, não são suportadas chaves globais.
- Atualmente, apenas o propósito "Symmetric encriptar/desencriptar" é suportado.
- Ao agente de serviço associado à conta de armazenamento é atribuída a função do IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" pelo backup e recuperação do BlueXP .

Ative backups no ONTAP volumes

Ative os backups a qualquer momento diretamente do seu ambiente de trabalho no local.

Um assistente leva você através dos seguintes passos principais:

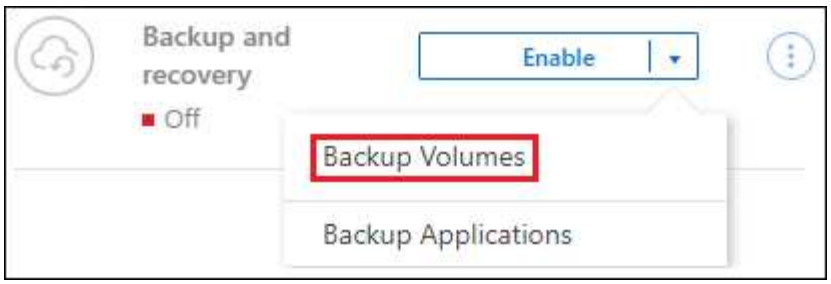
- Selecione os volumes que deseja fazer backup
- Defina a estratégia de backup
- Reveja as suas seleções

Você também pode Mostrar os comandos APIna etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para futuros ambientes de trabalho.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:
    - Na tela BlueXP , selecione o ambiente de trabalho e selecione **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.



Se o destino do GCP para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster do ONTAP para o armazenamento de objetos do GCP.

- Selecione **volumes** na barra de backup e recuperação. Na guia volumes, selecione o ícone **ações** ••• e selecione **Ativar Backup** para um único volume (que ainda não tem replicação ou backup para armazenamento de objetos já ativado).

A página Introdução do assistente mostra as opções de proteção, incluindo snapshots locais, replicação e backups. Se você fez a segunda opção nesta etapa, a página Definir estratégia de backup será exibida com um volume selecionado.

2. Continue com as seguintes opções:
   - Se já tiver um conetor BlueXP , está tudo definido. Basta selecionar **seguinte**.
   - Se você ainda não tiver um conetor BlueXP , a opção **Adicionar um conetor** será exibida. Prepare o conetor BlueXP Consulte a .

Selecione os volumes que deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem uma ou mais das seguintes opções: Política de snapshot, política de replicação, política de backup para objeto.

Você pode optar por proteger o FlexVol ou o FlexGroup volumes. No entanto, não é possível selecionar uma combinação desses volumes ao ativar o backup para um ambiente de trabalho. Veja como "ative o backup para volumes adicionais no ambiente de trabalho"(FlexVol ou FlexGroup) depois de configurar o backup para os volumes iniciais.

- Você pode ativar um backup apenas em um único volume FlexGroup de cada vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock. Todos os volumes devem ter o SnapLock Enterprise ativado ou o SnapLock desativado.

Passos

Observe que se os volumes escolhidos já tiverem políticas Snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que deseja proteger.
   - Opcionalmente, filtre as linhas para mostrar apenas volumes com determinados tipos de volume, estilos e muito mais para facilitar a seleção.
   - Depois de selecionar o primeiro volume, você pode selecionar todos os volumes FlexVol (volumes FlexGroup podem ser selecionados um de cada vez somente). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e marque a caixa na linha de título. (

).
   - Para fazer backup de volumes individuais, marque a caixa para cada volume (

).

2. Selecione **seguinte**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Quer você queira uma ou todas as opções de backup: Snapshots locais, replicação e backup no storage de objetos
- Arquitetura
- Política de instantâneo local
- Destino e política de replicação

> Se os volumes escolhidos tiverem políticas de Snapshot e replicação diferentes das políticas selecionadas nesta etapa, as políticas existentes serão sobrescritas.

- Backup para informações de armazenamento de objetos (provedor, criptografia, rede, política de backup e opções de exportação).

Passos

1. Na página Definir estratégia de backup, escolha uma ou todas as opções a seguir. Todos os três são selecionados por padrão:
   - **Instantâneos locais**: Se você estiver executando replicação ou fazendo backup em armazenamento de objetos, os snapshots locais devem ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP.
   - **Backup**: Faz backup de volumes para armazenamento de objetos.
2. **Arquitetura**: Se você escolheu replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascading**: As informações fluem do sistema de armazenamento primário para o secundário e do armazenamento secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do sistema de armazenamento primário para o secundário *e* do armazenamento primário para o armazenamento de objetos.

     Para obter detalhes sobre essas arquiteturas, "Planeje sua jornada de proteção"consulte .
3. **Snapshot local**: Escolha uma política Snapshot existente ou crie uma.

   > Para criar uma política personalizada antes de ativar a cópia de segurança, "Crie uma política"consulte .

   Para criar uma política, selecione **criar nova política** e faça o seguinte:
   - Introduza o nome da política.
   - Selecione até 5 programações, normalmente de frequências diferentes.
   - Selecione **criar**.
4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o ambiente de trabalho de destino e SVM. Opcionalmente, selecione o agregado de destino ou agregados e o prefixo ou sufixo que será adicionado ao nome do volume replicado.

- **Política de replicação**: Escolha uma política de replicação existente ou crie uma.

  Para criar uma política personalizada antes de ativar a replicação, "Crie uma política"consulte .

  Para criar uma política, selecione **criar nova política** e faça o seguinte:

  - Introduza o nome da política.
  - Selecione até 5 programações, normalmente de frequências diferentes.
  - Selecione **criar**.

5. **Fazer backup para Objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Fornecedor**: Selecione **Google Cloud**.
   - **Configurações do provedor**: Insira os detalhes do provedor e a região onde os backups serão armazenados.

     Crie um novo bucket ou selecione um existente.

   - **Chave de criptografia**: Se você criou um novo bucket do Google, insira as informações da chave de criptografia fornecidas pelo provedor. Escolha se você usará as chaves de criptografia padrão do Google Cloud ou escolha suas próprias chaves gerenciadas pelo cliente na sua conta do Google para gerenciar a criptografia de seus dados.

     Se você optar por usar suas próprias chaves gerenciadas pelo cliente, insira o cofre de chaves e as informações da chave.

     Se você escolheu um bucket existente do Google Cloud, as informações de criptografia já estão disponíveis, para que você não precise inseri-lo agora.

   - **Política de backup**: Selecione uma política de armazenamento de backup para objeto existente ou crie uma.

     Para criar uma política personalizada antes de ativar a cópia de segurança, "Crie uma política"consulte .

     Para criar uma política, selecione **criar nova política** e faça o seguinte:

     - Introduza o nome da política.
     - Selecione até 5 programações, normalmente de frequências diferentes.
     - Selecione **criar**.

   - **Exportar cópias Snapshot existentes para o armazenamento de objetos como cópias de backup**: Se houver cópias Snapshot locais para volumes neste ambiente de trabalho que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este ambiente de trabalho (por exemplo, diário, semanal, etc.), esse prompt adicional será exibido. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup para garantir a proteção mais completa para seus volumes.
6. Selecione **seguinte**.

Reveja as suas seleções

Esta é a oportunidade de rever as suas seleções e fazer ajustes, se necessário.

Passos

1. Na página Review (Revisão), reveja as suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos de política Snapshot com os rótulos de política de replicação e backup**. Isso cria snapshots com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O backup e a recuperação do BlueXP começam a fazer os backups iniciais dos seus volumes. A transferência de linha de base do volume replicado e do arquivo de backup inclui uma cópia completa dos dados do sistema de storage primário. As transferências subsequentes contêm cópias diferenciais dos dados do sistema de storage primário contidos nas cópias Snapshot.

Um volume replicado é criado no cluster de destino que será sincronizado com o volume do sistema de storage primário.

Um bucket do Google Cloud Storage é criado na conta de serviço indicada pela chave de acesso do Google e chave secreta que você inseriu, e os arquivos de backup são armazenados lá.

Os backups estão associados à classe de armazenamento *Standard* por padrão. Você pode usar as classes de armazenamento *Nearline*, *Coldline* ou *Archive* de menor custo. No entanto, você configura a classe de armazenamento por meio do Google, não pela interface do usuário de backup e recuperação do BlueXP . Consulte o tópico do Google "Alterar a classe de armazenamento padrão de um balde" para obter detalhes.

O Painel de backup de volume é exibido para que você possa monitorar o estado dos backups.

Também pode monitorizar o estado dos trabalhos de cópia de segurança e restauro utilizando o "Painel monitorização de trabalhos".

Mostrar os comandos API

Você pode querer exibir e, opcionalmente, copiar os comandos API usados no assistente Ativar backup e recuperação. Você pode querer fazer isso para automatizar a ativação de backup em futuros ambientes de trabalho.

Passos

1. No assistente Ativar backup e recuperação, selecione **Exibir solicitação de API**.
2. Para copiar os comandos para a área de transferência, selecione o ícone **Copiar**.

O que se segue?

- Você pode "gerencie seus arquivos de backup e políticas de backup". Isso inclui iniciar e parar backups, excluir backups, adicionar e alterar o agendamento de backup e muito mais.
- Você pode "gerencie as configurações de backup no nível do cluster". Isso inclui alterar a largura de banda da rede disponível para fazer upload de backups para o armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Você também pode "restaure volumes, pastas ou arquivos individuais a partir de um arquivo de backup"acessar um sistema Cloud Volumes ONTAP no Google ou um sistema ONTAP no local.

Fazer backup de dados ONTAP on-premises para o Amazon S3

Conclua algumas etapas para começar a fazer backup de dados de volume de seus sistemas ONTAP locais para um sistema de storage secundário e para o storage de nuvem Amazon S3.

"Sistemas ONTAP no local" incluem sistemas FAS, AFF e ONTAP Select.

Início rápido

Comece rapidamente seguindo estes passos. Os detalhes de cada etapa são fornecidos nas seções a seguir deste tópico.

1 Identifique o método de conexão que você usará

Escolha se você conetará seu cluster do ONTAP local diretamente ao AWS S3 pela Internet pública ou se usará uma VPN ou o AWS Direct Connect e roteará o tráfego por meio de uma interface de endpoint VPC privada para o AWS S3.

Identificar o método de ligação.

2 Prepare o conetor BlueXP

Se você já tiver um conetor implantado na AWS VPC ou no local, tudo estará pronto. Caso contrário, você precisará criar um BlueXP Connector para fazer backup dos dados do ONTAP no storage AWS S3. Você também precisará personalizar as configurações de rede para o conetor para que ele possa se conetar ao AWS S3.

Saiba como criar um conetor e como definir as definições de rede necessárias.

3 Verifique os requisitos de licença

Você precisará verificar os requisitos de licença para AWS e BlueXP .

Verifique os requisitos de licençaConsulte a .

4 Preparar os clusters do ONTAP

Descubra os clusters do ONTAP no BlueXP , verifique se os clusters atendem aos requisitos mínimos e personalize as configurações de rede para que os clusters possam se conectar ao AWS S3.

Saiba como preparar os clusters do ONTAP.

5 Prepare o Amazon S3 como destino de backup

Configure permissões para que o conetor crie e gerencie o bucket do S3. Você também precisará configurar permissões para o cluster do ONTAP no local para que ele possa ler e gravar dados no bucket do S3.

Opcionalmente, você pode configurar suas próprias chaves gerenciadas personalizadas para criptografia de dados em vez de usar as chaves de criptografia padrão do Amazon S3. Saiba como preparar seu ambiente AWS S3 para receber backups do ONTAP.

6 Ative backups no ONTAP volumes

Selecione o ambiente de trabalho e clique em **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito. Em seguida, siga o assistente de configuração para selecionar as políticas de replicação e backup que você usará e os volumes que você deseja fazer backup.

Ative backups no ONTAP volumes.

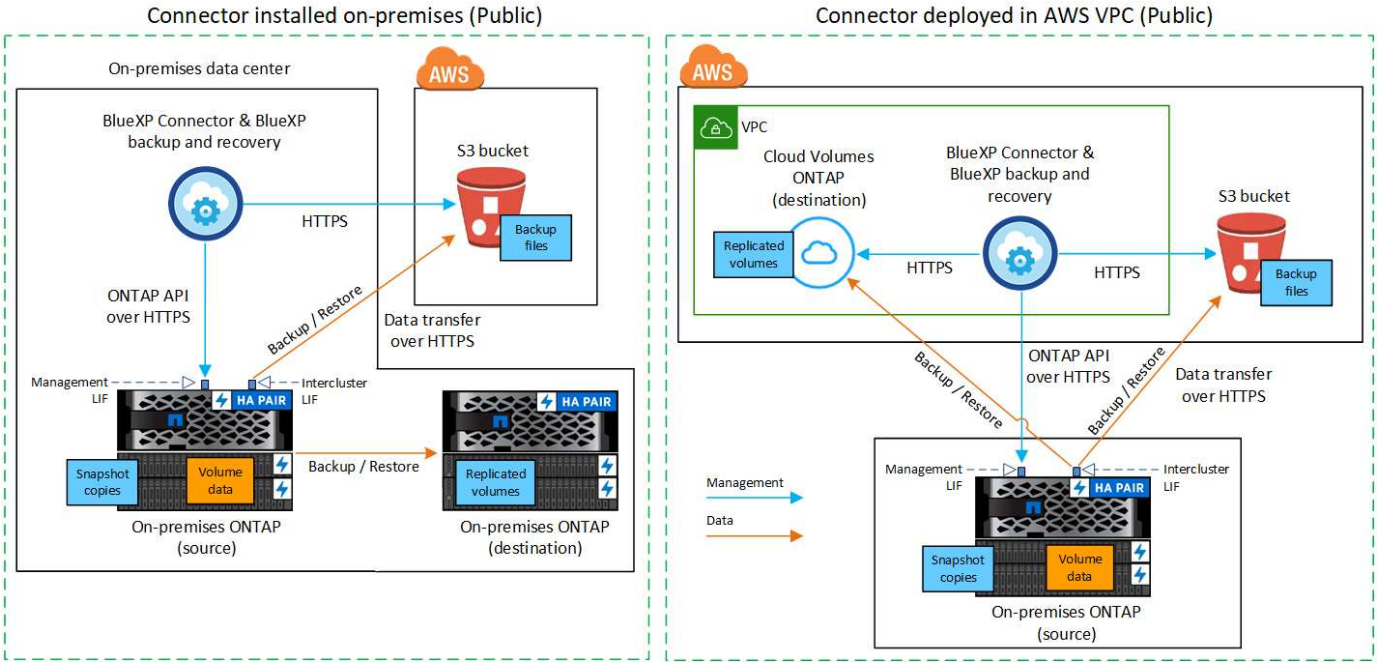
Identificar o método de ligação

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o AWS S3.

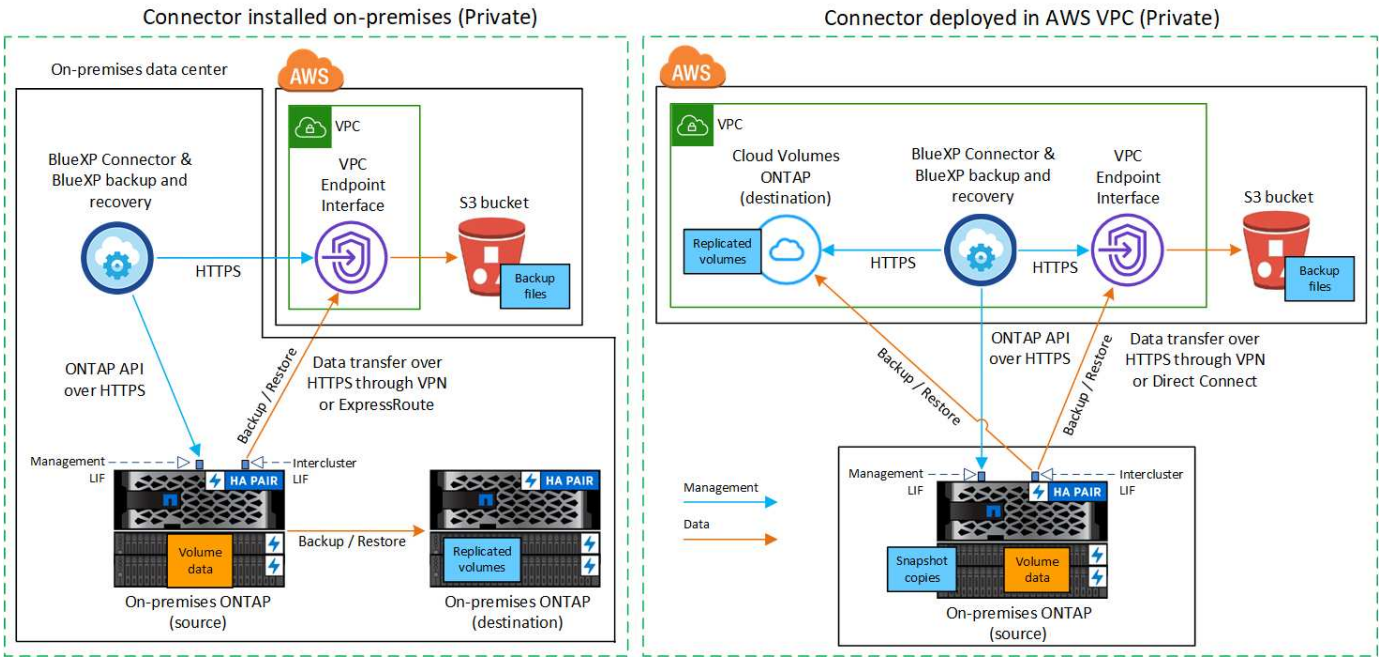
- * Conexão pública* - Conete diretamente o sistema ONTAP ao AWS S3 usando um endpoint S3 público.
- * Conexão privada* - Use uma VPN ou AWS Direct Connect e encaminhe o tráfego por meio de uma interface VPC Endpoint que usa um endereço IP privado.

Opcionalmente, você pode se conectar a um sistema ONTAP secundário para volumes replicados usando a conexão pública ou privada.

O diagrama a seguir mostra o método **public Connection** e as conexões que você precisa preparar entre os componentes. Você pode usar um conetor instalado no local ou um conetor implantado na VPC da AWS.



O diagrama a seguir mostra o método **private Connection** e as conexões que você precisa preparar entre os componentes. Você pode usar um conetor instalado no local ou um conetor implantado na VPC da AWS.



Prepare o conetor BlueXP

O conetor BlueXP é o software principal para a funcionalidade BlueXP . É necessário um conetor para fazer backup e restaurar os dados do ONTAP.

Crie ou troque os conetores

Se você já tiver um conetor implantado na AWS VPC ou no local, tudo estará pronto.

Caso contrário, você precisará criar um conetor em um desses locais para fazer backup dos dados do ONTAP no storage AWS S3. Não é possível usar um conetor que seja implantado em outro provedor de nuvem.

- "Saiba mais sobre conetores"
- "Instale um conetor na AWS"
- "Instale um conetor nas suas instalações"
- "Instale um conetor em uma região do AWS GovCloud"

  Backup e recuperação do BlueXP são suportados nas regiões GovCloud quando o conetor é implantado na nuvem, não quando ele é instalado em suas instalações. Além disso, você deve implantar o conetor no AWS Marketplace. Não é possível implantar o conetor em uma região do governo a partir do site SaaS da BlueXP .

Preparar os requisitos de rede do conetor

Certifique-se de que os seguintes requisitos de rede são atendidos:

- Certifique-se de que a rede onde o conetor está instalado permite as seguintes ligações:
  - Uma conexão HTTPS pela porta 443 ao serviço de backup e recuperação do BlueXP e ao storage de objetos S3 ("consulte a lista de endpoints")
  - Uma conexão HTTPS pela porta 443 ao LIF de gerenciamento de cluster do ONTAP
  - Regras adicionais de grupo de segurança de entrada e saída são necessárias para implantações AWS

e AWS GovCloud. "Regras para o conetor na AWS"Consulte para obter detalhes.

- "Certifique-se de que o conetor tem permissões para gerenciar o bucket do S3".
- 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 (uma conexão **privada**), será necessário habilitar uma interface de endpoint VPC para o S3. Veja como configurar uma interface de endpoint de VPC.

Verifique os requisitos de licença

Você precisará verificar os requisitos de licença para AWS e BlueXP :

- Antes de ativar o backup e a recuperação do BlueXP para seu cluster, você precisará inscrever-se em uma oferta de mercado BlueXP de pagamento conforme o uso (PAYGO) da AWS ou comprar e ativar uma licença BYOL de backup e recuperação do BlueXP da NetApp. Essas licenças são para sua conta e podem ser usadas em vários sistemas.
  - Para o licenciamento PAYGO de backup e recuperação do BlueXP , você precisará de uma assinatura do "Oferta da NetApp BlueXP no AWS Marketplace". A cobrança do backup e recuperação do BlueXP é feita por meio dessa assinatura.
  - Para o licenciamento BYOL de backup e recuperação do BlueXP , você precisará do número de série do NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Saiba como gerenciar suas licenças BYOL".
- Você precisa ter uma assinatura da AWS para o espaço de armazenamento de objetos onde seus backups estarão localizados.

Regiões suportadas

É possível criar backups de sistemas locais para o Amazon S3 em todas as "Onde o Cloud Volumes ONTAP é suportado"regiões , incluindo regiões do AWS GovCloud. Você especifica a região onde os backups serão armazenados quando você configurar o serviço.

Preparar os clusters do ONTAP

Você precisará preparar seu sistema ONTAP de origem no local e qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local.

Preparar os clusters do ONTAP envolve as etapas a seguir:

- Descubra os seus sistemas ONTAP no BlueXP
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos
- Verificar os requisitos de rede do ONTAP para replicação de volumes

Descubra os seus sistemas ONTAP no BlueXP

Tanto o sistema ONTAP de origem no local quanto qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local devem estar disponíveis no BlueXP Canvas.

Você precisará saber o endereço IP de gerenciamento de cluster e a senha da conta de usuário admin para adicionar o cluster. "Saiba como descobrir um cluster".

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP são atendidos:

- É recomendado um mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior.
- Uma licença SnapMirror (incluída como parte do pacote Premium ou do pacote de proteção de dados).

  Observação: o "pacote de nuvem híbrida" não é necessário ao usar o backup e a recuperação do BlueXP .

  Aprenda a "gerencie suas licenças de cluster".

- A hora e o fuso horário estão definidos corretamente. Aprenda a "configure a hora do cluster".
- Se você quiser replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar dados.

  "Veja versões compatíveis do ONTAP para relacionamentos do SnapMirror".

Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos

Você deve configurar os seguintes requisitos no sistema que se coneta ao storage de objetos.

- Para uma arquitetura de backup fan-out, configure as seguintes configurações no sistema *Primary*.
- Para uma arquitetura de backup em cascata, configure as seguintes configurações no sistema *secundário*.

São necessários os seguintes requisitos de rede de cluster do ONTAP:

- O cluster requer uma conexão HTTPS de entrada do conetor para o LIF de gerenciamento de cluster.
- É necessário um LIF entre clusters em cada nó do ONTAP que hospeda os volumes que você deseja fazer backup. Essas LIFs entre clusters devem ser capazes de acessar o armazenamento de objetos.

  O cluster inicia uma conexão HTTPS de saída pela porta 443 das LIFs entre clusters para o armazenamento Amazon S3 para operações de backup e restauração. O ONTAP lê e grava dados no storage de objetos e a partir dele. O storage de objetos nunca é iniciado, ele apenas responde.

- As LIFs entre clusters devem estar associadas ao *espaço_IPspace* que o ONTAP deve usar para se conetar ao armazenamento de objetos. "Saiba mais sobre IPspaces".

  Ao configurar o backup e a recuperação do BlueXP , você será solicitado a usar o IPspace. Você deve escolher o espaço IPspace ao qual essas LIFs estão associadas. Esse pode ser o espaço IPspace "padrão" ou um espaço IPspace personalizado que você criou.

  Se você usa um IPspace diferente de "padrão", talvez seja necessário criar uma rota estática para obter acesso ao armazenamento de objetos.

  Todas as LIFs entre clusters dentro do IPspace devem ter acesso ao armazenamento de objetos. Se você não puder configurar isso para o IPspace atual, precisará criar um IPspace dedicado onde todas as LIFs entre clusters tenham acesso ao armazenamento de objetos.

- Os servidores DNS devem ter sido configurados para a VM de armazenamento onde os volumes estão localizados. Consulte como "Configurar serviços DNS para o SVM" .
- Atualize regras de firewall, se necessário, para permitir conexões de backup e recuperação do BlueXP do ONTAP para o armazenamento de objetos através da porta 443 e tráfego de resolução de nomes da VM

de armazenamento para o servidor DNS através da porta 53 (TCP/UDP).

- Se você estiver usando um endpoint de interface VPC privada na AWS para a conexão S3, então, para que o HTTPS/443 seja usado, você precisará carregar o certificado de endpoint S3 no cluster do ONTAP. Veja como configurar uma interface de endpoint de VPC e carregar o certificado S3.
- "Verifique se o cluster do ONTAP tem permissões para acessar o bucket do S3".

Verificar os requisitos de rede do ONTAP para replicação de volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o backup e a recuperação do BlueXP , certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede da ONTAP no local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da rede corporativa à rede virtual no provedor de nuvem. Normalmente, esta é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou sistemas locais, revise os requisitos de peering para sistemas ONTAP locais. "Veja os pré-requisitos para peering de cluster na documentação do ONTAP".

Requisitos de rede da 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.

Prepare o Amazon S3 como destino de backup

Preparar o Amazon S3 como destino de backup envolve as seguintes etapas:

- Configure S3 permissões.
- (Opcional) Crie seus próprios buckets do S3. (O serviço criará buckets para você, se você quiser.)
- (Opcional) Configurar chaves AWS gerenciadas pelo cliente para criptografia de dados.
- (Opcional) Configure seu sistema para uma conexão privada usando uma interface de endpoint VPC.

Configure S3 permissões

Você precisará configurar dois conjuntos de permissões:

- Permissões para que o conetor crie e gerencie o bucket do S3.
- Permissões para o cluster do ONTAP no local para que ele possa ler e gravar dados no bucket do S3.

Passos

1. Certifique-se de que o conetor tem as permissões necessárias. Para obter detalhes, "Permissões de política do BlueXP " consulte .

Ao criar backups nas regiões da AWS China, você precisa alterar o Nome de recurso da AWS "ARN" em todas as seções *Resource* nas políticas do IAM de "aws" para "aws-cn"; por exemplo `arn:aws-cn:s3:::netapp-backup-*`.

2. Quando você ativa o serviço, o assistente Backup solicitará que você insira uma chave de acesso e uma chave secreta. Essas credenciais são passadas para o cluster do ONTAP para que o ONTAP possa fazer backup e restaurar os dados para o bucket do S3. Para isso, você precisará criar um usuário do IAM com as seguintes permissões.

   Consulte a "Documentação da AWS: Criando uma função para delegar permissões a um usuário do IAM" .

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

Crie seus próprios baldes

Por padrão, o serviço cria buckets para você. Ou, se você quiser usar seus próprios buckets, você pode criá-los antes de iniciar o assistente de ativação de backup e, em seguida, selecionar esses buckets no assistente.

"Saiba mais sobre como criar seus próprios buckets".

Se você criar seus próprios buckets, use um nome de bucket do "NetApp-backup". Se você precisar usar um nome personalizado, edite o `ontapcloud-instance-policy-netapp-backup` IAMRole para os CVOs existentes e adicione a seguinte lista às permissões do S3. Você precisa incluir `"Resource": "arn:aws:s3:::*"` e atribuir todas as permissões necessárias que precisam ser associadas ao bucket.

```
"Action": [ "S3 S3 S3 S3:ListBucket" "S3 S3 S3 S3:GetBucketLocation" ] "Resource": "arn:aws:S3 S3 S3 S3:::*", "Effect": "Allow", "Action": [ "S3:GetObject", "S3:PutObject", "S3
```

Configurar chaves AWS gerenciadas pelo cliente para criptografia de dados

Se você quiser usar as chaves de criptografia padrão do Amazon S3 para criptografar os dados passados entre o cluster no local e o bucket do S3, tudo estará definido porque a instalação padrão usa esse tipo de criptografia.

Se, em vez disso, você quiser usar suas próprias chaves gerenciadas pelo cliente para criptografia de dados em vez de usar as chaves padrão, precisará ter as chaves gerenciadas de criptografia já configuradas antes de iniciar o assistente de backup e recuperação do BlueXP . "Consulte como usar suas próprias chaves".

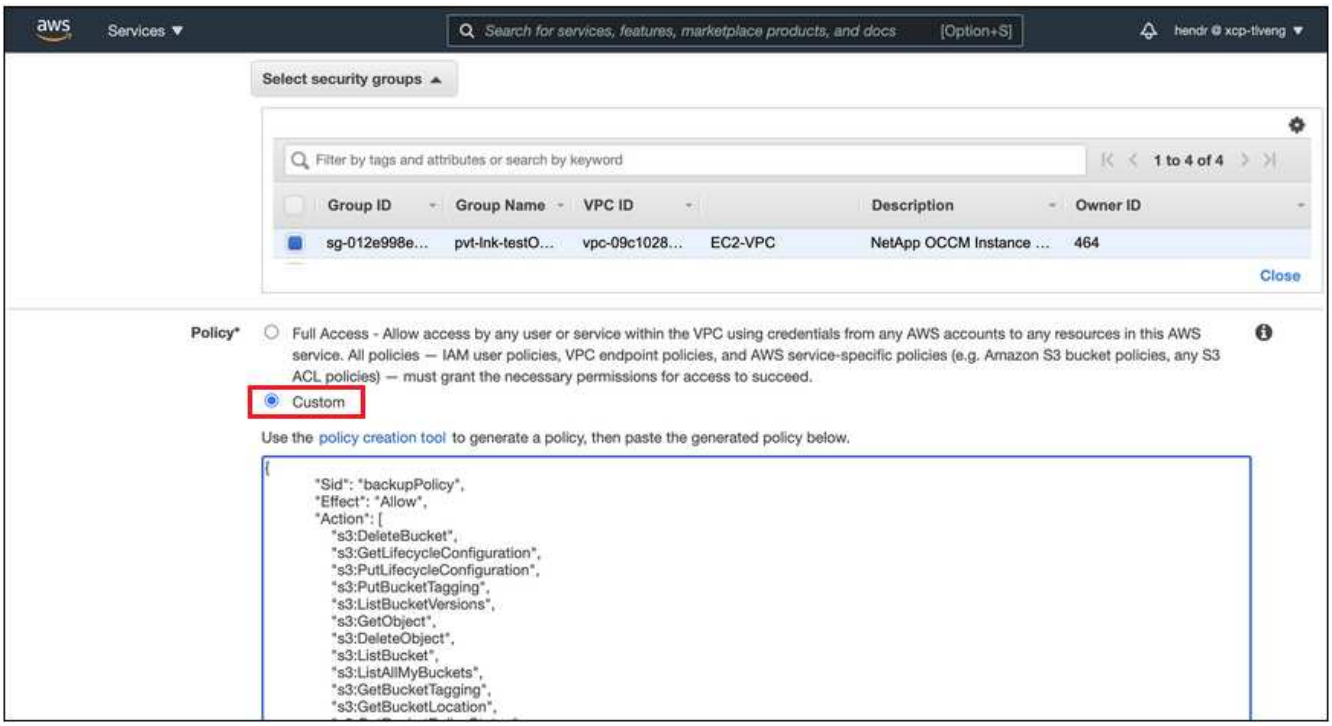
Configure seu sistema para uma conexão privada usando uma interface de endpoint VPC

Se você quiser usar uma conexão de internet pública padrão, todas as permissões serão definidas pelo conetor e não há mais nada que você precise fazer. Esse tipo de conexão é mostrado no "primeiro diagrama".

Se você quiser ter uma conexão mais segura pela Internet do data center local para a VPC, há uma opção para selecionar uma conexão do AWS PrivateLink no assistente de ativação do backup. É necessário se você planeja usar uma VPN ou o AWS Direct Connect para conetar seu sistema local por meio de uma interface VPC Endpoint que use um endereço IP privado. Este tipo de ligação é apresentado no "segundo diagrama".

Passos

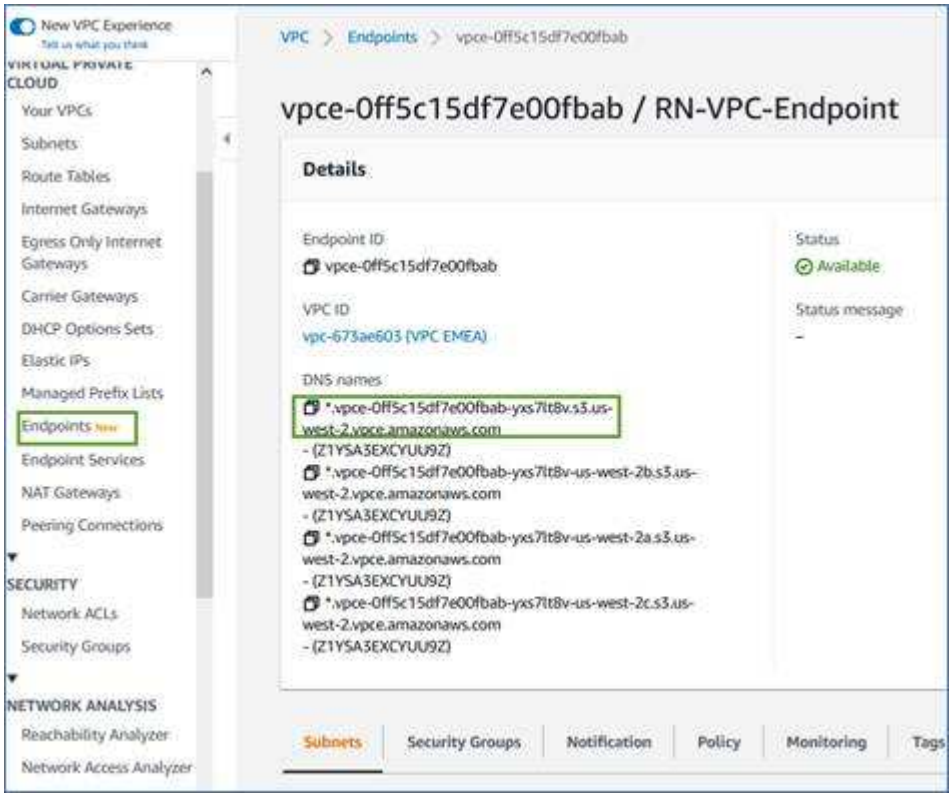
1. Crie uma configuração de endpoint de interface usando o console Amazon VPC ou a linha de comando. "Consulte detalhes sobre como usar o AWS PrivateLink para Amazon S3".
2. Modifique a configuração do grupo de segurança associada ao conetor BlueXP . Você deve alterar a política para "Personalizado" (de "Acesso total"), e você deveAdicione as permissões S3 da política de backup, como mostrado anteriormente.



Se você estiver usando a porta 80 (HTTP) para comunicação com o endpoint privado, você está tudo definido. Você pode habilitar o backup e a recuperação do BlueXP agora no cluster.

Se você estiver usando a porta 443 (HTTPS) para comunicação com o endpoint privado, copie o certificado do endpoint VPC S3 e adicione-o ao cluster do ONTAP, conforme mostrado nas próximas 4 etapas.

3. Obtenha o nome DNS do endpoint no Console AWS.



4. Obtenha o certificado do endpoint VPC S3. Você faz isso "Fazer login na VM que hospeda o BlueXP Connector" executando o seguinte comando. Ao inserir o nome DNS do endpoint, adicione "bucket" ao início, substituindo o "*":

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-
0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443
-showcerts
```

5. A partir da saída deste comando, copie os dados para o certificado S3 (todos os dados entre, e incluindo, as tags DE CERTIFICADO DE início / FIM):

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
…
…
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. Faça login na CLI do cluster do ONTAP e aplique o certificado copiado usando o seguinte comando (substitua o nome da VM de storage):

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

Ative backups no ONTAP volumes

Ative os backups a qualquer momento diretamente do seu ambiente de trabalho no local.

Um assistente leva você através dos seguintes passos principais:

- Selecione os volumes que deseja fazer backup
- Defina a estratégia de backup
- Reveja as suas seleções

Você também pode Mostrar os comandos APIna etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para futuros ambientes de trabalho.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:

- Na tela BlueXP , selecione o ambiente de trabalho e selecione **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.

  Se o destino do Amazon S3 para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster do ONTAP para o armazenamento de objetos do Amazon S3.

- Selecione **volumes** na barra de backup e recuperação. Na guia volumes, selecione o ícone **ações** ••• e selecione **Ativar Backup** para um único volume (que ainda não tem replicação ou backup para armazenamento de objetos já ativado).

A página Introdução do assistente mostra as opções de proteção, incluindo snapshots locais, replicação e backups. Se você fez a segunda opção nesta etapa, a página Definir estratégia de backup será exibida com um volume selecionado.

2. Continue com as seguintes opções:
   - Se já tiver um conetor BlueXP , está tudo definido. Basta selecionar **seguinte**.
   - Se você ainda não tiver um conetor BlueXP , a opção **Adicionar um conetor** será exibida. Prepare o conetor BlueXP Consulte a .

Selecione os volumes que deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem uma ou mais das seguintes opções: Política de snapshot, política de replicação, política de backup para objeto.

Você pode optar por proteger o FlexVol ou o FlexGroup volumes. No entanto, não é possível selecionar uma combinação desses volumes ao ativar o backup para um ambiente de trabalho. Veja como "ative o backup para volumes adicionais no ambiente de trabalho"(FlexVol ou FlexGroup) depois de configurar o backup para os volumes iniciais.

- Você pode ativar um backup apenas em um único volume FlexGroup de cada vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock. Todos os volumes devem ter o SnapLock Enterprise ativado ou o SnapLock desativado.

Passos

Observe que se os volumes escolhidos já tiverem políticas Snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que deseja proteger.
   - Opcionalmente, filtre as linhas para mostrar apenas volumes com determinados tipos de volume, estilos e muito mais para facilitar a seleção.
   - Depois de selecionar o primeiro volume, você pode selecionar todos os volumes FlexVol (volumes FlexGroup podem ser selecionados um de cada vez somente). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e marque a caixa na linha de título. (

).
   - Para fazer backup de volumes individuais, marque a caixa para cada volume (

).
2. Selecione **seguinte**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Quer você queira uma ou todas as opções de backup: Snapshots locais, replicação e backup no storage de objetos
- Arquitetura
- Política de instantâneo local
- Destino e política de replicação

> Se os volumes escolhidos tiverem políticas de Snapshot e replicação diferentes das políticas selecionadas nesta etapa, as políticas existentes serão sobrescritas.

- Backup para informações de armazenamento de objetos (provedor, criptografia, rede, política de backup e opções de exportação).

Passos

1. Na página Definir estratégia de backup, escolha uma ou todas as opções a seguir. Todos os três são selecionados por padrão:
   - **Instantâneos locais**: Se você estiver executando replicação ou fazendo backup em armazenamento de objetos, os snapshots locais devem ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP.
   - **Backup**: Faz backup de volumes para armazenamento de objetos.
2. **Arquitetura**: Se você escolheu replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascading**: As informações fluem do armazenamento primário para o secundário para o armazenamento de objetos e do armazenamento secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do primário para o secundário *e* do armazenamento primário para o objeto.

     Para obter detalhes sobre essas arquiteturas, "Planeje sua jornada de proteção"consulte .
3. **Snapshot local**: Escolha uma política Snapshot existente ou crie uma política.

   > Para criar uma política personalizada antes de ativar a captura Instantânea, "Crie uma política"consulte .

4. Para criar uma política, selecione **criar nova política** e faça o seguinte:
   - Introduza o nome da política.
   - Selecione até 5 programações, normalmente de frequências diferentes.
     - Para políticas de backup para objeto, defina as configurações DataLock e proteção contra ransomware. Para obter detalhes sobre DataLock e proteção contra ransomware, "Configurações de política de backup para objeto"consulte .
   - Selecione **criar**.
5. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o ambiente de trabalho de destino e SVM. Opcionalmente, selecione o agregado de destino ou agregados e o prefixo ou sufixo que será adicionado ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma política.

Para criar uma política personalizada antes de ativar a replicação, "Crie uma política"consulte .

Para criar uma política, selecione **criar nova política** e faça o seguinte:

- Introduza o nome da política.
- Selecione até 5 programações, normalmente de frequências diferentes.
- Selecione **criar**.

6. **Fazer backup para Objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Fornecedor**: Selecione **Amazon Web Services**.
   - **Configurações do provedor**: Insira os detalhes do provedor e a região da AWS onde os backups serão armazenados.

     A chave de acesso e a chave secreta destinam-se ao usuário do IAM criado para dar ao cluster do ONTAP acesso ao bucket do S3.

   - **Bucket**: Escolha um bucket S3 existente ou crie um novo. Consulte a "Adicione S3 baldes".
   - **Chave de criptografia**: Se você criou um novo bucket do S3, insira as informações da chave de criptografia fornecidas pelo provedor. Escolha se você usará as chaves de criptografia padrão do Amazon S3 ou escolha suas próprias chaves gerenciadas pelo cliente na sua conta da AWS para gerenciar a criptografia de seus dados.

     Se você escolheu um bucket existente, as informações de criptografia já estão disponíveis, para que você não precise inseri-lo agora.

   - **Rede**: Escolha o IPspace e se você usará um endpoint privado. O endpoint privado está desativado por predefinição.
     i. O espaço de IPspace no cluster do ONTAP onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.
     ii. Opcionalmente, escolha se você usará um AWS PrivateLink que você configurou anteriormente. "Veja detalhes sobre como usar o AWS PrivateLink para Amazon S3".
   - **Política de backup**: Selecione uma política de backup existente ou crie uma política.

     Para criar uma política personalizada antes de ativar a cópia de segurança, "Crie uma política"consulte .

     Para criar uma política, selecione **criar nova política** e faça o seguinte:

     - Introduza o nome da política.
     - Selecione até 5 programações, normalmente de frequências diferentes.
     - Selecione **criar**.

   - **Exportar cópias Snapshot existentes para o armazenamento de objetos como cópias de backup**: Se houver cópias Snapshot locais para volumes neste ambiente de trabalho que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este ambiente de trabalho (por exemplo, diário, semanal, etc.), esse prompt adicional será exibido. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup para garantir a proteção mais completa para seus volumes.

7. Selecione **seguinte**.

Reveja as suas seleções

Esta é a oportunidade de rever as suas seleções e fazer ajustes, se necessário.

Passos

1. Na página Review (Revisão), reveja as suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos de política Snapshot com os rótulos de política de replicação e backup**. Isso cria snapshots com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O backup e a recuperação do BlueXP começam a fazer os backups iniciais dos seus volumes. A transferência de linha de base do volume replicado e do arquivo de backup inclui uma cópia completa dos dados do sistema de storage primário. As transferências subsequentes contêm cópias diferenciais dos dados primários contidos nas cópias Snapshot.

Um volume replicado é criado no cluster de destino que será sincronizado com o volume de armazenamento primário.

O bucket do S3 é criado na conta de serviço indicada pela chave de acesso S3 e chave secreta que você inseriu, e os arquivos de backup são armazenados lá. O Painel de backup de volume é exibido para que você possa monitorar o estado dos backups.

Também pode monitorizar o estado dos trabalhos de cópia de segurança e restauro utilizando o "Painel monitorização de trabalhos".

Mostrar os comandos API

Você pode querer exibir e, opcionalmente, copiar os comandos API usados no assistente Ativar backup e recuperação. Você pode querer fazer isso para automatizar a ativação de backup em futuros ambientes de trabalho.

Passos

1. No assistente Ativar backup e recuperação, selecione **Exibir solicitação de API**.
2. Para copiar os comandos para a área de transferência, selecione o ícone **Copiar**.

O que se segue?

- Você pode "gerencie seus arquivos de backup e políticas de backup". Isso inclui iniciar e parar backups, excluir backups, adicionar e alterar o agendamento de backup e muito mais.
- Você pode "gerencie as configurações de backup no nível do cluster". Isso inclui a alteração das chaves de armazenamento que o ONTAP usa para acessar o armazenamento na nuvem, alterar a largura de banda da rede disponível para carregar backups para o armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Você também pode "restaure volumes, pastas ou arquivos individuais a partir de um arquivo de backup"acessar um sistema Cloud Volumes ONTAP na AWS ou um sistema ONTAP no local.

Fazer backup de dados do ONTAP no local para o storage Azure Blob

Conclua algumas etapas para começar a fazer backup de dados de volume de seus sistemas ONTAP locais para um sistema de storage secundário e para o storage de Blob do Azure.

"Sistemas ONTAP no local" incluem sistemas FAS, AFF e ONTAP Select.

Início rápido

Comece rapidamente seguindo estes passos. Os detalhes de cada etapa são fornecidos nas seções a seguir deste tópico.

1 Identifique o método de conexão que você usará

Escolha se você conetará seu cluster ONTAP local diretamente ao Azure pela Internet pública ou se usará uma VPN ou Azure ExpressRoute e roteará o tráfego por meio de uma interface de endpoint VPC privada para o Azure.

Identificar o método de ligação.

2 Prepare o conetor BlueXP

Se você já tiver um conetor implantado em seu Azure VNet ou em suas instalações, então você está tudo pronto. Caso contrário, você precisará criar um BlueXP Connector para fazer backup dos dados do ONTAP para o armazenamento de Blobs do Azure. Você também precisará personalizar as configurações de rede para o conetor para que ele possa se conetar ao Azure.

Saiba como criar um conetor e como definir as definições de rede necessárias.

3 Verifique os requisitos de licença

Você precisará verificar os requisitos de licença para o Azure e o BlueXP .

Verifique os requisitos de licençaConsulte a .

4 Preparar os clusters do ONTAP

Descubra os clusters do ONTAP no BlueXP , verifique se os clusters atendem aos requisitos mínimos e personalize as configurações de rede para que os clusters possam se conectar ao Azure.

Saiba como preparar os clusters do ONTAP.

5 Prepare o Azure Blob como destino do backup

Configure permissões para que o conetor crie e gerencie o bucket do Azure. Você também precisará configurar permissões para o cluster do ONTAP no local para que ele possa ler e gravar dados no bucket do

Azure.

Opcionalmente, você pode configurar suas próprias chaves gerenciadas personalizadas para criptografia de dados em vez de usar as chaves de criptografia padrão do Azure. Saiba como preparar seu ambiente Azure para receber backups do ONTAP.

6 Ative backups no ONTAP volumes

Selecione o ambiente de trabalho e clique em **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito. Em seguida, siga o assistente de configuração para selecionar as políticas de replicação e backup que você usará e os volumes que você deseja fazer backup.

Ative backups no ONTAP volumes.

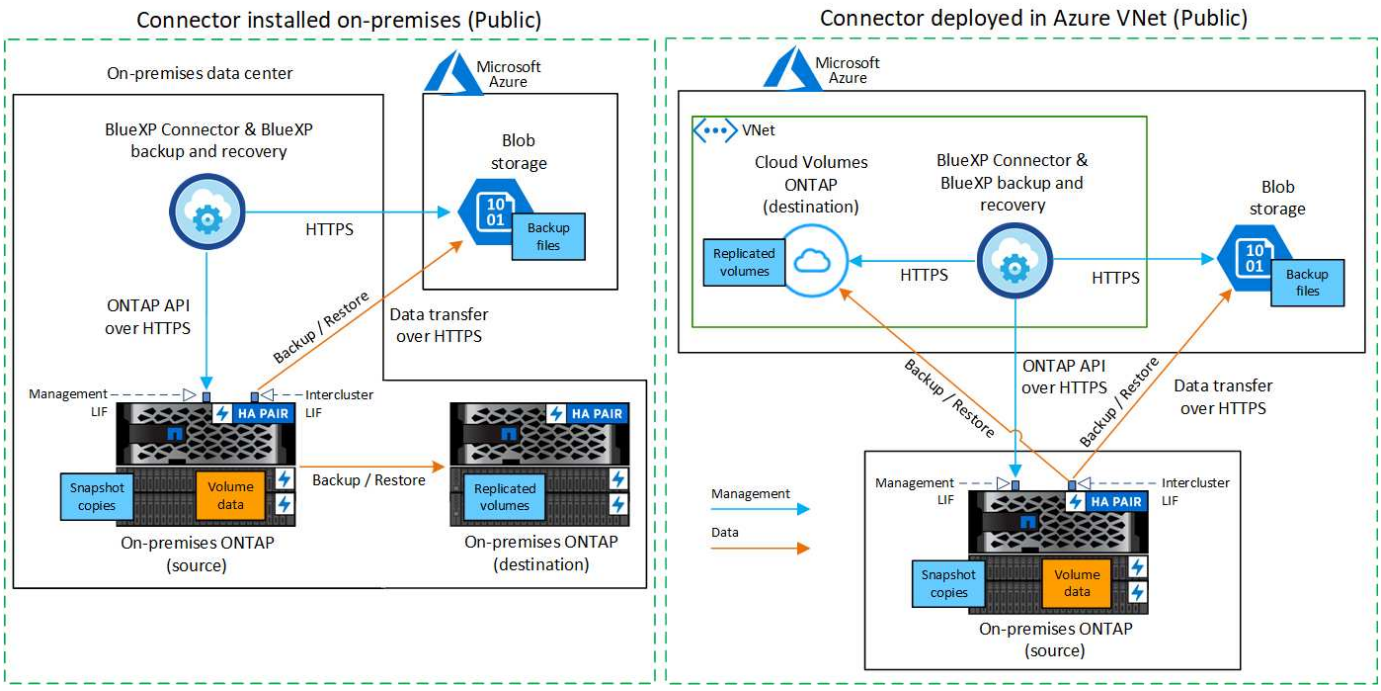
Identificar o método de ligação

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o Azure Blob.

- **Conexão pública** - Conete diretamente o sistema ONTAP ao armazenamento de Blobs do Azure usando um endpoint público do Azure.
- **Conexão privada** - Use uma VPN ou ExpressRoute e encaminhe o tráfego através de um endpoint privado VNet que usa um endereço IP privado.

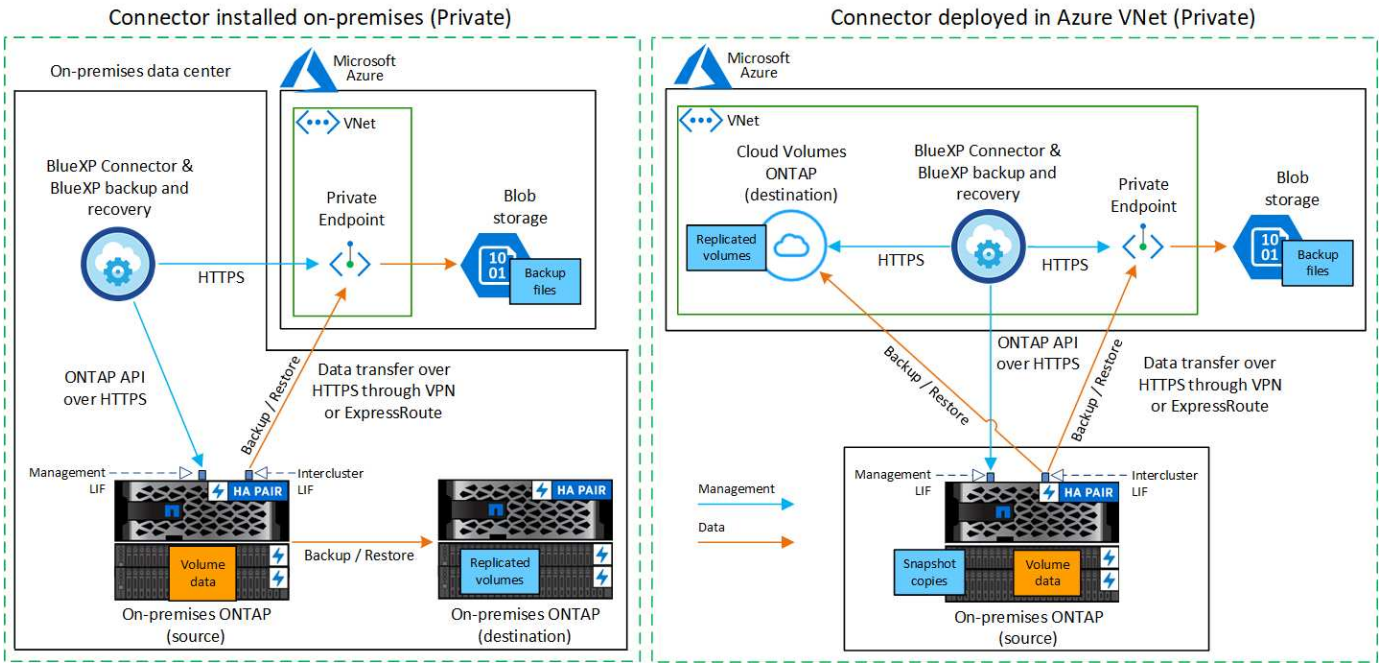
Opcionalmente, você pode se conectar a um sistema ONTAP secundário para volumes replicados usando a conexão pública ou privada.

O diagrama a seguir mostra o método **public Connection** e as conexões que você precisa preparar entre os componentes. Você pode usar um conetor instalado em suas instalações ou um conetor que você implantou no Azure VNet.



O diagrama a seguir mostra o método **private Connection** e as conexões que você precisa preparar entre os

componentes. Você pode usar um conetor instalado em suas instalações ou um conetor que você implantou no Azure VNet.



Prepare o conetor BlueXP

O conetor BlueXP é o software principal para a funcionalidade BlueXP . É necessário um conetor para fazer backup e restaurar os dados do ONTAP.

Crie ou troque os conetores

Se você já tiver um conetor implantado em seu Azure VNet ou em suas instalações, então você está tudo pronto.

Caso contrário, você precisará criar um conector em um desses locais para fazer backup de dados do ONTAP para o storage de Blob do Azure. Não é possível usar um conetor que seja implantado em outro provedor de nuvem.

- "Saiba mais sobre conetores"
- "Instale um conetor no Azure"
- "Instale um conetor nas suas instalações"
- "Instale um conetor em uma região do Azure Government"

  O backup e a recuperação do BlueXP são suportados nas regiões do governo do Azure quando o conetor é implantado na nuvem, não quando ele é instalado em suas instalações. Além disso, você deve implantar o conetor no Azure Marketplace. Não é possível implantar o conetor em uma região do governo a partir do site SaaS da BlueXP .

Prepare 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 HTTPS pela porta 443 ao serviço de backup e recuperação do BlueXP e ao storage de objetos Blob ("consulte a lista de endpoints")
   - Uma conexão HTTPS pela porta 443 ao LIF de gerenciamento de cluster do ONTAP
   - Para que a funcionalidade de pesquisa e restauração de backup e recuperação do BlueXP funcione, a porta 1433 deve estar aberta para comunicação entre o conetor e os serviços SQL do Azure Synapse.
   - Regras adicionais de grupo de segurança de entrada são necessárias para implantações do Azure e do Azure Government. "Regras para o conetor no Azure"Consulte para obter detalhes.
2. Ative um endpoint privado do VNet para o armazenamento do Azure. Isso é necessário se você tiver uma conexão ExpressRoute ou VPN do cluster ONTAP para o VNet e quiser que a comunicação entre o conetor e o armazenamento Blob permaneça em sua rede privada virtual (uma conexão **privada**).

Verifique ou adicione permissões ao conetor

Para usar a funcionalidade de pesquisa e restauração de backup e recuperação do BlueXP , você precisa ter permissões específicas na função do conetor para que ele possa acessar a conta de armazenamento de dados e espaço de trabalho do Synapse do Azure. Consulte as permissões abaixo e siga as etapas se precisar modificar a política.

Antes de começar

Você deve Registrar o Fornecedor de recursos do Azure Synapse Analytics (chamado "Microsoft.Synapse") com sua assinatura. "Veja como registar este fornecedor de recursos para a sua subscrição". Você deve ser a assinatura **proprietário** ou **Colaborador** para Registrar o provedor de recursos.

Passos

1. Identifique a função atribuída à máquina virtual do conetor:
   a. No portal do Azure, abra o serviço máquinas virtuais.
   b. Selecione a máquina virtual do conetor.
   c. Em **Configurações**, selecione **identidade**.
   d. Selecione **atribuições de função do Azure**.
   e. Anote a função personalizada atribuída à máquina virtual do conetor.
2. Atualize a função personalizada:
   a. No portal do Azure, abra sua assinatura do Azure.
   b. Selecione **Access Control (IAM) > Roles**.
   c. Selecione a elipse (**…**) para a função personalizada e, em seguida, selecione **Edit**.
   d. Selecione **JSON** e adicione as seguintes permissões:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Veja o formato JSON completo da política"

e. Selecione **Revisão e atualização** e, em seguida, selecione **Atualização**.

Verifique os requisitos de licença

Você precisará verificar os requisitos de licença para o Azure e o BlueXP :

- Antes de ativar o backup e a recuperação do BlueXP para seu cluster, você precisará inscrever-se em uma oferta de mercado BlueXP pay-as-you-go (PAYGO) do Azure ou comprar e ativar uma licença BYOL de backup e recuperação do BlueXP da NetApp. Essas licenças são para sua conta e podem ser usadas em vários sistemas.
  - Para o licenciamento PAYGO de backup e recuperação do BlueXP , você precisará de uma assinatura do "Oferta de NetApp BlueXP no mercado Azure". A cobrança do backup e recuperação do BlueXP é feita por meio dessa assinatura.
  - Para o licenciamento BYOL de backup e recuperação do BlueXP , você precisará do número de série do NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Saiba como gerenciar suas licenças BYOL".
- Você precisa ter uma assinatura do Azure para o espaço de armazenamento de objetos onde seus backups estarão localizados.

Regiões suportadas

É possível criar backups de sistemas locais para o Azure Blob em todas as "Onde o Cloud Volumes ONTAP é suportado"regiões , incluindo regiões do Azure Government. Você especifica a região onde os backups serão armazenados quando você configurar o serviço.

Preparar os clusters do ONTAP

Você precisará preparar seu sistema ONTAP de origem no local e qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local.

Preparar os clusters do ONTAP envolve as etapas a seguir:

- Descubra os seus sistemas ONTAP no BlueXP
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos
- Verificar os requisitos de rede do ONTAP para replicação de volumes

Descubra os seus sistemas ONTAP no BlueXP

Tanto o sistema ONTAP de origem no local quanto qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local devem estar disponíveis no BlueXP Canvas.

Você precisará saber o endereço IP de gerenciamento de cluster e a senha da conta de usuário admin para adicionar o cluster. "Saiba como descobrir um cluster".

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP são atendidos:

- É recomendado um mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior.
- Uma licença SnapMirror (incluída como parte do pacote Premium ou do pacote de proteção de dados).

  Observação: o "pacote de nuvem híbrida" não é necessário ao usar o backup e a recuperação do

BlueXP .

Aprenda a "gerencie suas licenças de cluster".

- A hora e o fuso horário estão definidos corretamente. Aprenda a "configure a hora do cluster".
- Se você quiser replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar dados.

  "Veja versões compatíveis do ONTAP para relacionamentos do SnapMirror".

Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos

Você deve configurar os seguintes requisitos no sistema que se coneta ao storage de objetos.

- Para uma arquitetura de backup fan-out, configure as seguintes configurações no sistema *Primary*.
- Para uma arquitetura de backup em cascata, configure as seguintes configurações no sistema *secundário*.

São necessários os seguintes requisitos de rede de cluster do ONTAP:

- O cluster do ONTAP inicia uma conexão HTTPS pela porta 443 do LIF entre clusters para o armazenamento de Blobs do Azure para operações de backup e restauração.

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

- O ONTAP requer uma conexão de entrada do conetor para o LIF de gerenciamento de cluster. O conetor pode residir em um Azure VNet.
- 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. "Saiba mais sobre IPspaces".

  Ao configurar o backup e a recuperação do BlueXP , 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.

- Os LIFs dos nós e dos clusters podem acessar o armazenamento de objetos.
- Os servidores DNS foram configurados para a VM de armazenamento onde os volumes estão localizados. Consulte como "Configurar serviços DNS para o SVM" .
- Se você usar um IPspace diferente do padrão, talvez seja necessário criar uma rota estática para obter acesso ao armazenamento de objetos.
- Atualize as regras de firewall, se necessário, para permitir conexões de serviço de backup e recuperação do BlueXP do ONTAP ao armazenamento de objetos através da porta 443 e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS através da porta 53 (TCP/UDP).

Verificar os requisitos de rede do ONTAP para replicação de volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o backup e a recuperação do BlueXP , certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede da ONTAP no local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da rede corporativa à rede virtual no provedor de nuvem. Normalmente, esta é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou sistemas locais, revise os requisitos de peering para sistemas ONTAP locais. "Veja os pré-requisitos para peering de cluster na documentação do ONTAP".

Requisitos de rede da 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.

Prepare o Azure Blob como destino do backup

1. Você pode usar suas próprias chaves gerenciadas personalizadas para criptografia de dados no assistente de ativação em vez de usar as chaves de criptografia gerenciadas pela Microsoft padrão. Nesse caso, você precisará ter a assinatura do Azure, o nome do Cofre-chave e a chave. "Saiba como usar suas próprias chaves".

   Observe que o backup e a recuperação oferecem suporte a *políticas de acesso do Azure* como o modelo de permissão. O modelo de permissão *Azure Role-Based Access Control* (Azure RBAC) não é suportado atualmente.

2. Se você quiser ter uma conexão mais segura pela Internet pública do seu data center local para o VNet, há uma opção para configurar um endpoint privado do Azure no assistente de ativação. Neste caso, você precisará conhecer o VNet e o Subnet para essa conexão. "Consulte os detalhes sobre como usar um endpoint privado".

Crie sua conta de armazenamento Azure Blob

Por padrão, o serviço cria contas de armazenamento para você. Se quiser usar suas próprias contas de armazenamento, você pode criá-las antes de iniciar o assistente de ativação de backup e, em seguida, selecionar essas contas de armazenamento no assistente.

"Saiba mais sobre como criar suas próprias contas de armazenamento".

Ative backups no ONTAP volumes

Ative os backups a qualquer momento diretamente do seu ambiente de trabalho no local.

Um assistente leva você através dos seguintes passos principais:

- Selecione os volumes que deseja fazer backup
- Defina a estratégia de backup
- Reveja as suas seleções

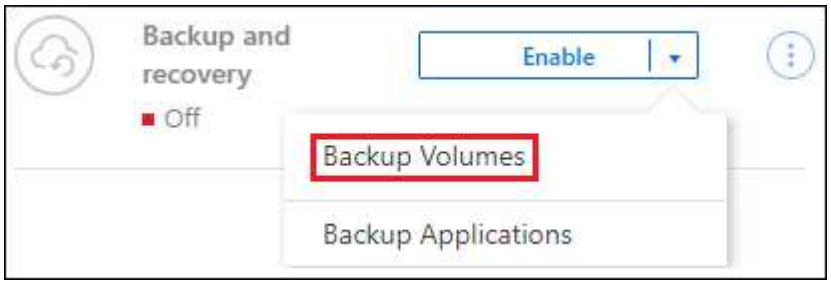
Você também pode Mostrar os comandos APIna etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para futuros ambientes de trabalho.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:

   - Na tela BlueXP , selecione o ambiente de trabalho e selecione **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.

     Se o destino do Azure para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster do ONTAP para o armazenamento de objetos Blob do Azure.

   - Selecione **volumes** na barra de backup e recuperação. Na guia volumes, selecione o ícone **ações** ••• e selecione **Ativar Backup** para um único volume (que ainda não tem replicação ou backup para armazenamento de objetos já ativado).

   A página Introdução do assistente mostra as opções de proteção, incluindo snapshots locais, replicação e backups. Se você fez a segunda opção nesta etapa, a página Definir estratégia de backup será exibida com um volume selecionado.

2. Continue com as seguintes opções:

   - Se já tiver um conetor BlueXP , está tudo definido. Basta selecionar **seguinte**.
   - Se você ainda não tiver um conetor BlueXP , a opção **Adicionar um conetor** será exibida. Prepare o conetor BlueXP Consulte a .

Selecione os volumes que deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem uma ou mais das seguintes opções: Política de snapshot, política de replicação, política de backup para objeto.

Você pode optar por proteger o FlexVol ou o FlexGroup volumes. No entanto, não é possível selecionar uma combinação desses volumes ao ativar o backup para um ambiente de trabalho. Veja como "ative o backup para volumes adicionais no ambiente de trabalho"(FlexVol ou FlexGroup) depois de configurar o backup para os volumes iniciais.

- Você pode ativar um backup apenas em um único volume FlexGroup de cada vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock. Todos os volumes devem ter o SnapLock Enterprise ativado ou o SnapLock desativado.

Passos

Observe que se os volumes escolhidos já tiverem políticas Snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que deseja proteger.

- Opcionalmente, filtre as linhas para mostrar apenas volumes com determinados tipos de volume, estilos e muito mais para facilitar a seleção.
- Depois de selecionar o primeiro volume, você pode selecionar todos os volumes FlexVol (volumes FlexGroup podem ser selecionados um de cada vez somente). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e marque a caixa na linha de título. (

).
- Para fazer backup de volumes individuais, marque a caixa para cada volume (

).

2. Selecione **seguinte**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Quer você queira uma ou todas as opções de backup: Snapshots locais, replicação e backup no storage de objetos
- Arquitetura
- Política de instantâneo local
- Destino e política de replicação

> Se os volumes escolhidos tiverem políticas de Snapshot e replicação diferentes das políticas selecionadas nesta etapa, as políticas existentes serão sobrescritas.

- Backup para informações de armazenamento de objetos (provedor, criptografia, rede, política de backup e opções de exportação).

Passos

1. Na página Definir estratégia de backup, escolha uma ou todas as opções a seguir. Todos os três são selecionados por padrão:
   - **Instantâneos locais**: Se você estiver executando replicação ou fazendo backup em armazenamento de objetos, os snapshots locais devem ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP.
   - **Backup**: Faz backup de volumes para armazenamento de objetos.
2. **Arquitetura**: Se você escolheu replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascading**: As informações fluem do primário para o secundário e do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do primário para o secundário *e* do armazenamento primário para o objeto.

     Para obter detalhes sobre essas arquiteturas, "Planeje sua jornada de proteção"consulte .
3. **Snapshot local**: Escolha uma política Snapshot existente ou crie uma nova.

   > Para criar uma política personalizada antes de ativar a captura Instantânea, "Crie uma política"consulte .

   Para criar uma política, selecione **criar nova política** e faça o seguinte:

- Introduza o nome da política.
- Selecione até 5 programações, normalmente de frequências diferentes.
- Selecione **criar**.

4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o ambiente de trabalho de destino e SVM. Opcionalmente, selecione o agregado de destino ou agregados e o prefixo ou sufixo que será adicionado ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma nova.

     Para criar uma política personalizada antes de ativar a replicação, "Crie uma política"consulte .

     Para criar uma política, selecione **criar nova política** e faça o seguinte:

     - Introduza o nome da política.
     - Selecione até 5 programações, normalmente de frequências diferentes.
     - Selecione **criar**.
5. **Fazer backup para Objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Fornecedor**: Selecione **Microsoft Azure**.
   - **Configurações do provedor**: Insira os detalhes do provedor e a região onde os backups serão armazenados.

     Crie uma nova conta de armazenamento ou selecione uma existente.

     Crie seu próprio grupo de recursos que gerencia o contentor Blob ou selecione o tipo e o grupo do grupo de recursos.

     Se você quiser proteger seus arquivos de backup de serem modificados ou excluídos, verifique se a conta de armazenamento foi criada com armazenamento imutável habilitado usando um período de retenção de 30 dias.

     Se você quiser categorizar arquivos de backup mais antigos no Azure Archive Storage para otimização de custo adicional, verifique se a conta de storage tem a regra de ciclo de vida apropriada.
   - **Chave de criptografia**: Se você criou uma nova conta de armazenamento do Azure, insira as informações da chave de criptografia fornecidas pelo provedor. Escolha se irá utilizar as chaves de encriptação padrão do Azure ou escolher as suas próprias chaves geridas pelo cliente na sua conta Azure para gerir a encriptação dos seus dados.

     Se você optar por usar suas próprias chaves gerenciadas pelo cliente, insira o cofre de chaves e as informações da chave.

     Se você escolheu uma conta de armazenamento Microsoft existente, as informações de criptografia já estão disponíveis, para que você não precise inseri-la agora.
   - **Rede**: Escolha o IPspace e se você usará um endpoint privado. O endpoint privado está desativado por predefinição.

i. O espaço de IPspace no cluster do ONTAP onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.

ii. Opcionalmente, escolha se você usará um endpoint privado do Azure que você configurou anteriormente. "Saiba mais sobre como usar um endpoint privado do Azure".

- **Política de backup**: Selecione uma política de armazenamento de backup para objetos existente ou crie uma nova.

  Para criar uma política personalizada antes de ativar a cópia de segurança, "Crie uma política"consulte .

  Para criar uma política, selecione **criar nova política** e faça o seguinte:

  - Introduza o nome da política.
  - Selecione até 5 programações, normalmente de frequências diferentes.
  - Para políticas de backup para objeto, defina as configurações DataLock e proteção contra ransomware. Para obter detalhes sobre DataLock e proteção contra ransomware, "Configurações de política de backup para objeto"consulte .
  - Selecione **criar**.

- **Exportar cópias Snapshot existentes para o armazenamento de objetos como cópias de backup**: Se houver cópias Snapshot locais para volumes neste ambiente de trabalho que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este ambiente de trabalho (por exemplo, diário, semanal, etc.), esse prompt adicional será exibido. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup para garantir a proteção mais completa para seus volumes.

6. Selecione **seguinte**.

Reveja as suas seleções

Esta é a oportunidade de rever as suas seleções e fazer ajustes, se necessário.

Passos

1. Na página Review (Revisão), reveja as suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos de política Snapshot com os rótulos de política de replicação e backup**. Isso cria snapshots com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O backup e a recuperação do BlueXP começam a fazer os backups iniciais dos seus volumes. A transferência de linha de base do volume replicado e do arquivo de backup inclui uma cópia completa dos dados do sistema de storage primário. As transferências subsequentes contêm cópias diferenciais dos dados do sistema de storage primário contidos nas cópias Snapshot.

Um volume replicado é criado no cluster de destino que será sincronizado com o volume primário.

Uma conta de armazenamento Blob é criada no grupo de recursos que você inseriu e os arquivos de backup são armazenados lá. O Painel de backup de volume é exibido para que você possa monitorar o estado dos backups.

Também pode monitorizar o estado dos trabalhos de cópia de segurança e restauro utilizando o "Painel

monitorização de trabalhos".

Mostrar os comandos API

Você pode querer exibir e, opcionalmente, copiar os comandos API usados no assistente Ativar backup e recuperação. Você pode querer fazer isso para automatizar a ativação de backup em futuros ambientes de trabalho.

Passos

1. No assistente Ativar backup e recuperação, selecione **Exibir solicitação de API**.
2. Para copiar os comandos para a área de transferência, selecione o ícone **Copiar**.

O que se segue?

- Você pode "gerencie seus arquivos de backup e políticas de backup". Isso inclui iniciar e parar backups, excluir backups, adicionar e alterar o agendamento de backup e muito mais.
- Você pode "gerencie as configurações de backup no nível do cluster". Isso inclui alterar a largura de banda da rede disponível para fazer upload de backups para o armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Você também pode "restaure volumes, pastas ou arquivos individuais a partir de um arquivo de backup"acessar um sistema Cloud Volumes ONTAP no Azure ou um sistema ONTAP no local.

Faça backup dos dados do ONTAP no local para o Google Cloud Storage

Siga estas etapas para começar a fazer backup de dados de volume de seus sistemas ONTAP primários no local para um sistema de storage secundário e para o Google Cloud Storage.

"Sistemas ONTAP no local" incluem sistemas FAS, AFF e ONTAP Select.

Início rápido

Comece rapidamente seguindo estes passos. Os detalhes de cada etapa são fornecidos nas seções a seguir deste tópico.

Identifique o método de conexão que você usará

Escolha se você conetará seu cluster ONTAP local diretamente ao Google Cloud Storage pela Internet pública ou se usará uma VPN ou o Google Cloud Interconnect e direcionará o tráfego por meio de uma interface privada do Google Access que usa um endereço IP privado.

Prepare o conetor BlueXP

Se você já tiver um conetor implantado na VPC do Google Cloud Platform, tudo estará definido. Caso contrário, você precisará criar um BlueXP Connector para fazer backup dos dados do ONTAP no storage do Google Cloud. Você também precisará personalizar as configurações de rede para o conetor para que ele possa se conetar ao Google Cloud.

3 Prepare a rede para o conetor

Certifique-se de que o conetor tem as ligações de rede necessárias.

4 Verifique os requisitos de licença

Você precisará verificar os requisitos de licença do Google Cloud e do BlueXP .

5 Preparar os clusters do ONTAP

Descubra os clusters do ONTAP no BlueXP , verifique se os clusters atendem aos requisitos mínimos e personalize as configurações de rede para que os clusters possam se conectar ao Google Cloud.

6 Prepare o Google Cloud como destino de backup

Configure permissões para que o conetor crie e gerencie o bucket do Google Cloud. Você também precisará configurar permissões para o cluster do ONTAP no local para que ele possa ler e gravar dados no bucket do Google Cloud.

Opcionalmente, você pode configurar suas próprias chaves gerenciadas personalizadas para criptografia de dados em vez de usar as chaves de criptografia padrão do Google Cloud.

7 Ative backups no ONTAP volumes

Selecione o ambiente de trabalho e clique em **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito. Em seguida, siga o assistente de configuração para selecionar as políticas de replicação e backup que você usará e os volumes que você deseja fazer backup.

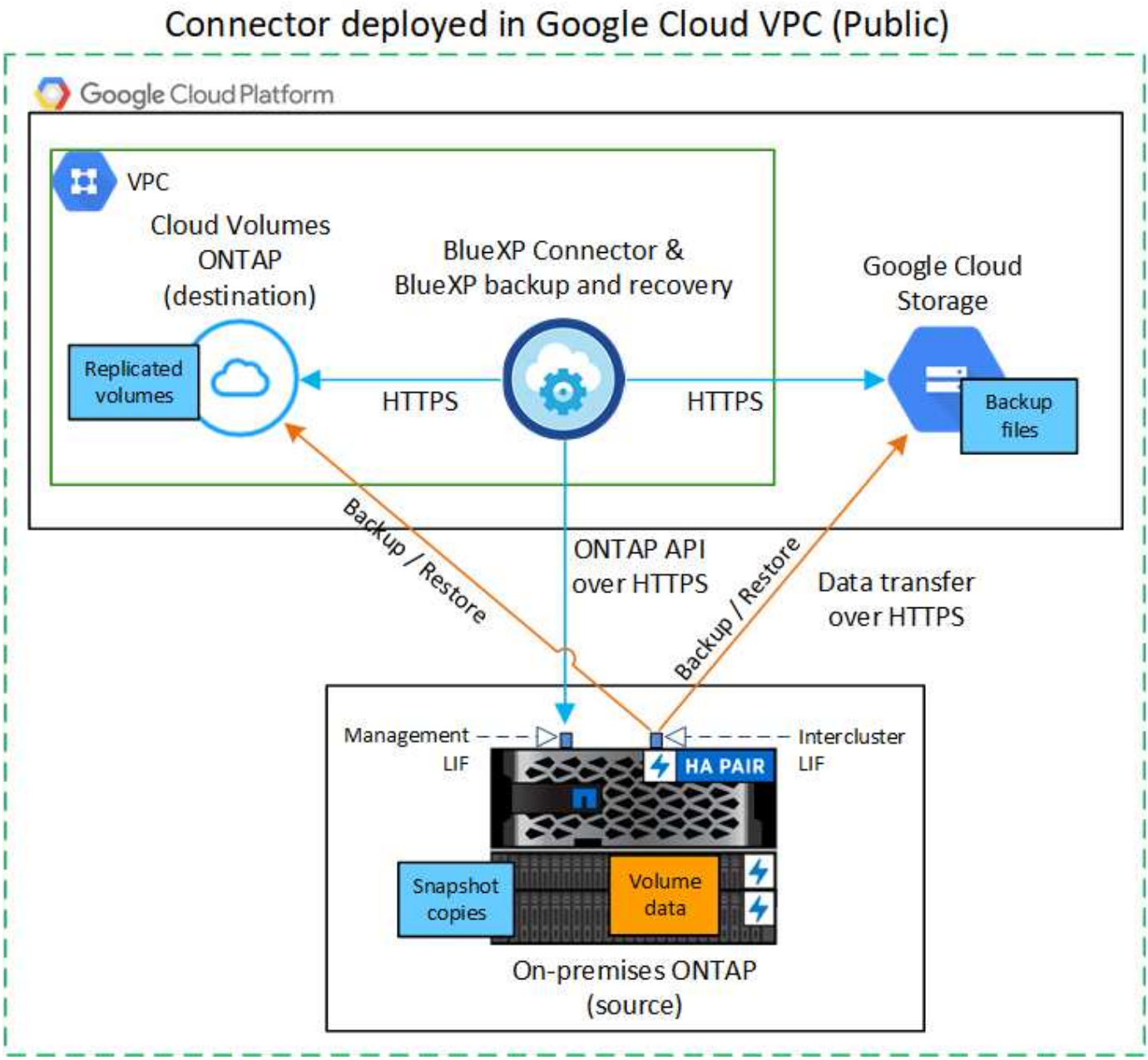
Identificar o método de ligação

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o Google Cloud Storage.

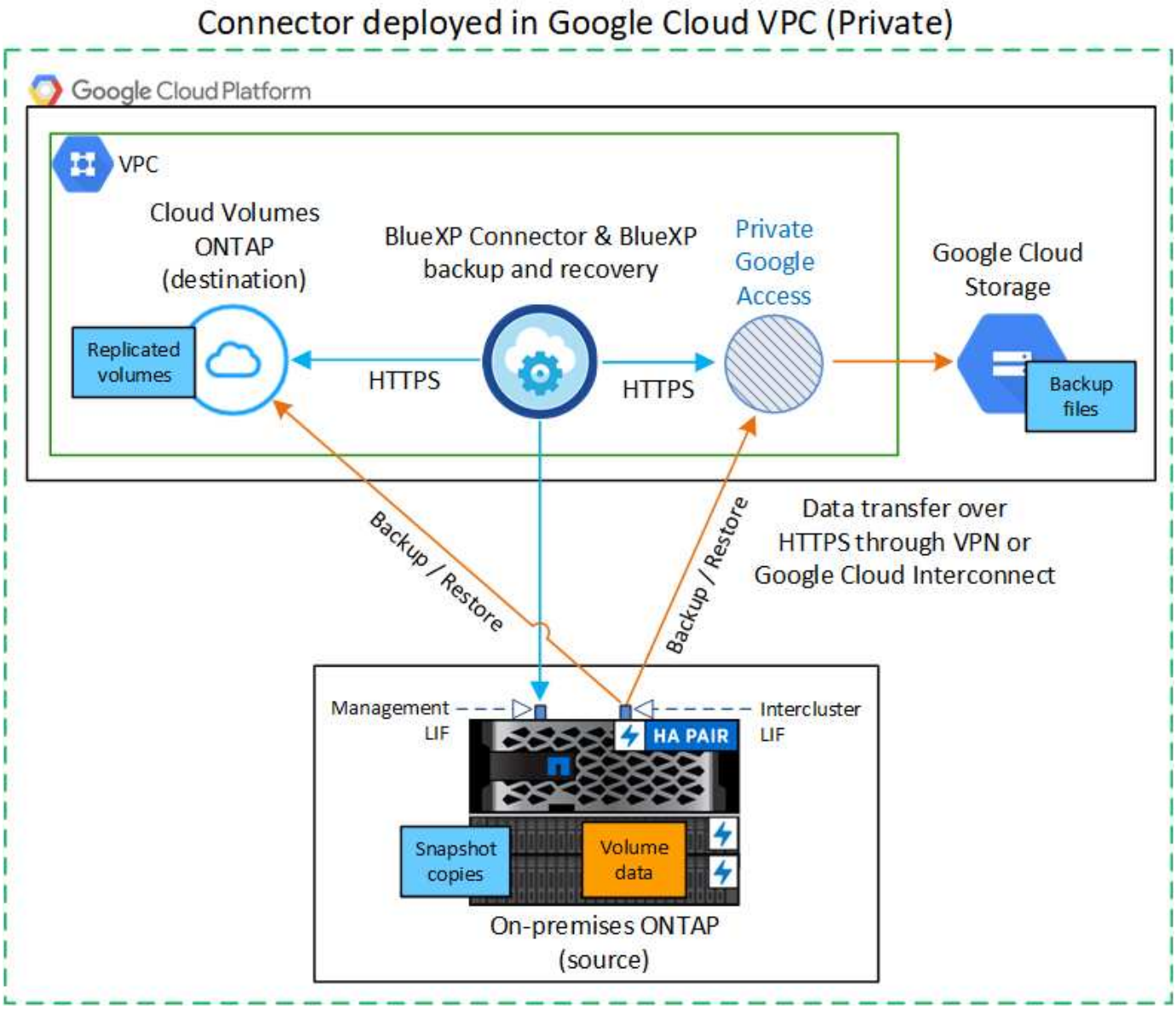
- **Conexão pública** - Conete diretamente o sistema ONTAP ao Google Cloud Storage usando um endpoint público do Google.
- * Conexão privada* - Use uma VPN ou o Google Cloud Interconnect e encaminhe o tráfego através de uma interface privada do Google Access que usa um endereço IP privado.

Opcionalmente, você pode se conectar a um sistema ONTAP secundário para volumes replicados usando a conexão pública ou privada.

O diagrama a seguir mostra o método **public Connection** e as conexões que você precisa preparar entre os componentes. O conetor deve ser implantado na VPC do Google Cloud Platform.



O diagrama a seguir mostra o método **private Connection** e as conexões que você precisa preparar entre os componentes. O conetor deve ser implantado na VPC do Google Cloud Platform.



Prepare o conetor BlueXP

O conetor BlueXP é o software principal para a funcionalidade BlueXP . É necessário um conetor para fazer backup e restaurar os dados do ONTAP.

Crie ou troque os conetores

Se você já tiver um conetor implantado na VPC do Google Cloud Platform, tudo estará definido.

Caso contrário, você precisará criar um conetor nesse local para fazer backup dos dados do ONTAP no Google Cloud Storage. Não é possível usar um conetor implantado em outro provedor de nuvem ou no local.

- "Saiba mais sobre conetores"
- "Instale um conetor no GCP"

Prepare 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 HTTPS pela porta 443 para o serviço de backup e recuperação do BlueXP e para o armazenamento do Google Cloud ("consulte a lista de endpoints")
   - Uma conexão HTTPS pela porta 443 ao LIF de gerenciamento de cluster do ONTAP
2. Ative o Acesso privado do Google (ou o Private Service Connect) na sub-rede onde pretende implementar o conetor. "Acesso privado ao Google" Ou "Conexão de serviço privado" são necessários 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 privada virtual (uma conexão **privada**).

   Siga as instruções do Google para configurar estas opções de Acesso Privado. Certifique-se de que os servidores DNS foram configurados para apontar `www.googleapis.com` e `storage.googleapis.com` para os endereços IP internos (privados) corretos.

Verifique ou adicione permissões ao conetor

Para usar a funcionalidade "pesquisar e restaurar" de backup e recuperação do BlueXP , você precisa ter permissões específicas na função do conetor para que ele possa acessar o serviço do Google Cloud BigQuery. Revise as permissões abaixo e siga as etapas se precisar modificar a política.

Passos

1. No "Google Cloud Console", vá para a página **Roles**.
2. Usando a lista suspensa na parte superior da página, selecione o projeto ou organização que contém a função que deseja editar.
3. Selecione uma função personalizada.
4. Selecione **Editar função** para atualizar as permissões da função.
5. Selecione **Adicionar permissões** para adicionar as seguintes novas permissões à função.

   ```
   bigquery.jobs.get
   bigquery.jobs.list
   bigquery.jobs.listAll
   bigquery.datasets.create
   bigquery.datasets.get
   bigquery.jobs.create
   bigquery.tables.get
   bigquery.tables.getData
   bigquery.tables.list
   bigquery.tables.create
   ```

6. Selecione **Atualizar** para salvar a função editada.

Verifique os requisitos de licença

- Antes de ativar o backup e a recuperação do BlueXP para o seu cluster, você precisará inscrever-se em uma oferta de mercado BlueXP de pagamento conforme o uso (PAYGO) do Google ou comprar e ativar uma licença BYOL de backup e recuperação do BlueXP da NetApp. Essas licenças são para sua conta e podem ser usadas em vários sistemas.
  - Para o licenciamento PAYGO de backup e recuperação do BlueXP , você precisará de uma assinatura do "Oferta de NetApp BlueXP do Google Marketplace". A cobrança do backup e recuperação do BlueXP é feita por meio dessa assinatura.
  - Para o licenciamento BYOL de backup e recuperação do BlueXP , você precisará do número de série do NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Saiba como gerenciar suas licenças BYOL".
- Você precisa ter uma assinatura do Google para o espaço de armazenamento de objetos onde seus backups serão localizados.

Regiões suportadas

É possível criar backups de sistemas locais para o Google Cloud Storage em todas as regiões "Onde o Cloud Volumes ONTAP é suportado". Você especifica a região onde os backups serão armazenados quando você configurar o serviço.

Preparar os clusters do ONTAP

Você precisará preparar seu sistema ONTAP de origem no local e qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local.

Preparar os clusters do ONTAP envolve as etapas a seguir:

- Descubra os seus sistemas ONTAP no BlueXP
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos
- Verificar os requisitos de rede do ONTAP para replicação de volumes

Descubra os seus sistemas ONTAP no BlueXP

Tanto o sistema ONTAP de origem no local quanto qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local devem estar disponíveis no BlueXP Canvas.

Você precisará saber o endereço IP de gerenciamento de cluster e a senha da conta de usuário admin para adicionar o cluster. "Saiba como descobrir um cluster".

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP são atendidos:

- É recomendado um mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior.
- Uma licença SnapMirror (incluída como parte do pacote Premium ou do pacote de proteção de dados).

  Observação: o "pacote de nuvem híbrida" não é necessário ao usar o backup e a recuperação do BlueXP .

Aprenda a "gerencie suas licenças de cluster".

- A hora e o fuso horário estão definidos corretamente. Aprenda a "configure a hora do cluster".
- Se você quiser replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar dados.

  "Veja versões compatíveis do ONTAP para relacionamentos do SnapMirror".

Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos

Você deve configurar os seguintes requisitos no sistema que se coneta ao storage de objetos.

- Para uma arquitetura de backup fan-out, configure as seguintes configurações no sistema *Primary*.
- Para uma arquitetura de backup em cascata, configure as seguintes configurações no sistema *secundário*.

São necessários os seguintes requisitos de rede de cluster do ONTAP:

- O cluster do ONTAP inicia uma conexão HTTPS pela porta 443 do LIF entre clusters para o Google Cloud Storage para operações de backup e restauração.

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

- O ONTAP requer uma conexão de entrada do conetor para o LIF de gerenciamento de cluster. O conetor pode residir em uma VPC do Google Cloud Platform.
- 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. "Saiba mais sobre IPspaces".

  Ao configurar o backup e a recuperação do BlueXP , 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.

- Os LIFs de clusters dos nós são capazes de acessar o armazenamento de objetos.
- Os servidores DNS foram configurados para a VM de armazenamento onde os volumes estão localizados. Consulte como "Configurar serviços DNS para o SVM" .

  Se estiver a utilizar o Private Google Access ou o Private Service Connect, certifique-se de que os seus servidores DNS foram configurados para apontar `storage.googleapis.com` para o endereço IP interno (privado) correto.

- Observe que, se você usar um IPspace diferente do padrão, talvez seja necessário criar uma rota estática para obter acesso ao armazenamento de objetos.
- Atualize regras de firewall, se necessário, para permitir conexões de backup e recuperação do BlueXP do ONTAP para o armazenamento de objetos através da porta 443, e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS através da porta 53 (TCP/UDP).

Verificar os requisitos de rede do ONTAP para replicação de volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o backup e a recuperação do BlueXP , certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede da ONTAP no local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da rede corporativa à rede virtual no provedor de nuvem. Normalmente, esta é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou sistemas locais, revise os requisitos de peering para sistemas ONTAP locais. "Veja os pré-requisitos para peering de cluster na documentação do ONTAP".

Requisitos de rede da 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.

Prepare o Google Cloud Storage como destino de backup

Preparar o Google Cloud Storage como destino de backup envolve as seguintes etapas:

- Configurar permissões.
- (Opcional) Crie seus próprios buckets. (O serviço criará buckets para você, se você quiser.)
- (Opcional) Configurar chaves gerenciadas pelo cliente para criptografia de dados

Configurar permissões

Você precisa fornecer chaves de acesso ao armazenamento para uma conta de serviço que tenha permissões específicas usando uma função personalizada. Uma conta de serviço permite que o backup e a recuperação do BlueXP autentiquem e acessem os buckets do Cloud Storage usados para armazenar backups. As chaves são necessárias para que o Google Cloud Storage saiba quem está fazendo a solicitação.

Passos

1. No "Google Cloud Console", vá para a página **Roles**.
2. "Crie uma nova função" com as seguintes permissões:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. No console do Google Cloud, "Vá para a página Contas de Serviço".
4. Selecione seu projeto Cloud.
5. Selecione **criar conta de serviço** e forneça as informações necessárias:
   a. **Detalhes da conta de serviço**: Insira um nome e uma descrição.
   b. **Conceder acesso a essa conta de serviço ao projeto**: Selecione a função personalizada que você acabou de criar.
   c. Selecione **Concluído**.
6. Vá para "Configurações de armazenamento do GCP" e crie chaves de acesso para a conta de serviço:
   a. Selecione um projeto e selecione **interoperabilidade**. Se ainda não o tiver feito, selecione **Ativar acesso à interoperabilidade**.
   b. Em **chaves de acesso para contas de serviço**, selecione **criar uma chave para uma conta de serviço**, selecione a conta de serviço que acabou de criar e clique em **criar chave**.

      Você precisará inserir as chaves no backup e recuperação do BlueXP mais tarde quando configurar o serviço de backup.

Crie seus próprios baldes

Por padrão, o serviço cria buckets para você. Ou, se você quiser usar seus próprios buckets, você pode criá-los antes de iniciar o assistente de ativação de backup e, em seguida, selecionar esses buckets no assistente.

"Saiba mais sobre como criar seus próprios buckets".

Configurar chaves de criptografia gerenciadas pelo cliente (CMEK) para criptografia de dados

Você pode usar suas próprias chaves gerenciadas pelo cliente para criptografia de dados em vez de usar as chaves de criptografia gerenciadas pelo Google padrão. As chaves entre regiões e entre projetos são suportadas, para que você possa escolher um projeto para um bucket diferente do projeto da chave CMEK.

Se você está planejando usar suas próprias chaves gerenciadas pelo cliente:

- Você precisará ter o Key Ring e o Key Name para poder adicionar essas informações no assistente de ativação. "Saiba mais sobre chaves de criptografia gerenciadas pelo cliente".
- Você precisará verificar se essas permissões necessárias estão incluídas na função do conetor:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Você precisará verificar se a API "Cloud Key Management Service (KMS)" do Google está habilitada em seu projeto. Consulte "Documentação do Google Cloud: Habilitando APIs" para obter detalhes.

Considerações CMEK:

- Tanto as chaves HSM (suportadas por hardware) como as chaves geradas por software são suportadas.
- As chaves do Cloud KMS recém-criadas ou importadas são suportadas.
- Apenas são suportadas chaves regionais, não são suportadas chaves globais.
- Atualmente, apenas o propósito "Symmetric encriptar/desencriptar" é suportado.
- Ao agente de serviço associado à conta de armazenamento é atribuída a função do IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" pelo backup e recuperação do BlueXP .

Ative backups no ONTAP volumes

Ative os backups a qualquer momento diretamente do seu ambiente de trabalho no local.

Um assistente leva você através dos seguintes passos principais:

- Selecione os volumes que deseja fazer backup
- Defina a estratégia de backup
- Reveja as suas seleções

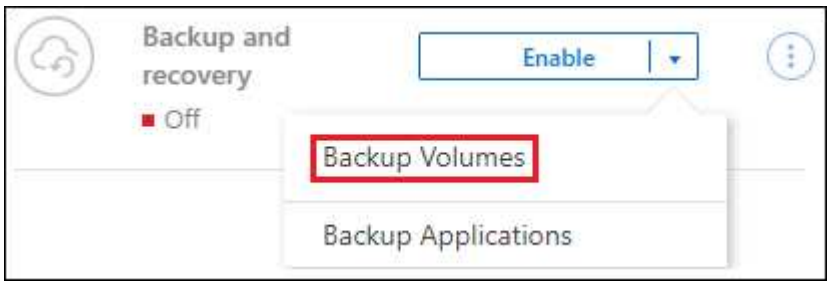
Você também pode Mostrar os comandos APIna etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para futuros ambientes de trabalho.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:

   - Na tela BlueXP , selecione o ambiente de trabalho e selecione **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.

     Se o destino do Google Cloud Storage para seus backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster do ONTAP para o armazenamento de objetos do Google Cloud.

   - Selecione **volumes** na barra de backup e recuperação. Na guia volumes, selecione o ícone **ações** ••• e selecione **Ativar Backup** para um único volume (que ainda não tem replicação ou backup para armazenamento de objetos já ativado). .

   A página Introdução do assistente mostra as opções de proteção, incluindo snapshots locais, replicação e backups. Se você fez a segunda opção nesta etapa, a página Definir estratégia de backup será exibida com um volume selecionado.

2. Continue com as seguintes opções:
   - Se já tiver um conetor BlueXP , está tudo definido. Basta selecionar **seguinte**.
   - Se você ainda não tiver um conetor BlueXP , a opção **Adicionar um conetor** será exibida. Prepare o conetor BlueXP Consulte a .

Selecione os volumes que deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem uma ou mais das seguintes opções: Política de snapshot, política de replicação, política de backup para objeto.

Você pode optar por proteger o FlexVol ou o FlexGroup volumes. No entanto, não é possível selecionar uma combinação desses volumes ao ativar o backup para um ambiente de trabalho. Veja como "ative o backup para volumes adicionais no ambiente de trabalho"(FlexVol ou FlexGroup) depois de configurar o backup para os volumes iniciais.

- Você pode ativar um backup apenas em um único volume FlexGroup de cada vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock. Todos os volumes devem ter o SnapLock Enterprise ativado ou o SnapLock desativado.

Passos

Observe que se os volumes escolhidos já tiverem políticas Snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que deseja proteger.
   - Opcionalmente, filtre as linhas para mostrar apenas volumes com determinados tipos de volume, estilos e muito mais para facilitar a seleção.
   - Depois de selecionar o primeiro volume, você pode selecionar todos os volumes FlexVol (volumes FlexGroup podem ser selecionados um de cada vez somente). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e marque a caixa na linha de título. (

).
   - Para fazer backup de volumes individuais, marque a caixa para cada volume (

).
2. Selecione **seguinte**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Quer você queira uma ou todas as opções de backup: Snapshots locais, replicação e backup no storage de objetos
- Arquitetura
- Política de instantâneo local
- Destino e política de replicação

Se os volumes escolhidos tiverem políticas de Snapshot e replicação diferentes das políticas selecionadas nesta etapa, as políticas existentes serão sobrescritas.

- Backup para informações de armazenamento de objetos (provedor, criptografia, rede, política de backup e opções de exportação).

Passos

1. Na página Definir estratégia de backup, escolha uma ou todas as opções a seguir. Todos os três são selecionados por padrão:
   - **Instantâneos locais**: Se você estiver executando replicação ou fazendo backup em armazenamento de objetos, os snapshots locais devem ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP.
   - **Backup**: Faz backup de volumes para armazenamento de objetos.
2. **Arquitetura**: Se você escolheu replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascading**: As informações fluem do primário para o secundário e do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do primário para o secundário *e* do armazenamento primário para o objeto.

     Para obter detalhes sobre essas arquiteturas, "Planeje sua jornada de proteção"consulte .
3. **Snapshot local**: Escolha uma política Snapshot existente ou crie uma nova.

   Para criar uma política personalizada antes de ativar a captura Instantânea, "Crie uma política"consulte .

   Para criar uma política, selecione **criar nova política** e faça o seguinte:
   - Introduza o nome da política.
   - Selecione até 5 programações, normalmente de frequências diferentes.
   - Selecione **criar**.
4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o ambiente de trabalho de destino e SVM. Opcionalmente, selecione o agregado de destino ou agregados e o prefixo ou sufixo que será adicionado ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma nova.

     Para criar uma política personalizada antes de ativar a replicação, "Crie uma política"consulte .

     Para criar uma política, selecione **criar nova política** e faça o seguinte:
     - Introduza o nome da política.
     - Selecione até 5 programações, normalmente de frequências diferentes.
     - Selecione **criar**.
5. **Fazer backup para Objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Fornecedor**: Selecione **Google Cloud**.
   - **Configurações do provedor**: Insira os detalhes do provedor e a região onde os backups serão armazenados.

     Crie um novo bucket ou selecione um que você já criou.

Se você quiser categorizar arquivos de backup mais antigos no storage do Google Cloud Archive para otimização adicional de custos, verifique se o intervalo tem a regra de ciclo de vida apropriada.

Insira a chave secreta e a chave secreta do Google Cloud Access.

- **Chave de criptografia**: Se você criou uma nova conta de armazenamento do Google Cloud, insira as informações da chave de criptografia fornecidas pelo provedor. Escolha se você usará as chaves de criptografia padrão do Google Cloud ou escolha suas próprias chaves gerenciadas pelo cliente na sua conta do Google Cloud para gerenciar a criptografia de seus dados.

  Se você escolher uma conta de armazenamento do Google Cloud existente, as informações de criptografia já estarão disponíveis, para que você não precise inseri-la agora.

  Se você optar por usar suas próprias chaves gerenciadas pelo cliente, digite o anel de chave e o nome da chave. "Saiba mais sobre chaves de criptografia gerenciadas pelo cliente".

- **Networking**: Escolha o IPspace.

  O espaço de IPspace no cluster do ONTAP onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet.

- **Política de backup**: Selecione uma política de armazenamento de backup para objetos existente ou crie uma nova.

  Para criar uma política personalizada antes de ativar a cópia de segurança, "Crie uma política"consulte .

  Para criar uma política, selecione **criar nova política** e faça o seguinte:

  - Introduza o nome da política.
  - Selecione até 5 programações, normalmente de frequências diferentes.
  - Selecione **criar**.

- **Exportar cópias Snapshot existentes para o armazenamento de objetos como cópias de backup**: Se houver cópias Snapshot locais para volumes neste ambiente de trabalho que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este ambiente de trabalho (por exemplo, diário, semanal, etc.), esse prompt adicional será exibido. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup para garantir a proteção mais completa para seus volumes.

6. Selecione **seguinte**.

Reveja as suas seleções

Esta é a oportunidade de rever as suas seleções e fazer ajustes, se necessário.

Passos

1. Na página Review (Revisão), reveja as suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos de política Snapshot com os rótulos de política de replicação e backup**. Isso cria snapshots com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.

3. Selecione **Ativar Backup**.

Resultado

O backup e a recuperação do BlueXP começam a fazer os backups iniciais dos seus volumes. A transferência de linha de base do volume replicado e do arquivo de backup inclui uma cópia completa dos dados do sistema de storage primário. As transferências subsequentes contêm cópias diferenciais dos dados do sistema de storage primário contidos nas cópias Snapshot.

Um volume replicado é criado no cluster de destino que será sincronizado com o volume de origem.

Um intervalo do Google Cloud Storage é criado automaticamente na conta de serviço indicada pela chave de acesso e chave secreta do Google que você inseriu, e os arquivos de backup são armazenados lá. O Painel de backup de volume é exibido para que você possa monitorar o estado dos backups.

Também pode monitorizar o estado dos trabalhos de cópia de segurança e restauro utilizando o "Painel monitorização de trabalhos".

Mostrar os comandos API

Você pode querer exibir e, opcionalmente, copiar os comandos API usados no assistente Ativar backup e recuperação. Você pode querer fazer isso para automatizar a ativação de backup em futuros ambientes de trabalho.

Passos

1. No assistente Ativar backup e recuperação, selecione **Exibir solicitação de API**.
2. Para copiar os comandos para a área de transferência, selecione o ícone **Copiar**.

O que se segue?

- Você pode "gerencie seus arquivos de backup e políticas de backup". Isso inclui iniciar e parar backups, excluir backups, adicionar e alterar o agendamento de backup e muito mais.
- Você pode "gerencie as configurações de backup no nível do cluster". Isso inclui a alteração das chaves de armazenamento que o ONTAP usa para acessar o armazenamento na nuvem, alterar a largura de banda da rede disponível para carregar backups para o armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Você também pode "restaure volumes, pastas ou arquivos individuais a partir de um arquivo de backup"acessar um sistema Cloud Volumes ONTAP no Google ou um sistema ONTAP no local.

Fazer backup de dados ONTAP on-premises para o ONTAP S3

Conclua algumas etapas para começar a fazer backup de dados de volume de seus principais sistemas ONTAP locais. Você pode enviar backups para um sistema de storage secundário da ONTAP (um volume replicado) ou para um bucket em um sistema ONTAP configurado como um servidor S3 (um arquivo de backup) ou ambos.

O principal sistema ONTAP no local pode ser um sistema FAS, AFF ou ONTAP Select. O sistema ONTAP secundário pode ser um sistema ONTAP ou Cloud Volumes ONTAP no local. O storage de objetos pode estar em um sistema ONTAP no local ou em um sistema Cloud Volumes ONTAP no qual você ativou um servidor de storage de objetos Simple Storage Service (S3).

Início rápido

Comece rapidamente seguindo estes passos. Os detalhes de cada etapa são fornecidos nas seções a seguir deste tópico.

1 Identifique o método de conexão que você usará

Veja como você conetará seu cluster ONTAP local primário ao cluster ONTAP secundário para replicação e ao cluster ONTAP configurado como um servidor S3 para backup no storage de objetos.

Identificar o método de ligação.

2 Prepare o conetor BlueXP

Se você já implantou um BlueXP Connector, então está tudo pronto. Caso contrário, você precisará criar um BlueXP Connector para fazer backup dos dados do ONTAP para o ONTAP S3. Você também precisará personalizar as configurações de rede para o conetor para que ele possa se conetar ao ONTAP S3.

Saiba como criar um conetor e como definir as definições de rede necessárias.

3 Verifique os requisitos de licença

Você precisará verificar os requisitos de licença para seus sistemas ONTAP e para backup e recuperação do BlueXP .

Verifique os requisitos de licença.

4 Preparar os clusters do ONTAP

Descubra seus clusters ONTAP primários e secundários no BlueXP , verifique se os clusters atendem a requisitos mínimos e personalize as configurações de rede para que os clusters possam se conectar ao storage de objetos do ONTAP S3.

Saiba como preparar os clusters do ONTAP.

5 Prepare o ONTAP S3 como destino de backup

Configure permissões para o conetor para que ele possa gerenciar o bucket do ONTAP S3. Você também precisará configurar permissões para o cluster do ONTAP local de origem para que ele possa ler e gravar dados no bucket do ONTAP S3.

Saiba como preparar seu ambiente ONTAP S3 para receber backups do ONTAP.

6 Ative backups no ONTAP volumes

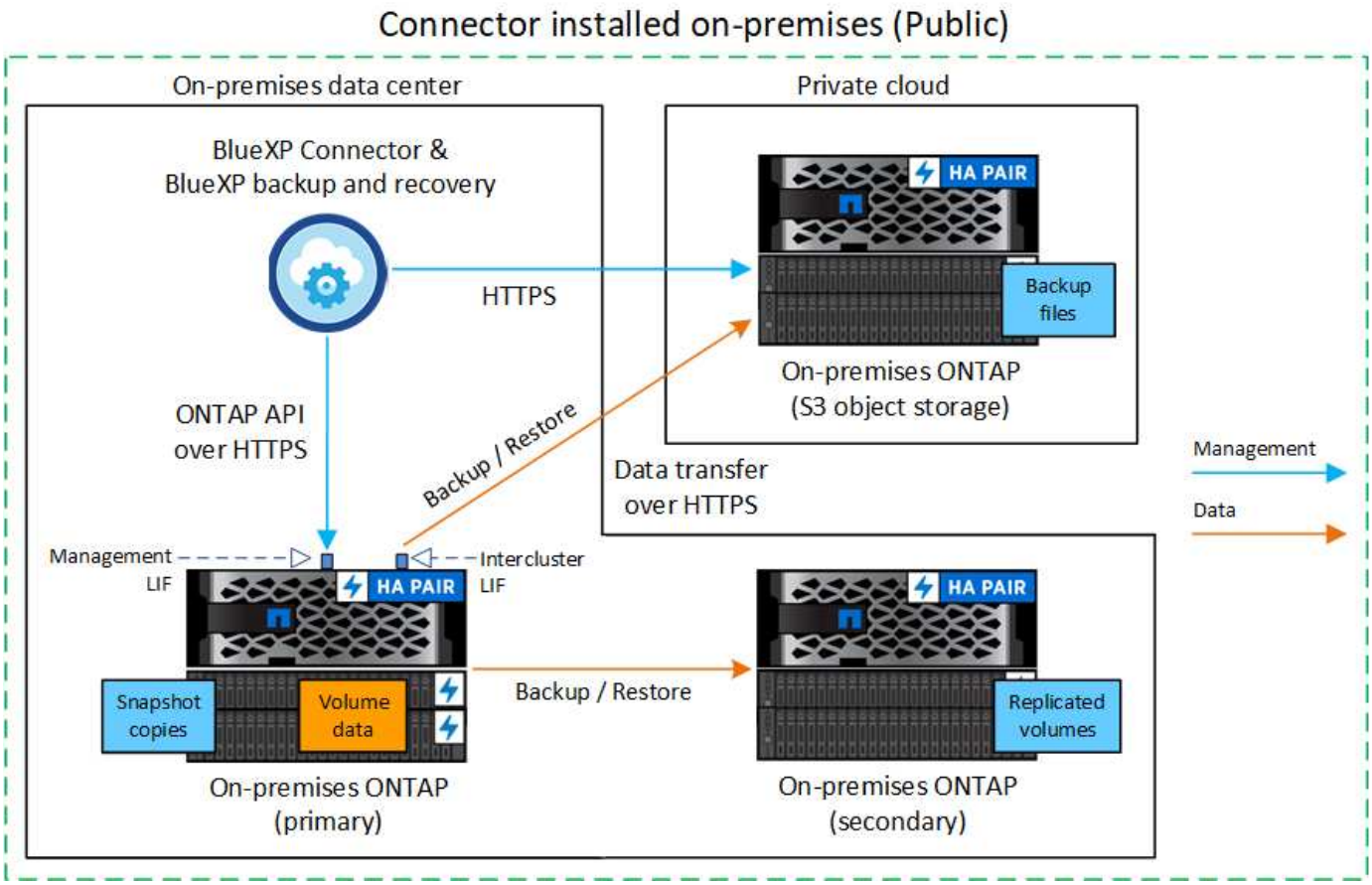
Selecione o ambiente de trabalho principal e clique em **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito. Em seguida, siga o assistente de configuração para selecionar os volumes que você deseja fazer backup e as políticas Snapshot, replicação e backup para objetos que você usará.

Ative backups no ONTAP volumes.

Identificar o método de ligação

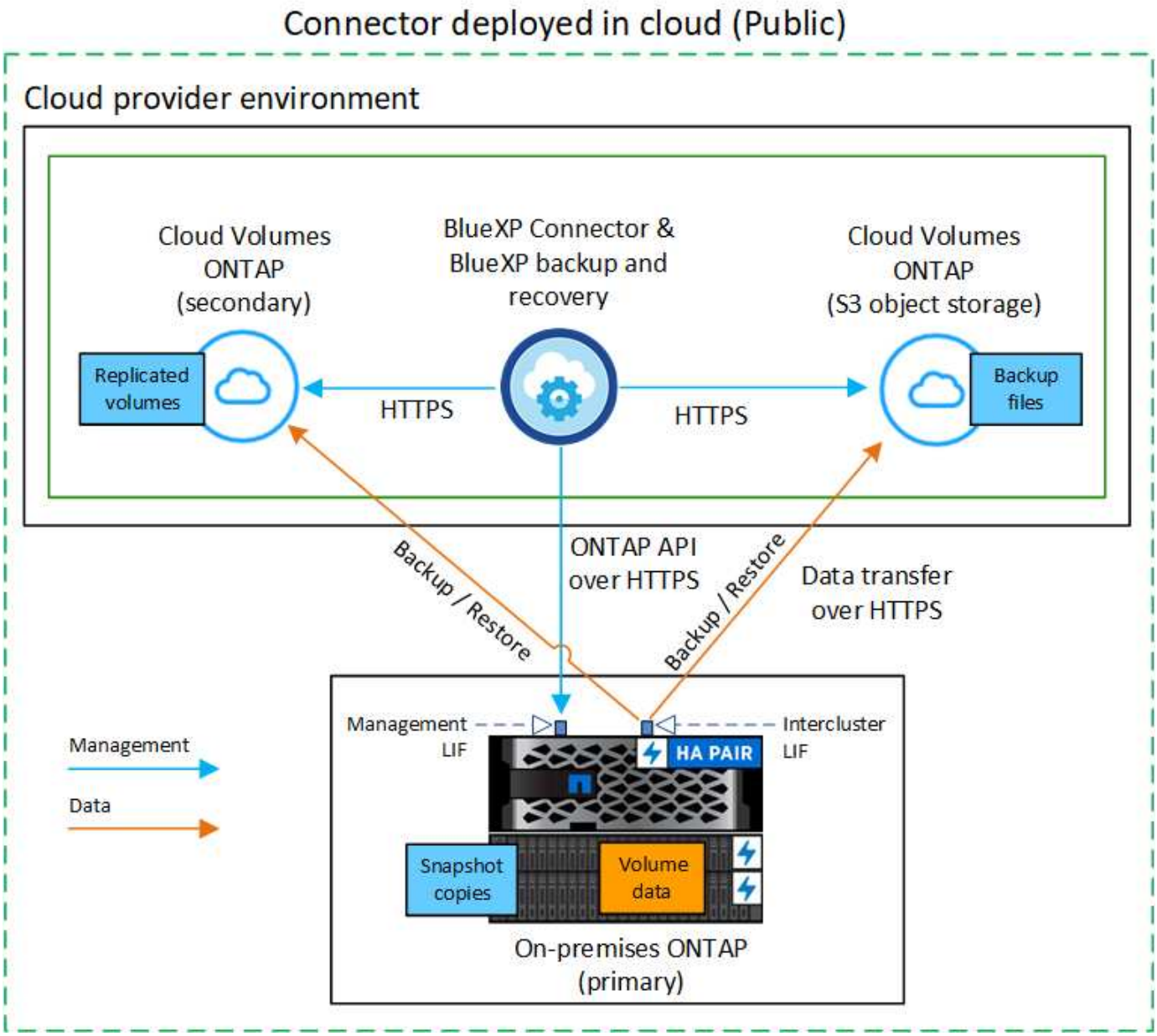
Há muitas configurações nas quais você pode criar backups para um bucket do S3 em um sistema ONTAP. Dois cenários são mostrados abaixo.

A imagem a seguir mostra cada componente ao fazer backup de um sistema ONTAP primário no local para um sistema ONTAP no local configurado para S3 e as conexões que você precisa preparar entre eles. Ele também mostra uma conexão com um sistema ONTAP secundário no mesmo local para replicar volumes.



Quando o conetor e o sistema ONTAP principal no local são instalados em um local local sem acesso à Internet (uma implantação de modo "privada"), o sistema ONTAP S3 deve estar localizado no mesmo data center local.

A imagem a seguir mostra cada componente ao fazer backup de um sistema ONTAP primário no local para um sistema Cloud Volumes ONTAP configurado para S3 e as conexões que você precisa preparar entre eles. Ele também mostra uma conexão com um sistema Cloud Volumes ONTAP secundário no mesmo ambiente de fornecedor de nuvem para replicar volumes.



Nesse cenário, o conetor deve ser implantado no mesmo ambiente de provedor de nuvem no qual os sistemas Cloud Volumes ONTAP são implantados.

Prepare o conetor BlueXP

O conetor BlueXP é o software principal para a funcionalidade BlueXP . É necessário um conetor para fazer backup e restaurar os dados do ONTAP.

Crie ou troque os conetores

Ao fazer backup dos dados no ONTAP S3, um BlueXP Connector deve estar disponível no local ou na nuvem. Você precisará instalar um novo conetor ou certificar-se de que o conetor atualmente selecionado reside em um desses locais. O conetor no local pode ser instalado em um site com ou sem acesso à Internet.

- "Saiba mais sobre conetores"
- "Instale o conetor em seu ambiente de nuvem"

- "Instalar o conetor em um host Linux com acesso à Internet"
- "Instalar o conetor em um host Linux sem acesso à Internet"
- "Comutação entre conetores"

Preparar os requisitos de rede do conetor

Certifique-se de que a rede onde o conetor está instalado permite as seguintes ligações:

- Uma conexão HTTPS pela porta 443 para o servidor ONTAP S3
- Uma conexão HTTPS pela porta 443 ao LIF de gerenciamento de cluster do ONTAP de origem
- Uma conexão de saída de Internet pela porta 443 para backup e recuperação do BlueXP (não é necessário quando o conetor é instalado em um site "escuro")

Considerações sobre o modo privado (local escuro)

A funcionalidade de backup e recuperação do BlueXP está integrada ao BlueXP Connector. Quando ele é instalado no modo privado, você precisará atualizar o software do conetor periodicamente para ter acesso a novos recursos. Verifique o "Novidades sobre backup e recuperação do BlueXP " para ver os novos recursos em cada versão de backup e recuperação do BlueXP . Quando quiser usar os novos recursos, siga as etapas para "Atualize o software do conetor".

Quando você usa o backup e a recuperação do BlueXP em um ambiente SaaS padrão, o backup e a configuração de recuperação do BlueXP fazem o backup na nuvem. Quando você usa o backup e a recuperação do BlueXP em um site sem acesso à Internet, os dados de configuração de backup e recuperação do BlueXP são copiados para o bucket do ONTAP S3, onde seus backups estão sendo armazenados. Se alguma vez tiver uma falha de conetor no seu site de modo privado, pode "Restaure os dados de backup e recuperação do BlueXP para um novo conetor".

Verifique os requisitos de licença

Antes de ativar o backup e a recuperação do BlueXP para seu cluster, você precisará comprar e ativar uma licença BYOL de recuperação e backup do BlueXP da NetApp. A licença é para backup e restauração no storage de objetos. Não é necessária licença para criar cópias Snapshot ou volumes replicados. Esta licença é para a conta e pode ser usada em vários sistemas.

Você precisará do número de série do NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Saiba como gerenciar suas licenças BYOL".

O licenciamento PAYGO não é suportado ao fazer backup de arquivos para o ONTAP S3.

Preparar os clusters do ONTAP

Você precisará preparar seu sistema ONTAP de origem no local e qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local.

Preparar os clusters do ONTAP envolve as etapas a seguir:

- Descubra os seus sistemas ONTAP no BlueXP
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos

- Verificar os requisitos de rede do ONTAP para replicação de volumes

Descubra os seus sistemas ONTAP no BlueXP

Tanto o sistema ONTAP de origem no local quanto qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local devem estar disponíveis no BlueXP Canvas.

Você precisará saber o endereço IP de gerenciamento de cluster e a senha da conta de usuário admin para adicionar o cluster. "Saiba como descobrir um cluster".

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP são atendidos:

- É recomendado um mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior.
- Uma licença SnapMirror (incluída como parte do pacote Premium ou do pacote de proteção de dados).

  Observação: o "pacote de nuvem híbrida" não é necessário ao usar o backup e a recuperação do BlueXP .

  Aprenda a "gerencie suas licenças de cluster".

- A hora e o fuso horário estão definidos corretamente. Aprenda a "configure a hora do cluster".
- Se você quiser replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar dados.

  "Veja versões compatíveis do ONTAP para relacionamentos do SnapMirror".

Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos

Você deve garantir que os seguintes requisitos sejam atendidos no sistema que se conecta ao storage de objetos.

- Quando você usa uma arquitetura de backup fan-out, as configurações devem ser configuradas no sistema de armazenamento *Primary*.
- Quando você usa uma arquitetura de backup em cascata, as configurações devem ser configuradas no sistema de armazenamento *secundário*.

  "Saiba mais sobre os tipos de arquitetura de backup".

São necessários os seguintes requisitos de rede de cluster do ONTAP:

- O cluster ONTAP inicia uma conexão HTTPS por uma porta especificada pelo usuário do LIF entre clusters para o servidor ONTAP S3 para operações de backup e restauração. A porta é configurável durante a configuração da cópia de segurança.

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

- O ONTAP requer uma conexão de entrada do conetor para o LIF de gerenciamento 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. "Saiba mais sobre IPspaces".

Ao configurar o backup e a recuperação do BlueXP , 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.

- Os LIFs de clusters dos nós são capazes de acessar o armazenamento de objetos (não é necessário quando o conetor é instalado em um local "escuro").
- Os servidores DNS foram configurados para a VM de armazenamento onde os volumes estão localizados. Consulte como "Configurar serviços DNS para o SVM" .
- Se você usar um IPspace diferente do padrão, talvez seja necessário criar uma rota estática para obter acesso ao armazenamento de objetos.
- Atualize regras de firewall, se necessário, para permitir conexões de serviço de backup e recuperação do BlueXP do ONTAP para o armazenamento de objetos através da porta especificada (normalmente porta 443) e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS através da porta 53 (TCP/UDP).

Verificar os requisitos de rede do ONTAP para replicação de volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o backup e a recuperação do BlueXP , certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede da ONTAP no local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da rede corporativa à rede virtual no provedor de nuvem. Normalmente, esta é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou sistemas locais, revise os requisitos de peering para sistemas ONTAP locais. "Veja os pré-requisitos para peering de cluster na documentação do ONTAP".

Requisitos de rede da 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.

Prepare o ONTAP S3 como destino de backup

É necessário habilitar um servidor de storage de objetos Simple Storage Service (S3) no cluster do ONTAP que você planeja usar para backups de storage de objetos. Consulte "Documentação do ONTAP S3" para obter detalhes.

Observação: você pode descobrir esse cluster no BlueXP Canvas, mas ele não é identificado como sendo um servidor de armazenamento de objetos S3 e não é possível arrastar e soltar um ambiente de trabalho de origem neste ambiente de trabalho S3 para iniciar a ativação de backup.

Este sistema ONTAP deve atender aos seguintes requisitos.

Versões de ONTAP compatíveis

O ONTAP 9.8 e posterior é necessário para sistemas ONTAP no local. ONTAP 9.9,1 e posterior são necessários para sistemas Cloud Volumes ONTAP.

S3 credenciais

Você deve ter criado um usuário S3 para controlar o acesso ao armazenamento do ONTAP S3. "Consulte os documentos do ONTAP S3 para obter detalhes".

Quando você configura o backup para o ONTAP S3, o assistente de backup solicita uma chave de acesso S3 e uma chave secreta para uma conta de usuário. A conta de usuário permite que o backup e a recuperação do BlueXP autentiquem e acessem os buckets do ONTAP S3 usados para armazenar backups. As chaves são necessárias para que o ONTAP S3 saiba quem está fazendo o pedido.

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"
```

Ative backups no ONTAP volumes

Ative os backups a qualquer momento diretamente do seu ambiente de trabalho no local.

Um assistente leva você através dos seguintes passos principais:

- Selecione os volumes que deseja fazer backup
- Defina a estratégia e as políticas de backup
- Reveja as suas seleções

Você também pode Mostrar os comandos APIna etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para futuros ambientes de trabalho.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:
    - Na tela BlueXP , selecione o ambiente de trabalho e selecione **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.
    - Selecione **volumes** na barra de backup e recuperação. Na guia volumes, selecione a opção **ações (…)** e selecione **Ativar Backup** para um único volume (que ainda não tem replicação ou backup para armazenamento de objetos ativado).

    A página Introdução do assistente mostra as opções de proteção, incluindo snapshots locais, replicações e backups. Se você fez a segunda opção nesta etapa, a página Definir estratégia de backup será exibida com um volume selecionado.

2. Continue com as seguintes opções:
    - Se já tiver um conetor BlueXP , está tudo definido. Basta selecionar **seguinte**.
    - Se você não tiver um conetor BlueXP , a opção **Adicionar um conetor** será exibida. Prepare o conetor BlueXP Consulte a .

Selecione os volumes que deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem uma ou mais das seguintes opções: Política de snapshot, política de replicação, política de backup para objeto.

Você pode optar por proteger o FlexVol ou o FlexGroup volumes. No entanto, não é possível selecionar uma combinação desses volumes ao ativar o backup para um ambiente de trabalho. Veja como "ative o backup para volumes adicionais no ambiente de trabalho"(FlexVol ou FlexGroup) depois de configurar o backup para os volumes iniciais.

- Você pode ativar um backup apenas em um único volume FlexGroup de cada vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock. Todos os volumes devem ter o SnapLock Enterprise ativado ou o SnapLock desativado.

Passos

Observe que se os volumes escolhidos já tiverem políticas Snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que deseja proteger.
    - Opcionalmente, filtre as linhas para mostrar apenas volumes com determinados tipos de volume, estilos e muito mais para facilitar a seleção.
    - Depois de selecionar o primeiro volume, você pode selecionar todos os volumes FlexVol (volumes FlexGroup podem ser selecionados um de cada vez somente). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e marque a caixa na linha de título. (

).
    - Para fazer backup de volumes individuais, marque a caixa para cada volume (

).
2. Selecione **seguinte**.

Defina a estratégia de backup

Definir a estratégia de backup envolve a configuração das seguintes opções:

- Opções de proteção: Se você deseja implementar uma ou todas as opções de backup: Snapshots locais, replicação e backup para armazenamento de objetos
- Arquitetura: Quer você queira usar uma arquitetura de backup em fan-out ou em cascata
- Política de instantâneo local
- Destino e política de replicação
- Backup para informações de armazenamento de objetos (provedor, criptografia, rede, política de backup e opções de exportação).

Passos

1. Na página Definir estratégia de backup, escolha uma ou todas as opções a seguir. Todos os três são selecionados por padrão:

- **Instantâneos locais**: Cria cópias Snapshot locais.
- **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP.
- **Backup**: Faz backup de volumes em um bucket em um sistema ONTAP configurado para S3.

2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascading**: Os dados de backup fluem do sistema primário para o sistema secundário e, em seguida, do armazenamento secundário para o objeto.
   - **Fan out**: Os dados de backup fluem do sistema primário para o sistema secundário *e* do armazenamento primário para o objeto.

     Para obter detalhes sobre essas arquiteturas, "Planeje sua jornada de proteção"consulte .

3. **Snapshot local**: Escolha uma política Snapshot existente ou crie uma nova.

   Se você quiser criar uma política personalizada antes de ativar o instantâneo, use o Gerenciador do sistema ou o comando CLI do ONTAP `snapmirror policy create`. Consulte a.

   Para criar uma política personalizada usando esse serviço antes de ativar a captura Instantânea, "Crie uma política"consulte .

   Para criar uma política, selecione **criar nova política** e faça o seguinte:

   - Introduza o nome da política.
   - Selecione até 5 programações, normalmente de frequências diferentes.
   - Selecione **criar**.

4. **Replicação**: Se você selecionou **replicação**, defina as seguintes opções:
   - **Destino de replicação**: Selecione o ambiente de trabalho de destino e SVM. Opcionalmente, selecione o agregado de destino (ou agregados para volumes FlexGroup) e um prefixo ou sufixo que será adicionado ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma nova.

     Para criar uma política, selecione **criar nova política** e faça o seguinte:

     - Introduza o nome da política.
     - Selecione até 5 programações, normalmente de frequências diferentes.
     - Selecione **criar**.

5. **Fazer backup para Objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Fornecedor**: Selecione **ONTAP S3**.
   - * Configurações do provedor*: Insira os detalhes do FQDN do servidor S3, a porta e a chave de acesso e a chave secreta dos usuários.

     A chave de acesso e a chave secreta destinam-se ao usuário que você criou para dar ao cluster do ONTAP acesso ao bucket do S3.

   - **Rede**: Escolha o espaço IPspace no cluster ONTAP de origem onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet (não é necessário quando o conetor é instalado em um site "escuro").

A seleção do espaço de IPspace correto garante que o backup e a recuperação do BlueXP possam configurar uma conexão do ONTAP para o armazenamento de objetos do ONTAP S3.

- **Política de backup**: Selecione uma política de backup existente ou crie uma nova.

  Você pode criar uma política com o Gerenciador do sistema ou com a CLI do ONTAP. Para criar uma política personalizada usando o comando ONTAP CLI `snapmirror policy create`, consulte .

  Para criar uma política personalizada antes de ativar o backup usando a IU, "Crie uma política"consulte .

  Para criar uma política, selecione **criar nova política** e faça o seguinte:

  - Introduza o nome da política.
  - Selecione até 5 programações, normalmente de frequências diferentes.
  - Para políticas de backup para objeto, defina as configurações DataLock e proteção contra ransomware. Para obter detalhes sobre DataLock e proteção contra ransomware, "Configurações de política de backup para objeto"consulte .
  - Selecione **criar**.

- **Exportar cópias Snapshot existentes para armazenamento de objetos como arquivos de backup**: Se houver cópias Snapshot locais para volumes neste ambiente de trabalho que correspondam ao rótulo de agendamento de backup que você acabou de selecionar (por exemplo, diário, semanal, etc.), esse prompt adicional será exibido. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup para garantir a proteção mais completa para seus volumes.

6. Selecione **seguinte**.

Reveja as suas seleções

Esta é a oportunidade de rever as suas seleções e fazer ajustes, se necessário.

Passos

1. Na página Review (Revisão), reveja as suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos de política Snapshot com os rótulos de política de replicação e backup**. Isso cria snapshots com um rótulo que corresponde aos rótulos nas políticas de replicação e backup. Se as políticas não corresponderem, os backups não serão criados.
3. Selecione **Ativar Backup**.

Resultado

O backup e a recuperação do BlueXP começam a fazer os backups iniciais dos seus volumes. A transferência de linha de base do volume replicado e do arquivo de backup inclui uma cópia completa dos dados de origem. As transferências subsequentes contêm cópias diferenciais dos dados de storage primário contidos nas cópias Snapshot.

Um volume replicado é criado no cluster de destino que será sincronizado com o volume de armazenamento primário.

Um bucket S3 é criado na conta de serviço indicada pela chave de acesso S3 e chave secreta que você inseriu e os arquivos de backup são armazenados lá.

O Painel de backup de volume é exibido para que você possa monitorar o estado dos backups.

Também pode monitorizar o estado dos trabalhos de cópia de segurança e restauro utilizando o "Painel monitorização de trabalhos".

Mostrar os comandos API

Você pode querer exibir e, opcionalmente, copiar os comandos API usados no assistente Ativar backup e recuperação. Você pode querer fazer isso para automatizar a ativação de backup em futuros ambientes de trabalho.

Passos

1. No assistente Ativar backup e recuperação, selecione **Exibir solicitação de API**.
2. Para copiar os comandos para a área de transferência, selecione o ícone **Copiar**.

O que se segue?

- Você pode "gerencie seus arquivos de backup e políticas de backup". Isso inclui iniciar e parar backups, excluir backups, adicionar e alterar o agendamento de backup e muito mais.
- Você pode "gerencie as configurações de backup no nível do cluster". Isso inclui alterar a largura de banda da rede disponível para fazer upload de backups para o armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Também "restaure volumes, pastas ou arquivos individuais a partir de um arquivo de backup" é possível acessar um sistema ONTAP no local.

Fazer backup de dados ONTAP on-premises para o StorageGRID

Siga estas etapas para começar a fazer backup de dados de volume de seus sistemas ONTAP primários no local para um sistema de storage secundário e para o storage de objetos em seus sistemas NetApp StorageGRID.

"Sistemas ONTAP no local" incluem sistemas FAS, AFF e ONTAP Select.

Início rápido

Comece rapidamente seguindo estes passos. Os detalhes de cada etapa são fornecidos nas seções a seguir deste tópico.

Identifique o método de conexão que você usará

Analise como você conetará seu cluster ONTAP local diretamente ao StorageGRID pela Internet pública ou se usará uma VPN e roteará o tráfego por meio de uma interface de endpoint VPC privada para o StorageGRID.

Identificar o método de ligação.

2 Prepare o conetor BlueXP

Se você já tem um conetor implantado em suas instalações, então você está pronto. Caso contrário, você precisará criar um BlueXP Connector para fazer backup dos dados do ONTAP no StorageGRID. Você também precisará personalizar as configurações de rede para o conetor para que ele possa se conetar ao StorageGRID.

Saiba como criar um conetor e como definir as definições de rede necessárias.

3 Verifique os requisitos de licença

Você precisará verificar os requisitos de licença para StorageGRID e BlueXP .

Verifique os requisitos de licençaConsulte a .

4 Preparar os clusters do ONTAP

Descubra os clusters do ONTAP no BlueXP , verifique se os clusters atendem aos requisitos mínimos e personalize as configurações de rede para que os clusters possam se conectar ao StorageGRID.

Saiba como preparar os clusters do ONTAP.

5 Prepare o StorageGRID como destino do backup

Configure permissões para que o conetor crie e gerencie o bucket do StorageGRID. Você também precisará configurar permissões para o cluster do ONTAP no local para que ele possa ler e gravar dados no bucket.

Opcionalmente, você pode configurar suas próprias chaves gerenciadas personalizadas para criptografia de dados em vez de usar as chaves de criptografia padrão do StorageGRID. Saiba como preparar seu ambiente StorageGRID para receber backups do ONTAP.

6 Ative backups no ONTAP volumes

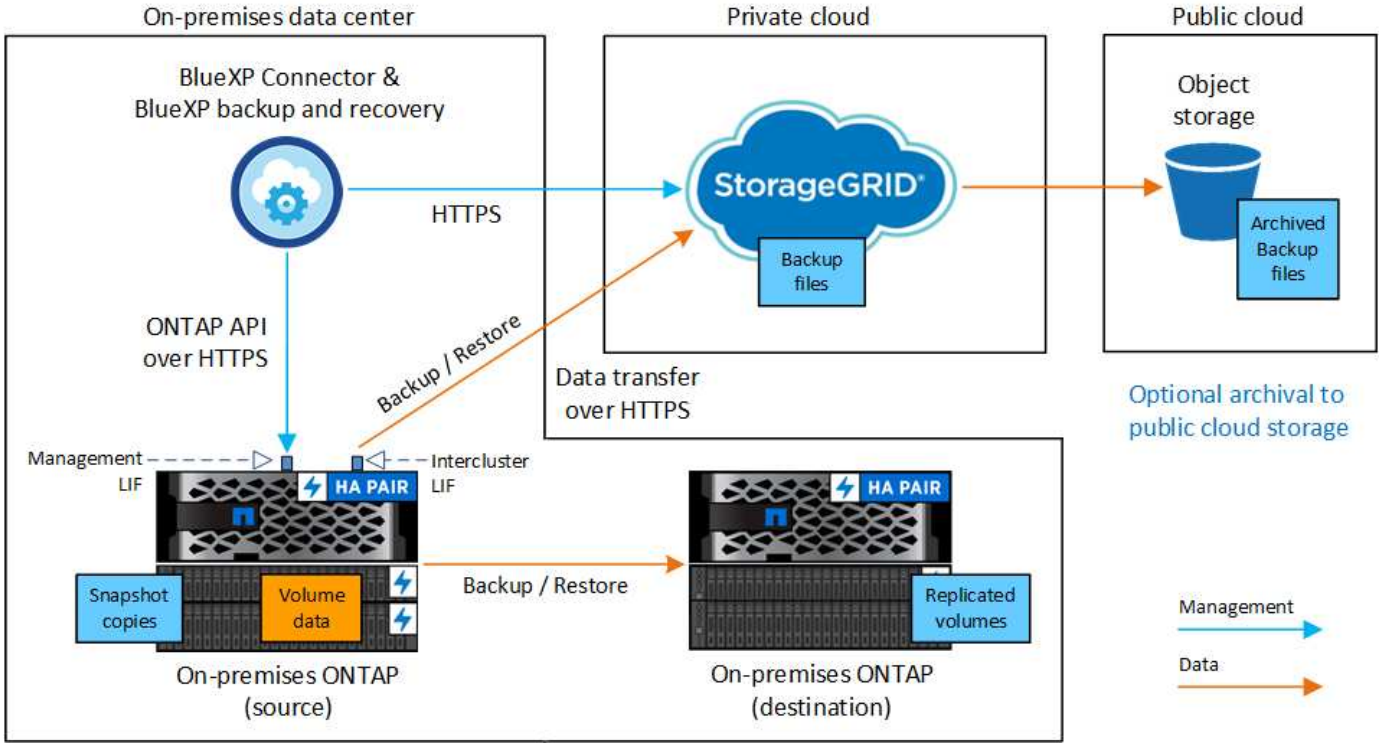
Selecione o ambiente de trabalho e clique em **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito. Em seguida, siga o assistente de configuração para selecionar as políticas de replicação e backup que você usará e os volumes que você deseja fazer backup.

Ative backups no ONTAP volumes.

Identificar o método de ligação

A imagem a seguir mostra cada componente ao fazer backup de um sistema ONTAP no local para o StorageGRID e as conexões que você precisa preparar entre eles.

Opcionalmente, você pode se conectar a um sistema ONTAP secundário no mesmo local para replicar volumes.



Quando o conetor e o sistema ONTAP no local são instalados em um local local sem acesso à Internet (um "local escuro"), o sistema StorageGRID deve estar localizado no mesmo data center local. O arquivamento de arquivos de backup mais antigos na nuvem pública não é suportado em configurações de site escuro.

Prepare o conetor BlueXP

O conetor BlueXP é o software principal para a funcionalidade BlueXP . É necessário um conetor para fazer backup e restaurar os dados do ONTAP.

Crie ou troque os conetores

Ao fazer backup dos dados para o StorageGRID, um BlueXP Connector deve estar disponível no local. Você precisará instalar um novo conetor ou certificar-se de que o conetor atualmente selecionado reside no local. O conetor pode ser instalado em um site com ou sem acesso à Internet.

- "Saiba mais sobre conetores"
- "Instalar o conetor em um host Linux com acesso à Internet"
- "Instalar o conetor em um host Linux sem acesso à Internet"
- "Comutação entre conetores"

Preparar os requisitos de rede do conetor

Certifique-se de que a rede onde o conetor está instalado permite as seguintes ligações:

- Uma conexão HTTPS pela porta 443 para o nó de gateway StorageGRID
- Uma conexão HTTPS pela porta 443 ao LIF de gerenciamento de cluster do ONTAP
- Uma conexão de saída de Internet pela porta 443 para backup e recuperação do BlueXP (não é necessário quando o conetor é instalado em um site "escuro")

Considerações sobre o modo privado (local escuro)

- A funcionalidade de backup e recuperação do BlueXP está integrada ao BlueXP Connector. Quando ele é instalado no modo privado, você precisará atualizar o software do conetor periodicamente para ter acesso a novos recursos. Verifique o "Novidades sobre backup e recuperação do BlueXP " para ver os novos recursos em cada versão de backup e recuperação do BlueXP . Quando quiser usar os novos recursos, siga as etapas para "Atualize o software do conetor".

  A nova versão do backup e recuperação do BlueXP , que inclui a capacidade de agendar e criar cópias Snapshot e volumes replicados, além da criação de backups para storage de objetos, exige que você esteja usando a versão 3.9.31 ou superior do BlueXP Connector. Portanto, é recomendável que você obtenha esta versão mais recente para gerenciar todos os seus backups.

- Quando você usa o backup e a recuperação do BlueXP em um ambiente SaaS, o backup e a configuração de recuperação do BlueXP fazem o backup na nuvem. Quando você usa backup e recuperação do BlueXP em um site sem acesso à Internet, os dados de configuração de backup e recuperação do BlueXP são copiados para o bucket do StorageGRID onde seus backups estão sendo armazenados. Se alguma vez tiver uma falha de conetor no seu site de modo privado, pode "Restaure os dados de backup e recuperação do BlueXP para um novo conetor".

Verifique os requisitos de licença

Antes de ativar o backup e a recuperação do BlueXP para seu cluster, você precisará comprar e ativar uma licença BYOL de recuperação e backup do BlueXP da NetApp. Esta licença é para a conta e pode ser usada em vários sistemas.

Você precisará do número de série do NetApp que permite usar o serviço durante a duração e a capacidade da licença. "Saiba como gerenciar suas licenças BYOL".

O licenciamento PAYGO não é suportado ao fazer backup de arquivos para o StorageGRID.

Preparar os clusters do ONTAP

Você precisará preparar seu sistema ONTAP de origem no local e qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local.

Preparar os clusters do ONTAP envolve as etapas a seguir:

- Descubra os seus sistemas ONTAP no BlueXP
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos
- Verificar os requisitos de rede do ONTAP para replicação de volumes

Descubra os seus sistemas ONTAP no BlueXP

Tanto o sistema ONTAP de origem no local quanto qualquer sistema ONTAP ou Cloud Volumes ONTAP secundário no local devem estar disponíveis no BlueXP Canvas.

Você precisará saber o endereço IP de gerenciamento de cluster e a senha da conta de usuário admin para adicionar o cluster. "Saiba como descobrir um cluster".

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP são atendidos:

- É recomendado um mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior.
- Uma licença SnapMirror (incluída como parte do pacote Premium ou do pacote de proteção de dados).

  Observação: o "pacote de nuvem híbrida" não é necessário ao usar o backup e a recuperação do BlueXP .

  Aprenda a "gerencie suas licenças de cluster".

- A hora e o fuso horário estão definidos corretamente. Aprenda a "configure a hora do cluster".
- Se você quiser replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar dados.

  "Veja versões compatíveis do ONTAP para relacionamentos do SnapMirror".

Verifique os requisitos de rede do ONTAP para fazer backup de dados para armazenamento de objetos

Você deve configurar os seguintes requisitos no sistema que se coneta ao storage de objetos.

- Quando você usa uma arquitetura de backup fan-out, as configurações a seguir devem ser configuradas no sistema de armazenamento *Primary*.
- Quando você usa uma arquitetura de backup em cascata, as configurações a seguir devem ser configuradas no sistema de armazenamento *secundário*.

São necessários os seguintes requisitos de rede de cluster do ONTAP:

- O cluster do ONTAP inicia uma conexão HTTPS por uma porta especificada pelo usuário do LIF entre clusters para o nó de gateway StorageGRID para operações de backup e restauração. A porta é configurável durante a configuração da cópia de segurança.

  O ONTAP lê e grava dados no storage de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

- O ONTAP requer uma conexão de entrada do conetor para o LIF de gerenciamento de cluster. O conetor deve estar no local.
- 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. "Saiba mais sobre IPspaces".

  Ao configurar o backup e a recuperação do BlueXP , 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.

- Os LIFs de clusters dos nós são capazes de acessar o armazenamento de objetos (não é necessário quando o conetor é instalado em um local "escuro").
- Os servidores DNS foram configurados para a VM de armazenamento onde os volumes estão localizados. Consulte como "Configurar serviços DNS para o SVM" .
- Se você usar um IPspace diferente do padrão, talvez seja necessário criar uma rota estática para obter acesso ao armazenamento de objetos.

- Atualize regras de firewall, se necessário, para permitir conexões de serviço de backup e recuperação do BlueXP do ONTAP para o armazenamento de objetos através da porta especificada (normalmente porta 443) e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS através da porta 53 (TCP/UDP).

Verificar os requisitos de rede do ONTAP para replicação de volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o backup e a recuperação do BlueXP , certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede da ONTAP no local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da rede corporativa à rede virtual no provedor de nuvem. Normalmente, esta é uma conexão VPN.
- Os clusters do ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou sistemas locais, revise os requisitos de peering para sistemas ONTAP locais. "Veja os pré-requisitos para peering de cluster na documentação do ONTAP".

Requisitos de rede da 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.

Prepare o StorageGRID como destino do backup

O StorageGRID deve atender aos seguintes requisitos. Consulte "Documentação do StorageGRID" para obter mais informações.

Para obter detalhes sobre os requisitos de proteção de DataLock e ransomware para StorageGRID, "Opções de política de backup para objeto"consulte .

Versões suportadas do StorageGRID

O StorageGRID 10,3 e posterior é suportado.

Para usar a proteção DataLock & ransomware para seus backups, seus sistemas StorageGRID devem estar executando a versão 11.6.0.3 ou superior.

Para categorizar backups mais antigos para storage de arquivamento em nuvem, seus sistemas StorageGRID precisam estar executando a versão 11,3 ou superior. Além disso, seus sistemas StorageGRID devem ser descobertos no BlueXP Canvas.

S3 credenciais

Você precisa ter criado uma conta de locatário do S3 para controlar o acesso ao storage do StorageGRID. "Consulte os documentos do StorageGRID para obter detalhes".

Quando você configura o backup no StorageGRID, o assistente de backup solicita uma chave de acesso S3 e uma chave secreta para uma conta de locatário. A conta de locatário permite que o backup e a recuperação do BlueXP autentiquem e acessem os buckets do StorageGRID usados para armazenar backups. As chaves são necessárias para que a StorageGRID saiba quem está fazendo o pedido.

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 manualmente no bucket do armazenamento de objetos.

Prepare-se para arquivar arquivos de backup mais antigos para o armazenamento em nuvem pública

A disposição em camadas de arquivos de backup mais antigos no storage de arquivamento economiza dinheiro ao usar uma classe de storage menos cara para backups que talvez você não precise. O StorageGRID é uma solução local (nuvem privada) que não oferece storage de arquivamento, mas você pode mover arquivos de backup mais antigos para storage de arquivamento em nuvem pública. Quando usados dessa forma, os dados dispostos em camadas no storage de nuvem ou restaurados do armazenamento em nuvem vão entre o StorageGRID e o armazenamento em nuvem - a BlueXP não está envolvida nessa transferência de dados.

O suporte atual permite arquivar backups no armazenamento AWS *S3 Glacier*/*S3 Glacier Deep Archive* ou *Azure Archive*.

Requisitos ONTAP

- O cluster deve estar usando o ONTAP 9.12,1 ou superior.

Requisitos StorageGRID

- Seu StorageGRID deve estar usando 11,4 ou superior.
- Seu StorageGRID deve ser "Descoberto e disponível na tela BlueXP ".

Requisitos do Amazon S3

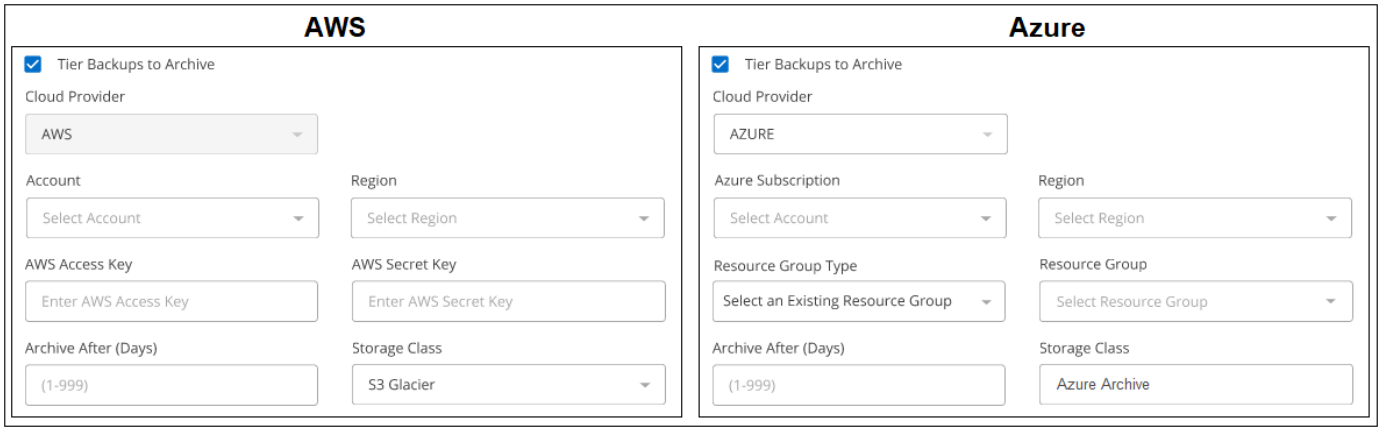
- Você precisará se inscrever em uma conta do Amazon S3 para o espaço de armazenamento onde seus backups arquivados estarão localizados.
- Você pode optar por categorizar backups no storage do AWS S3 Glacier ou do S3 Glacier Deep Archive. "Saiba mais sobre os níveis de arquivamento da AWS".
- O StorageGRID deve ter acesso de controle total ao bucket (`s3:*`); no entanto, se isso não for possível, a política de bucket deve conceder as seguintes permissões do S3 ao StorageGRID:
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`

- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

Requisitos de Blob do Azure

- Você precisará se inscrever em uma assinatura do Azure para o espaço de armazenamento onde seus backups arquivados estarão localizados.
- O assistente de ativação permite que você use um Grupo de recursos existente para gerenciar o contentor Blob que armazenará os backups ou você pode criar um novo Grupo de recursos.

Ao definir as configurações de arquivamento para a política de backup do cluster, insira as credenciais do provedor de nuvem e selecione a classe de armazenamento que deseja usar. O backup e a recuperação do BlueXP criam o bucket da nuvem quando você ativa o backup para o cluster. As informações necessárias para o armazenamento de arquivamento da AWS e do Azure são mostradas abaixo.



As configurações de política de arquivamento selecionadas gerarão uma política de gerenciamento de ciclo de vida de informações (ILM) no StorageGRID e adicionarão as configurações como "regras".

- Se houver uma política ILM ativa existente, novas regras serão adicionadas à política ILM para mover os dados para o nível de arquivo.
- Se houver uma política ILM existente no estado "proposto", a criação e ativação de uma nova política ILM não será possível. "Saiba mais sobre as políticas e regras do StorageGRID ILM".

Ative backups no ONTAP volumes

Ative os backups a qualquer momento diretamente do seu ambiente de trabalho no local.

Um assistente leva você através dos seguintes passos principais:

- Selecione os volumes que deseja fazer backup
- Defina a estratégia de backup
- Reveja as suas seleções

Você também pode Mostrar os comandos APIna etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para futuros ambientes de trabalho.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:

   - Na tela BlueXP , selecione o ambiente de trabalho e selecione **Ativar > volumes de backup** ao lado do serviço de backup e recuperação no painel direito.

     Se o destino dos backups existir como um ambiente de trabalho no Canvas, você poderá arrastar o cluster do ONTAP para o armazenamento de objetos.

   - Selecione **volumes** na barra de backup e recuperação. Na guia volumes, selecione a opção **ações (…)** e selecione **Ativar Backup** para um único volume (que ainda não tem replicação ou backup para armazenamento de objetos já ativado).

   A página Introdução do assistente mostra as opções de proteção, incluindo snapshots locais, replicação e backups. Se você fez a segunda opção nesta etapa, a página Definir estratégia de backup será exibida com um volume selecionado.

2. Continue com as seguintes opções:

   - Se já tiver um conetor BlueXP , está tudo definido. Basta selecionar **seguinte**.
   - Se você ainda não tiver um conetor BlueXP , a opção **Adicionar um conetor** será exibida. Prepare o conetor BlueXP Consulte a .

Selecione os volumes que deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem uma ou mais das seguintes opções: Política de snapshot, política de replicação, política de backup para objeto.

Você pode optar por proteger o FlexVol ou o FlexGroup volumes. No entanto, não é possível selecionar uma combinação desses volumes ao ativar o backup para um ambiente de trabalho. Veja como "ative o backup para volumes adicionais no ambiente de trabalho"(FlexVol ou FlexGroup) depois de configurar o backup para os volumes iniciais.

- Você pode ativar um backup apenas em um único volume FlexGroup de cada vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock. Todos os volumes devem ter o SnapLock Enterprise ativado ou o SnapLock desativado.

Passos

Observe que se os volumes escolhidos já tiverem políticas Snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que deseja proteger.

   - Opcionalmente, filtre as linhas para mostrar apenas volumes com determinados tipos de volume, estilos e muito mais para facilitar a seleção.
   - Depois de selecionar o primeiro volume, você pode selecionar todos os volumes FlexVol (volumes FlexGroup podem ser selecionados um de cada vez somente). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e marque a caixa na linha de título. (

).
   - Para fazer backup de volumes individuais, marque a caixa para cada volume (

).
2. Selecione **seguinte**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Quer você queira uma ou todas as opções de backup: Snapshots locais, replicação e backup no storage de objetos
- Arquitetura
- Política de instantâneo local
- Destino e política de replicação

> Se os volumes escolhidos tiverem políticas de Snapshot e replicação diferentes das políticas selecionadas nesta etapa, as políticas existentes serão sobrescritas.

- Backup para informações de armazenamento de objetos (provedor, criptografia, rede, política de backup e opções de exportação).

Passos

1. Na página Definir estratégia de backup, escolha uma ou todas as opções a seguir. Todos os três são selecionados por padrão:
   - **Instantâneos locais**: Se você estiver executando replicação ou fazendo backup em armazenamento de objetos, os snapshots locais devem ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP.
   - **Backup**: Faz backup de volumes para armazenamento de objetos.
2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascading**: A informação flui do primário para o secundário e, em seguida, do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do primário para o secundário *e* do armazenamento primário para o objeto.

     Para obter detalhes sobre essas arquiteturas, "Planeje sua jornada de proteção"consulte .
3. **Snapshot local**: Escolha uma política Snapshot existente ou crie uma nova.

   > Para criar uma política personalizada antes de ativar a captura Instantânea, "Crie uma política"consulte .

   Para criar uma política, selecione **criar nova política** e faça o seguinte:
   - Introduza o nome da política.
   - Selecione até 5 programações, normalmente de frequências diferentes.
   - Selecione **criar**.
4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o ambiente de trabalho de destino e SVM. Opcionalmente, selecione o agregado de destino ou agregados e o prefixo ou sufixo que será adicionado ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma.

Para criar uma política personalizada antes de ativar a replicação, "Crie uma política"consulte .

Para criar uma política, selecione **criar nova política** e faça o seguinte:

- Introduza o nome da política.
- Selecione até 5 programações, normalmente de frequências diferentes.
- Selecione **criar**.

5. **Fazer backup para Objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Fornecedor**: Selecione **StorageGRID**.
   - * Configurações do provedor*: Insira os detalhes do FQDN do nó de gateway do provedor, porta, chave de acesso e chave secreta.

     A chave de acesso e a chave secreta destinam-se ao usuário do IAM criado para dar ao cluster do ONTAP acesso ao intervalo.

   - **Rede**: Escolha o espaço de IPspace no cluster do ONTAP onde residem os volumes que você deseja fazer backup. As LIFs entre clusters para este espaço IPspace devem ter acesso de saída à Internet (não é necessário quando o conetor é instalado em um site "escuro").

     A seleção do espaço de IPspace correto garante que o backup e a recuperação do BlueXP possam configurar uma conexão do ONTAP para o armazenamento de objetos do StorageGRID.

   - **Política de backup**: Selecione uma política de armazenamento de backup para objetos existente ou crie uma.

     Para criar uma política personalizada antes de ativar a cópia de segurança, "Crie uma política"consulte .

     Para criar uma política, selecione **criar nova política** e faça o seguinte:

     - Introduza o nome da política.
     - Selecione até 5 programações, normalmente de frequências diferentes.
     - Para políticas de backup para objeto, defina as configurações DataLock e proteção contra ransomware. Para obter detalhes sobre DataLock e proteção contra ransomware, "Configurações de política de backup para objeto"consulte .

       Se o cluster estiver usando o ONTAP 9.11,1 ou superior, você pode optar por proteger seus backups contra exclusão e ataques de ransomware configurando *DataLock e ransomware Protection*. *DataLock* protege seus arquivos de backup de serem modificados ou excluídos, e *ransomware Protection* verifica seus arquivos de backup para procurar evidências de um ataque de ransomware em seus arquivos de backup.

     - Selecione **criar**.

     Se o cluster estiver usando o ONTAP 9.12,1 ou superior e o sistema StorageGRID estiver usando a versão 11,4 ou superior, você poderá categorizar backups mais antigos em categorias de arquivamento de nuvem pública após um determinado número de dias. O suporte atual é para camadas de storage do AWS S3 Glacier/S3 Glacier Deep Archive ou do Azure Archive. Veja como configurar seus sistemas para essa funcionalidade.

- **Tier backup em nuvem pública**: Selecione o provedor de nuvem para o qual você deseja categorizar backups e insira os detalhes do provedor.

  Selecione ou crie um novo cluster do StorageGRID. Para obter detalhes sobre como criar um cluster StorageGRID para que o BlueXP possa descobri-lo, "Documentação do StorageGRID" consulte .

- **Exportar cópias Snapshot existentes para o armazenamento de objetos como cópias de backup**: Se houver cópias Snapshot locais para volumes neste ambiente de trabalho que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este ambiente de trabalho (por exemplo, diário, semanal, etc.), esse prompt adicional será exibido. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup para garantir a proteção mais completa para seus volumes.

6. Selecione **seguinte**.

Reveja as suas seleções

Esta é a oportunidade de rever as suas seleções e fazer ajustes, se necessário.

Passos

1. Na página Review (Revisão), reveja as suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos de política Snapshot com os rótulos de política de replicação e backup**. Isso cria snapshots com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O backup e a recuperação do BlueXP começam a fazer os backups iniciais dos seus volumes. A transferência de linha de base do volume replicado e do arquivo de backup inclui uma cópia completa dos dados de origem. As transferências subsequentes contêm cópias diferenciais dos dados de storage primário contidos nas cópias Snapshot.

Um volume replicado é criado no cluster de destino que será sincronizado com o volume de armazenamento primário.

Um bucket S3 é criado na conta de serviço indicada pela chave de acesso S3 e chave secreta que você inseriu e os arquivos de backup são armazenados lá.

O Painel de backup de volume é exibido para que você possa monitorar o estado dos backups.

Também pode monitorizar o estado dos trabalhos de cópia de segurança e restauro utilizando o "Painel monitorização de trabalhos".

Mostrar os comandos API

Você pode querer exibir e, opcionalmente, copiar os comandos API usados no assistente Ativar backup e recuperação. Você pode querer fazer isso para automatizar a ativação de backup em futuros ambientes de trabalho.

Passos

1. No assistente Ativar backup e recuperação, selecione **Exibir solicitação de API**.
2. Para copiar os comandos para a área de transferência, selecione o ícone **Copiar**.

O que se segue?

- Você pode "gerencie seus arquivos de backup e políticas de backup". Isso inclui iniciar e parar backups, excluir backups, adicionar e alterar o agendamento de backup e muito mais.
- Você pode "gerencie as configurações de backup no nível do cluster". Isso inclui alterar a largura de banda da rede disponível para fazer upload de backups para o armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Também "restaure volumes, pastas ou arquivos individuais a partir de um arquivo de backup" é possível acessar um sistema ONTAP no local.

Gerenciar backups para seus sistemas ONTAP

Você pode gerenciar backups para seus sistemas Cloud Volumes ONTAP e ONTAP locais alterando o agendamento de backup, habilitando/desabilitando backups de volume, pausar backups, excluir backups e muito mais. Isso inclui todos os tipos de backups, incluindo cópias Snapshot, volumes replicados e arquivos de backup no storage de objetos.

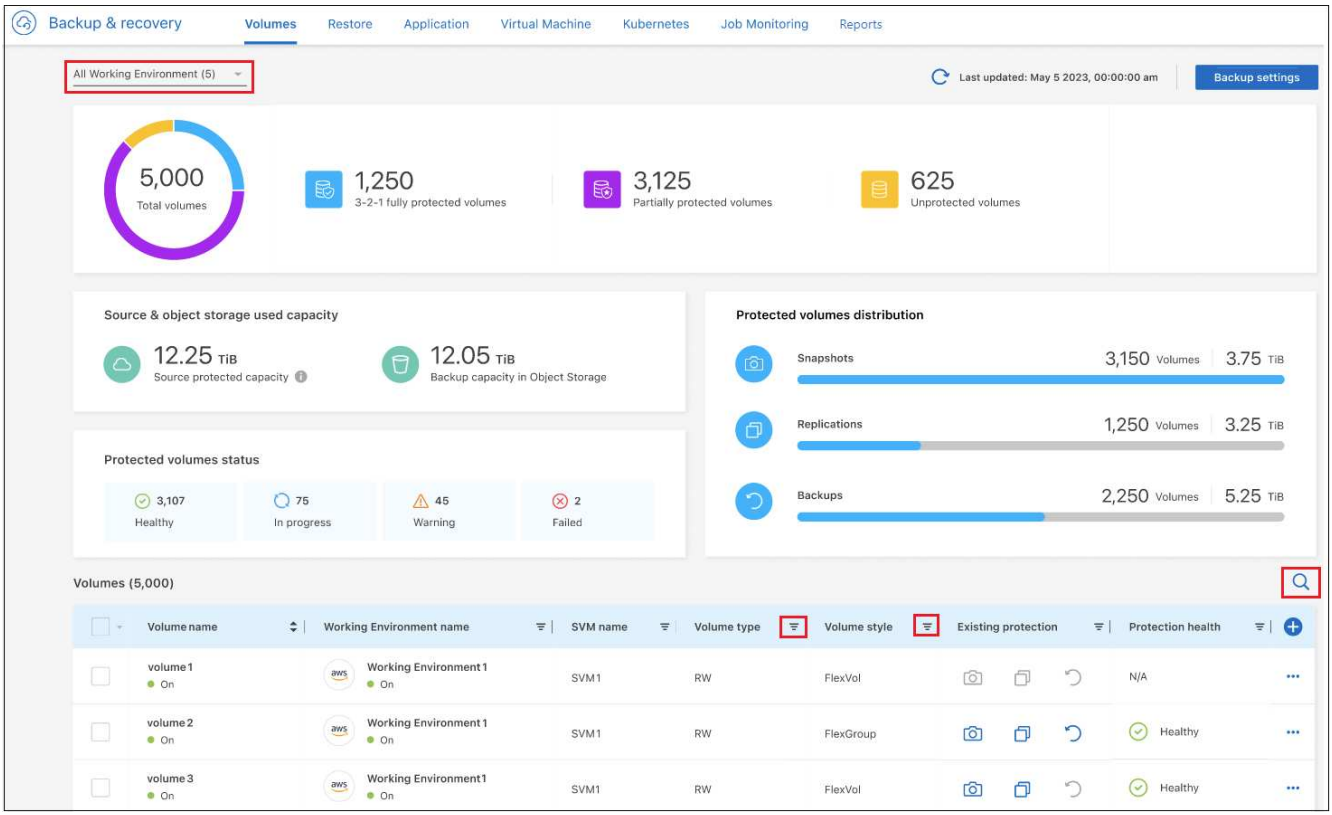
Não gerencie nem altere arquivos de backup diretamente nos sistemas de storage ou no ambiente do fornecedor de nuvem. Isso pode corromper os arquivos e resultará em uma configuração não suportada.

Exibir o status de backup dos volumes em seus ambientes de trabalho

Você pode exibir uma lista de todos os volumes que estão sendo copiados no Painel de backup do volumes. Isso inclui todos os tipos de backups, incluindo cópias Snapshot, volumes replicados e arquivos de backup no storage de objetos. Você também pode exibir os volumes nos ambientes de trabalho que não estão sendo feitos backup no momento.

Passos

1. No menu BlueXP , selecione **proteção > Backup e recuperação**.
2. Clique na guia **volumes** para exibir a lista de volumes de backup para seus sistemas Cloud Volumes ONTAP e ONTAP locais.



3. Se você estiver procurando volumes específicos em determinados ambientes de trabalho, você pode refinar a lista por ambiente de trabalho e volume. Você também pode usar o filtro de pesquisa ou classificar as colunas com base no estilo de volume (FlexVol ou FlexGroup), no tipo de volume e muito mais.

   Para mostrar colunas adicionais (agregados, estilo de segurança (Windows ou UNIX), política de instantâneos, política de replicação e política de backup), selecione .

4. Revise o status das opções de proteção na coluna "proteção existente". Os ícones 3 representam "cópias Snapshot locais", "volumes replicados" e "backups no storage de objetos".

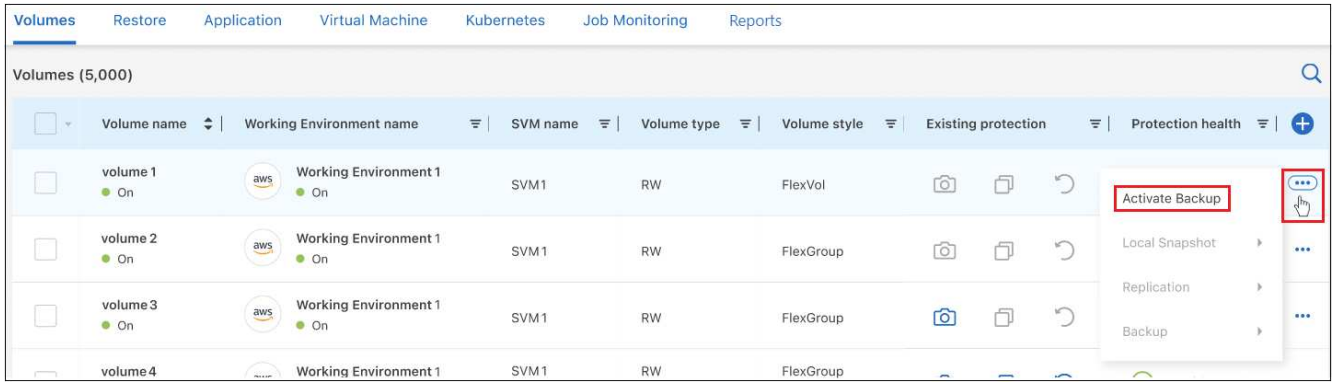
   Cada ícone fica azul quando esse tipo de backup é ativado e fica cinza quando o tipo de backup está inativo. Você pode passar o cursor sobre cada ícone para ver a política de backup que está sendo usada e outras informações pertinentes para cada tipo de backup.

Ative o backup em volumes adicionais em um ambiente de trabalho

Se você ativou o backup somente em alguns volumes em um ambiente de trabalho quando ativou o backup e a recuperação do BlueXP pela primeira vez, poderá ativar backups em volumes adicionais posteriormente.

Passos

1. Na guia **volumes**, identifique o volume no qual você deseja ativar os backups, selecione o menu ações no final da linha e selecione **Ativar backup**.



2. Na página *Definir estratégia de backup*, selecione a arquitetura de backup e defina as políticas e outros detalhes para cópias Snapshot locais, volumes replicados e arquivos de backup. Consulte os detalhes das opções de backup dos volumes iniciais ativados neste ambiente de trabalho. Em seguida, clique em **seguinte**.
3. Reveja as definições de cópia de segurança deste volume e, em seguida, clique em **Ativar cópia de segurança**.

Se pretender ativar a cópia de segurança em vários volumes ao mesmo tempo com definições de cópia de segurança idênticas, consulte Editar as definições de cópia de segurança em vários volumes para obter detalhes.

Altere as definições de cópia de segurança atribuídas aos volumes existentes

Você pode alterar as políticas de backup atribuídas aos volumes existentes que tenham atribuído políticas. É possível alterar as políticas para cópias Snapshot locais, volumes replicados e arquivos de backup. Qualquer nova política de Snapshot, replicação ou backup que você queira aplicar aos volumes já deve existir.

Editar as definições de cópia de segurança num único volume

Passos

1. Na guia **volumes**, identifique o volume que você deseja fazer alterações de política, selecione o menu ações •••no final da linha e selecione **Editar estratégia de backup**.

2. Na página *Editar estratégia de backup*, faça alterações nas políticas de backup existentes para cópias Snapshot locais, volumes replicados e arquivos de backup e clique em **Avançar**.

   Se você ativou o *DataLock e a proteção contra ransomware* para backups na nuvem na política de backup inicial ao ativar o backup e a recuperação do BlueXP para esse cluster, você verá apenas outras políticas

que foram configuradas com o DataLock. E se você não ativou o *DataLock e a proteção contra ransomware* ao ativar o backup e a recuperação do BlueXP , verá apenas outras políticas de backup na nuvem que não tenham o DataLock configurado.

3. Reveja as definições de cópia de segurança deste volume e, em seguida, clique em **Ativar cópia de segurança**.

Editar as definições de cópia de segurança em vários volumes

Se pretender utilizar as mesmas definições de cópia de segurança em vários volumes, pode ativar ou editar as definições de cópia de segurança em vários volumes ao mesmo tempo. Você pode selecionar volumes que não têm configurações de backup, apenas configurações de Snapshot, apenas backup em configurações de nuvem etc., e fazer alterações em massa em todos esses volumes com diversas configurações de backup.

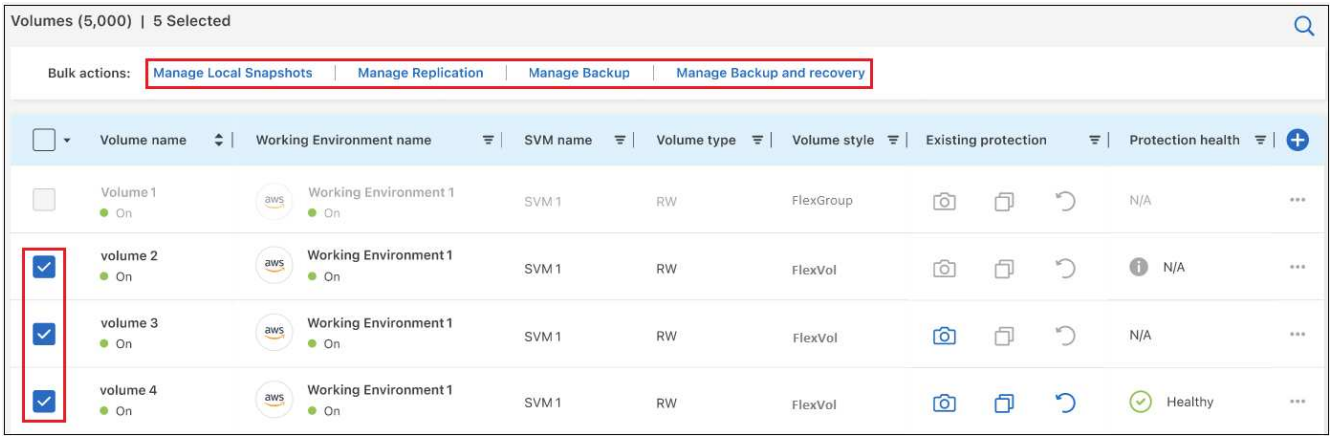
Ao trabalhar com vários volumes, todos os volumes devem ter estas caraterísticas comuns:

- mesmo ambiente de trabalho
- Mesmo estilo (volume FlexVol ou FlexGroup)
- Mesmo tipo (volume de leitura/gravação ou proteção de dados)

Quando mais de cinco volumes estão ativados para backup, o backup e a recuperação do BlueXP inicializam apenas cinco volumes de cada vez. Quando eles estiverem concluídos, ele cria o próximo lote de cinco subtrabalhos para iniciar o próximo conjunto e continua até que todos os volumes sejam inicializados.

Passos

1. Na guia **volumes**, filtre pelo ambiente de trabalho no qual os volumes residem.
2. Selecione todos os volumes nos quais deseja gerenciar as configurações de backup.
3. Dependendo do tipo de ação de backup que você deseja configurar, clique no botão no menu ações em massa:



Ação de cópia de segurança…	Clique neste botão…
Gerir as definições de cópia de segurança Snapshot	**Gerenciar snapshots locais**
Gerenciar configurações de backup de replicação	**Gerenciar replicação**
Gerenciar configurações de backup em nuvem	**Gerenciar Backup**
Gerencie vários tipos de configurações de backup. Essa opção permite que você altere a arquitetura de backup também.	**Gerenciar backup e recuperação**

4. Na página de backup exibida, faça alterações nas políticas de backup existentes para cópias Snapshot locais, volumes replicados ou arquivos de backup e clique em **Salvar**.

   Se você ativou o *DataLock e a proteção contra ransomware* para backups na nuvem na política de backup inicial ao ativar o backup e a recuperação do BlueXP para esse cluster, você verá apenas outras políticas que foram configuradas com o DataLock. E se você não ativou o *DataLock e a proteção contra ransomware* ao ativar o backup e a recuperação do BlueXP , verá apenas outras políticas de backup na nuvem que não tenham o DataLock configurado.

Crie um backup manual de volume a qualquer momento

Você pode criar um backup sob demanda a qualquer momento para capturar o estado atual do volume. Isso pode ser útil se alterações muito importantes tiverem sido feitas em um volume e você não quiser esperar pelo próximo backup programado para proteger esses dados. Você também pode usar essa funcionalidade para criar um backup para um volume que não está sendo feito o backup no momento e deseja capturar seu estado atual.

Você pode criar uma cópia Snapshot ad-hoc ou um backup para objeto de um volume. Não é possível criar um volume replicado ad hoc.

O nome do backup inclui o carimbo de data/hora para que você possa identificar seu backup sob demanda de outros backups programados.

Se você ativou *DataLock e proteção contra ransomware* ao ativar o backup e a recuperação do BlueXP para este cluster, o backup sob demanda também será configurado com DataLock, e o período de retenção será de 30 dias. Varreduras de ransomware não são compatíveis com backups ad-hoc. "Saiba mais sobre a proteção DataLock e ransomware".

Observe que ao criar um backup ad-hoc, um instantâneo é criado no volume de origem. Como esse instantâneo não faz parte de um agendamento de instantâneo normal, ele não será desligado. Você pode querer excluir manualmente esse instantâneo do volume de origem assim que o backup for concluído. Isso permitirá que os blocos relacionados a essa captura Instantânea sejam liberados. O nome do instantâneo começará com `cbs-snapshot-adhoc-`. "Veja como excluir um instantâneo usando a CLI do ONTAP".

O backup de volume sob demanda não é compatível com volumes de proteção de dados.

Passos

1. Na guia **volumes**, clique ••• para obter o volume e selecione **Backup** > **criar Backup ad hoc**.

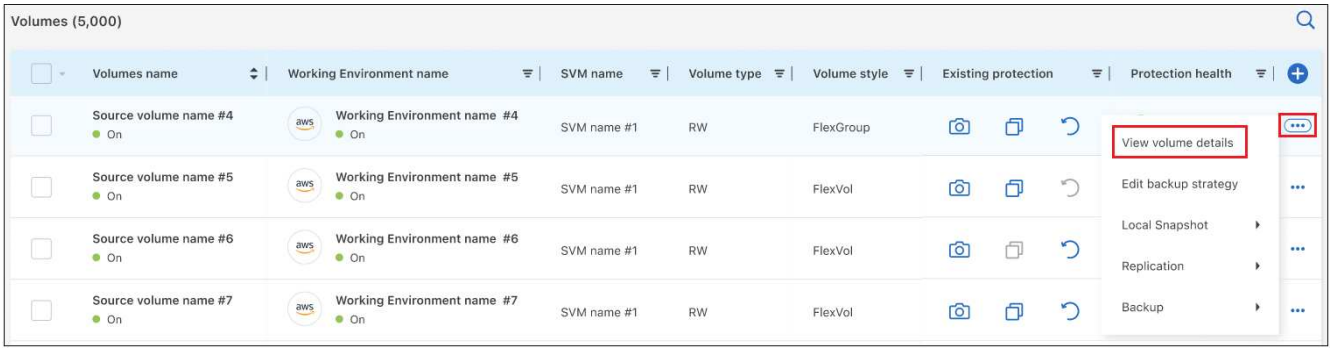
A coluna Estado da cópia de segurança para esse volume apresenta "em curso" até que a cópia de segurança seja criada.

Veja a lista de backups para cada volume

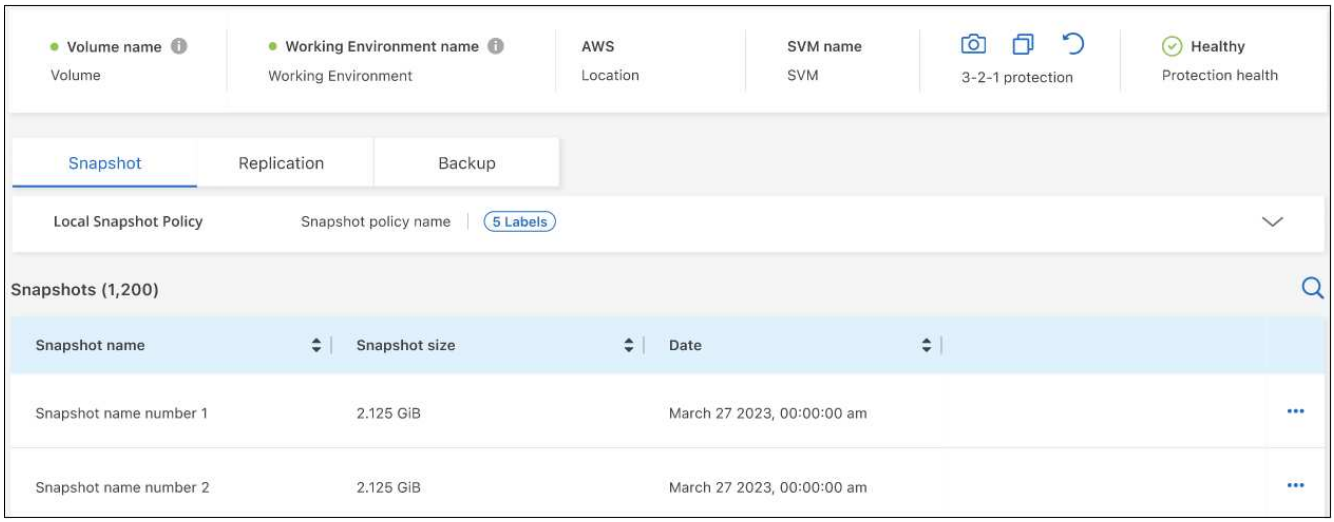
Pode ver a lista de todos os ficheiros de cópia de segurança existentes para cada volume. Esta página exibe detalhes sobre o volume de origem, o local de destino e os detalhes do backup, como o último backup realizado, a política de backup atual, o tamanho do arquivo de backup e muito mais.

Passos

1. Na guia **volumes**, clique ••• para obter o volume de origem e selecione **Exibir detalhes do volume**.



Os detalhes do volume e da lista de cópias Snapshot são exibidos por padrão.



2. Selecione **Snapshot**, **replicação** ou **Backup** para ver a lista de todos os arquivos de backup para cada tipo de backup.

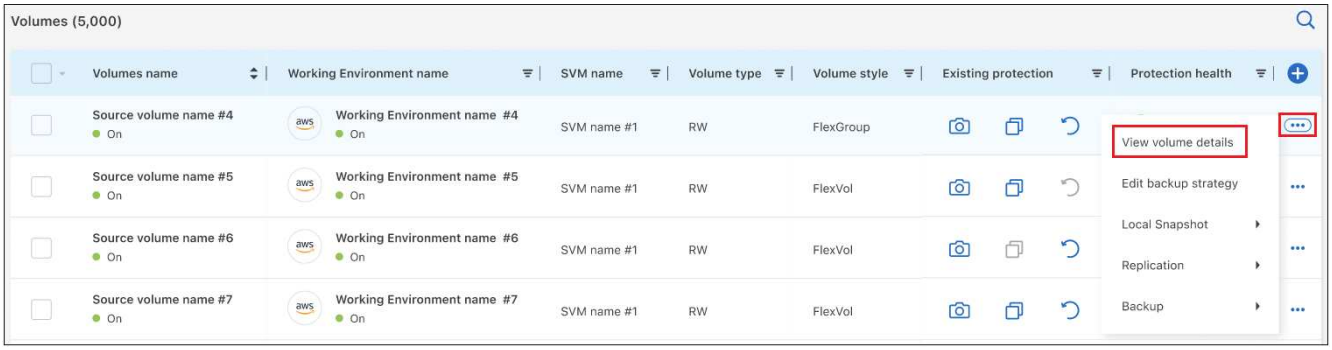
Executar uma verificação de ransomware em um backup de volume no storage de objetos

O software de proteção contra ransomware do NetApp verifica seus arquivos de backup para procurar evidências de um ataque de ransomware quando um backup para arquivo de objeto é criado e quando os dados de um arquivo de backup estão sendo restaurados. Você também pode executar uma verificação de proteção contra ransomware sob demanda a qualquer momento para verificar a usabilidade de um arquivo de backup específico no storage de objetos. Isso pode ser útil se você tiver um problema de ransomware em um determinado volume e quiser verificar se os backups desse volume não são afetados.

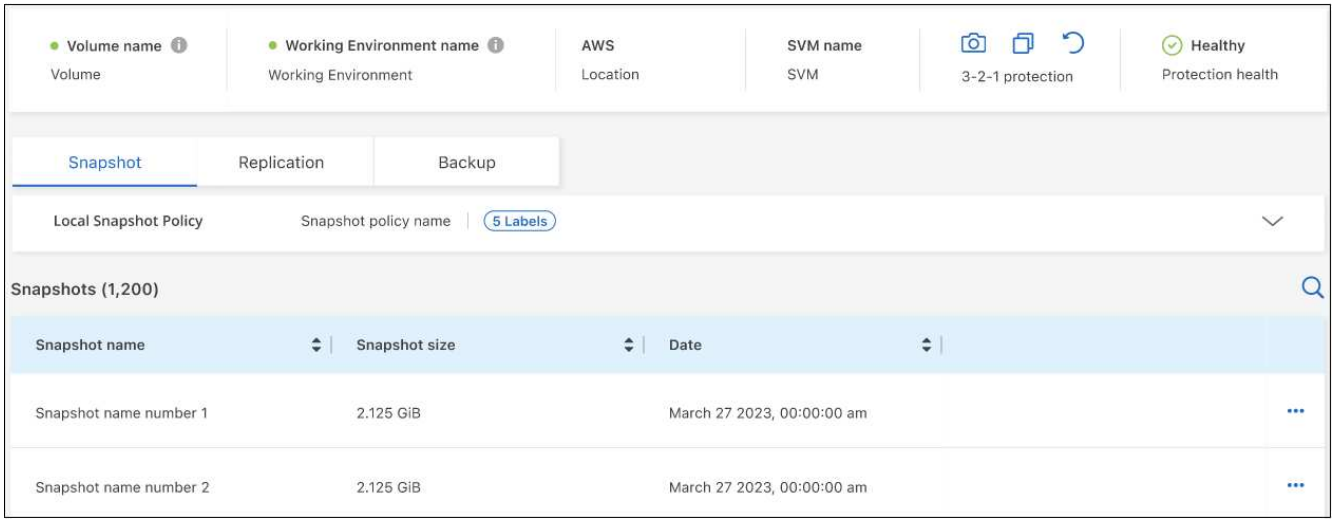
Esse recurso estará disponível somente se o backup de volume tiver sido criado a partir de um sistema com ONTAP 9.11,1 ou superior e se você tiver ativado *DataLock e ransomware Protection* na política de backup para objeto.

Passos

1. Na guia **volumes**, clique ••• para obter o volume de origem e selecione **Exibir detalhes do volume**.

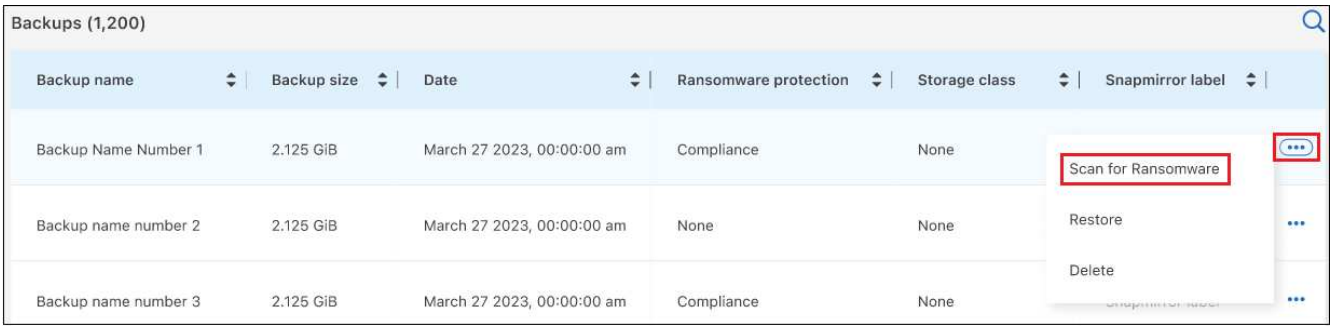


São apresentados os detalhes do volume.



2. Selecione **Backup** para ver a lista de arquivos de backup no armazenamento de objetos.

3. Clique ••• no arquivo de backup de volume que você deseja verificar para ransomware e clique em **Scan for ransomware**.



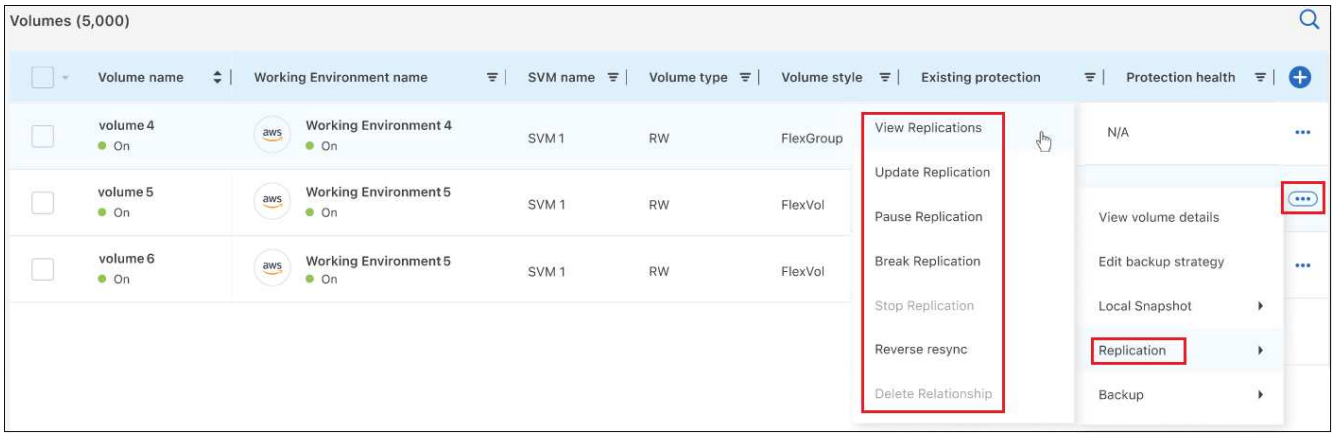
A coluna proteção contra ransomware mostrará que a verificação está em andamento.

Gerenciar a relação de replicação com o volume de origem

Depois de configurar a replicação de dados entre dois sistemas, você pode gerenciar a relação de replicação de dados.

Passos

1. Na guia **volumes**, clique ••• para obter o volume de origem e selecione a opção **replicação**. Você pode ver todas as opções disponíveis.
2. Selecione a ação de replicação que deseja executar.



A tabela a seguir descreve as ações disponíveis:

Ação	Descrição
Ver replicação	Mostra detalhes sobre a relação de volume: Informações de transferência, informações sobre a última transferência, detalhes sobre o volume e informações sobre a política de proteção atribuída à relação.
Atualizar replicação	Inicia uma transferência incremental para atualizar o volume de destino a ser sincronizado com o volume de origem.
Pausar replicação	Pausar a transferência incremental de cópias Snapshot para atualizar o volume de destino. Você pode continuar mais tarde se quiser reiniciar as atualizações incrementais.
Quebrar replicação	Quebra a relação entre os volumes de origem e destino e ativa o volume de destino para acesso aos dados - faz com que ele leia-escreva. 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. "Saiba como configurar um volume de destino para acesso a dados e reativar um volume de origem na documentação do ONTAP"
Abortar replicação	Desativa backups deste volume para o sistema de destino e também desativa a capacidade de restaurar um volume. Quaisquer backups existentes não serão excluídos. Isso não exclui a relação de proteção de dados entre os volumes de origem e destino.
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.
Eliminar relação	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, o que significa que não faz leitura-gravação. Essa ação também excluirá o relacionamento entre pares de cluster e o relacionamento entre pares de VM de storage (SVM), se não houver outros relacionamentos de proteção de dados entre os sistemas.

Resultado

Depois de selecionar uma ação, o BlueXP atualiza a relação.

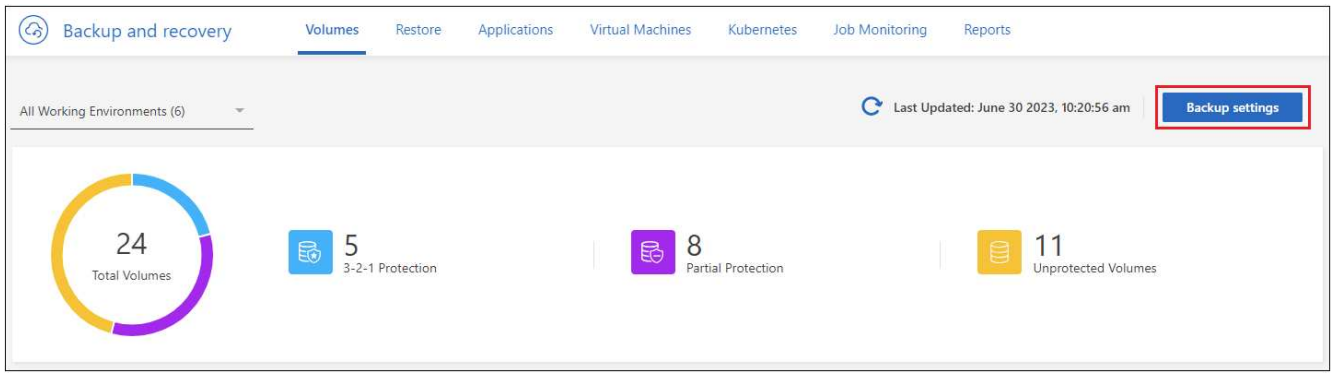
Editar uma política de backup para nuvem existente

Você pode alterar os atributos de uma política de backup aplicada atualmente a volumes em um ambiente de trabalho. A alteração da política de backup afeta todos os volumes existentes que estão usando a diretiva.

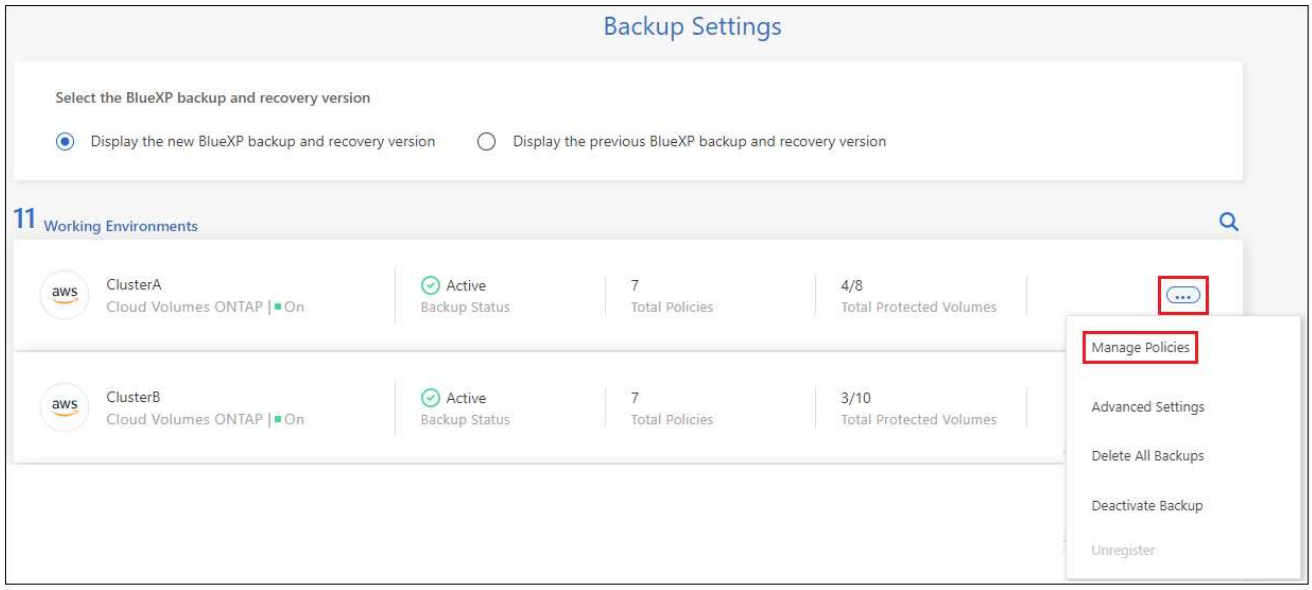
- Se você ativou o *DataLock e a proteção contra ransomware* na política inicial ao ativar o backup e a recuperação do BlueXP para esse cluster, todas as políticas editadas devem ser configuradas com a mesma configuração do DataLock (Governança ou conformidade). E se você não ativou o *DataLock e a proteção contra ransomware* ao ativar o backup e a recuperação do BlueXP , você não poderá ativar o DataLock agora.
- Ao criar backups na AWS, se você escolher *S3 Glacier* ou *S3 Glacier Deep Archive* na sua primeira política de backup ao ativar o backup e a recuperação do BlueXP , esse nível será o único nível de arquivamento disponível ao editar políticas de backup. E se você não selecionou nenhum nível de arquivamento em sua primeira política de backup, *S3 Glacier* será sua única opção de arquivamento ao editar uma política.

Passos

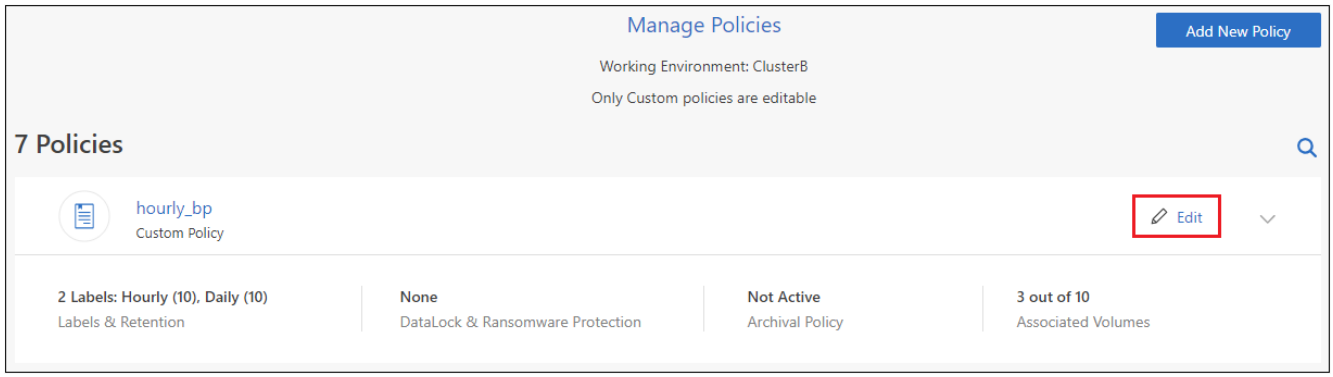
1. Na guia **volumes**, selecione **Configurações de backup**.



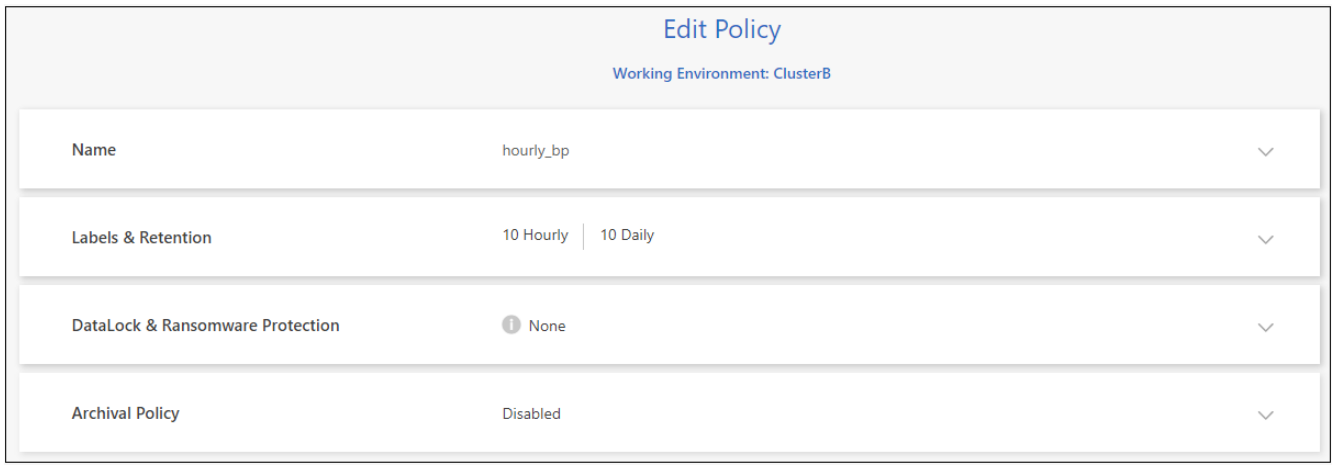
2. Na página *Configurações de backup*, clique ••• em para o ambiente de trabalho onde você deseja alterar as configurações de política e selecione **Gerenciar políticas**.



3. Na página *Gerenciar políticas*, clique em **Editar** para a política de backup que você deseja alterar nesse ambiente de trabalho.



4. Na página *Editar política*, clique ⌄ para expandir a seção *rótulos e retenção* para alterar a retenção de agendamento e/ou backup e clique em **Salvar**.



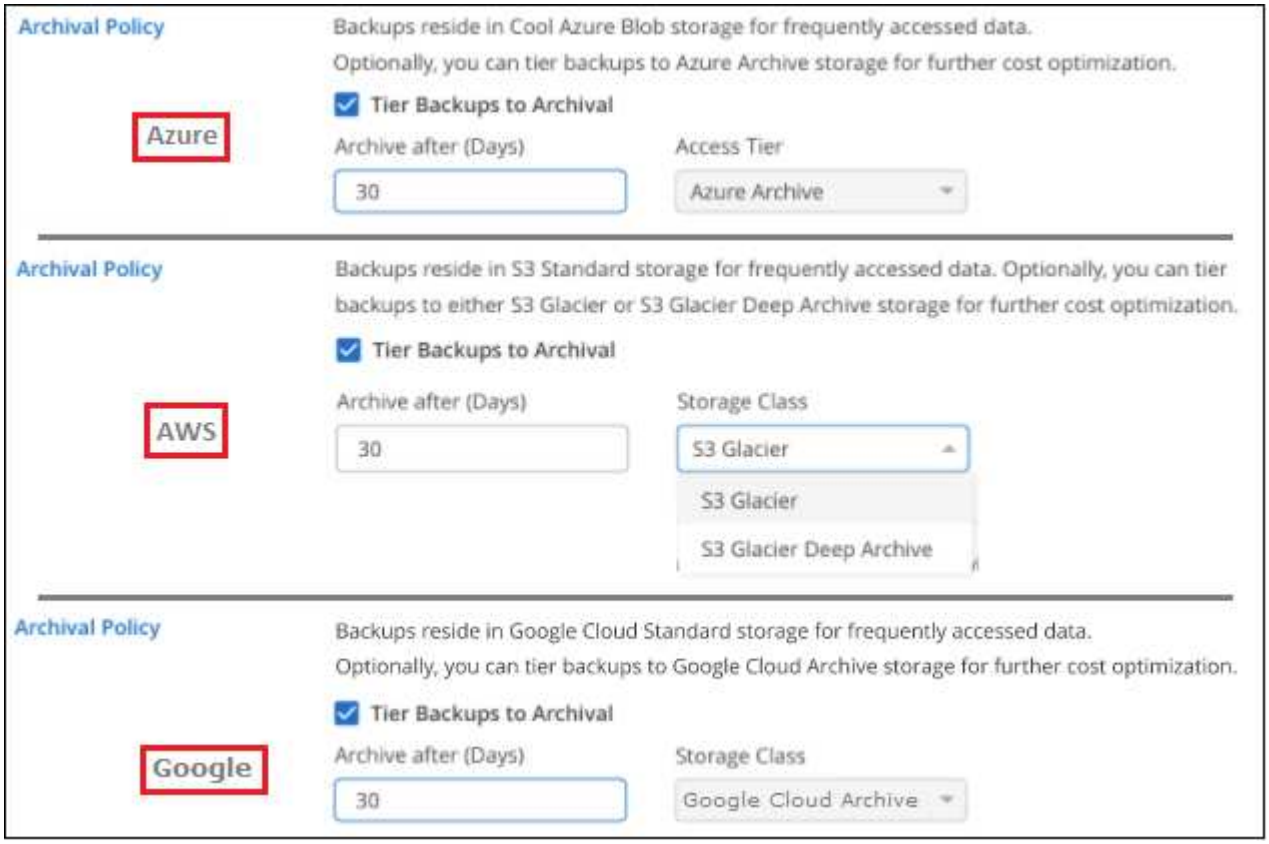
Se o cluster estiver executando o ONTAP 9.10,1 ou superior, você também terá a opção de ativar ou desativar a disposição em camadas de backups em armazenamento de arquivamento após um determinado número de dias.

"Saiba mais sobre como usar o armazenamento de arquivamento da AWS".

"Saiba mais sobre como usar o armazenamento de arquivamento do Azure".

"Saiba mais sobre como usar o armazenamento de arquivos do Google". (Requer ONTAP 9.12,1.)

E



Observe que todos os arquivos de backup que foram dispostos em camadas para armazenamento de arquivamento são deixados nesse nível se você parar de separar os backups para arquivamento - eles não serão movidos automaticamente de volta para o nível padrão. Somente novos backups de volume residirão na camada padrão.

Adicione uma nova política de backup na nuvem

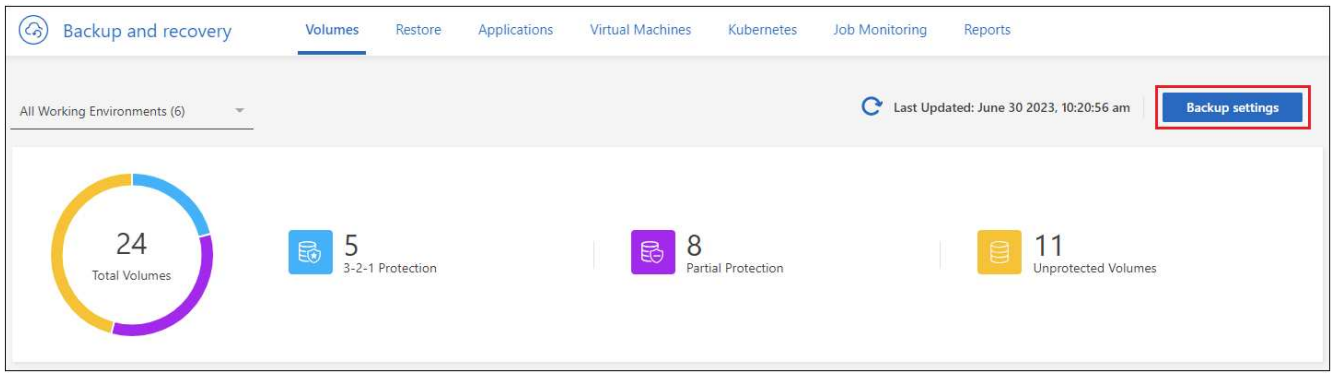
Quando você ativa o backup e a recuperação do BlueXP em um ambiente de trabalho, todos os volumes selecionados inicialmente são copiados usando a política de backup padrão definida por você. Se você quiser atribuir políticas de backup diferentes a determinados volumes que tenham objetivos de ponto de restauração (RPO) diferentes, poderá criar políticas adicionais para esse cluster e atribuir essas políticas a outros volumes.

Se você quiser aplicar uma nova política de backup a determinados volumes em um ambiente de trabalho, primeiro é necessário adicionar a política de backup ao ambiente de trabalho. Então você pode aplicar a política a volumes nesse ambiente de trabalho.

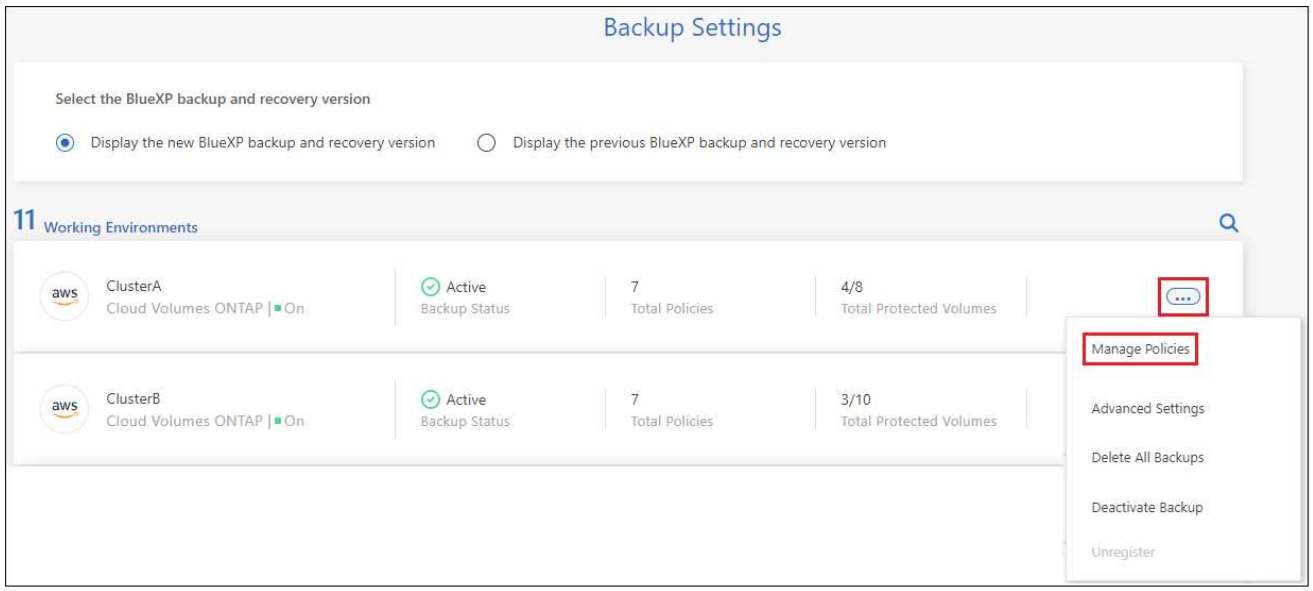
- Se você ativou o *DataLock e a proteção contra ransomware* na política inicial ao ativar o backup e a recuperação do BlueXP para esse cluster, quaisquer políticas adicionais criadas devem ser configuradas com a mesma configuração do DataLock (Governança ou conformidade). E se você não ativou o *DataLock e a proteção contra ransomware* ao ativar o backup e a recuperação do BlueXP , não será possível criar novas políticas que usem o DataLock.
- Ao criar backups na AWS, se você escolher *S3 Glacier* ou *S3 Glacier Deep Archive* na sua primeira política de backup ao ativar o backup e a recuperação do BlueXP , esse nível será o único nível de arquivamento disponível para futuras políticas de backup desse cluster. E se você não selecionou nenhum nível de arquivamento em sua primeira política de backup, o *S3 Glacier* será sua única opção de arquivamento para políticas futuras.

Passos

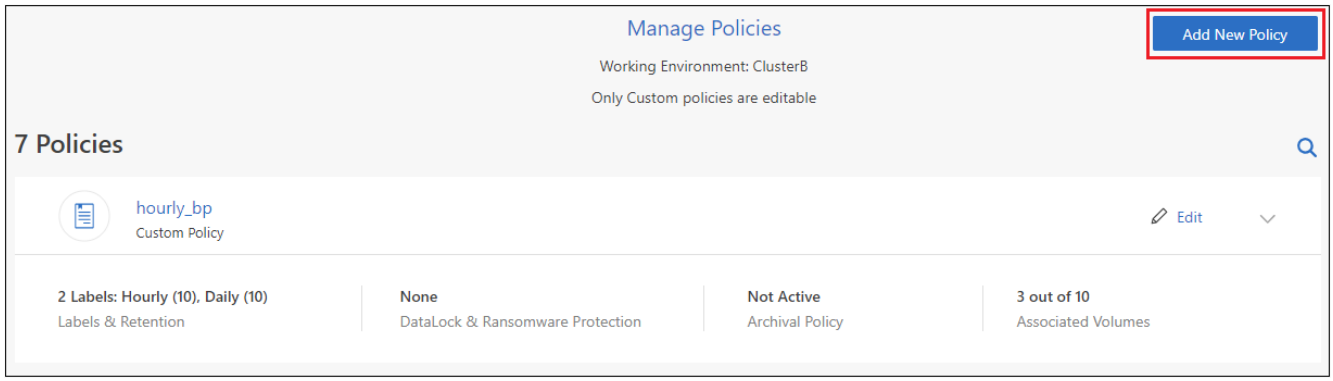
1. Na guia **volumes**, selecione **Configurações de backup**.



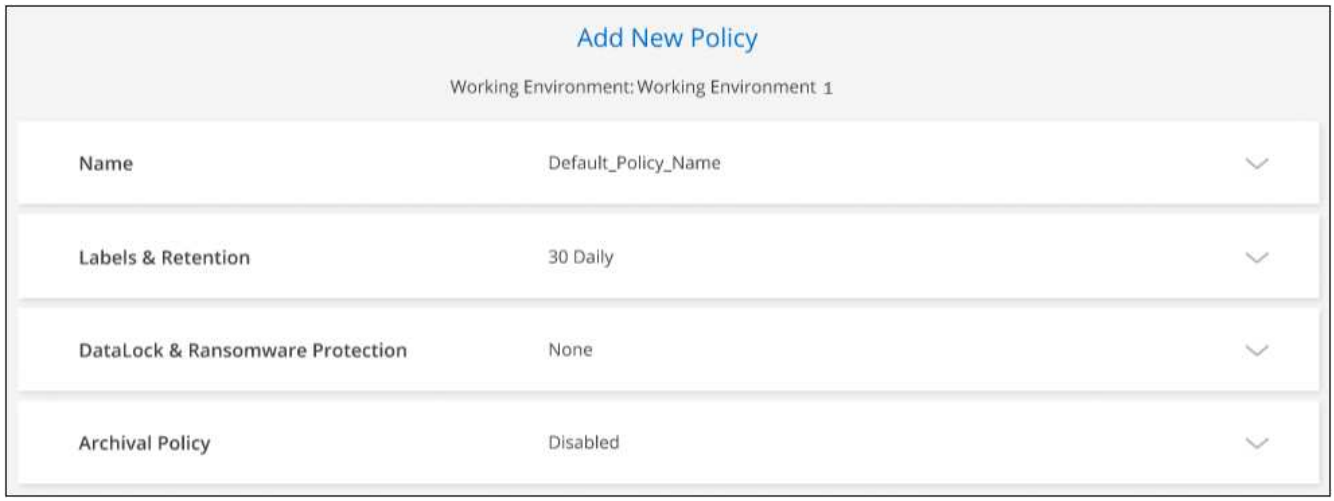
2. Na página *Configurações de backup*, clique ••• em para o ambiente de trabalho onde você deseja adicionar a nova política e selecione **Gerenciar políticas**.



3. Na página *Gerenciar políticas*, clique em **Adicionar nova política**.



4. Na página *Adicionar nova política*, clique ⌄ para expandir a seção *rótulos e retenção* para definir a retenção de agendamento e backup e clique em **Salvar**.



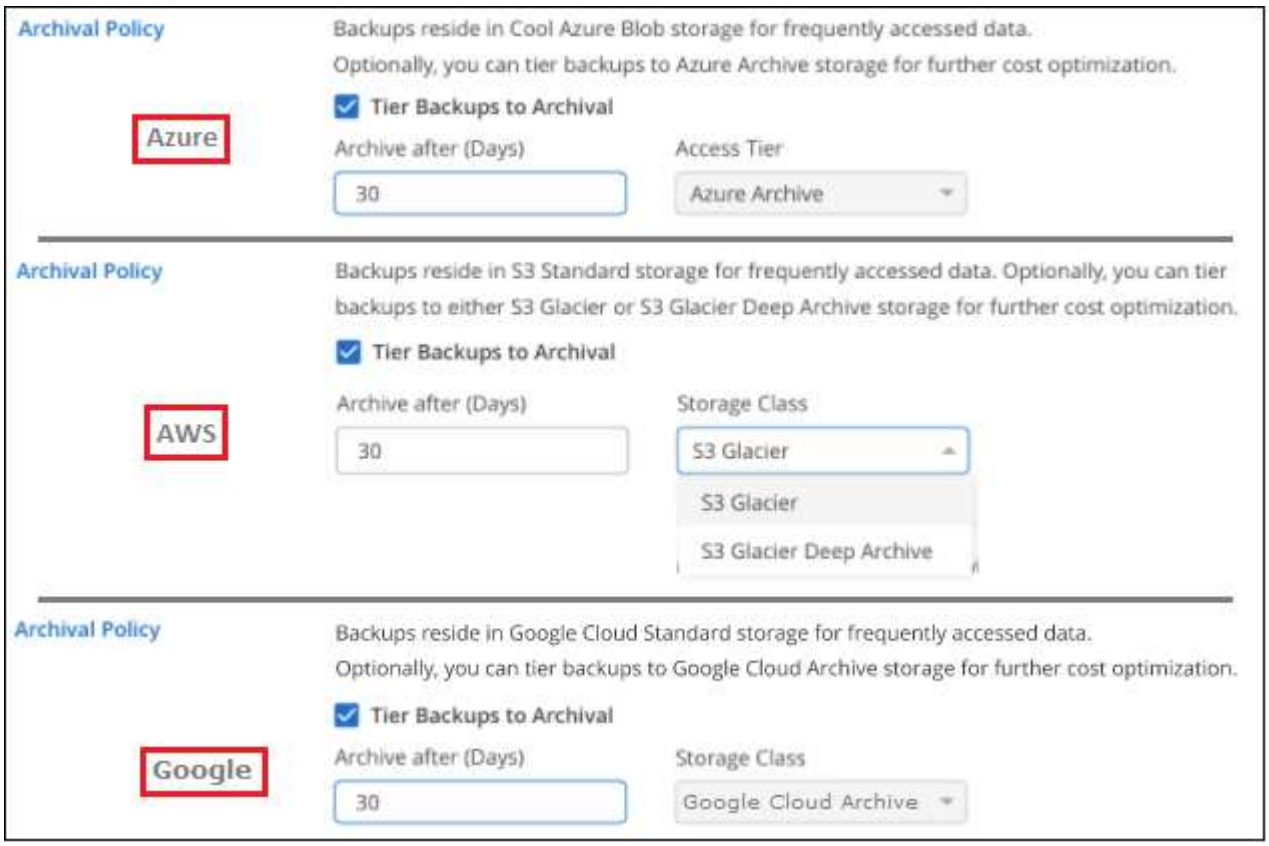
Se o cluster estiver executando o ONTAP 9.10,1 ou superior, você também terá a opção de ativar ou desativar a disposição em camadas de backups em armazenamento de arquivamento após um determinado número de dias.

"Saiba mais sobre como usar o armazenamento de arquivamento da AWS".

"Saiba mais sobre como usar o armazenamento de arquivamento do Azure".

"Saiba mais sobre como usar o armazenamento de arquivos do Google". (Requer ONTAP 9.12,1.)

E



Eliminar cópias de segurança

O backup e a recuperação do BlueXP permitem excluir um único arquivo de backup, excluir todos os backups de um volume ou excluir todos os backups de todos os volumes em um ambiente de trabalho. Talvez você queira excluir todos os backups se não precisar mais dos backups ou se você excluiu o volume de origem e deseja remover todos os backups.

Observe que você não pode excluir arquivos de backup bloqueados usando a proteção DataLock e ransomware. A opção "Delete" (Eliminar) não estará disponível na IU se tiver selecionado um ou mais ficheiros de cópia de segurança bloqueados.

> Se você pretende excluir um ambiente de trabalho ou cluster que tenha backups, exclua os backups **antes** de excluir o sistema. O backup e a recuperação do BlueXP não excluem automaticamente os backups quando você exclui um sistema, e não há suporte atual na IU para excluir os backups depois que o sistema for excluído. Você continuará sendo cobrado pelos custos de storage de objetos para quaisquer backups restantes.

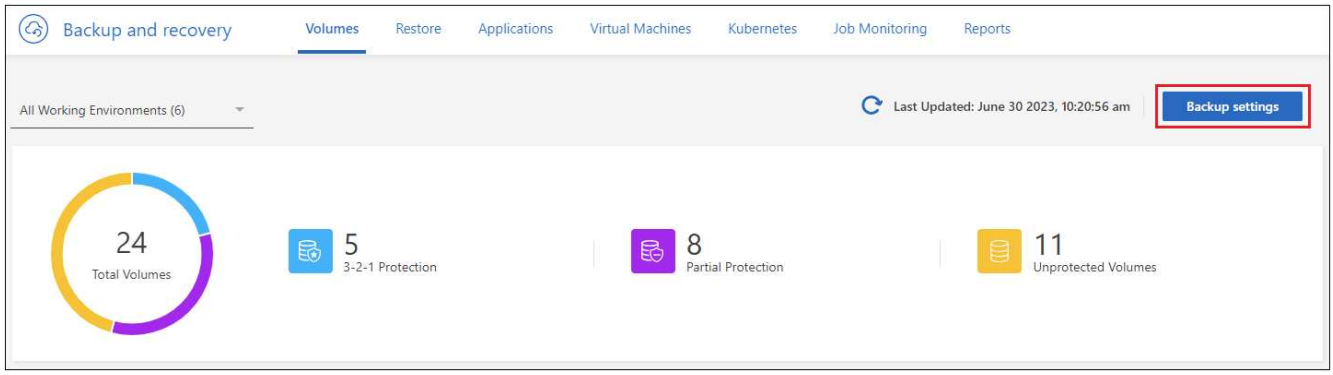
Exclua todos os arquivos de backup de um ambiente de trabalho

A exclusão de todos os backups no armazenamento de objetos para um ambiente de trabalho não desativa backups futuros de volumes neste ambiente de trabalho. Se você quiser parar de criar backups de todos os volumes em um ambiente de trabalho, desative backups como descrito aqui.

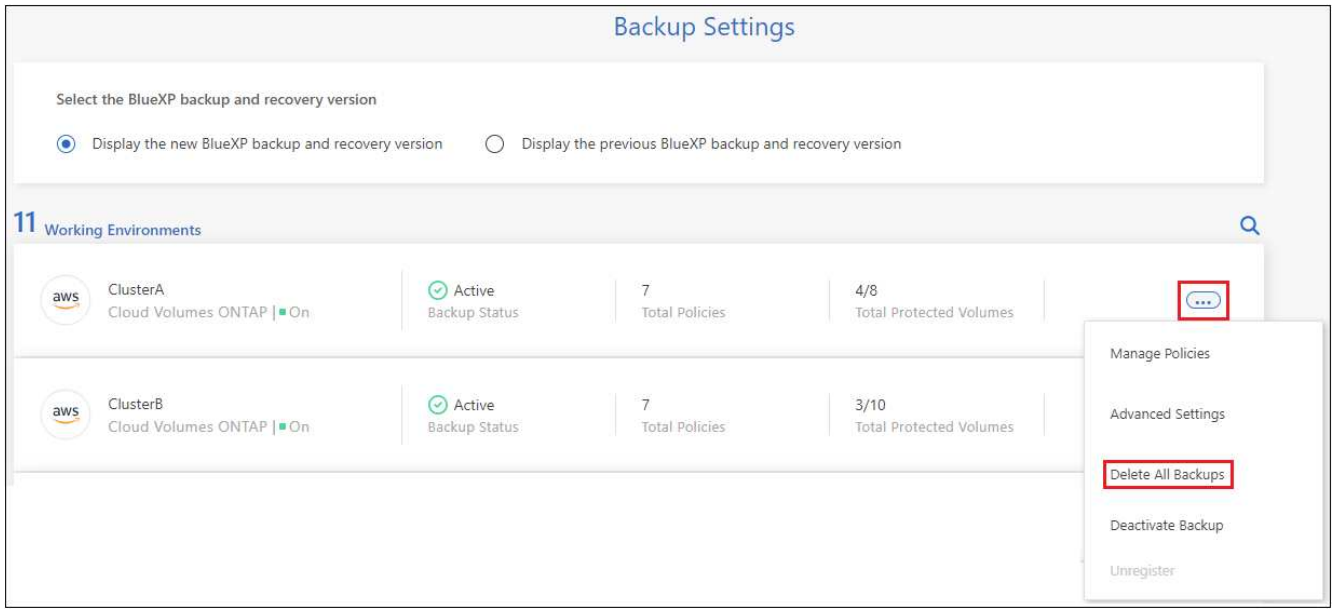
Observe que essa ação não afeta cópias Snapshot ou volumes replicados - esses tipos de arquivos de backup não são excluídos.

Passos

1. Na guia **volumes**, selecione **Configurações de backup**.



2. Clique ••• em para o ambiente de trabalho onde deseja excluir todos os backups e selecione **Excluir todos os backups**.



3. Na caixa de diálogo de confirmação, digite o nome do ambiente de trabalho e clique em **Excluir**.

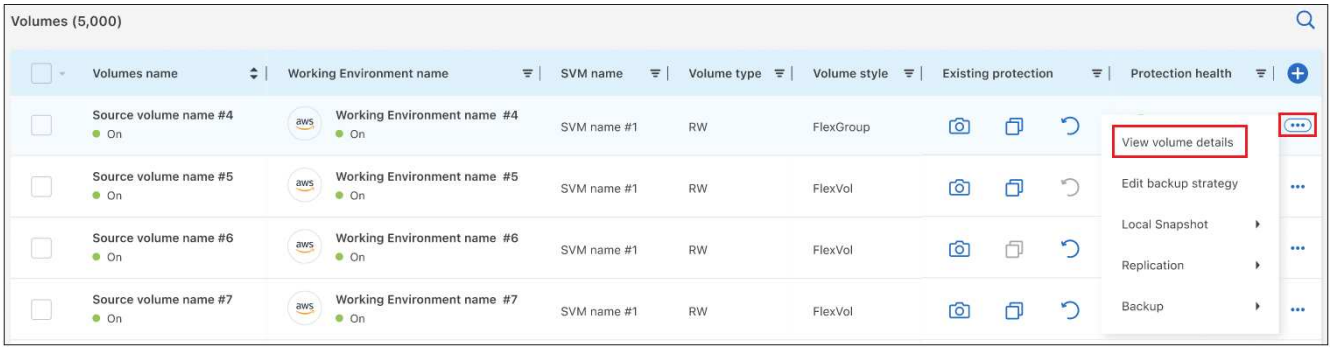
Exclua um único arquivo de backup para um volume

Você pode excluir um único arquivo de backup se não precisar mais dele. Isso inclui a exclusão de um único backup de uma cópia Snapshot de volume ou de um backup no storage de objetos.

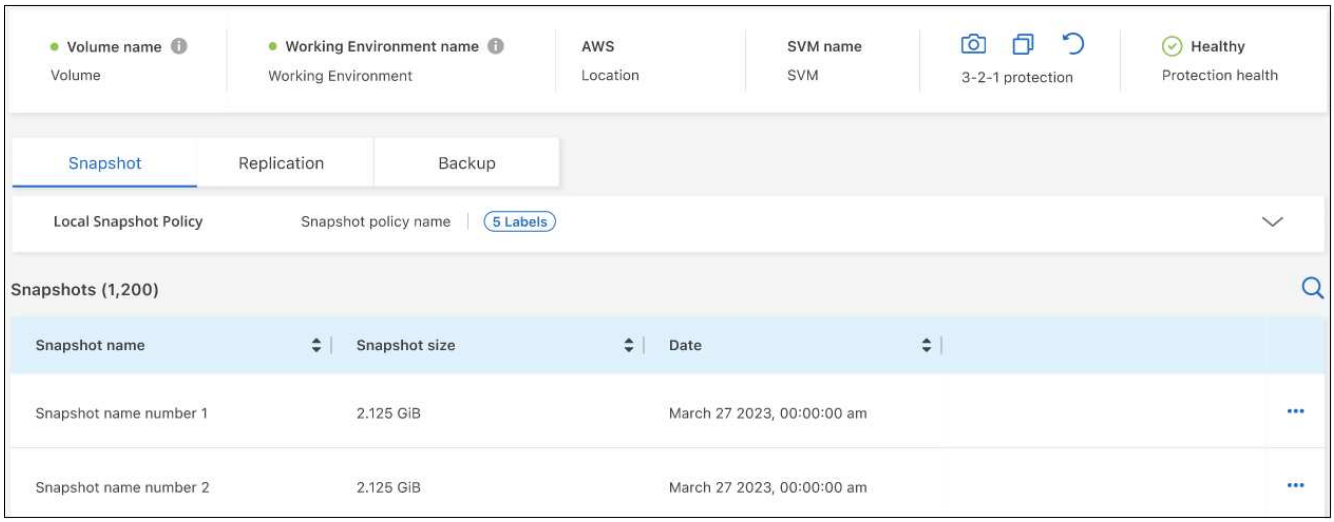
Não é possível excluir volumes replicados (volumes de proteção de dados).

Passos

1. Na guia **volumes**, clique ••• para obter o volume de origem e selecione **Exibir detalhes do volume**.

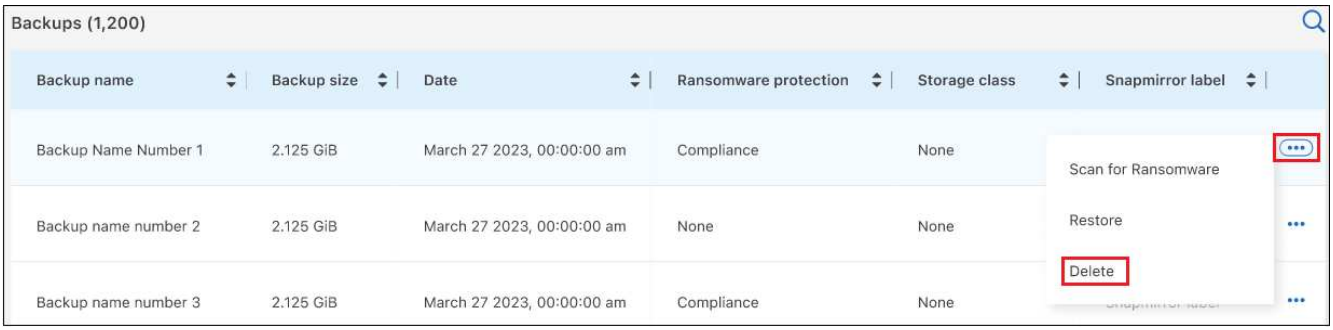


Os detalhes do volume são exibidos e você pode selecionar **Snapshot**, **Replication** ou **Backup** para ver a lista de todos os arquivos de backup do volume. Por padrão, as cópias Snapshot disponíveis são exibidas.



2. Selecione **Snapshot** ou **Backup** para ver o tipo de arquivos de backup que você deseja excluir.

3. Clique ••• em para o arquivo de backup de volume que você deseja excluir e clique em **Excluir**. A captura de tela abaixo é de um arquivo de backup no armazenamento de objetos.



4. Na caixa de diálogo de confirmação, clique em **Excluir**.

Eliminar relações de cópia de segurança de volume

A exclusão do relacionamento de backup de um volume fornece um mecanismo de arquivamento se você quiser interromper a criação de novos arquivos de backup e excluir o volume de origem, mas manter todos os arquivos de backup existentes. Isso permite que você restaure o volume do arquivo de backup no futuro, se necessário, enquanto limpa espaço do sistema de armazenamento de origem.

Você não precisa necessariamente excluir o volume de origem. Pode eliminar a relação de cópia de segurança de um volume e manter o volume de origem. Neste caso, você pode "ativar" o backup no volume posteriormente. A cópia de backup da linha de base original continua a ser usada neste caso - uma nova cópia de backup da linha de base não é criada e exportada para a nuvem. Observe que se você reativar um relacionamento de backup, o volume receberá a política de backup padrão.

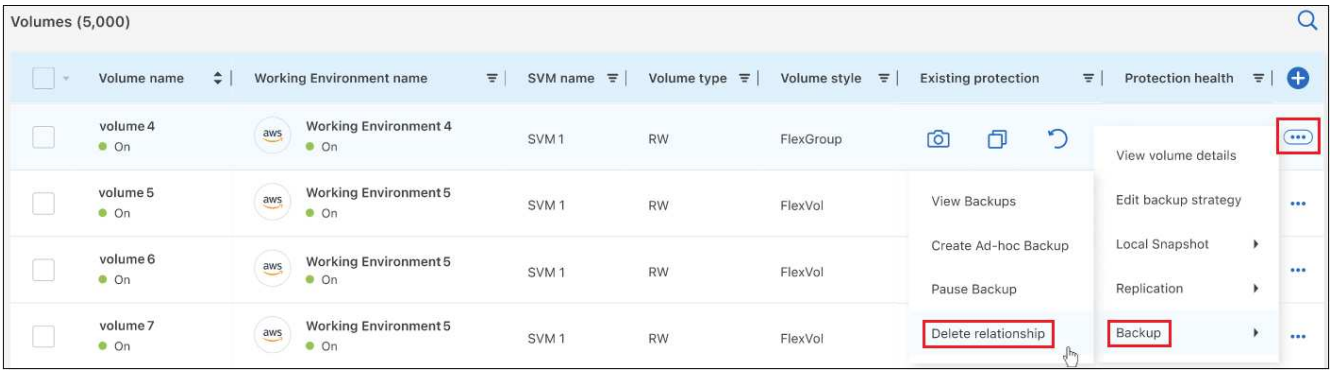
Esta funcionalidade só está disponível se o sistema estiver a executar o ONTAP 9.12,1 ou superior.

Não é possível excluir o volume de origem da interface do usuário de backup e recuperação do BlueXP . No entanto, você pode abrir a página Detalhes do volume na tela "elimine o volume a partir daí" e .

Não é possível excluir arquivos individuais de backup de volume uma vez que o relacionamento tenha sido excluído. No entanto, você pode excluir todos os backups do volume.

Passos

1. Na guia **volumes**, clique ••• para obter o volume de origem e selecione **Backup** > **Excluir relacionamento**.



Desative o backup e a recuperação do BlueXP para um ambiente de trabalho

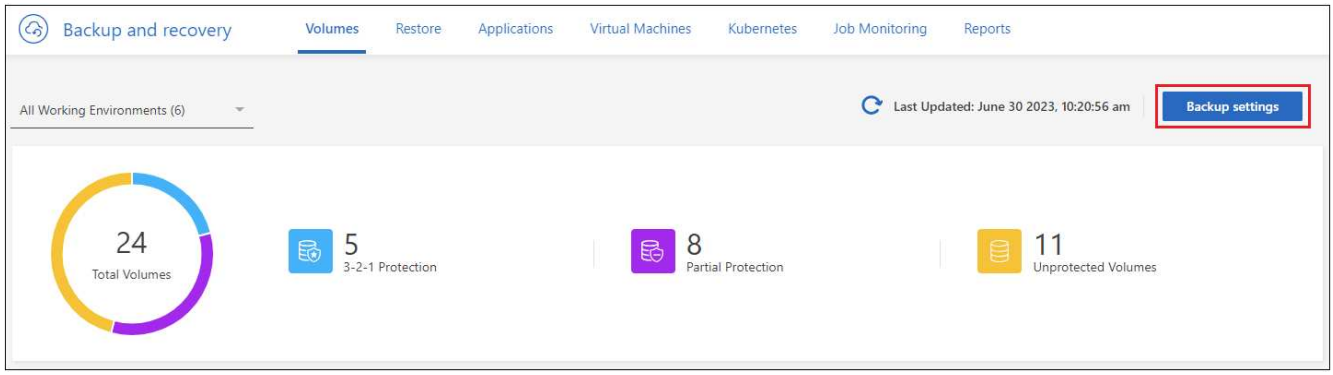
A desativação do backup e recuperação do BlueXP para um ambiente de trabalho desativa backups de cada volume no sistema e também desativa a capacidade de restaurar um volume. Quaisquer backups existentes

não serão excluídos. Isso não desRegistra o serviço de backup deste ambiente de trabalho - basicamente permite que você pause todas as atividades de backup e restauração por um período de tempo.

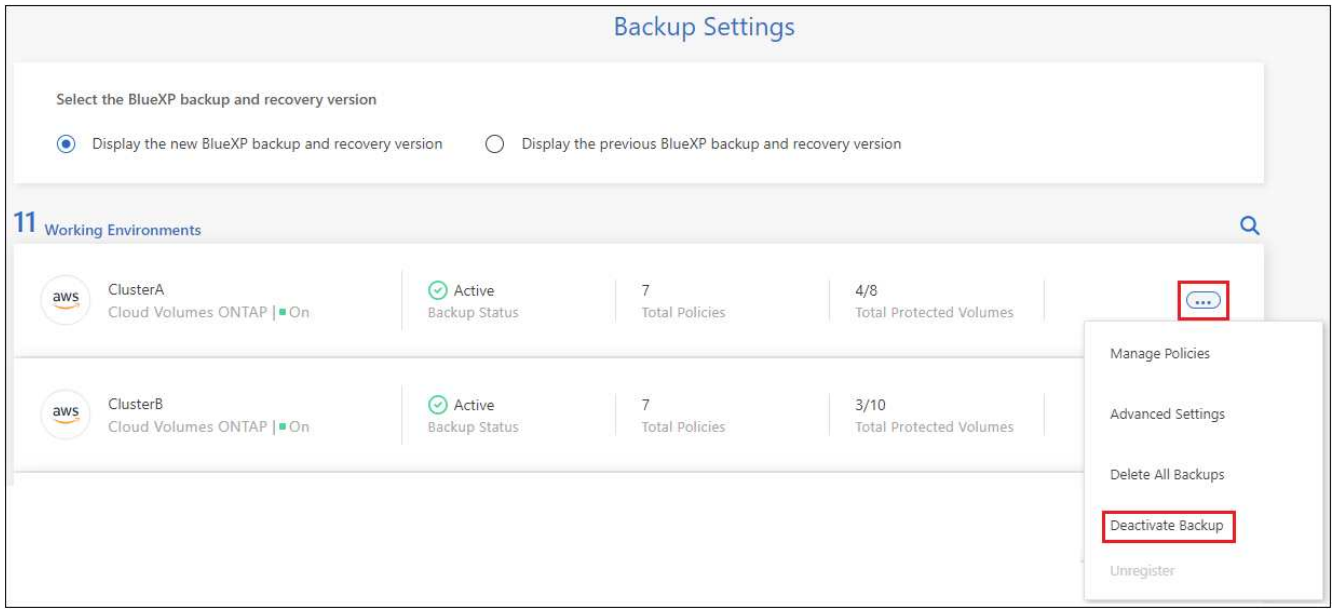
Observe que você continuará sendo cobrado pelo seu provedor de nuvem pelos custos de storage de objetos pela capacidade usada pelos backups, a menos que você exclua os backups.

Passos

1. Na guia **volumes**, selecione **Configurações de backup**.



2. Na página *Backup Settings*, clique ••• em para o ambiente de trabalho onde você deseja desativar os backups e selecione **Deactivate Backup**.



3. Na caixa de diálogo de confirmação, clique em **Desativar**.

Um botão **Ativar Backup** é exibido para esse ambiente de trabalho enquanto o backup está desativado. Pode clicar neste botão quando pretender reativar a funcionalidade de cópia de segurança para esse ambiente de trabalho.

Anular o registo do backup e recuperação do BlueXP para um ambiente de trabalho

Você pode cancelar o Registro do backup e da recuperação do BlueXP em um ambiente de trabalho se não quiser mais usar a funcionalidade de backup e desejar parar de ser cobrado por backups nesse ambiente de

trabalho. Normalmente, esse recurso é usado quando você está planejando excluir um ambiente de trabalho e deseja cancelar o serviço de backup.

Você também pode usar esse recurso se quiser alterar o armazenamento de objetos de destino onde os backups do cluster estão sendo armazenados. Depois de cancelar o Registro do backup e da recuperação do BlueXP para o ambiente de trabalho, você poderá habilitar o backup e a recuperação do BlueXP para esse cluster usando as novas informações do provedor de nuvem.

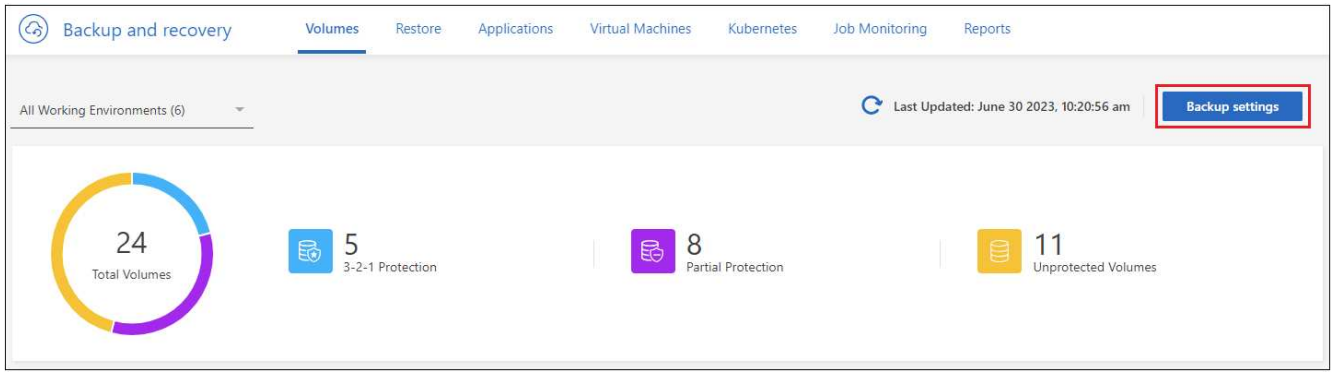
Antes de anular o registo da cópia de segurança e recuperação do BlueXP , tem de executar as seguintes etapas, nesta ordem:

- Desative o backup e a recuperação do BlueXP para o ambiente de trabalho
- Exclua todos os backups desse ambiente de trabalho

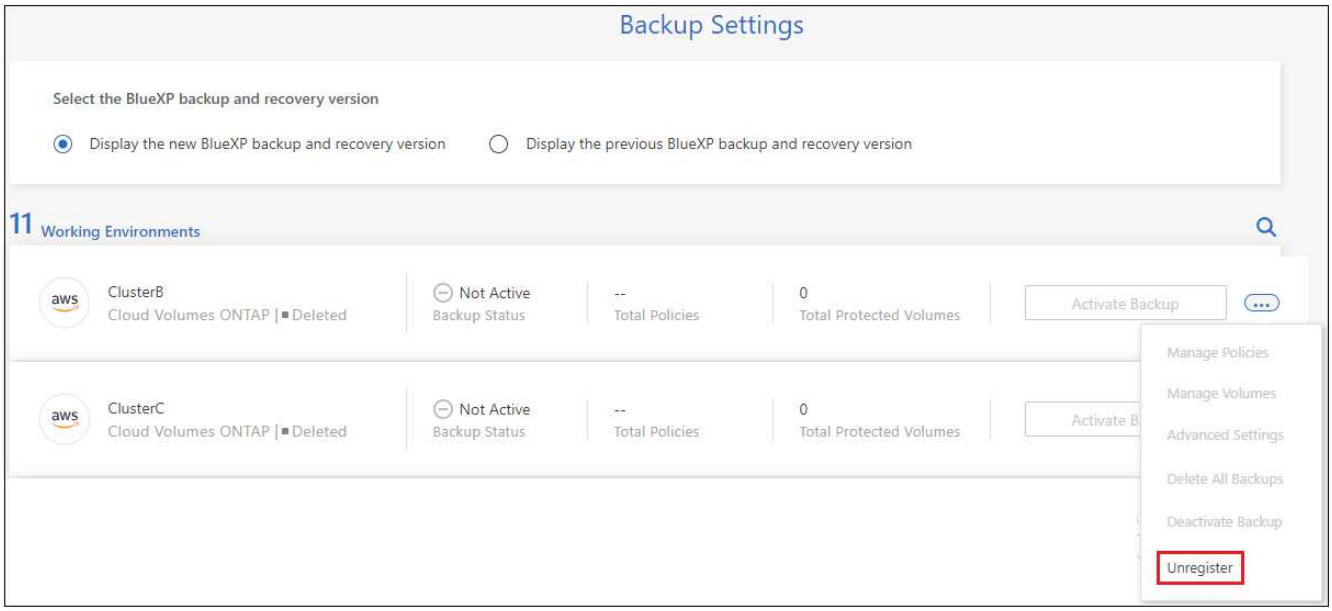
A opção Unregister (Desregistar) não está disponível até que estas duas ações estejam concluídas.

Passos

1. Na guia **volumes**, selecione **Configurações de backup**.



2. Na página *Configurações de backup*, clique ••• em para o ambiente de trabalho onde você deseja cancelar o Registro do serviço de backup e selecione **Cancelar Registro**.



3. Na caixa de diálogo de confirmação, clique em **Unregister**.

Restaure dados do ONTAP a partir de arquivos de backup

Os backups dos dados de volume do ONTAP estão disponíveis nos locais em que você criou backups: Cópias snapshot, volumes replicados e backups armazenados no storage de objetos. Você pode restaurar dados de um ponto específico no tempo a partir de qualquer um desses locais de backup. Pode restaurar um volume ONTAP inteiro a partir de um ficheiro de cópia de segurança ou, se necessitar apenas de restaurar alguns ficheiros, pode restaurar uma pasta ou ficheiros individuais.

- Você pode restaurar um **volume** (como um novo volume) para o ambiente de trabalho original, para um ambiente de trabalho diferente que esteja usando a mesma conta na nuvem ou para um sistema ONTAP local.
- Você pode restaurar uma pasta * para um volume no ambiente de trabalho original, para um volume em um ambiente de trabalho diferente que esteja usando a mesma conta na nuvem ou para um volume em um sistema ONTAP local.
- Você pode restaurar **Files** para um volume no ambiente de trabalho original, para um volume em um ambiente de trabalho diferente que esteja usando a mesma conta na nuvem ou para um volume em um sistema ONTAP local.

É necessária uma licença válida de backup e recuperação do BlueXP para restaurar dados de arquivos de backup para um sistema de produção.

Para resumir, esses são os fluxos válidos que você pode usar para restaurar dados de volume para um ambiente de trabalho do ONTAP:

- Ficheiro de cópia de segurança → volume restaurado
- Volume replicado → volume restaurado
- Cópia Snapshot → volume restaurado

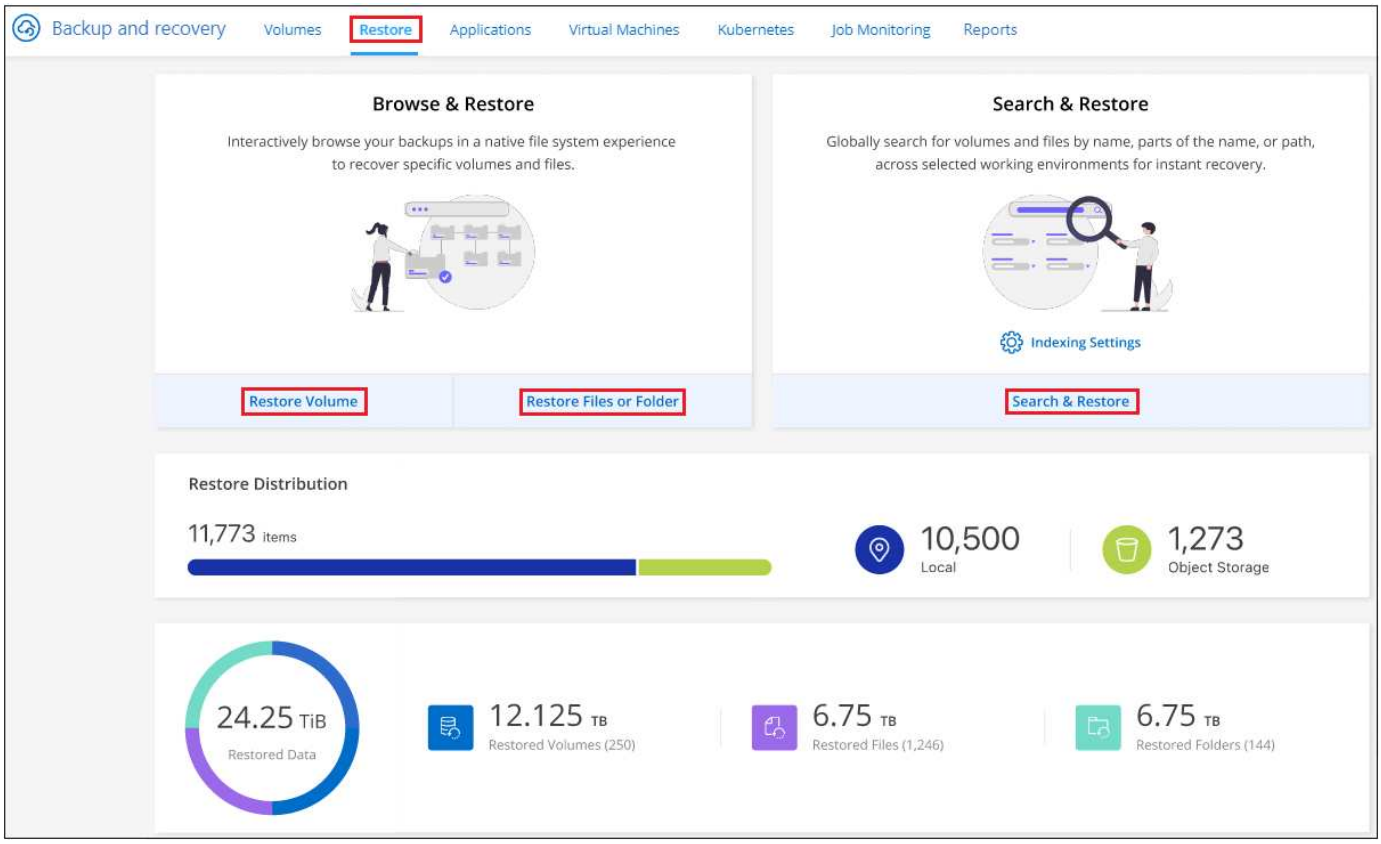
Se a operação de restauração não for concluída, não tente o processo de restauração novamente até que o Monitor de trabalho mostre que a operação de restauração falhou. Se você tentar o processo de restauração novamente antes que o Monitor de trabalho mostre que a operação de restauração falhou, a operação de restauração falhará novamente. Quando o status do Monitor de trabalho for exibido como "Falha", você poderá tentar o processo de restauração novamente.

Para obter limitações relacionadas à restauração de dados do ONTAP, "Limitações de backup e restauração para volumes ONTAP"consulte .

O Painel de Restauro

Você usa o Painel de Restauração para executar operações de restauração de volume, pasta e arquivo. Você acessa o Painel de Restauração clicando em **Backup e recuperação** no menu BlueXP e, em seguida, clicando na guia **Restaurar**. Você também pode clicar em > **Exibir Painel de Restauração** no serviço de backup e recuperação do painel Serviços.

O backup e a recuperação do BlueXP já devem estar ativados para pelo menos um ambiente de trabalho e os arquivos de backup iniciais devem existir.



Como você pode ver, o Painel de Restauração oferece 2 maneiras diferentes de restaurar dados de arquivos de backup: **Procurar e Restaurar** e **pesquisar e Restaurar**.

Comparar Procurar e Restaurar e pesquisar e Restaurar

Em termos gerais, *Browse & Restore* normalmente é melhor quando você precisa restaurar um volume, pasta ou arquivo específico da última semana ou mês — e você sabe o nome e a localização do arquivo e a data em que ele foi último em boa forma. *Search & Restore* normalmente é melhor quando você precisa restaurar um volume, pasta ou arquivo, mas você não se lembra do nome exato, do volume em que reside, ou da data em que foi a última em boa forma.

Esta tabela fornece uma comparação de recursos dos 2 métodos.

Procurar e restaurar	Pesquisa e restauração
Navegue por uma estrutura de estilo de pasta para encontrar o volume, a pasta ou o arquivo dentro de um único arquivo de backup.	Procure um volume, pasta ou arquivo em **todos os arquivos de backup** por nome de volume parcial ou completo, nome de pasta/arquivo parcial ou completo, intervalo de tamanho e filtros de pesquisa adicionais.
Não manipula a recuperação de arquivos se o arquivo foi excluído ou renomeado e o usuário não sabe o nome do arquivo original	Lida com diretórios recém-criados/excluídos/renomeados e arquivos recém-criados/excluídos/renomeados
Não são necessários recursos adicionais do fornecedor de nuvem	Ao restaurar a partir da nuvem, são necessários recursos adicionais de bucket e fornecedor de nuvem pública por conta.

Procurar e restaurar	Pesquisa e restauração
Não são necessários custos adicionais de fornecedor de nuvem	Ao restaurar a partir da nuvem, são necessários custos adicionais ao digitalizar seus backups e volumes para obter resultados de pesquisa.
A restauração rápida é suportada.	A restauração rápida não é suportada.

Esta tabela fornece uma lista de operações de restauração válidas com base no local onde os arquivos de backup residem.

Tipo de cópia de segurança	Procurar e restaurar			Pesquisa e restauração		
	Restaurar volume	Restaurar arquivos	Restaurar pasta	Restaurar volume	Restaurar arquivos	Restaurar pasta
Cópia Snapshot	Sim	Não	Não	Sim	Sim	Sim
Volume replicado	Sim	Não	Não	Sim	Sim	Sim
Ficheiro de cópia de segurança	Sim	Sim	Sim	Sim	Sim	Sim

Antes de usar qualquer um dos métodos de restauração, certifique-se de que configurou o ambiente para os requisitos de recursos exclusivos. Esses requisitos estão descritos nas seções abaixo.

Consulte os requisitos e as etapas de restauração para o tipo de operação de restauração que deseja usar:

- <<Restaurar volumes utilizando Procurar Restaurar,Restaurar volumes utilizando Procurar Restaurar
- <<Restaure pastas e ficheiros utilizando Procurar Restaurar,Restaure pastas e ficheiros utilizando Procurar Restaurar
- <<restore-ontap-data-using-search-restore,Restaure volumes, pastas e ficheiros utilizando a função pesquisar Restaurar

Restaure os dados do ONTAP usando Procurar e Restaurar

Antes de iniciar a restauração de um volume, pasta ou arquivo, você deve saber o nome do volume a partir do qual deseja restaurar, o nome do ambiente de trabalho e SVM onde o volume reside e a data aproximada do arquivo de backup do qual deseja restaurar. É possível restaurar os dados do ONTAP a partir de uma cópia Snapshot, de um volume replicado ou de backups armazenados no storage de objetos.

Observação: se o arquivo de backup que contém os dados que você deseja restaurar reside no armazenamento em nuvem de arquivamento (começando com ONTAP 9.10,1), a operação de restauração levará um tempo maior e incorrerá em um custo. Além disso, o cluster de destino também deve estar executando o ONTAP 9.10,1 ou superior para restauração de volume, 9.11.1 para restauração de arquivos, 9.12.1 para arquivamento e StorageGRID do Google e 9.13.1 para restauração de pastas.

"Saiba mais sobre como restaurar o armazenamento de arquivamento da AWS".

"Saiba mais sobre como restaurar a partir do armazenamento de arquivos do Azure".

"Saiba mais sobre como restaurar a partir do armazenamento de arquivos do Google".

A alta prioridade não é suportada ao restaurar dados do armazenamento de arquivos do Azure para sistemas StorageGRID.

Navegue e restaure ambientes de trabalho e provedores de storage de objetos compatíveis

É possível restaurar os dados do ONTAP a partir de um arquivo de backup que reside em um ambiente de trabalho secundário (um volume replicado) ou no storage de objetos (um arquivo de backup) para os seguintes ambientes de trabalho. As cópias Snapshot residem no ambiente de trabalho de origem e podem ser restauradas somente nesse mesmo sistema.

Observação: você pode restaurar um volume de qualquer tipo de arquivo de backup, mas você pode restaurar uma pasta ou arquivos individuais apenas de um arquivo de backup no armazenamento de objetos neste momento.

De Object Store (Backup)	Do primário (instantâneo)	Do sistema secundário (replicação)	Para o ambiente de trabalho de destino ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP on-premises da AWS	Cloud Volumes ONTAP no AWS on-premises ONTAP system endif::aws[] ifdef::azure[]	Blob do Azure
Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP in Azure on-premises ONTAP system endif::azul[] ifdef::gcp[]	Google Cloud Storage	Cloud Volumes ONTAP no sistema ONTAP local do Google
Cloud Volumes ONTAP no Google on-premises ONTAP system endif::gcp[]	NetApp StorageGRID	Sistema ONTAP no local	ONTAP System Cloud Volumes ONTAP no local
Para o sistema ONTAP no local	ONTAP S3	Sistema ONTAP no local	ONTAP System Cloud Volumes ONTAP no local

Para Procurar e Restaurar, o conetor pode ser instalado nos seguintes locais:

- Para o Amazon S3, o conetor pode ser implantado na AWS ou em suas instalações
- Para o Azure Blob, o conetor pode ser implantado no Azure ou no local
- Para o Google Cloud Storage, o conetor deve ser implantado na VPC do Google Cloud Platform
- Para o StorageGRID, o conetor deve ser implantado em suas instalações, com ou sem acesso à Internet
- Para o ONTAP S3, o conetor pode ser implantado em suas instalações (com ou sem acesso à Internet) ou em um ambiente de provedor de nuvem

Observe que as referências a "sistemas ONTAP on-premises" incluem sistemas FAS, AFF e ONTAP Select.

Se a versão do ONTAP no seu sistema for inferior a 9.13.1, não será possível restaurar pastas ou arquivos se o arquivo de backup tiver sido configurado com DataLock & ransomware. Neste caso, você pode restaurar todo o volume do arquivo de backup e, em seguida, acessar os arquivos que você precisa.

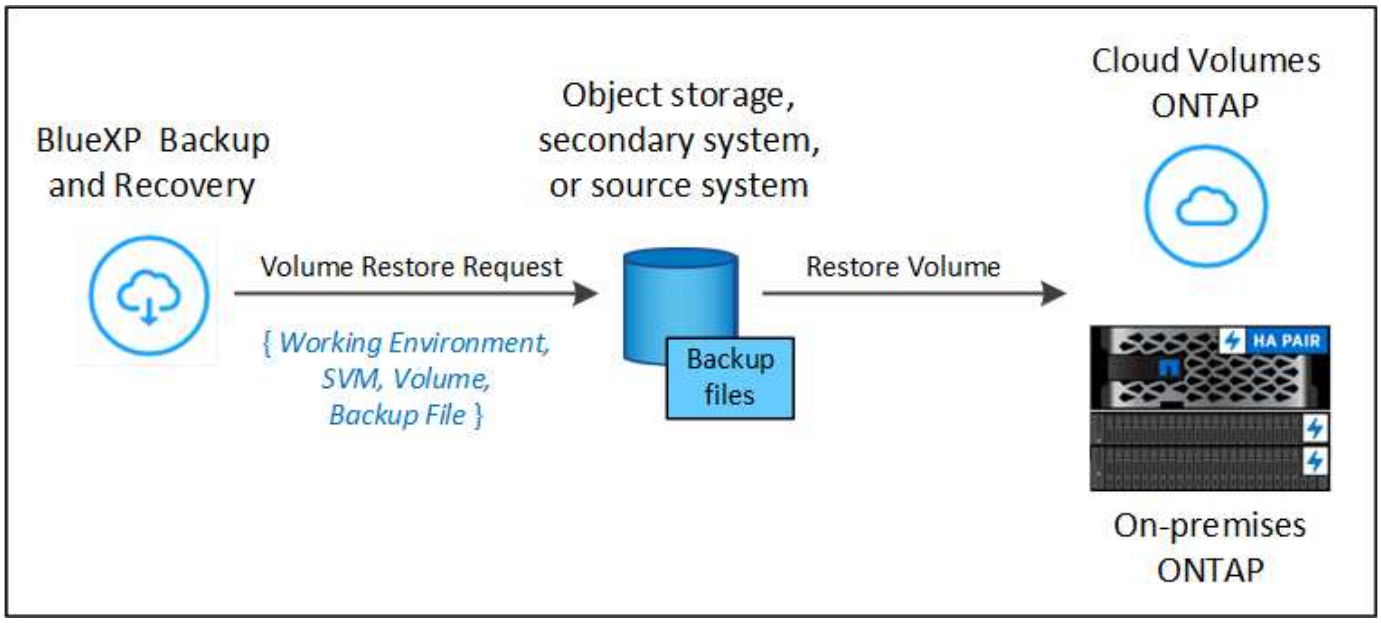
Restaure volumes utilizando Procurar e Restaurar

Quando você restaura um volume de um arquivo de backup, o backup e a recuperação do BlueXP criam um volume *new* usando os dados do backup. Ao usar um backup do storage de objetos, é possível restaurar os dados para um volume no ambiente de trabalho original, para um ambiente de trabalho diferente localizado na mesma conta de nuvem que o ambiente de trabalho de origem ou para um sistema ONTAP no local.

Ao restaurar um backup em nuvem para um sistema Cloud Volumes ONTAP usando o ONTAP 9.13,0 ou superior ou para um sistema ONTAP local executando o ONTAP 9.14,1, você terá a opção de executar uma operação de restauração *rápida*. A restauração rápida é ideal para situações de recuperação de desastres em que você precisa fornecer acesso a um volume o mais rápido possível. Uma restauração rápida restaura os metadados do arquivo de backup para um volume em vez de restaurar todo o arquivo de backup. A restauração rápida não é recomendada para aplicações sensíveis à performance ou à latência, e não é compatível com backups em storage arquivado.

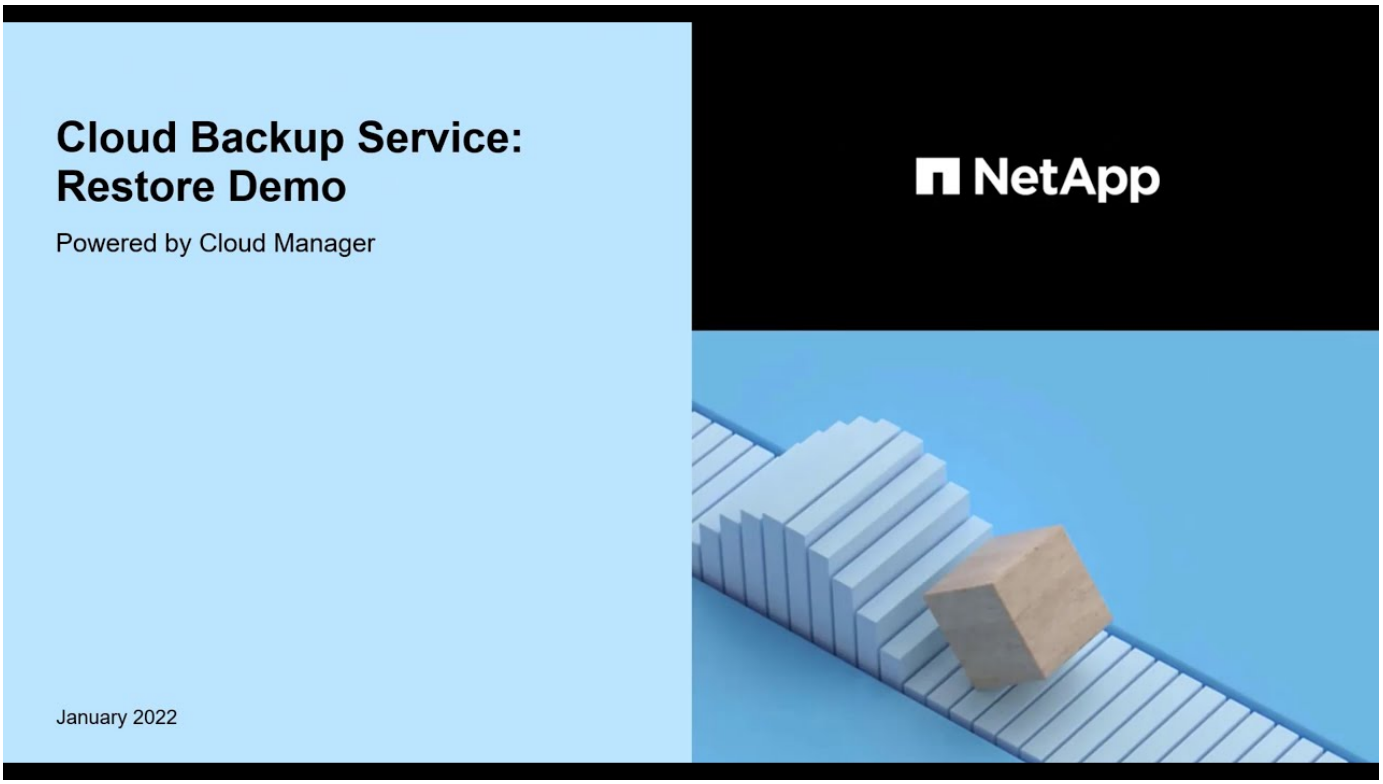
> A restauração rápida só é compatível com volumes FlexGroup se o sistema de origem do qual o backup na nuvem foi criado estiver executando o ONTAP 9.12,1 ou superior. E é compatível com volumes SnapLock somente se o sistema de origem estiver executando o ONTAP 9.11,0 ou superior.

Ao restaurar a partir de um volume replicado, você pode restaurar o volume para o ambiente de trabalho original ou para um sistema Cloud Volumes ONTAP ou ONTAP no local.



Como você pode ver, você precisará saber o nome do ambiente de trabalho de origem, a VM de armazenamento, o nome do volume e a data do arquivo de backup para executar uma restauração de volume.

O vídeo a seguir mostra um passo a passo para restaurar um volume:

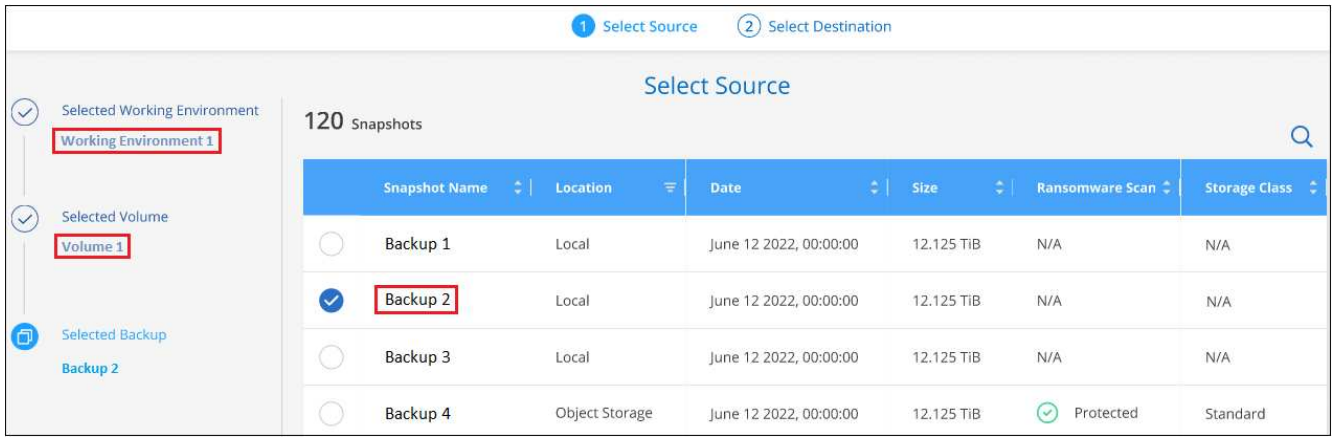


Passos

1. No menu BlueXP , selecione **proteção > Backup e recuperação**.
2. Clique na guia **Restore** e o Restore Dashboard será exibido.
3. Na seção *Browse & Restore*, clique em **Restore volume**.

4. Na página *Select Source*, navegue até o arquivo de backup do volume que você deseja restaurar. Selecione o **ambiente de trabalho**, o **volume** e o ficheiro **Backup** que tem o carimbo de data/hora a partir do qual pretende restaurar.

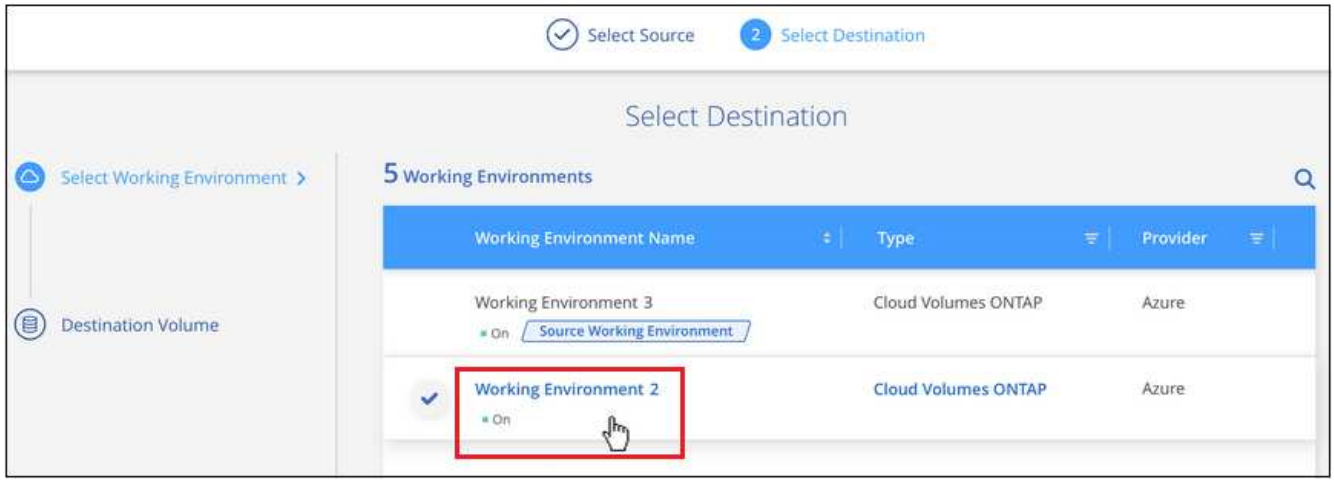
A coluna **localização** mostra se o arquivo de backup (instantâneo) é **local** (uma cópia Snapshot no sistema de origem), **secundário** (um volume replicado em um sistema ONTAP secundário) ou **armazenamento de objetos** (um arquivo de backup no armazenamento de objetos). Escolha o arquivo que você deseja restaurar.



5. Clique em **seguinte**.

   Observe que se você selecionar um arquivo de backup no armazenamento de objetos e a proteção contra ransomware estiver ativa para esse backup (se você ativou o DataLock e a proteção contra ransomware na política de backup), será solicitado que você execute uma verificação adicional de ransomware no arquivo de backup antes de restaurar os dados. Recomendamos que você verifique o arquivo de backup para ransomware. (Você incorrerá em custos extras de saída do seu provedor de nuvem para acessar o conteúdo do arquivo de backup.)

6. Na página *Selecionar destino*, selecione o **ambiente de trabalho** onde deseja restaurar o volume.

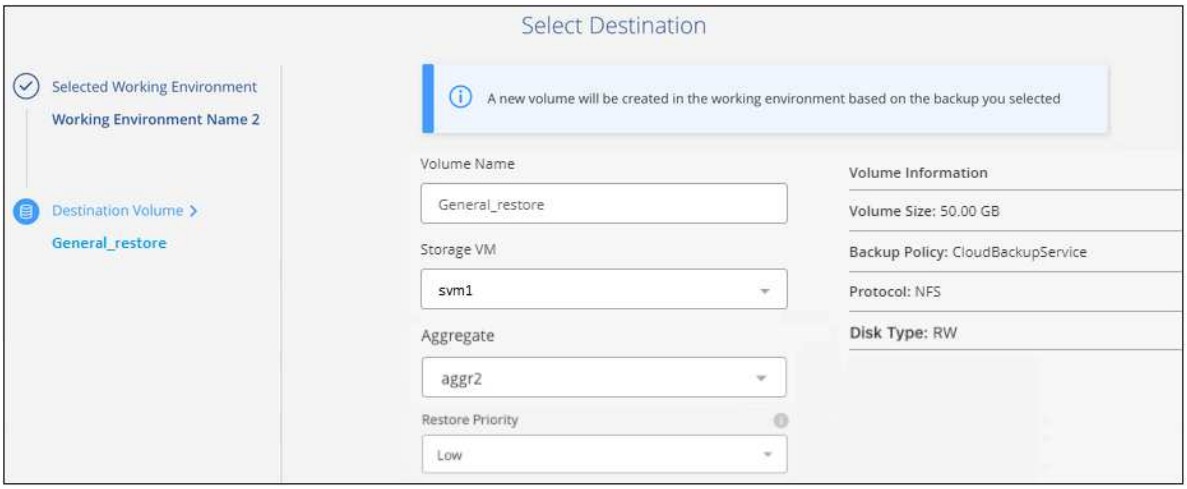


7. Ao restaurar um arquivo de backup do armazenamento de objetos, se você selecionar um sistema ONTAP local e ainda não tiver configurado a conexão de cluster para o armazenamento de objetos, você será solicitado a obter informações adicionais:
   - Ao restaurar a partir do Amazon S3, selecione o espaço IPspace no cluster do ONTAP onde o volume de destino residirá, insira a chave de acesso e a chave secreta para o usuário criado para dar ao cluster do ONTAP acesso ao bucket do S3 e, opcionalmente, escolha um endpoint VPC privado para transferência segura de dados.
     - Ao restaurar a partir do Blob do Azure, selecione o espaço IPspace no cluster do ONTAP onde o volume de destino residirá, selecione a assinatura do Azure para acessar o armazenamento de

objetos e, opcionalmente, escolha um ponto de extremidade privado para transferência de dados segura selecionando a VNet e a sub-rede.

- Ao restaurar a partir do Google Cloud Storage, selecione o Projeto Google Cloud e a chave de acesso e chave secreta para acessar o armazenamento de objetos, a região onde os backups são armazenados e o espaço IPspace no cluster do ONTAP onde o volume de destino residirá.
- Ao restaurar a partir do StorageGRID, digite o FQDN do servidor StorageGRID e a porta que o ONTAP deve usar para comunicação HTTPS com o StorageGRID, selecione a chave de acesso e a chave secreta necessárias para acessar o armazenamento de objetos e o espaço de IPspace no cluster ONTAP onde o volume de destino residirá.
- Ao restaurar a partir do ONTAP S3, digite o FQDN do servidor ONTAP S3 e a porta que o ONTAP deve usar para comunicação HTTPS com o ONTAP S3, selecione a chave de acesso e chave secreta necessárias para acessar o armazenamento de objetos e o espaço de IPspace no cluster ONTAP onde o volume de destino residirá.

a. Insira o nome que deseja usar para o volume restaurado e selecione a VM de armazenamento e o agregado onde o volume residirá. Ao restaurar um volume FlexGroup, você precisará selecionar vários agregados. Por padrão, **<source_volume_name>_restore** é usado como o nome do volume.



Ao restaurar um backup do armazenamento de objetos para um sistema Cloud Volumes ONTAP usando o ONTAP 9.13,0 ou superior ou para um sistema ONTAP local executando o ONTAP 9.14,1, você terá a opção de executar uma operação de *restauração rápida*.

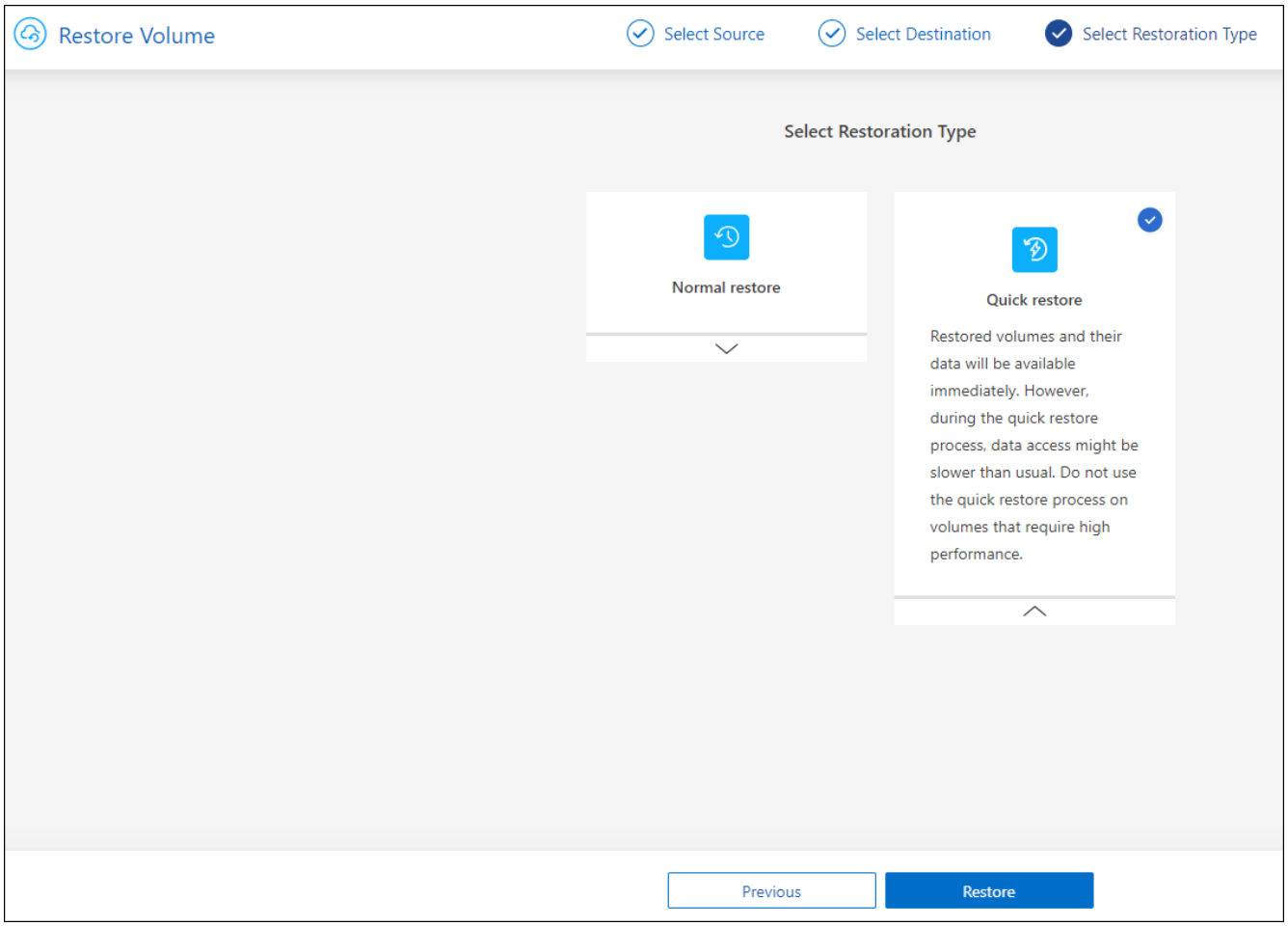
E se você estiver restaurando o volume de um arquivo de backup que reside em uma camada de storage de arquivamento (disponível a partir do ONTAP 9.10,1), poderá selecionar a prioridade de restauração.

"Saiba mais sobre como restaurar o armazenamento de arquivamento da AWS".

"Saiba mais sobre como restaurar a partir do armazenamento de arquivos do Azure".

"Saiba mais sobre como restaurar a partir do armazenamento de arquivos do Google". Os arquivos de backup na camada de storage do Google Archive são restaurados quase imediatamente e não exigem prioridade de restauração.

1. Clique em **seguinte** para escolher se deseja fazer uma restauração normal ou um processo de restauração rápida:



- * Restauração normal*: Use restauração normal em volumes que exigem alto desempenho. Os volumes não estarão disponíveis até que o processo de restauração esteja concluído.
- **Quick restore**: Volumes e dados restaurados estarão disponíveis imediatamente. Não use isso em volumes que exigem alto desempenho, pois durante o processo de restauração rápida, o acesso aos dados pode ser mais lento do que o habitual.

2. Clique em **Restaurar** e você será retornado ao Painel de Restauração para que você possa revisar o andamento da operação de restauração.

Resultado

O backup e a recuperação do BlueXP criam um novo volume com base no backup selecionado.

Observe que a restauração de um volume de um arquivo de backup que reside no storage de arquivamento pode levar muitos minutos ou horas, dependendo do nível de arquivamento e da prioridade de restauração. Você pode clicar na guia **Monitoramento de trabalho** para ver o progresso da restauração.

Restaure pastas e ficheiros utilizando Procurar e Restaurar

Se você precisar restaurar apenas alguns arquivos de um backup de volume do ONTAP, poderá optar por restaurar uma pasta ou arquivos individuais em vez de restaurar todo o volume. Você pode restaurar pastas e arquivos para um volume existente no ambiente de trabalho original ou para um ambiente de trabalho diferente que esteja usando a mesma conta na nuvem. Você também pode restaurar pastas e arquivos para um volume em um sistema ONTAP local.

Você pode restaurar uma pasta ou arquivos individuais apenas de um arquivo de backup no armazenamento de objetos neste momento. A restauração de arquivos e pastas não é suportada atualmente a partir de uma cópia Snapshot local ou de um arquivo de backup que reside em um ambiente de trabalho secundário (um volume replicado).

Se você selecionar vários arquivos, todos os arquivos serão restaurados para o mesmo volume de destino que você escolher. Então, se você quiser restaurar arquivos para diferentes volumes, você precisará executar o processo de restauração várias vezes.

Ao usar o ONTAP 9.13,0 ou superior, você pode restaurar uma pasta juntamente com todos os arquivos e subpastas dentro dela. Ao usar uma versão do ONTAP antes de 9.13.0, somente os arquivos dessa pasta são restaurados - nenhuma subpasta ou arquivos em subpastas são restaurados.

- Se o arquivo de backup tiver sido configurado com proteção DataLock & ransomware, a restauração em nível de pasta será suportada somente se a versão do ONTAP for 9.13.1 ou superior. Se você estiver usando uma versão anterior do ONTAP, poderá restaurar todo o volume do arquivo de backup e, em seguida, acessar a pasta e os arquivos necessários.
- Se o arquivo de backup residir no armazenamento de arquivamento, a restauração em nível de pasta será suportada somente se a versão do ONTAP for 9.13.1 ou superior. Se estiver a utilizar uma versão anterior do ONTAP, pode restaurar a pasta a partir de um ficheiro de cópia de segurança mais recente que não tenha sido arquivado ou pode restaurar todo o volume a partir da cópia de segurança arquivada e, em seguida, aceder à pasta e aos ficheiros de que necessita.
- Com o ONTAP 9.15,1, você pode restaurar pastas do FlexGroup usando a opção "Procurar e restaurar". Este recurso está em um modo de visualização da tecnologia.

  Você pode testá-lo usando uma bandeira especial descrita no "Backup e recuperação do BlueXP julho de 2024 Release blog".

Pré-requisitos

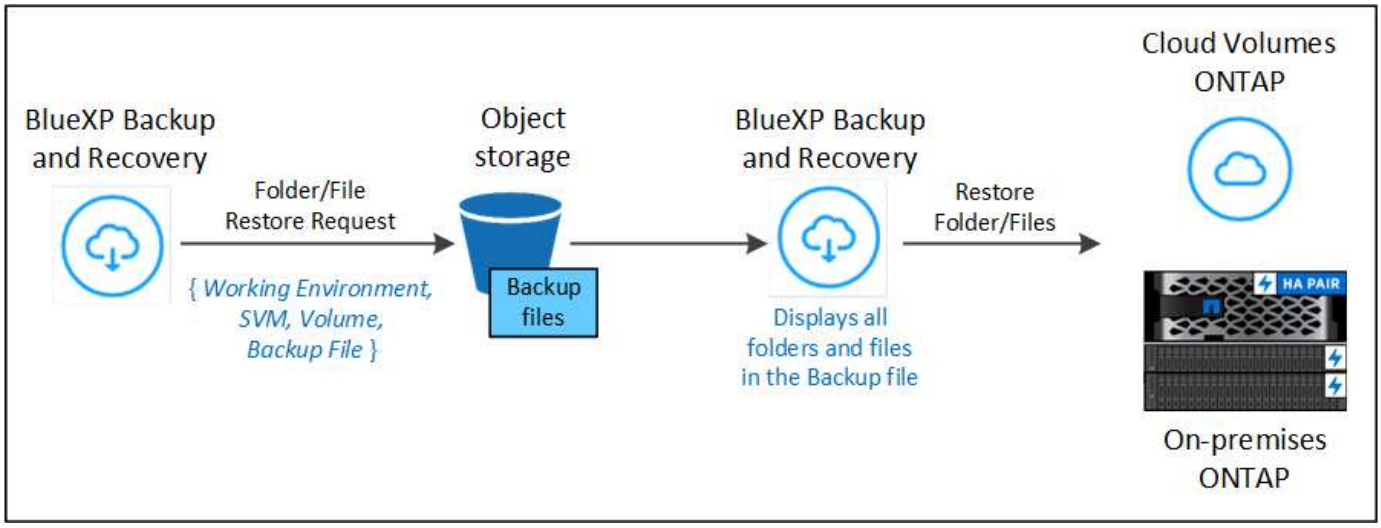
- A versão do ONTAP deve ser 9,6 ou superior para executar operações de restauração *file*.
- A versão do ONTAP deve ser 9.11.1 ou superior para executar operações de restauração *folder*. O ONTAP versão 9.13.1 é necessário se os dados estiverem em armazenamento de arquivamento ou se o arquivo de backup estiver usando a proteção DataLock e ransomware.
- A versão do ONTAP deve ser 9.15.1 P2 ou superior para restaurar diretórios do FlexGroup usando a opção Procurar e restaurar.

Processo de restauração de pasta e arquivo

O processo é assim:

1. Quando você quiser restaurar uma pasta, ou um ou mais arquivos, a partir de um backup de volume, clique na guia **Restaurar** e clique em **Restaurar arquivos ou pasta** em *Procurar e Restaurar*.
2. Selecione o ambiente de trabalho de origem, o volume e o arquivo de backup em que a pasta ou o(s) arquivo(s) residem(ão).
3. Backup e recuperação do BlueXP exibe as pastas e arquivos que existem dentro do arquivo de backup selecionado.
4. Selecione a pasta ou o(s) arquivo(s) que você deseja restaurar a partir desse backup.

5. Selecione o local de destino onde deseja que a pasta ou o(s) arquivo(s) sejam restaurados (ambiente de trabalho, volume e pasta) e clique em **Restaurar**.
6. Os ficheiros são restaurados.

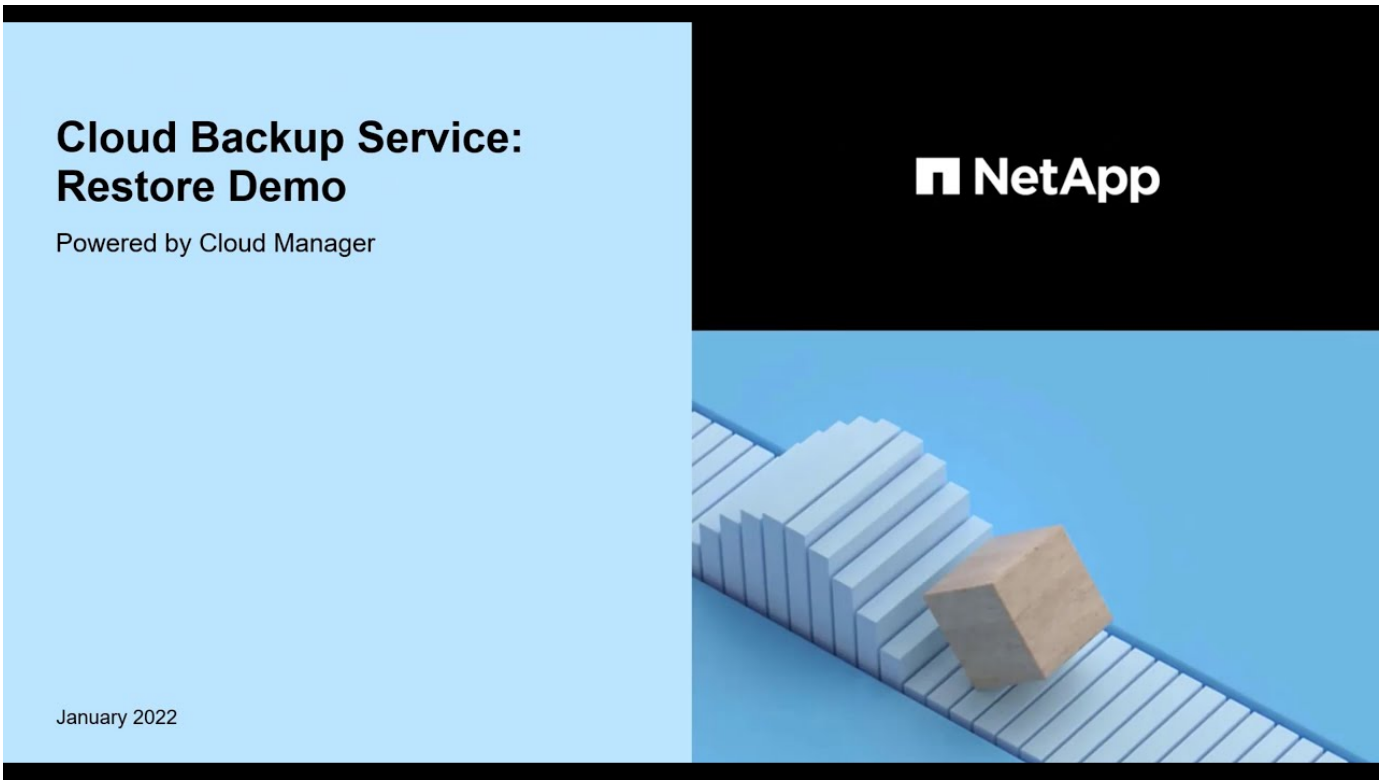


Como você pode ver, você precisa saber o nome do ambiente de trabalho, o nome do volume, a data do arquivo de backup e o nome da pasta/arquivo para executar uma restauração de pasta ou arquivo.

Restaure pastas e arquivos

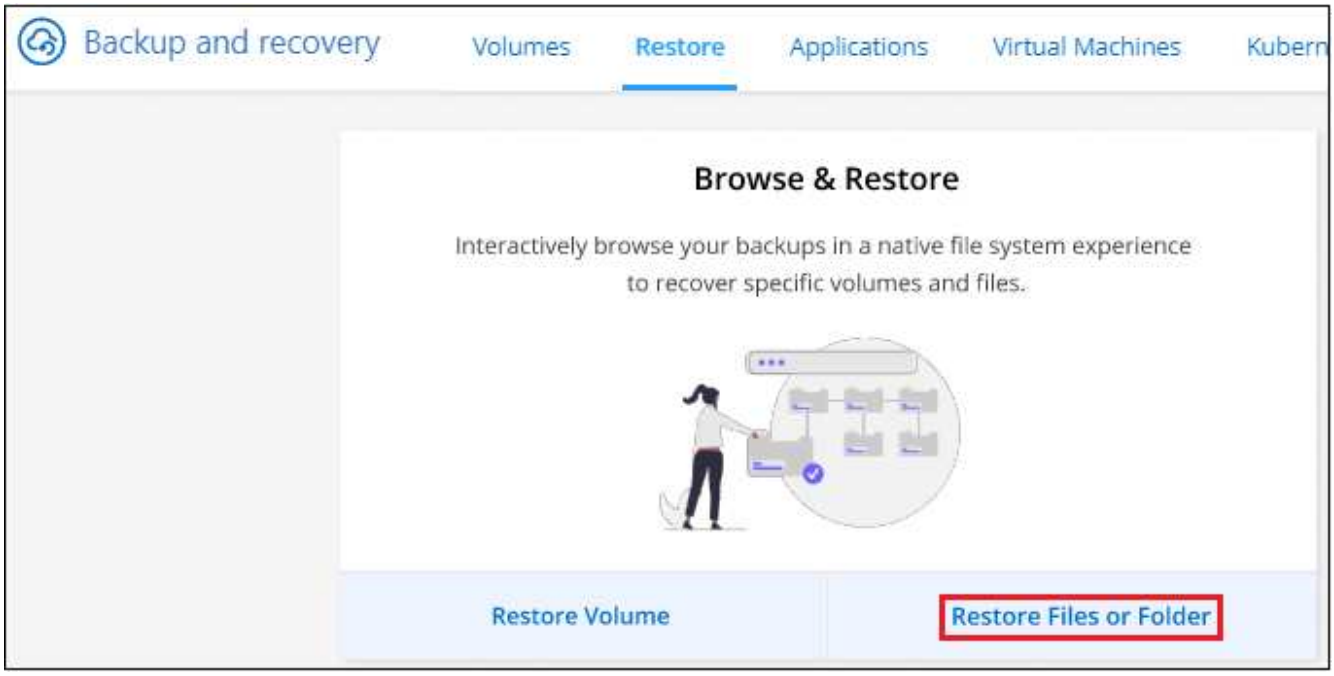
Siga estas etapas para restaurar pastas ou arquivos para um volume a partir de um backup de volume do ONTAP. Você deve saber o nome do volume e a data do arquivo de backup que deseja usar para restaurar a pasta ou arquivo(s). Esta funcionalidade utiliza o Live Browsing para que possa visualizar a lista de diretórios e ficheiros dentro de cada ficheiro de cópia de segurança.

O vídeo a seguir mostra um passo rápido de restaurar um único arquivo:

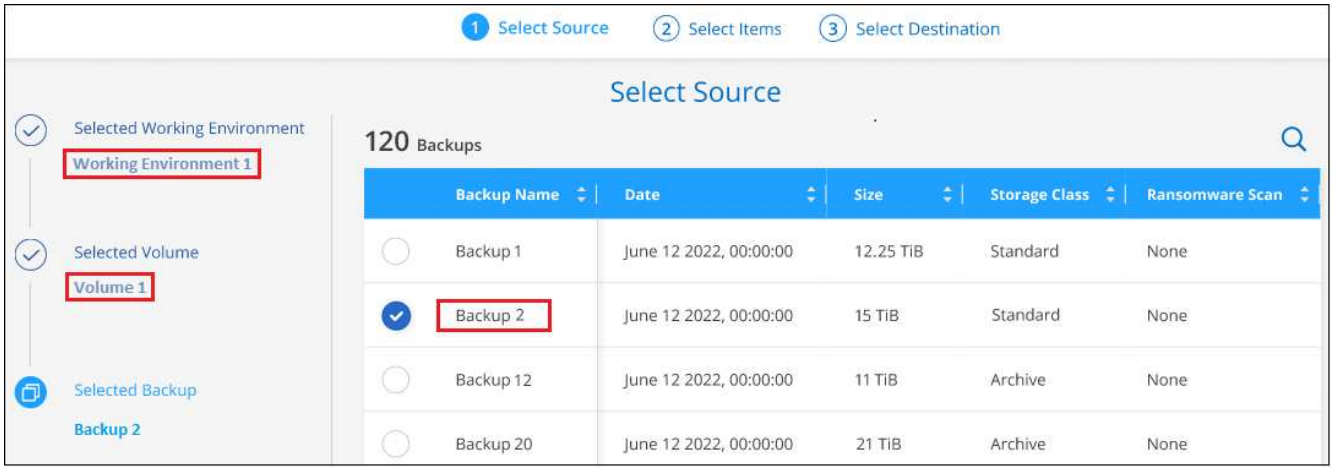


Passos

1. No menu BlueXP , selecione **proteção > Backup e recuperação**.
2. Clique na guia **Restore** e o Restore Dashboard será exibido.
3. Na seção *Browse & Restore*, clique em **Restore Files or Folder** (Restaurar arquivos ou pasta).



4. Na página *Select Source*, navegue até o arquivo de backup do volume que contém a pasta ou os arquivos que você deseja restaurar. Selecione o **ambiente de trabalho**, o **volume** e o **Backup** que tem o carimbo de data/hora a partir do qual você deseja restaurar arquivos.



5. Clique em **Next** (seguinte) e a lista de pastas e arquivos do backup de volume será exibida.

   Se você estiver restaurando pastas ou arquivos de um arquivo de backup que reside em um nível de armazenamento de arquivamento, poderá selecionar a prioridade Restaurar.

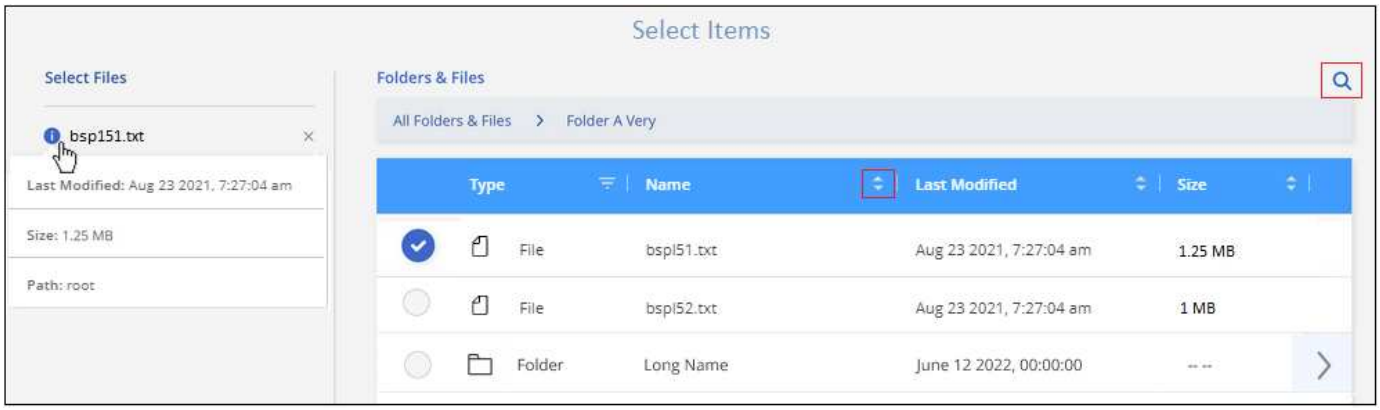
"Saiba mais sobre como restaurar o armazenamento de arquivamento da AWS".

"Saiba mais sobre como restaurar a partir do armazenamento de arquivos do Azure".

"Saiba mais sobre como restaurar a partir do armazenamento de arquivos do Google". Os arquivos de backup na camada de storage do Google Archive são restaurados quase imediatamente e não exigem prioridade de restauração.

E se a proteção contra ransomware estiver ativa para o arquivo de backup (se você ativou o DataLock e a proteção contra ransomware na política de backup), você será solicitado a executar uma verificação adicional de ransomware no arquivo de backup antes de restaurar os dados. Recomendamos que você verifique o arquivo de backup para ransomware. (Você incorrerá em custos extras de saída do seu provedor de nuvem para acessar o conteúdo do arquivo de backup.)

E

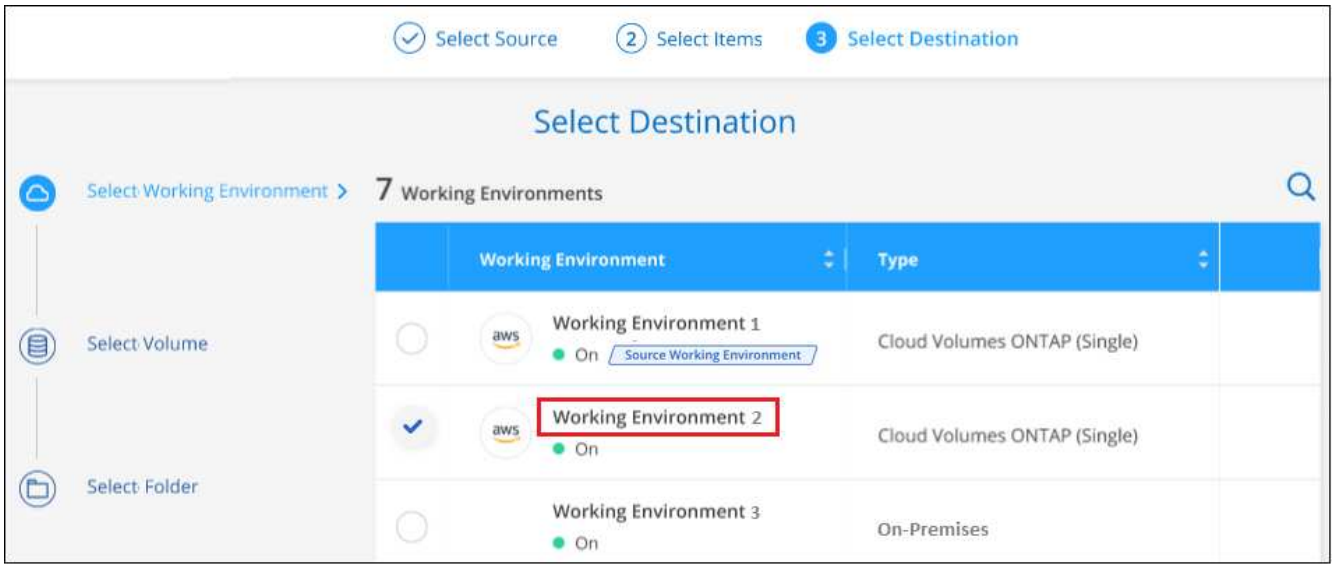


1. Na página *Selecionar itens*, selecione a pasta ou arquivo(s) que deseja restaurar e clique em **continuar**. Para ajudá-lo a encontrar o item:
   - Você pode clicar na pasta ou no nome do arquivo, se você vê-lo.
   - Pode clicar no ícone de pesquisa e introduzir o nome da pasta ou ficheiro para navegar diretamente para o item.

◦ Você pode navegar para baixo níveis em pastas usando o botão no final da linha para encontrar arquivos específicos.

À medida que você seleciona arquivos, eles são adicionados ao lado esquerdo da página para que você possa ver os arquivos que você já escolheu. Você pode remover um arquivo dessa lista, se necessário, clicando no **x** ao lado do nome do arquivo.

2. Na página *Selecionar destino*, selecione o **ambiente de trabalho** onde deseja restaurar os itens.



Se você selecionar um cluster no local e ainda não tiver configurado a conexão do cluster com o armazenamento de objetos, você será solicitado a obter informações adicionais:

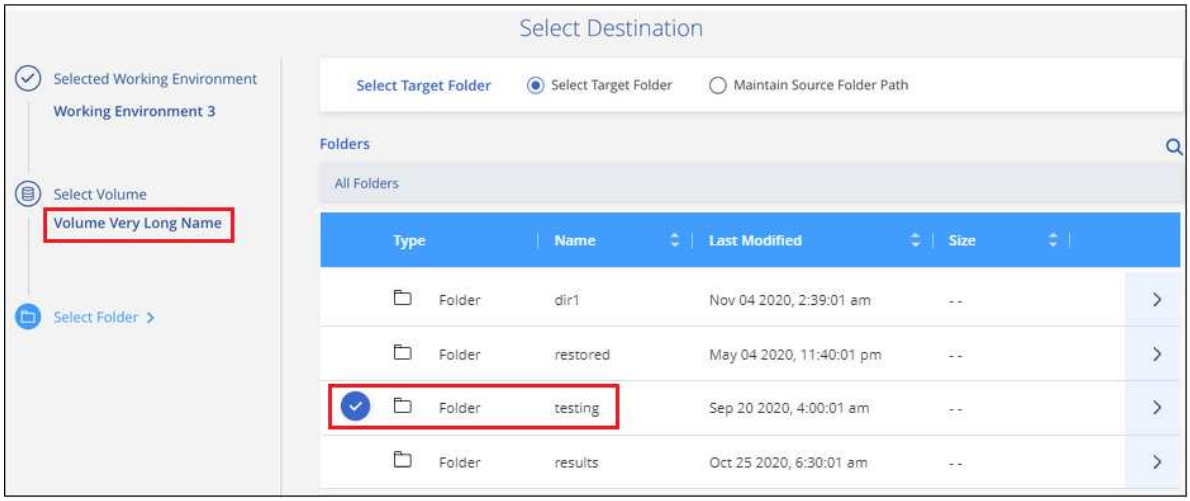
◦ Ao restaurar a partir do Amazon S3, insira o espaço de IPspace no cluster do ONTAP onde reside o volume de destino e a chave de acesso e chave secreta da AWS necessárias para acessar o armazenamento de objetos. Também pode selecionar uma Configuração de ligação privada para a ligação ao cluster.

▪ Ao restaurar a partir do Blob do Azure, insira o espaço IPspace no cluster do ONTAP onde reside o volume de destino. Você também pode selecionar uma Configuração de endpoints privados para a conexão com o cluster.

▪ Ao restaurar a partir do Google Cloud Storage, insira o espaço IPspace no cluster do ONTAP onde residem os volumes de destino e a chave de acesso e chave secreta necessárias para acessar o armazenamento de objetos.

▪ Ao restaurar a partir do StorageGRID, digite o FQDN do servidor StorageGRID e a porta que o ONTAP deve usar para comunicação HTTPS com o StorageGRID, digite a chave de acesso e a chave secreta necessárias para acessar o armazenamento de objetos e o espaço de IPspace no cluster do ONTAP onde reside o volume de destino.

a. Em seguida, selecione **volume** e **pasta** onde deseja restaurar a pasta ou arquivo(s).



Você tem algumas opções para o local ao restaurar pastas e arquivos.

- Quando tiver escolhido **Selecione pasta de destino**, conforme mostrado acima:
  - Você pode selecionar qualquer pasta.
  - Você pode passar o Mouse sobre uma pasta e clicar no final da linha para detalhar subpastas e, em seguida, selecionar uma pasta.
- Se tiver selecionado o mesmo ambiente de trabalho de destino e volume que o local da pasta/ficheiro de origem estava localizado, pode selecionar **manter caminho da pasta de origem** para restaurar a pasta ou ficheiro(s) na mesma pasta onde existiam na estrutura de origem. Todas as mesmas pastas e subpastas já devem existir; as pastas não são criadas. Ao restaurar arquivos para seu local original, você pode optar por substituir o(s) arquivo(s) de origem ou criar novo(s) arquivo(s).
  a. Clique em **Restaurar** e você será retornado ao Painel de Restauração para que você possa revisar o andamento da operação de restauração. Você também pode clicar na guia **Monitoramento de tarefas** para ver o progresso da restauração.

Restaure os dados do ONTAP utilizando a Pesquisa e a Restauração

Pode restaurar um volume, pasta ou ficheiros a partir de um ficheiro de cópia de segurança do ONTAP utilizando a Pesquisa e restauro. Pesquisa e restauração permite pesquisar um volume, pasta ou arquivo específico de todos os backups e, em seguida, executar uma restauração. Você não precisa saber o nome exato do ambiente de trabalho, o nome do volume ou o nome do arquivo - a pesquisa analisa todos os arquivos de backup de volume.

A operação de pesquisa analisa todas as cópias Snapshot locais que existem para seus volumes ONTAP, todos os volumes replicados em sistemas de storage secundário e todos os arquivos de backup que existem no storage de objetos. Como a restauração de dados de uma cópia Snapshot local ou de um volume replicado pode ser mais rápida e menos cara do que a restauração de um arquivo de backup no storage de objetos, talvez você queira restaurar os dados desses outros locais.

Quando você restaura um volume *completo* de um arquivo de backup, o backup e a recuperação do BlueXP criam um volume *new* usando os dados do backup. Você pode restaurar os dados como um volume no ambiente de trabalho original, em um ambiente de trabalho diferente localizado na mesma conta de nuvem que o ambiente de trabalho de origem ou em um sistema ONTAP no local.

Você pode restaurar *pastas ou arquivos* para o local do volume original, para um volume diferente no mesmo ambiente de trabalho, para um ambiente de trabalho diferente que esteja usando a mesma conta na nuvem ou para um volume em um sistema ONTAP local.

Ao usar o ONTAP 9.13,0 ou superior, você pode restaurar uma pasta juntamente com todos os arquivos e subpastas dentro dela. Ao usar uma versão do ONTAP antes de 9.13.0, somente os arquivos dessa pasta são restaurados - nenhuma subpasta ou arquivos em subpastas são restaurados.

Se o arquivo de backup do volume que você deseja restaurar residir no storage de arquivamento (disponível a partir do ONTAP 9.10,1), a operação de restauração levará um tempo maior e incorrerá em custos adicionais. Observe que o cluster de destino também deve estar executando o ONTAP 9.10,1 ou superior para restauração de volume, 9.11.1 para restauração de arquivos, 9.12.1 para arquivamento e StorageGRID do Google e 9.13.1 para restauração de pastas.

"Saiba mais sobre como restaurar o armazenamento de arquivamento da AWS".

"Saiba mais sobre como restaurar a partir do armazenamento de arquivos do Azure".

"Saiba mais sobre como restaurar a partir do armazenamento de arquivos do Google".

- Se o arquivo de backup no armazenamento de objetos tiver sido configurado com proteção DataLock & ransomware, a restauração em nível de pasta será suportada somente se a versão do ONTAP for 9.13.1 ou superior. Se você estiver usando uma versão anterior do ONTAP, poderá restaurar todo o volume do arquivo de backup e, em seguida, acessar a pasta e os arquivos necessários.
- Se o arquivo de backup no armazenamento de objetos residir no armazenamento de arquivamento, a restauração em nível de pasta será suportada somente se a versão do ONTAP for 9.13.1 ou superior. Se estiver a utilizar uma versão anterior do ONTAP, pode restaurar a pasta a partir de um ficheiro de cópia de segurança mais recente que não tenha sido arquivado ou pode restaurar todo o volume a partir da cópia de segurança arquivada e, em seguida, aceder à pasta e aos ficheiros de que necessita.
- A prioridade de restauração "alta" não é suportada ao restaurar dados do armazenamento de arquivamento do Azure para sistemas StorageGRID.
- A restauração de pastas não é atualmente suportada a partir de volumes no armazenamento de objetos do ONTAP S3.

Antes de começar, você deve ter alguma ideia do nome ou localização do volume ou arquivo que deseja restaurar.

O vídeo a seguir mostra um passo rápido de restaurar um único arquivo:

Pesquisa e restauração ambientes de trabalho e provedores de storage de objetos compatíveis

É possível restaurar os dados do ONTAP a partir de um arquivo de backup que reside em um ambiente de trabalho secundário (um volume replicado) ou no storage de objetos (um arquivo de backup) para os seguintes ambientes de trabalho. As cópias Snapshot residem no ambiente de trabalho de origem e podem ser restauradas somente nesse mesmo sistema.

Observação: você pode restaurar volumes e arquivos de qualquer tipo de arquivo de backup, mas você pode restaurar uma pasta somente de arquivos de backup no armazenamento de objetos neste momento.

Localização do ficheiro de cópia de segurança		**Ambiente de trabalho de destino**
Object Store (Backup)	**Sistema secundário (replicação)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP on-premises da AWS	Cloud Volumes ONTAP no AWS on-premises ONTAP system endif::aws[] ifdef::azure[]
Blob do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP in Azure on-premises ONTAP system endif::azul[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP no sistema ONTAP local do Google	Cloud Volumes ONTAP no Google on-premises ONTAP system endif::gcp[]
NetApp StorageGRID	ONTAP System Cloud Volumes ONTAP no local	Sistema ONTAP no local
ONTAP S3	ONTAP System Cloud Volumes ONTAP no local	Sistema ONTAP no local

Para pesquisar e restaurar, o conetor pode ser instalado nos seguintes locais:

- Para o Amazon S3, o conetor pode ser implantado na AWS ou em suas instalações
- Para o Azure Blob, o conetor pode ser implantado no Azure ou no local
- Para o Google Cloud Storage, o conetor deve ser implantado na VPC do Google Cloud Platform
- Para o StorageGRID, o conetor deve ser implantado em suas instalações, com ou sem acesso à Internet
- Para o ONTAP S3, o conetor pode ser implantado em suas instalações (com ou sem acesso à Internet) ou em um ambiente de provedor de nuvem

Observe que as referências a "sistemas ONTAP on-premises" incluem sistemas FAS, AFF e ONTAP Select.

Pré-requisitos

- Requisitos do cluster:
  - A versão ONTAP deve ser 9,8 ou superior.
  - A VM de storage (SVM) na qual o volume reside deve ter um LIF de dados configurado.
  - O NFS deve estar ativado no volume (os volumes NFS e SMB/CIFS são compatíveis).
  - O SnapDiff RPC Server deve ser ativado no SVM. O BlueXP faz isso automaticamente quando você ativa a Indexação no ambiente de trabalho. (O SnapDiff é a tecnologia que identifica rapidamente as diferenças de arquivo e diretório entre cópias Snapshot.)
- Requisitos da AWS:
  - Permissões específicas do Amazon Athena, AWS Glue e e AWS S3 devem ser adicionadas à função de usuário que fornece permissões ao BlueXP . "Certifique-se de que todas as permissões estão configuradas corretamente".

    Observe que se você já estava usando backup e recuperação do BlueXP com um conetor configurado no passado, você precisará adicionar as permissões Athena e Glue à função de usuário do BlueXP agora. Eles são necessários para Pesquisa e Restauração.
- Requisitos do Azure:
  - Você deve Registrar o Fornecedor de recursos do Azure Synapse Analytics (chamado "Microsoft.Synapse") com sua assinatura. "Veja como registar este fornecedor de recursos para a sua subscrição". Você deve ser a assinatura **proprietário** ou **Colaborador** para Registrar o provedor de recursos.
  - As permissões específicas da conta de armazenamento de dados e espaço de trabalho do Azure Synapse devem ser adicionadas à função de usuário que fornece permissões ao BlueXP . "Certifique-se de que todas as permissões estão configuradas corretamente".

    Observe que se você já estava usando o backup e a recuperação do BlueXP com um conetor que você configurou no passado, você precisará adicionar as permissões da conta de armazenamento do Azure Synapse Workspace e do data Lake à função de usuário do BlueXP agora. Eles são necessários para Pesquisa e Restauração.
  - O conetor deve ser configurado **sem** um servidor proxy para comunicação HTTP com a Internet. Se tiver configurado um servidor proxy HTTP para o seu conetor, não poderá utilizar a funcionalidade pesquisar e substituir.
- Requisitos do Google Cloud:
  - Permissões específicas do Google BigQuery devem ser adicionadas à função de usuário que fornece permissões ao BlueXP . "Certifique-se de que todas as permissões estão configuradas corretamente".

Observe que se você já estava usando backup e recuperação do BlueXP com um conetor configurado anteriormente, será necessário adicionar as permissões do BigQuery à função de usuário do BlueXP agora. Eles são necessários para Pesquisa e Restauração.

- Requisitos do StorageGRID e do ONTAP S3:

  Dependendo da sua configuração, existem 2 maneiras pelas quais a Pesquisa e Restauração é implementada:

  - Se não houver credenciais de provedor de nuvem em sua conta, as informações do Catálogo indexado serão armazenadas no conetor.
  - Se você estiver usando um conetor em um site privado (escuro), as informações do Catálogo indexado serão armazenadas no conetor (requer a versão 3.9.25 ou superior do conetor).
  - Se você tiver "Credenciais AWS" ou "Credenciais do Azure" estiver na conta, o Catálogo indexado será armazenado no provedor de nuvem, assim como com um conetor implantado na nuvem. (Se você tiver ambas as credenciais, a AWS será selecionada por padrão.)

    Mesmo que você esteja usando um conector no local, os requisitos do fornecedor de nuvem devem ser atendidos tanto para permissões de conetores quanto para recursos do fornecedor de nuvem. Consulte os requisitos da AWS e do Azure acima ao usar essa implementação.

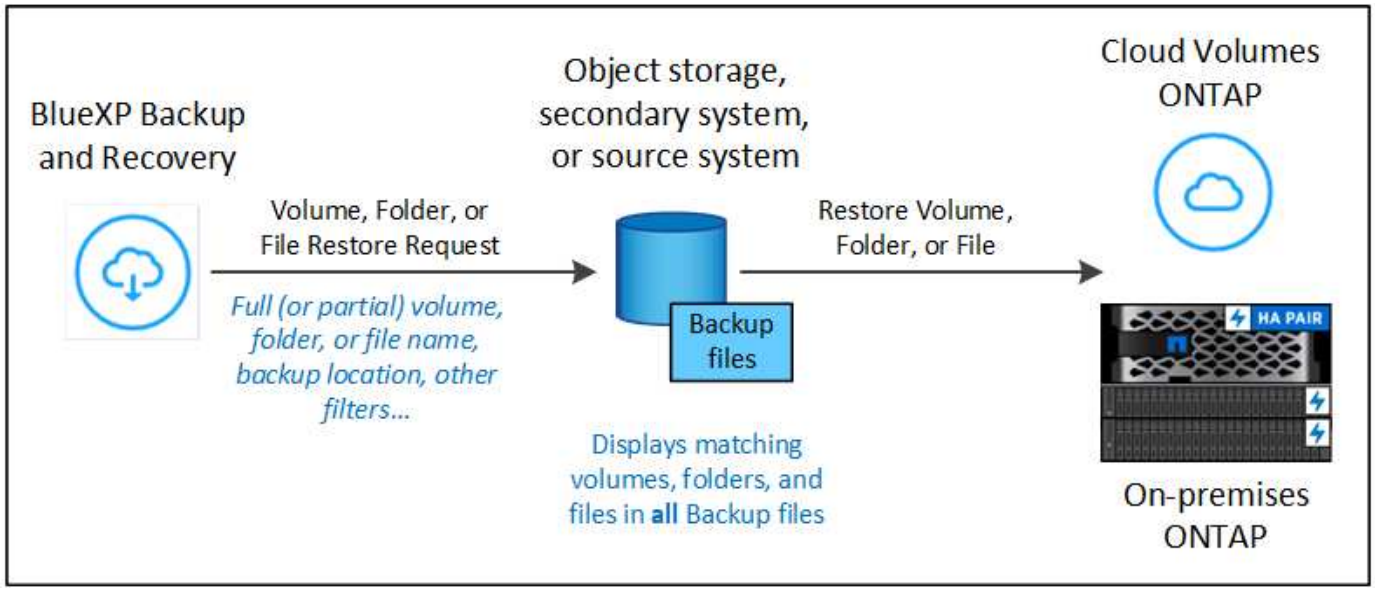
Processo de pesquisa e restauração

O processo é assim:

1. Antes de poder utilizar a Pesquisa e Restauro, tem de ativar a "Indexação" em cada ambiente de trabalho de origem a partir do qual pretende restaurar os dados de volume. Isso permite que o Catálogo indexado acompanhe os arquivos de backup para cada volume.
2. Quando pretender restaurar um volume ou ficheiros a partir de uma cópia de segurança de volume, em *Search & Restore*, clique em **Search & Restore**.
3. Introduza os critérios de pesquisa para um volume, pasta ou ficheiro por nome de volume parcial ou completo, nome de ficheiro parcial ou completo, localização de cópia de segurança, intervalo de tamanho, intervalo de datas de criação, outros filtros de pesquisa e clique em **pesquisar**.

   A página resultados da pesquisa exibe todos os locais que têm um arquivo ou volume que corresponde aos seus critérios de pesquisa.

4. Clique em **Exibir todos os backups** para o local que você deseja usar para restaurar o volume ou arquivo e clique em **Restaurar** no arquivo de backup real que deseja usar.
5. Selecione o local onde deseja restaurar o volume, a pasta ou o(s) arquivo(s) e clique em **Restaurar**.
6. O volume, a pasta ou o(s) ficheiro(s) são restaurados.



Como você pode ver, você realmente só precisa saber um nome parcial e pesquisas de backup e recuperação do BlueXP através de todos os arquivos de backup que correspondem à sua pesquisa.

Ative o Catálogo indexado para cada ambiente de trabalho

Antes de poder utilizar a Pesquisa e Restauro, tem de ativar a "Indexação" em cada ambiente de trabalho de origem a partir do qual está a planear restaurar volumes ou ficheiros. Isso permite que o Catálogo indexado acompanhe cada volume e cada arquivo de backup - tornando suas pesquisas muito rápidas e eficientes.

Ao habilitar esse recurso, o backup e a recuperação do BlueXP habilitam o SnapDiff v3 no SVM para seus volumes, e ele executa as seguintes ações:

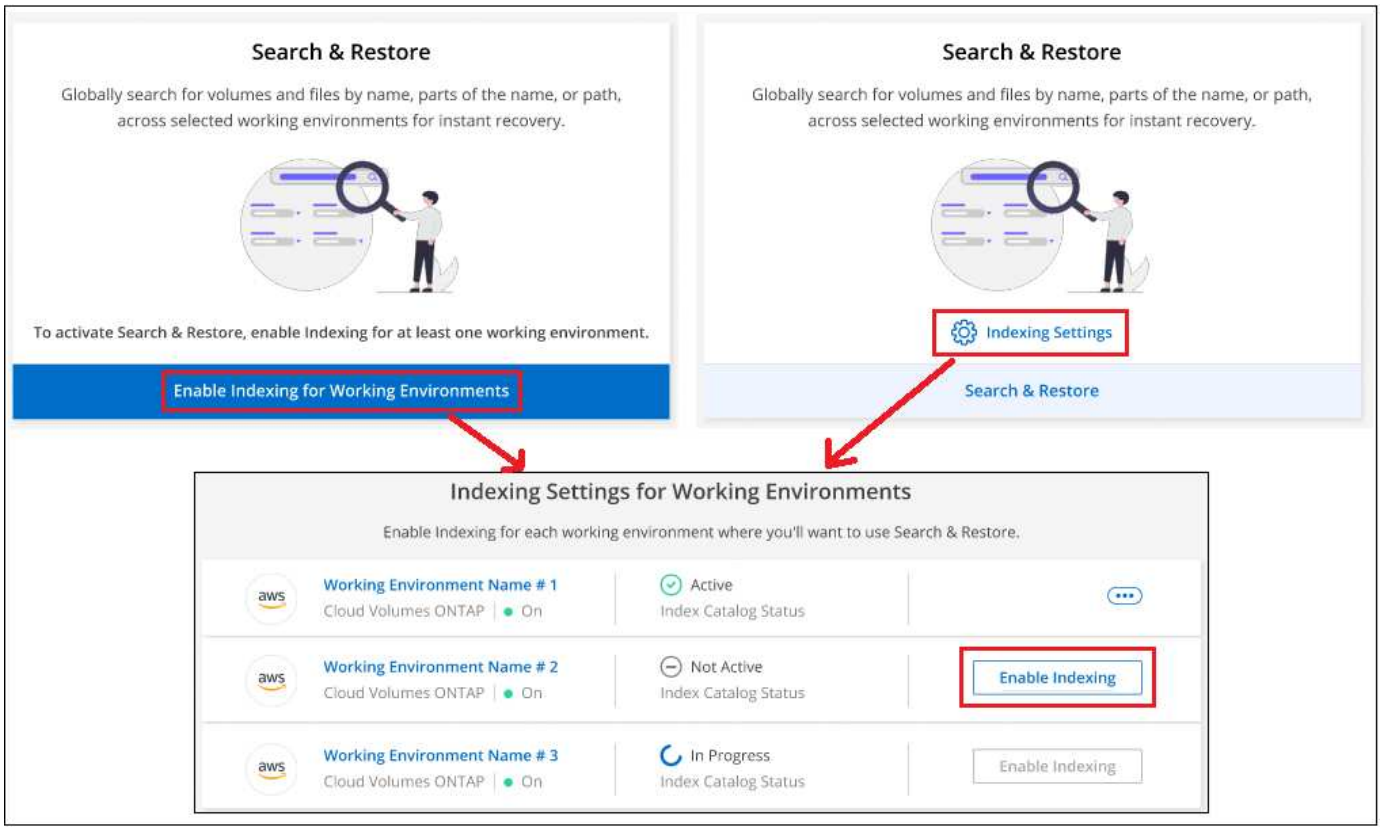
- Para backups armazenados na AWS, ele provisiona um novo bucket do S3 e o "Serviço de consulta interativa do Amazon Athena" e "Serviço de integração de dados sem servidor do AWS Glue"o .
- Para backups armazenados no Azure, ele provisiona uma área de trabalho do Azure Synapse e um sistema de arquivos do Data Lake como o contentor que armazenará os dados da área de trabalho.
- Para backups armazenados no Google Cloud, ele provisiona um novo bucket e os "Serviços do Google Cloud BigQuery" são provisionados em um nível de conta/projeto.
- Para backups armazenados no StorageGRID ou no ONTAP S3, ele provisiona espaço no conetor ou no ambiente do provedor de nuvem.

Se a Indexação já tiver sido ativada para o seu ambiente de trabalho, vá para a próxima seção para restaurar seus dados.

Para ativar a Indexação para um ambiente de trabalho:

- Se nenhum ambiente de trabalho tiver sido indexado, no Painel de Restauro em *Search & Restore*, clique em **Enable Indexing for Working Environments** (Ativar Indexação para ambientes de trabalho) e clique em **Enable Indexing** (Ativar Indexação) para o ambiente de trabalho.
- Se pelo menos um ambiente de trabalho já tiver sido indexado, no Painel de Restauro em *Search & Restore*, clique em **Indexing Settings** e clique em **Enable Indexing** para o ambiente de trabalho.

Depois que todos os serviços são provisionados e o Catálogo indexado foi ativado, o ambiente de trabalho é mostrado como "Ativo".



Dependendo do tamanho dos volumes no ambiente de trabalho e do número de arquivos de backup em todos os 3 locais de backup, o processo de indexação inicial pode levar até uma hora. Depois disso, é atualizado de forma transparente a cada hora com mudanças incrementais para se manter atualizado.

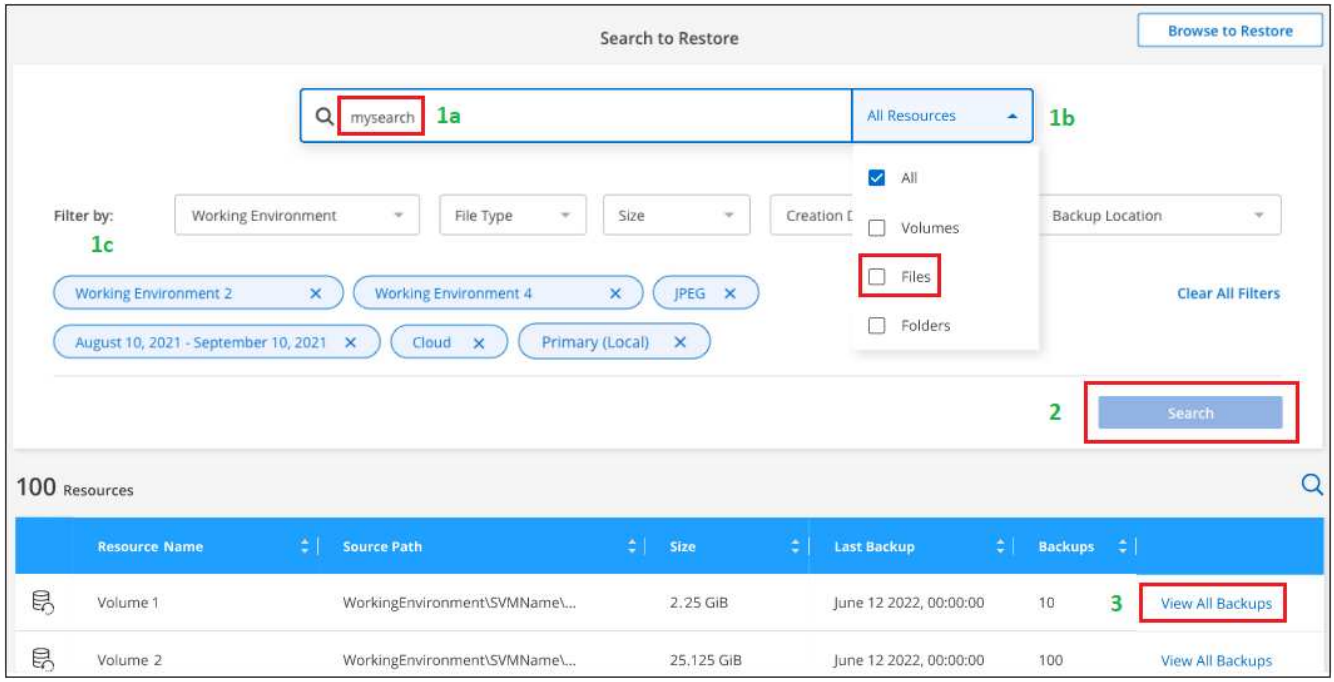
Restaure volumes, pastas e arquivos usando a Pesquisa e Restauração

Depois do Indexação ativada para o seu ambiente de trabalho, você pode restaurar volumes, pastas e arquivos usando a Pesquisa e Restauração. Isso permite que você use uma ampla gama de filtros para encontrar o arquivo ou volume exato que você deseja restaurar a partir de todos os arquivos de backup.

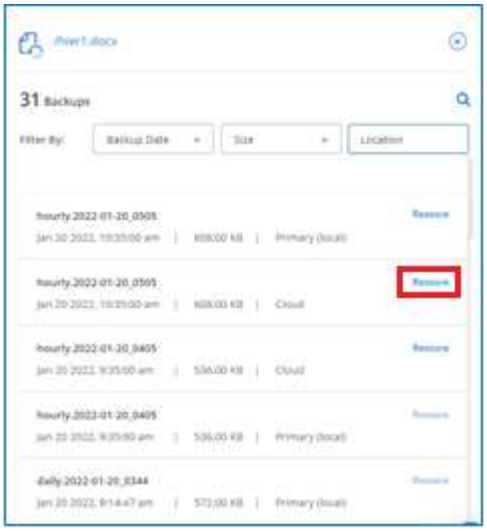
Passos

1. No menu BlueXP , selecione **proteção > Backup e recuperação**.
2. Clique na guia **Restore** e o Restore Dashboard será exibido.
3. Na seção *Search & Restore*, clique em **Search & Restore**.

4. Na página pesquisar para restaurar:
   a. Na barra *Search*, insira um nome de volume completo ou parcial, nome da pasta ou nome de arquivo.
   b. Selecione o tipo de recurso: **Volumes**, **arquivos**, **pastas** ou **todos**.
   c. Na área *Filtrar por*, selecione os critérios de filtro. Por exemplo, você pode selecionar o ambiente de trabalho onde os dados residem e o tipo de arquivo, por exemplo, um arquivo .JPEG. Ou você pode selecionar o tipo de local de backup se quiser pesquisar resultados somente nas cópias Snapshot disponíveis ou arquivos de backup no storage de objetos.
5. Clique em **pesquisar** e a área resultados da pesquisa exibe todos os recursos que têm um arquivo, pasta ou volume que corresponde à sua pesquisa.



6. Localize o recurso que tem os dados que você deseja restaurar e clique em **Exibir todos os backups** para exibir todos os arquivos de backup que contêm o volume, pasta ou arquivo correspondentes.



7. Localize o arquivo de backup que você deseja usar para restaurar os dados e clique em **Restaurar**.

   Observe que os resultados identificam cópias Snapshot de volume local e volumes replicados remotos que contêm o arquivo na pesquisa. Você pode optar por restaurar a partir do arquivo de backup em nuvem, da cópia Snapshot ou do volume replicado.

8. Selecione o local de destino onde deseja restaurar o volume, a pasta ou o(s) arquivo(s) e clique em **Restaurar**.
   - Para volumes, você pode selecionar o ambiente de trabalho de destino original ou selecionar um ambiente de trabalho alternativo. Ao restaurar um volume FlexGroup, você precisará escolher vários agregados.
   - Para pastas, você pode restaurar o local original ou selecionar um local alternativo, incluindo o ambiente de trabalho, o volume e a pasta.
   - Para arquivos, você pode restaurar o local original ou selecionar um local alternativo, incluindo o ambiente de trabalho, o volume e a pasta. Ao selecionar a localização original, pode optar por substituir o(s) ficheiro(s) de origem ou criar um(s) novo(s) ficheiro(s).

     Se você selecionar um sistema ONTAP local e ainda não tiver configurado a conexão de cluster com o armazenamento de objetos, será solicitado que você forneça informações adicionais:

     - Ao restaurar a partir do Amazon S3, selecione o espaço IPspace no cluster do ONTAP onde o volume de destino residirá, insira a chave de acesso e a chave secreta para o usuário criado para dar ao cluster do ONTAP acesso ao bucket do S3 e, opcionalmente, escolha um endpoint VPC privado para transferência segura de dados. "Veja detalhes sobre esses requisitos".
       - Ao restaurar a partir do Blob do Azure, selecione o espaço IPspace no cluster do ONTAP onde o volume de destino residirá e, opcionalmente, escolha um endpoint privado para transferência segura de dados selecionando a rede VNet e a sub-rede. "Veja detalhes sobre esses requisitos".
       - Ao restaurar a partir do Google Cloud Storage, selecione o espaço IPspace no cluster do ONTAP onde o volume de destino residirá e a chave de acesso e chave secreta para acessar o armazenamento de objetos. "Veja detalhes sobre esses requisitos".
       - Ao restaurar a partir do StorageGRID, digite o FQDN do servidor StorageGRID e a porta que o ONTAP deve usar para comunicação HTTPS com o StorageGRID, digite a chave de acesso e a chave secreta necessárias para acessar o armazenamento de objetos e o espaço de IPspace no cluster do ONTAP onde reside o volume de destino. "Veja detalhes sobre esses requisitos".

- Ao restaurar a partir do ONTAP S3, digite o FQDN do servidor ONTAP S3 e a porta que o ONTAP deve usar para comunicação HTTPS com o ONTAP S3, selecione a chave de acesso e chave secreta necessárias para acessar o armazenamento de objetos e o espaço de IPspace no cluster ONTAP onde o volume de destino residirá. "Veja detalhes sobre esses requisitos".

Resultados

O volume, a pasta ou o(s) arquivo(s) são restaurados e você é retornado ao Painel de Restauração para que você possa revisar o andamento da operação de restauração. Você também pode clicar na guia **Monitoramento de tarefas** para ver o progresso da restauração.

Para volumes restaurados, você pode"gerencie as configurações de backup para este novo volume", conforme necessário.

Fazer backup e restaurar dados de aplicações no local

Proteja os dados das aplicações no local

O backup e a recuperação do BlueXP para aplicações fornecem recursos de proteção de dados para snapshots consistentes com aplicações, desde ONTAP primário no local até fornecedor de nuvem.

Você pode fazer backup dos dados de aplicações Oracle, Microsoft SQL, SAP HANA, MongoDB, MySQL e PostgreSQL de sistemas ONTAP locais para Amazon Web Services, Microsoft Azure, Google Cloud Platform e StorageGRID.

Para obter mais informações sobre backup e recuperação do BlueXP para aplicativos, consulte:

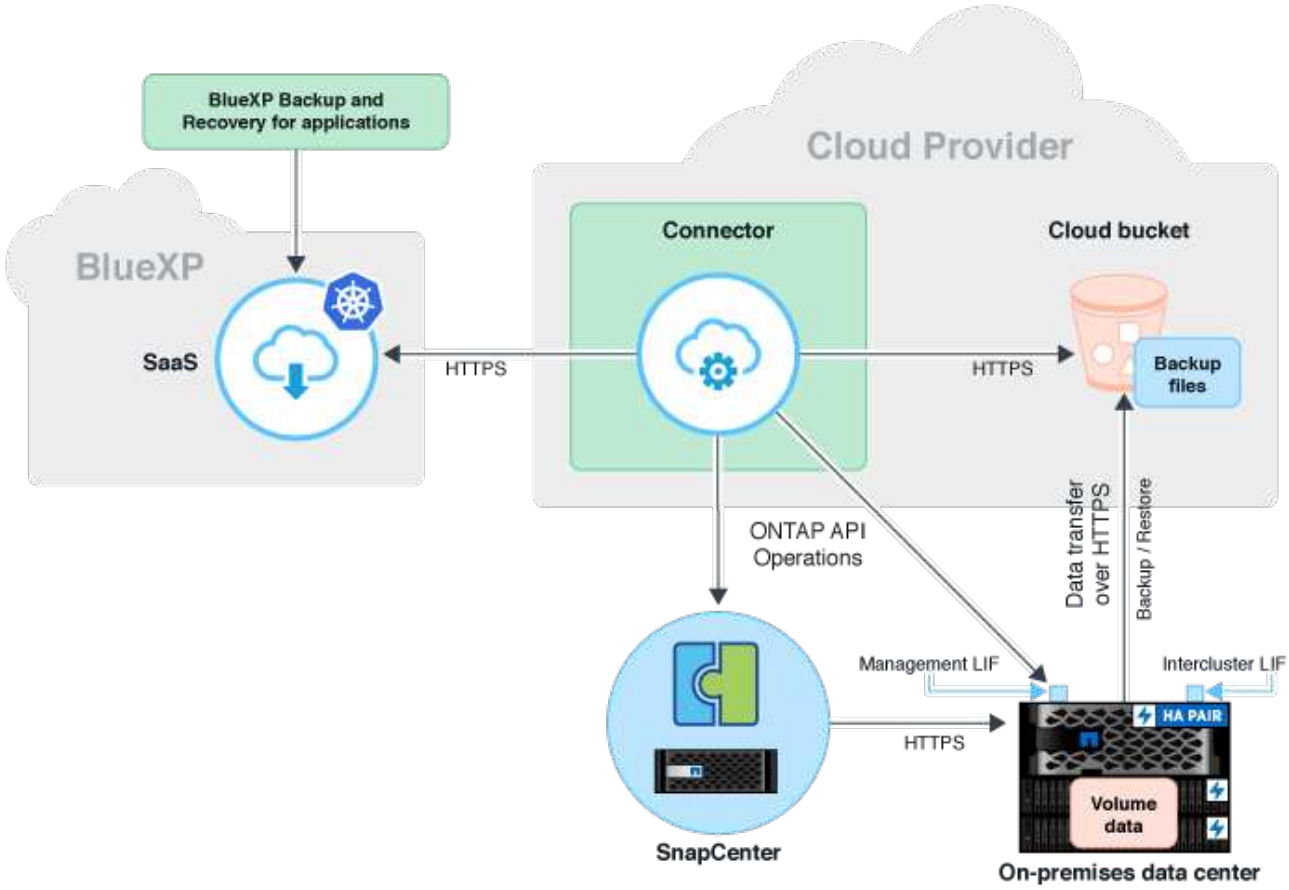
- "Backup com reconhecimento de aplicativos com backup e recuperação BlueXP e SnapCenter"
- "Backup e recuperação do BlueXP para podcast de aplicativos"

Requisitos

Leia os requisitos a seguir para garantir que você tenha uma configuração compatível antes de iniciar o backup dos dados do aplicativo para o provedor de nuvem.

- ONTAP 9 .8 ou posterior
- BlueXP
- Servidor SnapCenter 4,6 ou posterior
  - Você deve usar o servidor SnapCenter 4,7 ou posterior se quiser usar os seguintes recursos:
    - Proteger backups de storage secundário no local
    - Proteger aplicações SAP HANA
    - Proteja as aplicações Oracle e SQL que estão no ambiente VMware
    - Exportação de armazenamento de um backup
    - Desativar cópias de segurança
    - Anular o registo do servidor SnapCenter
  - Você deve usar o servidor SnapCenter 4,9 ou posterior se quiser usar os seguintes recursos:
    - Monte backups de bancos de dados Oracle
    - Restaure o armazenamento alternativo
  - Você deve usar o servidor SnapCenter 4.9P1 se quiser proteger os aplicativos MongoDB, MySQL e PostgreSQL
- Pelo menos um backup por aplicativo deve estar disponível no servidor SnapCenter
- Pelo menos uma política diária, semanal ou mensal no SnapCenter sem rótulo ou mesmo rótulo que a da política no BlueXP

A imagem a seguir mostra cada componente ao fazer backup na nuvem e as conexões que você precisa preparar entre eles:



Registre o servidor SnapCenter

Somente um usuário com a função SnapCenterAdmin pode Registrar o host no qual o servidor SnapCenter 4,6 ou posterior está sendo executado. Você pode Registrar vários hosts do servidor SnapCenter no BlueXP .

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. Na lista suspensa **Configurações**, clique em **servidores SnapCenter**.
3. Clique em **Register SnapCenter Server**.
4. Especifique os seguintes detalhes:
   a. No campo servidor SnapCenter , especifique o FQDN ou o endereço IP do host do servidor SnapCenter.
   b. No campo porta , especifique o número da porta na qual o host do servidor SnapCenter está sendo executado.

      Você deve garantir que a porta esteja aberta para que a comunicação aconteça entre o servidor SnapCenter e o BlueXP .

   c. No campo Tags , especifique um nome de site, nome de cidade ou qualquer nome personalizado com o qual você deseja marcar o servidor SnapCenter.

As tags são separadas por vírgulas.

d. No campo Nome de usuário e Senha, especifique as credenciais do usuário com a função SnapCenterAdmin.

5. Selecione o conetor na lista suspensa **Connector**.
6. Clique em **Register**.

Depois de terminar

Clique em **Backup & Restore** > **Applications** (cópia de segurança e restauro) para visualizar todas as aplicações protegidas utilizando o anfitrião do servidor SnapCenter registado. Por padrão, os aplicativos são automaticamente descobertos todos os dias da meia-noite.

Os aplicativos suportados e suas configurações são:

- Banco de dados Oracle:
  - Backups completos (dados e log) criados com pelo menos uma programação diária, semanal ou mensal
  - SAN, NFS, VMDK-SAN, VMDK-NFS E RDM
- Base de dados Microsoft SQL Server:
  - Instâncias autônomas de cluster de failover e grupos de disponibilidade
  - Backups completos criados com pelo menos uma programação diária, semanal ou mensal
  - SAN, VMDK-SAN, VMDK-NFS E RDM
- Banco de dados SAP HANA:
  - Recipiente único 1.x
  - Contentor de banco de dados múltiplo 2.x
  - Replicação do sistema HANA (HSR)

    Você deve ter pelo menos um backup em locais primários e secundários. Você pode decidir fazer uma falha pró-ativa ou um failover diferido para o secundário.

  - Recursos de volumes que não são de dados (NDV), como binários HANA, volume de log de arquivamento HANA, volume compartilhado HANA, etc.
- MongoDB
- MySQL
- PostgreSQL

As seguintes bases de dados não são apresentadas:

- Bancos de dados que não têm backups
- Bancos de dados que têm apenas políticas sob demanda ou por hora
- Bancos de dados Oracle residentes no NVMe

Crie uma política para fazer backup de aplicativos

Você deve criar uma política para fazer backup dos dados do aplicativo na nuvem.

Antes de começar

- Se você quiser mover backups do armazenamento de objetos para o armazenamento de arquivamento, verifique se está usando a versão ONTAP necessária.
  - Se você estiver usando o Amazon Web Services, você deve usar o ONTAP 9.10,1 ou posterior
  - Se estiver a utilizar o Microsoft Azure, deverá utilizar o ONTAP 9.10,1 ou posterior
  - Se você estiver usando o Google Cloud, você deve usar o ONTAP 9.12,1 ou posterior
  - Se estiver a utilizar o StorageGRID, deverá utilizar o ONTAP 9.12,1 ou posterior
- Você deve configurar o nível de acesso de arquivamento para cada provedor de nuvem.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. Na lista suspensa Configurações, clique em **políticas** > **criar política**.
3. Na seção Detalhes da política, especifique o nome da política.
4. Na seção retenção, selecione um dos tipos de retenção e especifique o número de backups a serem mantidos.
5. Selecione primário ou secundário como origem de armazenamento de backup.
6. (Opcional) se você quiser mover backups do armazenamento de objetos para o armazenamento de arquivos após um determinado número de dias para otimização de custos, marque a caixa de seleção **backups de nível para arquivamento**.
7. Clique em **criar**.

Você não pode editar ou excluir uma política, que está associada a um aplicativo.

Faça backup dos dados de aplicativos locais para o Amazon Web Services

Execute algumas etapas para fazer backup dos dados de aplicativos do ONTAP para o Amazon Web Services.

O BlueXP é compatível com bloqueio de dados e proteção contra ransomware. Se o cluster do ONTAP estiver em execução no ONTAP 9.11,1 ou posterior e não tiver configurado o storage de arquivamento, os backups podem ser protegidos contra a substituição, a exclusão e as ameaças de ransomware.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. Clique ••• em correspondente ao aplicativo e clique em **Ativar Backup**.
3. Na página atribuir política, selecione a política e clique em **seguinte**.
4. Adicione o ambiente de trabalho.

   Configure o LIF de gerenciamento de cluster que você deseja que o BlueXP descubra. Depois de adicionar o ambiente de trabalho para um dos aplicativos, ele pode ser reutilizado para todos os outros aplicativos que residem no mesmo cluster do ONTAP.

   a. Selecione o SVM e clique em **Adicionar ambiente de trabalho**.

b. No assistente Adicionar ambiente de trabalho:

i. Especifique o endereço IP do LIF de gerenciamento de cluster.

ii. Especifique as credenciais do usuário do cluster do ONTAP.

O backup e a recuperação do BlueXP para aplicações são compatíveis apenas com o administrador do cluster.

c. Clique em **Adicionar ambiente de trabalho**.

5. Selecione **Amazon Web Services** como provedor de nuvem.

a. Especifique a conta da AWS.

b. No campo chave de acesso da AWS, especifique a chave.

c. No campo chave secreta da AWS, especifique a senha.

d. Selecione a região onde deseja criar os backups.

e. Especifique o espaço IP.

f. Selecione o nível de arquivamento se tiver configurado o armazenamento de arquivamento na política.

Recomenda-se definir o nível de arquivo porque esta é uma atividade única e você não poderá configurá-lo mais tarde.

6. Configurar o bloqueio de dados e a proteção contra ransomware.

7. Revise os detalhes e clique em **Ativar Backup**.

Faça backup dos dados das aplicações locais para o Microsoft Azure

Conclua algumas etapas para fazer backup dos dados de aplicativos do ONTAP para o Microsoft Azure.

O BlueXP é compatível com bloqueio de dados e proteção contra ransomware. Se o cluster do ONTAP estiver em execução no ONTAP 9.12,1 ou posterior e não tiver configurado o storage de arquivamento, os backups podem ser protegidos contra a substituição, a exclusão e as ameaças de ransomware.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. Clique ••• em correspondente ao aplicativo e clique em **Ativar Backup**.
3. Na página atribuir política, selecione a política e clique em **seguinte**.
4. Adicione o ambiente de trabalho.

Configure o LIF de gerenciamento de cluster que você deseja que o BlueXP descubra. Depois de adicionar o ambiente de trabalho para um dos aplicativos, ele pode ser reutilizado para todos os outros aplicativos que residem no mesmo cluster do ONTAP.

a. Selecione o SVM e clique em **Adicionar ambiente de trabalho**.

b. No assistente Adicionar ambiente de trabalho:

i. Especifique o endereço IP do LIF de gerenciamento de cluster.

ii. Especifique as credenciais do usuário do cluster do ONTAP.

O backup e a recuperação do BlueXP para aplicações são compatíveis apenas com o administrador do cluster.

c. Clique em **Adicionar ambiente de trabalho**.

5. Selecione **Microsoft Azure** como provedor de nuvem.
   a. Especifique o ID de assinatura do Azure.
   b. Selecione a região onde deseja criar os backups.
   c. Crie um novo grupo de recursos ou use um grupo de recursos existente.
   d. Especifique o espaço IP.
   e. Selecione o nível de arquivamento se tiver configurado o armazenamento de arquivamento na política.

      Recomenda-se definir o nível de arquivo porque esta é uma atividade única e você não poderá configurá-lo mais tarde.

6. Configurar o bloqueio de dados e a proteção contra ransomware.
7. Revise os detalhes e clique em **Ativar Backup**.

Fazer backup dos dados das aplicações locais no Google Cloud Platform

Execute algumas etapas para fazer backup dos dados de aplicativos do ONTAP para o Google Cloud Platform.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. Clique ••• em correspondente ao aplicativo e clique em **Ativar Backup**.
3. Na página atribuir política, selecione a política e clique em **seguinte**.
4. Adicione o ambiente de trabalho.

   Configure o LIF de gerenciamento de cluster que você deseja que o BlueXP descubra. Depois de adicionar o ambiente de trabalho para um dos aplicativos, ele pode ser reutilizado para todos os outros aplicativos que residem no mesmo cluster do ONTAP.

   a. Selecione o SVM e clique em **Adicionar ambiente de trabalho**.
   b. No assistente Adicionar ambiente de trabalho:
      i. Especifique o endereço IP do LIF de gerenciamento de cluster.
      ii. Especifique as credenciais do usuário do cluster do ONTAP.

      O backup e a recuperação do BlueXP para aplicações são compatíveis apenas com o administrador do cluster.

   c. Clique em **Adicionar ambiente de trabalho**.
5. Selecione **Google Cloud Platform** como provedor de nuvem.
   a. Selecione o projeto do Google Cloud onde você deseja que o bucket do Google Cloud Storage seja

criado para backups.

b. No campo chave de acesso do Google Cloud, especifique a chave.

c. No campo chave secreta do Google Cloud, especifique a senha.

d. Selecione a região onde deseja criar os backups.

e. Especifique o espaço IP.

f. Selecione o nível de arquivamento.

   Recomenda-se definir o nível de arquivo porque esta é uma atividade única e você não poderá configurá-lo mais tarde.

6. Revise os detalhes e clique em **Ativar Backup**.

Fazer backup dos dados das aplicações locais no StorageGRID

Execute algumas etapas para fazer backup dos dados de aplicativos do ONTAP para o StorageGRID.

O BlueXP é compatível com bloqueio de dados e proteção contra ransomware. Se o cluster do ONTAP estiver sendo executado no ONTAP 9.11,1 ou posterior, os sistemas StorageGRID são 11.6.0.3 ou posterior e, se você não tiver configurado o storage de arquivamento, poderá proteger os backups contra a substituição, a exclusão e ameaças de ransomware.

Antes de começar

Ao fazer backup de dados para o 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. O conetor pode ser instalado em um site com ou sem acesso à Internet.

Para obter informações, "Crie conetores para StorageGRID"consulte .

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. Clique ••• em correspondente ao aplicativo e clique em **Ativar Backup**.
3. Na página atribuir política, selecione a política e clique em **seguinte**.
4. Adicione o ambiente de trabalho.

   Configure o LIF de gerenciamento de cluster que você deseja que o BlueXP descubra. Depois de adicionar o ambiente de trabalho para um dos aplicativos, ele pode ser reutilizado para todos os outros aplicativos que residem no mesmo cluster do ONTAP.

   a. Selecione o SVM e clique em **Adicionar ambiente de trabalho**.

   b. No assistente Adicionar ambiente de trabalho:

      i. Especifique o endereço IP do LIF de gerenciamento de cluster.

      ii. Especifique as credenciais do usuário do cluster do ONTAP.

      O backup e a recuperação do BlueXP para aplicações são compatíveis apenas com o administrador do cluster.

c. Clique em **Adicionar ambiente de trabalho**.

5. Selecione **StorageGRID**.
   a. Especifique o FQDN do servidor StorageGRID e a porta na qual o servidor StorageGRID está sendo executado.

      Insira os detalhes no formato FQDN:PORT.

   b. No campo chave de acesso , especifique a chave.
   c. No campo chave secreta , especifique a senha.
   d. Especifique o espaço IP.
   e. Especifique o nível de arquivamento se você configurou o armazenamento de arquivamento na política.

Se selecionar…	Execute o seguinte…
AWS	i. Selecione o StorageGRID na lista suspensa ou adicione o cluster StorageGRID. ii. Especifique a conta da AWS. iii. No campo chave de acesso da AWS, especifique a chave. iv. No campo chave secreta da AWS, especifique a senha. v. Selecione a região onde deseja criar os backups. vi. Clique em **Salvar**.
Azure	i. Selecione o cluster StorageGRID no menu suspenso ou adicione o cluster. ii. Especifique o ID de assinatura do Azure. iii. Selecione a região onde deseja criar os backups. iv. Crie um novo grupo de recursos ou use um grupo de recursos existente. v. Clique em **Salvar**.

      Recomenda-se definir o nível de arquivo porque esta é uma atividade única e você não poderá configurá-lo mais tarde.

6. Configurar o bloqueio de dados e a proteção contra ransomware.
7. Revise os detalhes e clique em **Ativar Backup**.

Gerenciar a proteção de aplicativos

Você pode gerenciar a proteção de aplicativos exibindo políticas, exibindo backups, exibindo as alterações no layout do banco de dados, políticas e grupo de recursos, além

de monitorar todas as operações a partir da IU do BlueXP .

Ver políticas

Você pode visualizar todas as políticas. Para cada uma dessas políticas, quando você exibe os detalhes, todos os aplicativos associados são listados.

Passos

1. Clique em **Backup e recuperação** > **aplicativos**.
2. Na lista suspensa **Configurações**, clique em **políticas**.
3. Clique em **Ver detalhes** correspondente à política cujos detalhes você deseja visualizar.

   Os aplicativos associados são listados.

   Você não pode editar ou excluir uma política, que está associada a um aplicativo.

Você também pode exibir políticas SnapCenter estendidas na nuvem executando `Get-SmResources` o cmdlet no SnapCenter. As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando o nome do comando Get-Help.

Ver backups na nuvem

Você pode visualizar os backups na nuvem na IU do BlueXP .

Passos

1. Clique em **Backup e recuperação** > **aplicativos**.
2. Clique ••• em correspondente ao aplicativo e clique em **Exibir detalhes**.

   O tempo necessário para que os backups sejam listados depende da programação de replicação padrão do ONTAP.

- Para bancos de dados Oracle, tanto os backups de dados quanto os de log, o número de mudança do sistema (SCN) para cada backup, a data final para cada backup são listados. Você pode selecionar apenas o backup de dados e restaurar o banco de dados para o local original. Você pode montar o backup de dados e o backup de log para um local alternativo.
- Para bancos de dados do Microsoft SQL Server, apenas os backups completos e a data final de cada backup são listados. Você pode selecionar o backup e restaurar o banco de dados para o local original ou alternativo.
- Para instância do Microsoft SQL Server, os backups dos bancos de dados sob essa instância são listados.
- Para bancos de dados SAP HANA, somente os backups de dados e a data de término de cada backup são listados. Você pode selecionar o backup e executar a exportação de armazenamento em um determinado host.
- Para MongoDB, MySQL e PostgreSQL, apenas os backups de dados e a data final de cada backup são listados. Você pode selecionar o backup e executar a exportação de armazenamento em um determinado host.

   Os backups criados antes de ativar a proteção na nuvem não estão listados para restauração.

Você também pode exibir esses backups executando `Get-SmBackup` o cmdlet no SnapCenter. As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando o nome do comando Get-Help.

Desativar a cópia de segurança

Você pode excluir todos os backups movidos para o armazenamento de objetos do SnapCenter e do armazenamento de objetos.

Passos

1. Clique em **Backup e recuperação** > **aplicativos**.
2. Clique ••• em correspondente à aplicação e clique em Desativar cópia de segurança.

   Por padrão, a caixa de seleção está selecionada e exclui todos os backups movidos para o armazenamento de objetos do SnapCenter e do armazenamento de objetos.

   Se você desmarcar a caixa de seleção, os backups serão retidos somente no armazenamento de objetos, mas esses backups não poderão ser usados para restauração no nível do aplicativo. Mais tarde, quando você ativa o backup para este aplicativo, os backups retidos no armazenamento de objetos não são listados para restauração.

3. Clique em **Desativar Backup**.

Alteração do layout do banco de dados

Quando os volumes são adicionados ao banco de dados, o servidor SnapCenter rotula os snapshots nos novos volumes automaticamente de acordo com a política e a programação. Esses novos volumes não terão o ponto final do armazenamento de objetos e você deve atualizar os volumes executando as seguintes etapas:

Passos

1. Clique em **Backup e recuperação** > **aplicativos**.
2. Na lista suspensa **Configurações**, clique em **servidores SnapCenter**.
3. Clique ••• em correspondente ao servidor SnapCenter que hospeda o aplicativo e clique em **Atualizar**.

   Os novos volumes são descobertos.

4. Clique ••• em correspondente ao aplicativo e clique em **Refresh Protection** para ativar a proteção na nuvem para o novo volume.
   - Se um volume de armazenamento for adicionado ao aplicativo após a configuração do provedor de nuvem, o servidor SnapCenter rotula os snapshots para novos backups nos quais o aplicativo está residindo.
   - Você deve excluir manualmente a relação de armazenamento de objetos se o volume removido não for usado por outros aplicativos.
   - Se você atualizar o inventário do aplicativo, ele conterá o layout de armazenamento atual do aplicativo.

Mudança de política ou grupo de recursos

Se houver uma alteração na política ou no grupo de recursos do SnapCenter, atualize a relação de proteção.

Passos

1. Clique em **Backup e recuperação** > **aplicativos**.
2. Clique ••• em correspondente ao aplicativo e clique em **Refresh Protection**.

Anular o registo do servidor SnapCenter

Passos

1. Clique em **Backup e recuperação** > **aplicativos**.
2. Na lista suspensa **Configurações**, clique em **servidores SnapCenter**.
3. Clique ••• em correspondente ao servidor SnapCenter e clique em **Anular Registro**.

   Por padrão, a caixa de seleção está selecionada e exclui todos os backups movidos para o armazenamento de objetos do SnapCenter e do armazenamento de objetos.

   Se você desmarcar a caixa de seleção, os backups serão retidos somente no armazenamento de objetos, mas esses backups não poderão ser usados para restauração no nível do aplicativo. Mais tarde, quando você ativa o backup para este aplicativo, os backups retidos no armazenamento de objetos não são listados para restauração.

Monitorizar trabalhos

As tarefas são criadas para todas as operações do Cloud Backup. Pode monitorizar todos os trabalhos e todas as subtarefas que são executadas como parte de cada tarefa.

Passos

1. Clique em **Backup e recuperação** > **Monitoramento de tarefas**.

   Quando inicia uma operação, é apresentada uma janela a indicar que o trabalho foi iniciado. Pode clicar na ligação para monitorizar o trabalho.

2. Clique na tarefa principal para visualizar as subtarefas e o estado de cada uma destas subtarefas.

Configurar certificados de CA

Você pode configurar o certificado assinado pela CA se quiser incluir segurança adicional ao seu ambiente.

Configure o certificado assinado CA do SnapCenter no conetor BlueXP

Você deve configurar o certificado assinado pela CA do SnapCenter no conetor BlueXP para que o conetor possa verificar o certificado do SnapCenter.

Antes de começar

Você deve executar o seguinte comando no conetor BlueXP para obter o *<base_mount_path>*:

```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

Passos

1. Inicie sessão no conetor.

   ```
   cd <base_mount_path> mkdir -p server/certificate
   ```

2. Copie os arquivos CA raiz e CA intermediária para o diretório *<base_mount_path>/Server/certificate*.

Os arquivos da CA devem estar no formato .pem.

3. Se você tiver arquivos CRL, execute as seguintes etapas:
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. Copie os arquivos CRL para o diretório *<base_mount_path>/Server/crl*.
4. Conete-se ao cloudmanager_SnapCenter e modifique o enableCACert em config.yml para true.
   `sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert: false/enableCACert: true/g' /opt/netapp/cloudmanager-snapcenter/config/config.yml`
5. Reinicie o container cloudmanager_SnapCenter.
   `sudo docker restart cloudmanager_snapcenter`

Configure o certificado assinado CA para o conetor BlueXP

Se o SSL 2way estiver habilitado no SnapCenter, execute as seguintes etapas no conetor para usar o certificado CA como o certificado de cliente quando o conetor estiver se conetando ao SnapCenter.

Antes de começar

Você deve executar o seguinte comando para obter o *<base_mount_path>*:
`sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

Passos

1. Inicie sessão no conetor.
   `cd <base_mount_path> mkdir -p client/certificate`
2. Copie o certificado assinado pela CA e o arquivo de chave para o *<base_mount_path>/cliente/certificado* no conetor.

   O nome do arquivo deve ser certificate.pem e key.pem. O certificado.pem deve ter toda a cadeia de certificados como CA intermediária e CA raiz.
3. Crie o formato PKCS12 do certificado com o nome certificate.p12 e mantenha em *<base_mount_path>/client/certificate*.

   Exemplo: openssl PKCS12 -inkey key.pem -in certificate.pem -export -out certificate.p12
4. Conete-se ao cloudmanager_SnapCenter e modifique o sendCACert em config.yml para true.
   `sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert: false/sendCACert: true/g' /opt/netapp/cloudmanager-snapcenter/config/config.yml`
5. Reinicie o container cloudmanager_SnapCenter.
   `sudo docker restart cloudmanager_snapcenter`
6. Execute as seguintes etapas no SnapCenter para validar o certificado enviado pelo conetor.
   a. Faça login no host do SnapCenter Sever.
   b. Clique em **Iniciar** > **Iniciar Pesquisa**.
   c. Digite mmc e pressione **Enter**.
   d. Clique em **Sim**.

e. No menu Arquivo, clique em **Adicionar/Remover Snap-in**.

f. Clique em **certificados** > **Adicionar** > **conta de computador** > **seguinte**.

g. Clique em **local Computer** > **Finish**.

h. Se você não tiver mais snap-ins para adicionar ao console, clique em **OK**.

i. Na árvore de console, clique duas vezes em **certificados**.

j. Clique com o botão direito do rato no **Trusted Root Certification Authorities store**.

k. Clique em **Importar** para importar os certificados e siga as etapas no **Assistente de importação de certificados**.

Restaure os dados das aplicações no local

Restaure o banco de dados Oracle

Você pode restaurar o banco de dados Oracle para o local original ou para o local alternativo. Para um banco de dados RAC, os dados são restaurados para o nó local onde o backup foi criado.

Apenas é suportado um banco de dados completo com restauração de arquivos de controle. Se os registos de arquivo não estiverem presentes no AFS, deve especificar a localização que contém os registos de arquivo necessários para a recuperação.

A Restauração de Arquivo único (SFR) não é suportada.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. No campo **Filtrar por**, selecione o filtro **tipo** e, na lista suspensa, selecione **Oracle**.
3. Clique em **Exibir detalhes** correspondente ao banco de dados que você deseja restaurar e clique em **Restaurar**.
4. Na página Restaurar opções, especifique o local onde deseja restaurar os arquivos do banco de dados.

Se você…	Faça isso…
Deseja restaurar o local original	a. Selecione **Restaurar para a localização original**. b. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento. c. Clique em **seguinte**. d. Selecione **Estado da base de dados** se pretender alterar o estado da base de dados para o estado necessário para executar operações de restauro e recuperação. Os vários estados de um banco de dados de cima para baixo são abertos, montados, iniciados e desligados. ◦ Se o banco de dados estiver em um estado superior, mas o estado tiver de ser alterado para um estado inferior para executar uma operação de restauração, você deve selecionar esta caixa de seleção. ◦ Se o banco de dados estiver em um estado inferior, mas o estado tiver de ser alterado para um estado superior para executar a operação de restauração, o estado do banco de dados será alterado automaticamente, mesmo que você não marque a caixa de seleção. ◦ Se um banco de dados estiver no estado aberto e, para restaurar, o banco de dados precisar estar no estado montado, o estado do banco de dados será alterado somente se você selecionar essa caixa de seleção. e. Especifique o escopo de recuperação. ◦ Selecione **todos os Logs** se quiser recuperar para a última transação. ◦ Selecione **Until SCN (System Change Number)** se quiser recuperar para um SCN específico. ◦ Selecione **Data e hora** se quiser recuperar dados e hora específicos. Você deve especificar a data e a hora do fuso horário do host do banco de dados. ◦ Selecione **sem recuperação** se não quiser recuperar. f. Se os registos de arquivo não estiverem presentes no sistema de ficheiros ativo, deve especificar a localização que contém os registos de arquivo necessários para a recuperação.

Se você…	Faça isso…
Deseja restaurar temporariamente para outro armazenamento e, em seguida, copiar os arquivos restaurados para o local original	a. Selecione **Restaurar para a localização original**. b. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento. c. Selecione **alterar localização de armazenamento**. Se selecionar **alterar localização de armazenamento**, pode anexar um sufixo ao volume de destino. Se você não selecionou a caixa de seleção, por padrão **_Restore** é anexado ao volume de destino. d. Clique em **seguinte**. e. Na página de mapeamento de armazenamento, especifique os detalhes do local de armazenamento alternativo onde os dados restaurados do armazenamento de objetos serão armazenados temporariamente. Se você selecionar um sistema ONTAP local e não tiver configurado a conexão do cluster com o armazenamento de objetos, será solicitado que você forneça informações adicionais sobre o armazenamento de objetos. f. Clique em **seguinte**. g. Selecione **Estado da base de dados** se pretender alterar o estado da base de dados para o estado necessário para executar operações de restauro e recuperação. Os vários estados de um banco de dados de cima para baixo são abertos, montados, iniciados e desligados. ◦ Se o banco de dados estiver em um estado superior, mas o estado tiver de ser alterado para um estado inferior para executar uma operação de restauração, você deve selecionar esta caixa de seleção. ◦ Se o banco de dados estiver em um estado inferior, mas o estado tiver de ser alterado para um estado superior para executar a operação de restauração, o estado do banco de dados será alterado automaticamente, mesmo que você não marque a caixa de seleção. ◦ Se um banco de dados estiver no estado aberto e, para restaurar, o banco de dados precisar estar no estado montado, o estado do banco de dados será alterado somente se você selecionar essa caixa de seleção.

Se você…	Faça isso…
Deseja restaurar para um local alternativo	a. Selecione **Restaurar para local alternativo**. b. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento. c. Se você quiser restaurar o armazenamento alternativo, execute o seguinte procedimento: i. Selecione **alterar localização de armazenamento**. Se selecionar **alterar localização de armazenamento**, pode anexar um sufixo ao volume de destino. Se você não selecionou a caixa de seleção, por padrão **_Restore** é anexado ao volume de destino. ii. Clique em **seguinte**. iii. Na página de mapeamento de armazenamento, especifique os detalhes do local de armazenamento alternativo em que os dados do armazenamento de objetos precisam ser restaurados. d. Clique em **seguinte**. e. Na página Destination host (anfitrião de destino), selecione o anfitrião no qual a base de dados será montada. i. (Opcional) para o ambiente nas, especifique o FQDN ou o endereço IP do host para o qual os volumes restaurados do armazenamento de objetos devem ser exportados. ii. (Opcional) para o ambiente SAN, especifique os iniciadores do host para os quais LUNs dos volumes restaurados do armazenamento de objetos devem ser mapeados. f. Clique em **seguinte**.

5. Revise os detalhes e clique em **Restaurar**.

Resultados

A opção **Restore to alternate location** (Restaurar para local alternativo) monta o backup selecionado no host fornecido. Você deve abrir manualmente o banco de dados.

Depois de montar o backup, você não pode montá-lo novamente até que ele seja desmontado. Você pode usar a opção **Desmontar** da IU para desmontar o backup.

Para obter informações sobre como abrir o banco de dados Oracle, consulte "artigo da base de conhecimento"

.

Se a operação de restauração não for concluída, não tente o processo de restauração novamente até que o Monitor de trabalho mostre que a operação de restauração falhou. Se você tentar o processo de restauração novamente antes que o Monitor de trabalho mostre que a operação de restauração falhou, a operação de restauração falhará novamente. Quando o status do Monitor de trabalho for exibido como "Falha", você poderá tentar o processo de restauração novamente.

Restaure o banco de dados do SQL Server

Você pode restaurar o banco de dados do SQL Server para o local original ou para o local alternativo.

Restauração de arquivo único (SFR), recuperação de backups de log e repleed de grupos de disponibilidade não são suportados.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. No campo **Filtrar por**, selecione o filtro **tipo** e, na lista suspensa, selecione **SQL**.
3. Clique em **Exibir detalhes** para exibir todos os backups disponíveis.
4. Selecione o backup e clique em **Restore**.
5. Na página Restaurar opções, especifique o local onde deseja restaurar os arquivos do banco de dados.

Se você…	Faça isso…
Deseja restaurar o local original	a. Selecione **Restaurar para a localização original**. b. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento. c. Clique em **seguinte**.

Se você…	Faça isso…
Deseja restaurar temporariamente para outro armazenamento e, em seguida, copiar os arquivos restaurados para o local original	a. Selecione **Restaurar para a localização original**. b. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento. c. Selecione **alterar localização de armazenamento**. Se selecionar **alterar localização de armazenamento**, pode anexar um sufixo ao volume de destino. Se você não selecionou a caixa de seleção, por padrão **_Restore** é anexado ao volume de destino. d. Clique em **seguinte**. e. Na página de mapeamento de armazenamento, especifique os detalhes do local de armazenamento alternativo onde os dados restaurados do armazenamento de objetos serão armazenados temporariamente. f. Clique em **seguinte**.
Deseja restaurar para um local alternativo	a. Selecione **Restaurar para local alternativo**. b. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento. c. Clique em **seguinte**. d. Na página host de destino, selecione um nome de host, forneça um nome de banco de dados (opcional), selecione uma instância e especifique os caminhos de restauração. A extensão de arquivo fornecida no caminho alternativo deve ser igual à extensão de arquivo do arquivo de banco de dados original. e. Clique em **seguinte**.

Se você…	Faça isso…
Deseja restaurar temporariamente para outro armazenamento e, em seguida, copiar os arquivos restaurados para o local alternativo	a. Selecione **Restaurar para local alternativo**. b. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento. c. Selecione **alterar localização de armazenamento**. Se selecionar **alterar localização de armazenamento**, pode anexar um sufixo ao volume de destino. Se você não selecionou a caixa de seleção, por padrão **_Restore** é anexado ao volume de destino. d. Clique em **seguinte**. e. Na página de mapeamento de armazenamento, especifique os detalhes do local de armazenamento alternativo onde os dados restaurados do armazenamento de objetos serão armazenados temporariamente. f. Clique em **seguinte**. g. Na página host de destino, selecione um nome de host, forneça um nome de banco de dados (opcional), selecione uma instância e especifique os caminhos de restauração. A extensão de arquivo fornecida no caminho alternativo deve ser igual à extensão de arquivo do arquivo de banco de dados original. h. Clique em **seguinte**.

6. Na opção **Pre-operations** (Pré-operações), selecione uma das seguintes opções:
   - Selecione **Substituir o banco de dados com o mesmo nome durante a restauração** para restaurar o banco de dados com o mesmo nome.
   - Selecione **reter configurações de replicação do banco de dados SQL** para restaurar o banco de dados e manter as configurações de replicação existentes.
7. Na seção **Pós-operações**, para especificar o estado do banco de dados para restaurar logs transacionais adicionais, selecione uma das seguintes opções:
   - Selecione **operacional, mas indisponível** se você estiver restaurando todos os backups necessários agora.

     Esse é o comportamento padrão, que deixa o banco de dados pronto para uso, revertendo as transações não confirmadas. Não é possível restaurar registos de transações adicionais até criar uma cópia de segurança.

- Selecione **não operacional, mas disponível** para deixar o banco de dados não operacional sem reverter as transações não confirmadas.

  Logs de transação adicionais podem ser restaurados. Você não pode usar o banco de dados até que ele seja recuperado.

- Selecione **modo somente leitura e disponível** para deixar o banco de dados no modo somente leitura.

  Essa opção desfaz transações não confirmadas, mas salva as ações desfeitas em um arquivo de espera para que os efeitos de recuperação possam ser revertidos.

Se a opção Desfazer diretório estiver ativada, mais logs de transações serão restaurados. Se a operação de restauração do log de transações não for bem-sucedida, as alterações podem ser revertidas. A documentação do SQL Server contém mais informações.

8. Clique em **seguinte**.
9. Revise os detalhes e clique em **Restaurar**.

> Se a operação de restauração não for concluída, não tente o processo de restauração novamente até que o Monitor de trabalho mostre que a operação de restauração falhou. Se você tentar o processo de restauração novamente antes que o Monitor de trabalho mostre que a operação de restauração falhou, a operação de restauração falhará novamente. Quando o status do Monitor de trabalho for exibido como "Falha", você poderá tentar o processo de restauração novamente.

Restaure o banco de dados SAP HANA

É possível restaurar o banco de dados SAP HANA para qualquer host.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. No campo **Filtrar por**, selecione o filtro **tipo** e, na lista suspensa, selecione **HANA**.
3. Clique em **Exibir detalhes** correspondente ao banco de dados que você deseja restaurar e clique em **Restaurar**.
4. Na página Restaurar opções, especifique uma das seguintes opções:
   a. No ambiente nas, especifique o FQDN ou o endereço IP do host para o qual os volumes restaurados do armazenamento de objetos devem ser exportados.
   b. No ambiente SAN, especifique os iniciadores do host para os quais LUNs dos volumes restaurados do armazenamento de objetos devem ser mapeados.
5. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento.
6. Se não houver espaço suficiente no armazenamento de origem ou se o armazenamento de origem estiver inativo, selecione **alterar local de armazenamento**.

   Se selecionar **alterar localização de armazenamento**, pode anexar um sufixo ao volume de destino. Se você não selecionou a caixa de seleção, por padrão **_Restore** é anexado ao volume de destino.

7. Clique em **seguinte**.

8. Na página de mapeamento de armazenamento, especifique os detalhes do local de armazenamento alternativo onde os dados restaurados do armazenamento de objetos serão armazenados.
9. Clique em **seguinte**.
10. Revise os detalhes e clique em **Restaurar**.

Esta operação faz apenas a exportação de armazenamento do backup selecionado no host fornecido. Você deve montar manualmente o sistema de arquivos e abrir o banco de dados. Depois de utilizar o volume, o administrador de armazenamento pode eliminar o volume do cluster ONTAP.

Para obter informações sobre como abrir o banco de dados SAP HANA, consulte "TR-4667: Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter" .

> Se a operação de restauração não for concluída, não tente o processo de restauração novamente até que o Monitor de trabalho mostre que a operação de restauração falhou. Se você tentar o processo de restauração novamente antes que o Monitor de trabalho mostre que a operação de restauração falhou, a operação de restauração falhará novamente. Quando o status do Monitor de trabalho for exibido como "Falha", você poderá tentar o processo de restauração novamente.

Restaure bancos de dados MongoDB, MySQL e PostgreSQL

Você pode restaurar bancos de dados MongoDB, MySQL e PostgreSQL para qualquer host.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **aplicativos**.
2. No campo **Filtrar por**, selecione o filtro **tipo** e, na lista suspensa, selecione **MongoDB**, **MySQL** ou **PostgreSQL**.
3. Clique em **Exibir detalhes** correspondente ao banco de dados que você deseja restaurar e clique em **Restaurar**.
4. Na página Restaurar opções, especifique uma das seguintes opções:
   a. No ambiente nas, especifique o FQDN ou o endereço IP do host para o qual os volumes restaurados do armazenamento de objetos devem ser exportados.
   b. No ambiente SAN, especifique os iniciadores do host para os quais LUNs dos volumes restaurados do armazenamento de objetos devem ser mapeados.
5. Se o instantâneo estiver em armazenamento de arquivo, selecione a prioridade para restaurar os dados do armazenamento de arquivamento.
6. Se não houver espaço suficiente no armazenamento de origem ou se o armazenamento de origem estiver inativo, selecione **alterar local de armazenamento**.

   Se selecionar **alterar localização de armazenamento**, pode anexar um sufixo ao volume de destino. Se você não selecionou a caixa de seleção, por padrão **_Restore** é anexado ao volume de destino.
7. Clique em **seguinte**.
8. Na página de mapeamento de armazenamento, especifique os detalhes do local de armazenamento alternativo onde os dados restaurados do armazenamento de objetos serão armazenados.
9. Clique em **seguinte**.

10. Revise os detalhes e clique em **Restaurar**.

Esta operação faz apenas a exportação de armazenamento do backup selecionado no host fornecido. Você deve montar manualmente o sistema de arquivos e abrir o banco de dados. Depois de utilizar o volume, o administrador de armazenamento pode eliminar o volume do cluster ONTAP.

Se a operação de restauração não for concluída, não tente o processo de restauração novamente até que o Monitor de trabalho mostre que a operação de restauração falhou. Se você tentar o processo de restauração novamente antes que o Monitor de trabalho mostre que a operação de restauração falhou, a operação de restauração falhará novamente. Quando o status do Monitor de trabalho for exibido como "Falha", você poderá tentar o processo de restauração novamente.

Faça backup e restaure os dados das máquinas virtuais

Proteja seus dados de máquinas virtuais

O backup e a recuperação do BlueXP para máquinas virtuais fornecem recursos de proteção de dados, fazendo backup de datastores e restaurando máquinas virtuais.

É possível fazer backup de armazenamentos de dados no Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform e StorageGRID e restaurar máquinas virtuais de volta ao plug-in do SnapCenter no local para host VMware vSphere. O backup e a recuperação do BlueXP para máquinas virtuais também oferecem suporte ao modelo de implantação de proxy de conetor.

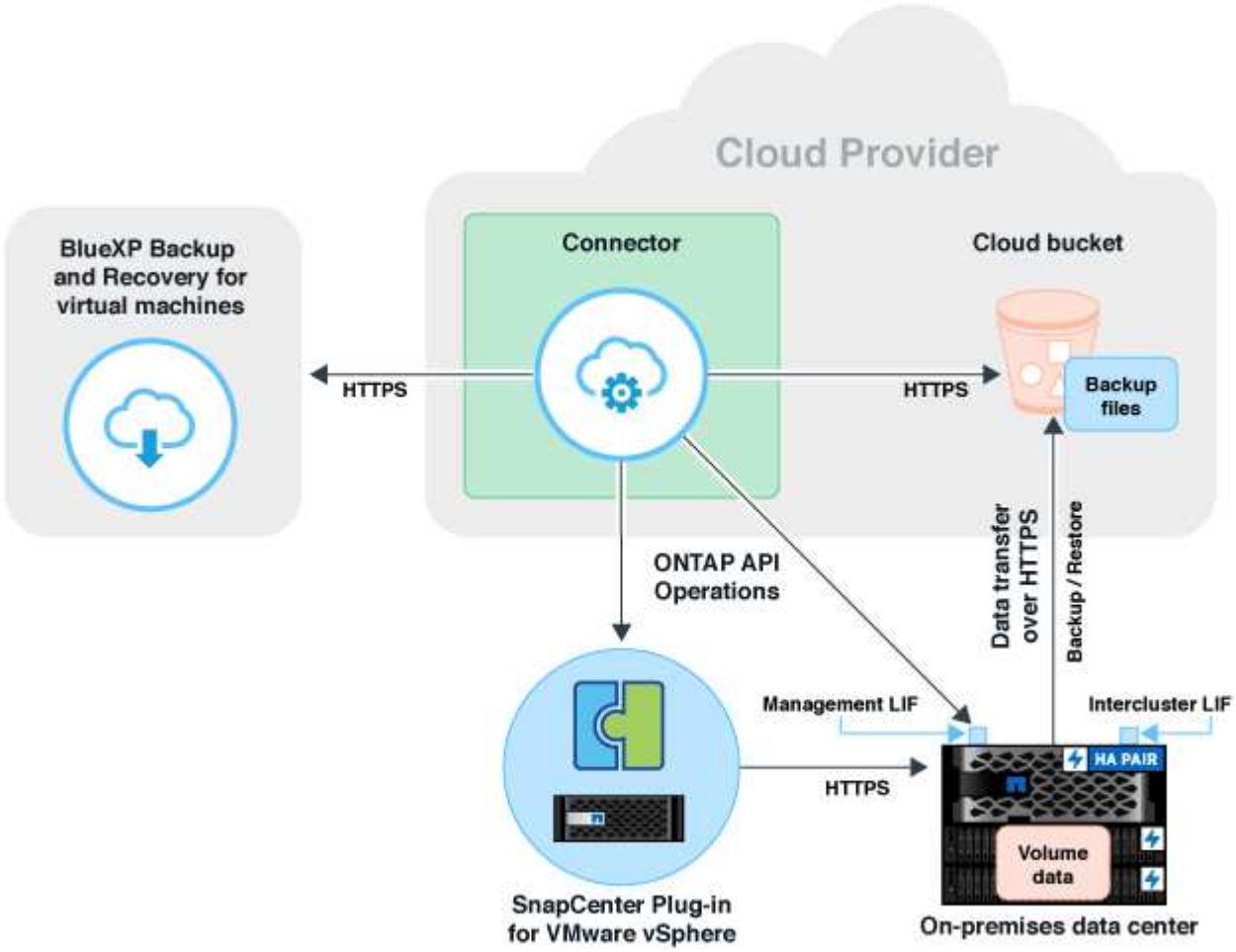
Antes de começar

Leia os requisitos a seguir para garantir que você tenha uma configuração compatível antes de iniciar o backup de datastores e máquinas virtuais para um provedor de nuvem.

- Plug-in do SnapCenter para VMware vSphere 4.6P1 ou posterior
  - Você deve usar o plug-in do SnapCenter para VMware vSphere 4.7P1 ou posterior para fazer backup de armazenamentos de dados a partir do storage secundário no local.
- ONTAP 9 .8 ou posterior
- BlueXP
- Armazenamentos de dados NFS e VMFS são compatíveis. VVols não são compatíveis.
- Para suporte ao VMFS, o plug-in do SnapCenter para host VMware vSphere deve ser executado no 4,9 ou posterior. Certifique-se de fazer um backup do armazenamento de dados VMFS se o plug-in do SnapCenter para o host VMware vSphere tiver sido atualizado de uma versão anterior para a versão 4,9.
- Pelo menos um backup deve ter sido feito no plug-in do SnapCenter para o VMware vSphere 4.6P1.
- Pelo menos uma política diária, semanal ou mensal no plug-in do SnapCenter para VMware vSphere sem rótulo ou mesmo rótulo da política de máquinas virtuais no BlueXP .
- Para a política pré-definida, o nível de agendamento deve ser o mesmo para o armazenamento de dados no plug-in do SnapCenter para VMware vSphere e na nuvem.
- Certifique-se de que não haja volumes FlexGroup no datastore porque não há suporte para backup e restauração de volumes FlexGroup.
- Desative "**_recent**" nos grupos de recursos necessários. Se você tiver "**_recent**" habilitado para o grupo de recursos, os backups desses grupos de recursos não poderão ser usados para proteção de dados para a nuvem e, posteriormente, não poderão ser usados para a operação de restauração.
- Certifique-se de que o armazenamento de dados de destino onde a máquina virtual será restaurada tenha espaço suficiente para acomodar uma cópia de todos os arquivos de máquina virtual, como VMDK, VMX, VMSD e assim por diante.
- Certifique-se de que o datastore de destino não tenha arquivos de máquina virtual obsoletos no formato de restore_xxx_xxxxxx_filename das falhas de operação de restauração anteriores. Você deve excluir os arquivos obsoletos antes de acionar uma operação de restauração.
- Para implantar um conetor com proxy configurado, certifique-se de que todas as chamadas do conetor de saída sejam roteadas pelo servidor proxy.
- Se um volume que faz backup de um datastore já estiver protegido da guia volumes (Backup e

recuperação do BlueXP → volumes), o mesmo datastore não poderá ser protegido novamente da guia máquinas virtuais (Backup e recuperação do BlueXP → máquinas virtuais).

A imagem a seguir mostra cada componente e as conexões que você precisa preparar entre eles:



Registre o plug-in do SnapCenter para o host VMware vSphere

Você deve Registrar o plug-in do SnapCenter para o host VMware vSphere no BlueXP para que os datastores e as máquinas virtuais sejam exibidos. Somente um usuário com acesso administrativo pode Registrar o plug-in do SnapCenter para o host VMware vSphere.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais**.
2. Na lista suspensa **Configurações**, clique em **Plug-in SnapCenter para VMware vSphere**.
3. Clique em **Register SnapCenter Plug-in para VMware vSphere**.
4. Especifique os seguintes detalhes:

a. No campo Plug-in do SnapCenter para VMware vSphere, especifique o FQDN ou o endereço IP do plug-in do SnapCenter para o host VMware vSphere.

b. No campo porta , especifique o número da porta na qual o plug-in do SnapCenter para o host VMware vSphere está sendo executado.

   Você deve garantir que a comunicação esteja aberta entre o plug-in do SnapCenter no local para o host VMware vSphere que está sendo executado na porta 8144 padrão e na instância do BlueXP Connector que pode ser executado em qualquer provedor de nuvem (Amazon Web Services, Microsoft Azure, Google Cloud Platform) ou no local.

c. No campo Nome de usuário e senha , especifique as credenciais do usuário do vCenter com a função de administrador.

5. Clique em **Register**.

Depois de terminar

Clique em **Backup e recuperação** > **máquinas virtuais** para visualizar todos os datastores e máquinas virtuais protegidos usando o plug-in SnapCenter registrado para o host VMware vSphere.

Crie uma política para fazer backup de armazenamentos de dados

Você pode criar uma política ou usar uma das seguintes políticas predefinidas que estão disponíveis no BlueXP .

Antes de começar

- Você deve criar políticas se não quiser editar as políticas predefinidas.
- Para mover backups do armazenamento de objetos para o armazenamento de arquivamento, você deve executar o ONTAP 9.10,1 ou posterior e o Amazon Web Services ou o Microsoft Azure deve ser o provedor de nuvem.
- Você deve configurar o nível de acesso de arquivamento para cada provedor de nuvem.

Sobre esta tarefa

As seguintes políticas predefinidas estão disponíveis no BlueXP :

Nome da política	Etiqueta	Valor de retenção
LTR diário de 1 anos (retenção de longo prazo)	Diariamente	366
5 anos diários LTR	Diariamente	1830
LTR semanal de 7 anos	Semanalmente	370
LTR mensal de 10 anos	Mensalmente	120

Passos

1. Na página máquinas virtuais, na lista suspensa Configurações, selecione **políticas**.

2. Clique em **criar política**.
3. Na seção Detalhes da política, especifique o nome da política.
4. Na seção retenção, selecione um dos tipos de retenção e especifique o número de backups a serem mantidos.
5. Selecione primário ou secundário como origem de armazenamento de backup.
6. (Opcional) se você quiser mover backups do armazenamento de objetos para o armazenamento de arquivos após um determinado número de dias para otimização de custos, marque a caixa de seleção **Tier backups to Archival** e insira o número de dias após os quais o backup deve ser arquivado.
7. Clique em **criar**.

Você não pode editar ou excluir uma política, que está associada a um datastore.

Faça backup de armazenamentos de dados no Amazon Web Services

Você pode fazer backup e arquivar um ou mais datastores no Amazon Web Services para melhorar a eficiência de storage e a transição para a nuvem.

Se o datastore estiver associado a uma política de arquivamento, você terá a opção de selecionar o nível de arquivamento. Os níveis de arquivamento compatíveis são Glacier e Glacier Deep.

Antes de começar

Certifique-se de que você atendeu a todos os "requisitos"antes de fazer backup de armazenamentos de dados na nuvem.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais**.
2. Clique em correspondente ao datastore que você deseja fazer backup e clique em **Ativar Backup**.
3. Na página atribuir política, selecione a política e clique em **seguinte**.
4. Adicione o ambiente de trabalho.

   Configure o LIF de gerenciamento de cluster que você deseja que o BlueXP descubra. Depois de adicionar o ambiente de trabalho para um dos datastores, ele pode ser reutilizado para todos os outros datastores que residem no mesmo cluster do ONTAP.

   a. Clique em **Adicionar ambiente de trabalho** correspondente ao SVM.
   b. No assistente Adicionar ambiente de trabalho:
      i. Especifique o endereço IP do LIF de gerenciamento de cluster.
      ii. Especifique as credenciais do usuário do cluster do ONTAP.
   c. Clique em **Adicionar ambiente de trabalho**.
5. Selecione **Amazon Web Services** para configurá-lo como o provedor de nuvem.
   a. Especifique a conta da AWS.
   b. No campo chave de acesso da AWS, especifique a chave para criptografia de dados.
   c. No campo chave secreta da AWS, especifique a senha para criptografia de dados.

d. Selecione a região onde deseja criar os backups.

e. Especifique os endereços IP do LIF de gerenciamento de cluster que foram adicionados como os ambientes de trabalho.

f. Selecione o nível de arquivamento.

Recomenda-se definir o nível de arquivo porque esta é uma atividade única e não é possível configurá-lo mais tarde.

6. Revise os detalhes e clique em **Ativar Backup**.

Faça backup de armazenamentos de dados no Microsoft Azure

Você pode fazer backup de um ou mais datastores no Microsoft Azure integrando o plug-in do SnapCenter para host VMware vSphere com o BlueXP . Isso ajudará os administradores de VMs a fazer backup e arquivamento de dados com facilidade e rapidez para eficiência de storage e acelerar a transição para a nuvem.

Se o datastore estiver associado a uma política de arquivamento, você receberá uma opção para selecionar o nível de arquivamento. A camada de arquivamento compatível é o Azure Archive Blob Storage.

Antes de começar

Certifique-se de que você atendeu a todos os "requisitos"antes de fazer backup de armazenamentos de dados na nuvem.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais**.
2. Clique ••• em correspondente ao datastore que você deseja fazer backup e clique em **Ativar Backup**.
3. Na página atribuir política, selecione a política e clique em **seguinte**.
4. Adicione o ambiente de trabalho.

Configure o LIF de gerenciamento de cluster que você deseja que o BlueXP descubra. Depois de adicionar o ambiente de trabalho para um dos datastores, ele pode ser reutilizado para todos os outros datastores que residem no mesmo cluster do ONTAP.

a. Clique em **Adicionar ambiente de trabalho** correspondente ao SVM.

b. No assistente Adicionar ambiente de trabalho:

i. Especifique o endereço IP do LIF de gerenciamento de cluster.

ii. Especifique as credenciais do usuário do cluster do ONTAP.

c. Clique em **Adicionar ambiente de trabalho**.

5. Selecione **Microsoft Azure** para configurá-lo como o provedor de nuvem.

a. Especifique o ID de assinatura do Azure.

b. Selecione a região onde deseja criar os backups.

c. Crie um novo grupo de recursos ou use um grupo de recursos existente.

d. Especifique os endereços IP do LIF de gerenciamento de cluster que foram adicionados como os ambientes de trabalho.

e. Selecione o nível de arquivamento.

   Recomenda-se definir o nível de arquivo porque esta é uma atividade única e você não poderá configurá-lo mais tarde.

6. Revise os detalhes e clique em **Ativar Backup**.

Faça backup de armazenamentos de dados no Google Cloud Platform

Você pode fazer backup de um ou mais datastores no Google Cloud Platform integrando o plug-in do SnapCenter para host VMware vSphere ao BlueXP . Isso ajudará os administradores de VMs a fazer backup e arquivamento de dados com facilidade e rapidez para eficiência de storage e acelerar a transição para a nuvem.

Antes de começar

Certifique-se de que você atendeu a todos os "requisitos"antes de fazer backup de armazenamentos de dados na nuvem.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais**.
2. Clique ••• em correspondente ao datastore que você deseja fazer backup e clique em **Ativar Backup**.
3. Na página atribuir política, selecione a política e clique em **seguinte**.
4. Adicione o ambiente de trabalho.

   Configure o LIF de gerenciamento de cluster que você deseja que o BlueXP descubra. Depois de adicionar o ambiente de trabalho para um dos datastores, ele pode ser reutilizado para todos os outros datastores que residem no mesmo cluster do ONTAP.

   a. Clique em **Adicionar ambiente de trabalho** correspondente ao SVM.
   b. No assistente Adicionar ambiente de trabalho:
      i. Especifique o endereço IP do LIF de gerenciamento de cluster.
      ii. Especifique as credenciais do usuário do cluster do ONTAP.
   c. Clique em **Adicionar ambiente de trabalho**.
5. Selecione **Google Cloud Platform** para configurá-lo como o provedor de nuvem.
   a. Selecione o projeto do Google Cloud onde você deseja que o bucket do Google Cloud Storage seja criado para backups.
   b. No campo chave de acesso do Google Cloud, especifique a chave.
   c. No campo chave secreta do Google Cloud, especifique a senha.
   d. Selecione a região onde deseja criar os backups.
   e. Especifique o espaço IP.
6. Revise os detalhes e clique em **Ativar Backup**.

Faça backup de armazenamentos de dados no StorageGRID

É possível fazer backup de um ou mais datastores no StorageGRID integrando o plug-in do SnapCenter para host VMware vSphere ao BlueXP . Isso ajudará os administradores de VMs a fazer backup e arquivamento de dados com facilidade e rapidez para eficiência de storage e acelerar a transição para a nuvem.

Antes de começar

Certifique-se de que você atendeu a todos os "requisitos"antes de fazer backup de armazenamentos de dados na nuvem.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais**.
2. Clique ••• em correspondente ao datastore que você deseja fazer backup e clique em **Ativar Backup**.
3. Na página atribuir política, selecione a política e clique em **seguinte**.
4. Adicione o ambiente de trabalho.

   Configure o LIF de gerenciamento de cluster que você deseja que o BlueXP descubra. Depois de adicionar o ambiente de trabalho para um dos datastores, ele pode ser reutilizado para todos os outros datastores que residem no mesmo cluster do ONTAP.

   a. Clique em **Adicionar ambiente de trabalho** correspondente ao SVM.
   b. No assistente Adicionar ambiente de trabalho:
      i. Especifique o endereço IP do LIF de gerenciamento de cluster.
      ii. Especifique as credenciais do usuário do cluster do ONTAP.
   c. Clique em **Adicionar ambiente de trabalho**.
5. Selecione **StorageGRID**.
   a. Especifique o IP do servidor de armazenamento.
   b. Selecione a chave de acesso e a chave secreta.
6. Revise os detalhes e clique em **Ativar Backup**.

Gerenciar a proteção dos dados de datastores e máquinas virtuais

É possível exibir políticas, armazenamentos de dados e máquinas virtuais antes de fazer backup e restaurar dados. Dependendo da alteração no banco de dados, políticas ou grupos de recursos, você pode exibir as atualizações da IU do BlueXP .

Ver políticas

Pode ver todas as políticas pré-configuradas predefinidas. Para cada uma dessas políticas, quando você visualiza os detalhes, todas as políticas e máquinas virtuais associadas são listadas.

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais**.
2. Na lista suspensa **Configurações**, clique em **políticas**.

3. Clique em **Ver detalhes** correspondente à política cujos detalhes você deseja visualizar.

As políticas e máquinas virtuais associadas são listadas.

Visualize datastores e máquinas virtuais

Os armazenamentos de dados e máquinas virtuais protegidos usando o plug-in SnapCenter registrado para o host VMware vSphere são exibidos.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais** > **Configurações** > **Plug-in SnapCenter para VMware vSphere**.
2. Clique no plug-in do SnapCenter para o host VMware vSphere para o qual você deseja ver os datastores e as máquinas virtuais.

Desproteger armazenamentos de dados

Você pode desproteger um datastore que já estava protegido anteriormente. Você pode desproteger um datastore quando quiser excluir os backups na nuvem ou não quiser mais fazer backup na nuvem. O datastore pode ser protegido novamente depois que a desproteção for bem-sucedida.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais**.
2. Clique ••• em correspondente ao datastore que você deseja desproteger e clique em **Unprotect**.

Edite o plug-in do SnapCenter para a instância do VMware vSphere

Você pode editar os detalhes do plug-in do SnapCenter para o host VMware vSphere no BlueXP .

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais** > **Configurações** > **Plug-in SnapCenter para VMware vSphere**.
2. Clique ••• e selecione **Editar**.
3. Modifique os detalhes conforme necessário.
4. Clique em **Salvar**.

Atualizar recursos e backups

Se você quiser exibir os armazenamentos de dados e backups mais recentes que foram adicionados ao aplicativo, atualize os recursos e os backups. Isso iniciará a descoberta dos recursos e backups e os detalhes mais recentes serão exibidos.

1. Clique em **Backup e recuperação** > **máquinas virtuais**.
2. Na lista suspensa **Configurações**, clique em **Plug-in SnapCenter para VMware vSphere**.
3. Clique ••• em correspondente ao plug-in do SnapCenter para o host VMware vSphere e clique em **Atualizar recursos e backups**.

Atualizar política ou grupo de recursos

Se houver uma alteração na política ou no grupo de recursos, atualize a relação de proteção.

1. Clique em **Backup e recuperação** > **máquinas virtuais**.
2. Clique ••• em correspondente ao datastore e clique em **Refresh Protection**.

Anule o Registro do plug-in do SnapCenter para o host VMware vSphere

Todos os datastores e máquinas virtuais associados ao plug-in do SnapCenter para o host VMware vSphere estarão desprotegidos.

1. Clique em **Backup e recuperação** > **máquinas virtuais**.
2. Na lista suspensa **Configurações**, clique em **Plug-in SnapCenter para VMware vSphere**.
3. Clique ••• em correspondente ao plug-in do SnapCenter para o host VMware vSphere e clique em **Cancelar Registro**.

Monitorizar trabalhos

Os trabalhos são criados para todas as operações de backup e recuperação do BlueXP . Pode monitorizar todos os trabalhos e todas as subtarefas que são executadas como parte de cada tarefa.

1. Clique em **Backup e recuperação** > **Monitoramento de tarefas**.

   Quando inicia uma operação, é apresentada uma janela a indicar que o trabalho foi iniciado. Pode clicar na ligação para monitorizar o trabalho.

2. Clique na tarefa principal para visualizar as subtarefas e o estado de cada uma destas subtarefas.

Restaure os dados das máquinas virtuais a partir da nuvem

Você pode restaurar os dados das máquinas virtuais da nuvem de volta para o vCenter no local. Você pode restaurar a máquina virtual para o mesmo local exato de onde o backup foi feito ou para um local alternativo. Se o backup da máquina virtual foi feito usando política de arquivamento, você pode definir a prioridade de restauração de arquivamento.

Não é possível restaurar máquinas virtuais que se estendem por armazenamentos de dados.

Antes de começar

- Certifique-se de que você atendeu a todas as "requisitos"antes de restaurar as máquinas virtuais da nuvem.
- Se você estiver restaurando para um local alternativo:
  - Certifique-se de que os vCenters de origem e destino estão no modo vinculado.
  - Verifique se os detalhes do cluster de origem e destino são adicionados no BlueXP Canvas e em vCenters de modo vinculado no plug-in do SnapCenter para o host VMware vSphere.
  - Certifique-se de que o ambiente de trabalho (NÓS) é adicionado correspondente ao local alternativo no BlueXP Canvas.

Passos

1. Na IU do BlueXP , clique em **proteção** > **Backup e recuperação** > **máquinas virtuais** > **Plug-in do SnapCenter para VMware vSphere** e selecione o plug-in do SnapCenter para o host VMware vSphere.

Se a máquina virtual de origem for movida para outro local (vMotion) e se o usuário acionar uma restauração dessa máquina virtual do BlueXP , a máquina virtual será restaurada para o local de origem de onde o backup foi feito.

1. É possível restaurar a máquina virtual para o local original ou para um local alternativo do datastore ou de máquinas virtuais:

Se você quiser restaurar a máquina virtual…	Faça isso…
para o local original do datastore	1. Clique ••• em correspondente ao datastore que você deseja restaurar e clique em **Exibir detalhes**. 2. Clique em **Restore** correspondente ao backup que você deseja restaurar. 3. Selecione a máquina virtual que deseja restaurar a partir do backup e clique em **Next**. 4. Certifique-se de que **original** está selecionado e clique em **continuar**. 5. Se a máquina virtual estiver protegida usando uma política em que as configurações de arquivamento estejam configuradas, selecione **prioridade de restauração de arquivamento** e clique em **Avançar**. A prioridade de restauração de arquivamento suportada para Amazon Web Services é alta, padrão e baixa, e a prioridade de restauração de arquivamento suportada para Microsoft Azure é alta e padrão. 6. Revise os detalhes e clique em **Restaurar**.

Se você quiser restaurar a máquina virtual…	Faça isso…
para um local alternativo do datastore	1. Clique ••• em correspondente ao datastore que você deseja restaurar e clique em **Exibir detalhes**. 2. Clique em **Restore** correspondente ao backup que você deseja restaurar. 3. Selecione a máquina virtual que deseja restaurar a partir do backup e clique em **Next**. 4. Selecione **alternativa**. 5. Selecione o vCenter Server, o host ESXi, o datastore e a rede alternativos. 6. Forneça um nome para a VM após a restauração e clique em **continuar**. 7. Se a máquina virtual estiver protegida usando uma política em que as configurações de arquivamento estejam configuradas, selecione **prioridade de restauração de arquivamento** e clique em **Avançar**. A prioridade de restauração de arquivamento suportada para Amazon Web Services é alta, padrão e baixa, e a prioridade de restauração de arquivamento suportada para Microsoft Azure é alta e padrão. 8. Revise os detalhes e clique em **Restaurar**.
para o local original de máquinas virtuais	1. Clique ••• em correspondente à máquina virtual que você deseja restaurar e clique em **Restaurar**. 2. Selecione a cópia de segurança através da qual pretende restaurar a máquina virtual. 3. Certifique-se de que **original** está selecionado e clique em **continuar**. 4. Se a máquina virtual estiver protegida usando uma política em que as configurações de arquivamento estejam configuradas, selecione **prioridade de restauração de arquivamento** e clique em **Avançar**. A prioridade de restauração de arquivamento suportada para Amazon Web Services é alta, padrão e baixa, e a prioridade de restauração de arquivamento suportada para Microsoft Azure é alta e padrão. 5. Revise os detalhes e clique em **Restaurar**.

Se você quiser restaurar a máquina virtual…	Faça isso…
para um local alternativo de máquinas virtuais	1. Clique ••• em correspondente à máquina virtual que você deseja restaurar e clique em **Restaurar**. 2. Selecione a cópia de segurança através da qual pretende restaurar a máquina virtual. 3. Selecione **alternativa**. 4. Selecione o vCenter Server, o host ESXi, o datastore e a rede alternativos. 5. Forneça um nome para a VM após a restauração e clique em **continuar**. 6. Se a máquina virtual estiver protegida usando uma política em que as configurações de arquivamento estejam configuradas, selecione **prioridade de restauração de arquivamento** e clique em **Avançar**. A prioridade de restauração de arquivamento suportada para Amazon Web Services é alta, padrão e baixa, e a prioridade de restauração de arquivamento suportada para Microsoft Azure é alta e padrão. 7. Revise os detalhes e clique em **Restaurar**.

Se a operação de restauração não for concluída, não tente o processo de restauração novamente até que o Monitor de trabalho mostre que a operação de restauração falhou. Se você tentar o processo de restauração novamente antes que o Monitor de trabalho mostre que a operação de restauração falhou, a operação de restauração falhará novamente. Quando o status do Monitor de trabalho for exibido como "Falha", você poderá tentar o processo de restauração novamente.

APIs de backup e recuperação do BlueXP

Os recursos de backup e recuperação do BlueXP disponíveis na IU da Web também estão disponíveis por meio da API RESTful.

Existem dez categorias de endpoints definidos no backup e recuperação do BlueXP :

- backup - gerencia as operações de backup de recursos na nuvem e no local e recupera detalhes dos dados de backup
- catálogo - gerencia a pesquisa de catálogo indexado para arquivos com base em uma consulta (Pesquisa e restauração)
- Nuvem - recupera informações sobre vários recursos do provedor de nuvem do BlueXP
- Tarefa - gerencia as entradas de detalhes do trabalho na base de dados do BlueXP
- Licença - recupera a validade da licença dos ambientes de trabalho do BlueXP
- verificação de ransomware - inicia uma verificação de ransomware em um arquivo de backup específico
- restaurar - permite executar operações de restauração em nível de volume, arquivo e pasta
- sfr - recupera arquivos de um arquivo de backup para operações de restauração em nível de arquivo único (Browse & Restore)
- StorageGRID - recupera detalhes sobre um servidor StorageGRID e permite que você descubra um servidor StorageGRID
- ambiente de trabalho - gerencia as políticas de backup e configura o armazenamento de objetos de destino associado a um ambiente de trabalho

Como começar

Para começar a usar as APIs de backup e recuperação do BlueXP , você precisará obter um token de usuário, sua ID de conta do BlueXP e o ID do conetor do BlueXP .

Ao fazer chamadas de API, você adicionará o token de usuário no cabeçalho autorização e o ID do conetor BlueXP no cabeçalho x-Agent-id. Você deve usar o ID da conta do BlueXP nas APIs.

Passos

1. Obtenha um token de usuário no site da NetApp BlueXP .

   Certifique-se de gerar o token de atualização a partir do seguinte xref:./ https://services.cloud.NetApp.com/refresh-token/. O token de atualização é uma cadeia alfanumérica que você usará para gerar um token de usuário.

```
curl --location --request POST 'https://netapp-cloud-
account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
    "grant_type": "refresh_token",
    "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
    "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

O token de usuário do site da BlueXP tem uma data de expiração. A resposta da API inclui um campo "expires_in" que indica quando o token expira. Para atualizar o token, você precisará chamar essa API novamente.

2. Obtenha a sua ID de conta BlueXP .

```
GET 'https://api.bluexp.netapp.com/tenancy/account' -H 'authority:
api.bluexp.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR.....
```

Esta API retornará uma resposta como a seguinte. Você pode recuperar o ID da conta analisando a saída de **[0].[accountPublicId]**.

```
 [{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}.....
. Obtenha o x-Agent-id que contém a ID do conetor BlueXP .
```

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
  -H 'authority: api.services.cloud.netapp.com' \
  -H 'accept: application/json' \
  -H 'accept-language: en-GB,en;q=0.9' \
  -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5.....
```

Esta API retornará uma resposta como a seguinte. Você pode recuperar o id do agente analisando a saída de **occm.[0].[Agent].[agentId]**.

```
{"occms":[{"account":"account-
OOnAR4ZS","accountName":"cbs","occm":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
"agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z","status":"ready","occmName"
:"cbsgcpdevcntsg-
asia","primaryCallbackUri":"http://34.93.197.21","manualOverrideUris":[]
,"automaticCallbackUris":["http://34.93.197.21","http://34.93.197.21/occ
mui","https://34.93.197.21","https://34.93.197.21/occmui","http://10.138
.0.16","http://10.138.0.16/occmui","https://10.138.0.16","https://10.138
.0.16/occmui","http://localhost","http://localhost/occmui","http://local
host:1337","http://localhost:1337/occmui","https://localhost","https://l
ocalhost/occmui","https://localhost:1337","https://localhost:1337/occmui
"],"createDate":"1652120369286","agent":{"useDockerInfra":true,"network"
:"default","name":"cbsgcpdevcntsg-
asia","agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Zclients","provider":"gc
p","systemId":"a3aa3578-bfee-4d16-9e10-
```


Exemplo usando as APIs

O exemplo a seguir mostra uma chamada de API para ativar o backup e a recuperação do BlueXP em um ambiente de trabalho com uma nova política que tem rótulos diários, horários e semanais definidos, arquivamento após dias definidos para 180 dias, na região Leste dos EUA-2 na nuvem Azure. Observe que isso só permite o backup no ambiente de trabalho, mas não há backup de volumes.

Solicitação de API

Você verá que usamos o ID da conta do BlueXP `account-DpTFcxN3` , o ID do conetor do BlueXP `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients` e o token de usuário `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4V alobjUmju2x0xUH48g` neste comando.

```
curl --location --request POST
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
    "provider":"AZURE",
    "backup-policy": {
      "archive-after-days": 180,
      "rule": [
        {
          "label": "hourly",
          "retention": "2"
        },
        {
          "label": "daily",
          "retention": "30"
        },
        {
          "label": "weekly",
          "retention": "52"
        }
      ]
    },
    "ip-space": "Default",
    "region": "eastus2",
    "azure": {
      "resource-group": "rn-test-backup-rg",
      "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
    }
  }'
```

Resposta é um ID de tarefa que você pode monitorar.

```
{
 "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

Monitore a resposta.

```
curl --location --request GET
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

Resposta.

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "PENDING",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

Monitorize até que "status" seja "CONCLUÍDO".

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "COMPLETED",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

Referência da API

A documentação para cada API de backup e recuperação do BlueXP está disponível no "Automação da

BlueXP ".

Referência

Classes de armazenamento de arquivamento do AWS S3 e tempos de recuperação de restauração

O backup e a recuperação do BlueXP são compatíveis com duas classes de armazenamento de arquivamento S3 e a maioria das regiões.

Classes de armazenamento de arquivamento S3 compatíveis para backup e recuperação do BlueXP

Quando os arquivos de backup são criados inicialmente, eles são armazenados no armazenamento S3 *Standard*. Esse nível é otimizado para armazenar dados que são acessados com pouca frequência, mas que também permite acessá-los imediatamente. Depois de 30 dias, os backups passam para a classe de armazenamento S3 *Standard-unusual access* para economizar nos custos.

Se os clusters de origem estiverem executando o ONTAP 9.10,1 ou superior, você poderá optar por categorizar backups no armazenamento *S3 Glacier* ou *S3 Glacier Deep Archive* após um determinado número de dias (normalmente mais de 30 dias) para otimização de custos adicional. Você pode definir isso para "0" ou para 1-999 dias. Se você configurá-lo para "0" dias, você não pode alterá-lo mais tarde para 1-999 dias.

Os dados nesses níveis não podem ser acessados imediatamente quando necessário e exigirão um custo de recuperação mais alto, portanto, você precisa considerar a frequência com que você pode precisar restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre como restaurar dados do armazenamento de arquivos.

- Se você selecionar nenhum nível de arquivamento na primeira política de backup ao ativar o backup e a recuperação do BlueXP , o *S3 Glacier* será a única opção de arquivamento para políticas futuras.
- Se você selecionar *S3 Glacier* em sua primeira política de backup, poderá alterar para o nível *S3 Glacier Deep Archive* para futuras políticas de backup para esse cluster.
- Se você selecionar *S3 Glacier Deep Archive* em sua primeira política de backup, esse nível será o único nível de arquivamento disponível para políticas futuras de backup para esse cluster.

Observe que ao configurar o backup e a recuperação do BlueXP com esse tipo de regra de ciclo de vida, você não deve configurar nenhuma regra de ciclo de vida ao configurar o bucket na sua conta da AWS.

"Saiba mais sobre as classes de armazenamento S3".

Restaurar dados do armazenamento de arquivamento

Embora armazenar arquivos de backup mais antigos no armazenamento de arquivamento seja muito mais barato do que o armazenamento Standard ou Standard-IA, acessar dados de um arquivo de backup no armazenamento de arquivamento para operações de restauração levará um tempo maior e custará mais dinheiro.

Quanto custa restaurar dados do Amazon S3 Glacier e do Amazon S3 Glacier Deep Archive?

Há 3 prioridades de restauração que você pode escolher ao recuperar dados do Amazon S3 Glacier e 2 prioridades de restauração ao recuperar dados do Amazon S3 Glacier Deep Archive. S3 Glacier Deep Archive custa menos de S3 Glacier:

Nível de arquivamento	Restaurar prioridade e custo		
	Alta	**Standard**	**Baixo**
S3 Glacier	Recuperação mais rápida, custo mais alto	Recuperação mais lenta, menor custo	Recuperação mais lenta, menor custo
S3 Glacier Deep Archive		Recuperação mais rápida, custo mais elevado	Recuperação mais lenta, menor custo

Cada método tem uma taxa de recuperação por GB diferente e taxa por solicitação. Para obter a definição de preço detalhada do S3 Glacier por região da AWS, visite o "Página de definição de preço do Amazon S3".

Quanto tempo levará para restaurar meus objetos arquivados no Amazon S3 Glacier?

Existem 2 partes que compõem o tempo total de restauração:

- **Tempo de recuperação**: O tempo para recuperar o arquivo de backup do arquivo e colocá-lo em armazenamento padrão. Isso às vezes é chamado de tempo de "reidratação". O tempo de recuperação é diferente dependendo da prioridade de restauração escolhida.

Nível de arquivamento	Restaurar prioridade e tempo de recuperação		
	Alta	**Standard**	**Baixo**
S3 Glacier	3-5 minutos	3-5 horas	5-12 horas
S3 Glacier Deep Archive		12 horas	48 horas

- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento padrão. Esse tempo não é diferente da operação de restauração típica diretamente do armazenamento padrão, quando não está usando uma camada de arquivamento.

Para obter mais informações sobre as opções de recuperação do Amazon S3 Glacier e do S3 Glacier Deep Archive, "As perguntas frequentes sobre essas classes de armazenamento da Amazon" consulte .

Camadas de arquivamento do Azure e tempos de recuperação de restauração

Backup e recuperação do BlueXP são compatíveis com uma camada de acesso de arquivamento do Azure e a maioria das regiões.

Categorias de acesso de Blob do Azure compatíveis para backup e recuperação do BlueXP

Quando os arquivos de backup são criados inicialmente, eles são armazenados no nível de acesso *Cool*. Esse nível é otimizado para armazenar dados que não são acessados com frequência; mas, quando necessário, pode ser acessado imediatamente.

Se seus clusters de origem estiverem executando o ONTAP 9.10,1 ou superior, você poderá optar por categorizar backups do armazenamento *Cool* para o armazenamento *Azure Archive* após um determinado número de dias (normalmente mais de 30 dias) para otimização de custos adicional. Os dados neste nível não podem ser acessados imediatamente quando necessário e exigirão um custo de recuperação mais alto,

portanto, você precisa considerar com que frequência você pode precisar restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre como restaurar dados do armazenamento de arquivos.

Observe que ao configurar o backup e a recuperação do BlueXP com esse tipo de regra de ciclo de vida, você não deve configurar nenhuma regra de ciclo de vida ao configurar o contentor na sua conta do Azure.

"Saiba mais sobre os níveis de acesso ao Blob do Azure".

Restaurar dados do armazenamento de arquivamento

Embora armazenar arquivos de backup mais antigos no armazenamento de arquivamento seja muito mais barato do que o armazenamento Cool, acessar dados de um arquivo de backup no Azure Archive para operações de restauração levará um tempo maior e custará mais dinheiro.

Quanto custa restaurar dados do Azure Archive?

Há duas prioridades de restauração que você pode escolher ao recuperar dados do Azure Archive:

- **High**: Recuperação mais rápida, custo mais alto
- **Standard**: Recuperação mais lenta, menor custo

Cada método tem uma taxa de recuperação por GB diferente e taxa por solicitação. Para obter preços detalhados do Azure Archive pela região do Azure, visite o "Página de preços do Azure".

A alta prioridade não é suportada ao restaurar dados do Azure para sistemas StorageGRID.

Quanto tempo levará para restaurar meus dados arquivados no Azure Archive?

Existem 2 partes que compõem o tempo de restauração:

- **Retrieval Time**: A hora de recuperar o arquivo de backup arquivado do Azure Archive e colocá-lo em armazenamento Cool. Isso às vezes é chamado de tempo de "reidratação". O tempo de recuperação é diferente dependendo da prioridade de restauração que você escolher:
  - **Alta**: Menos de 1 hora
  - **Standard**: Menos de 15 horas
- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento Cool. Esse tempo não é diferente da operação de restauração típica diretamente do armazenamento Cool - quando não está usando um nível de arquivamento.

Para obter mais informações sobre as opções de recuperação do Azure Archive, "Este FAQ do Azure" consulte .

Classes de armazenamento de arquivamento do Google e restaurar tempos de recuperação

Backup e recuperação do BlueXP são compatíveis com uma classe de storage de arquivamento do Google e a maioria das regiões.

Classes de armazenamento de arquivamento do Google compatíveis para backup e recuperação do BlueXP

Quando os arquivos de backup são criados inicialmente, eles são armazenados no armazenamento *Standard*. Esse nível é otimizado para armazenar dados que são acessados com pouca frequência, mas que também permite acessá-los imediatamente.

Se o cluster no local estiver usando o ONTAP 9.12,1 ou superior, você poderá optar por categorizar backups mais antigos para o storage *Archive* na IU de backup e recuperação do BlueXP após um determinado número de dias (geralmente mais de 30 dias) para otimização adicional de custos. Os dados nesse nível exigirão um custo de recuperação mais alto, então você precisa considerar com que frequência você pode precisar restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre como restaurar dados do armazenamento de arquivos.

Observe que ao configurar o backup e a recuperação do BlueXP com esse tipo de regra de ciclo de vida, você não deve configurar nenhuma regra de ciclo de vida ao configurar o bucket em sua conta do Google.

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

Restaurar dados do armazenamento de arquivamento

Embora armazenar arquivos de backup mais antigos no armazenamento de arquivos seja muito mais barato do que o armazenamento padrão, acessar dados de um arquivo de backup no armazenamento de arquivos para operações de restauração levará um pouco mais de tempo e custará mais dinheiro.

Quanto custa restaurar dados do Google Archive?

Para obter preços detalhados do Google Cloud Storage por região, visite o "Página de preços do Google Cloud Storage".

Quanto tempo levará para restaurar meus objetos arquivados no Google Archive?

Existem 2 partes que compõem o tempo total de restauração:

- **Tempo de recuperação**: O tempo para recuperar o arquivo de backup do Archive e colocá-lo em armazenamento padrão. Isso às vezes é chamado de tempo de "reidratação". Ao contrário das soluções de storage "mais frias" fornecidas por outros fornecedores de nuvem, seus dados ficam acessíveis em milissegundos.
- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento padrão. Esse tempo não é diferente da operação de restauração típica diretamente do armazenamento padrão, quando não está usando uma camada de arquivamento.

Configure o backup para acesso a várias contas no Azure

O backup e a recuperação do BlueXP permitem que você crie arquivos de backup em uma conta do Azure diferente de onde residem seus volumes Cloud Volumes ONTAP de origem. Ambas as contas podem ser diferentes da conta onde reside o BlueXP Connector.

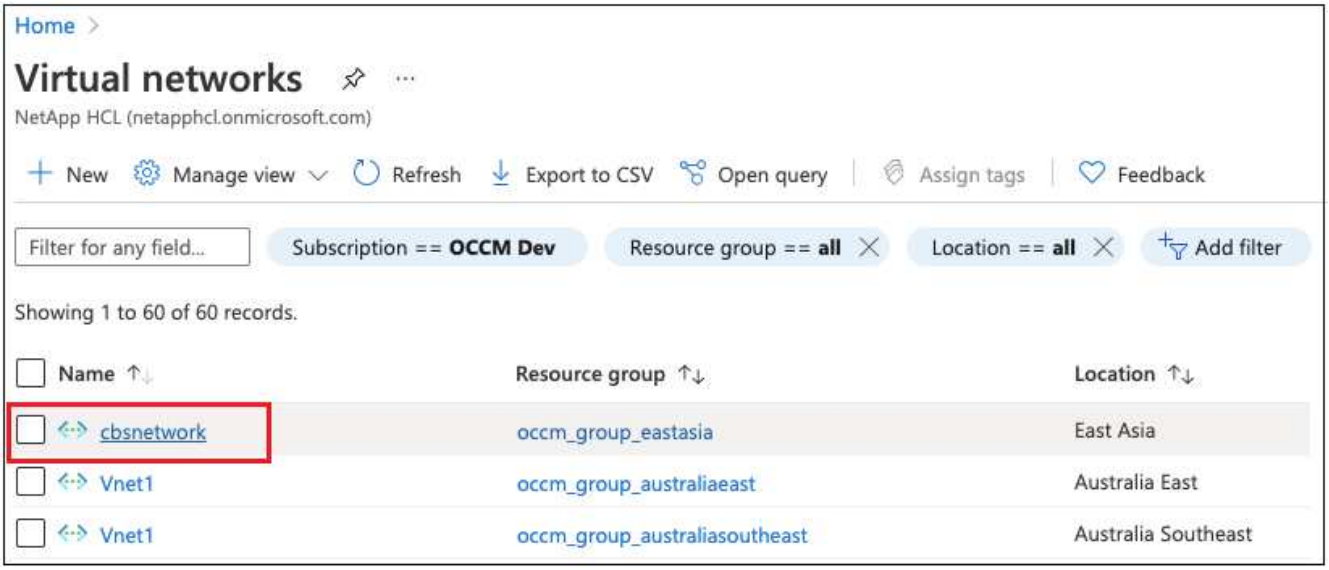
Estas etapas são necessárias somente quando você é "Fazer backup de dados do Cloud Volumes ONTAP para o armazenamento de Blobs do Azure".

Basta seguir os passos abaixo para configurar sua configuração desta maneira.

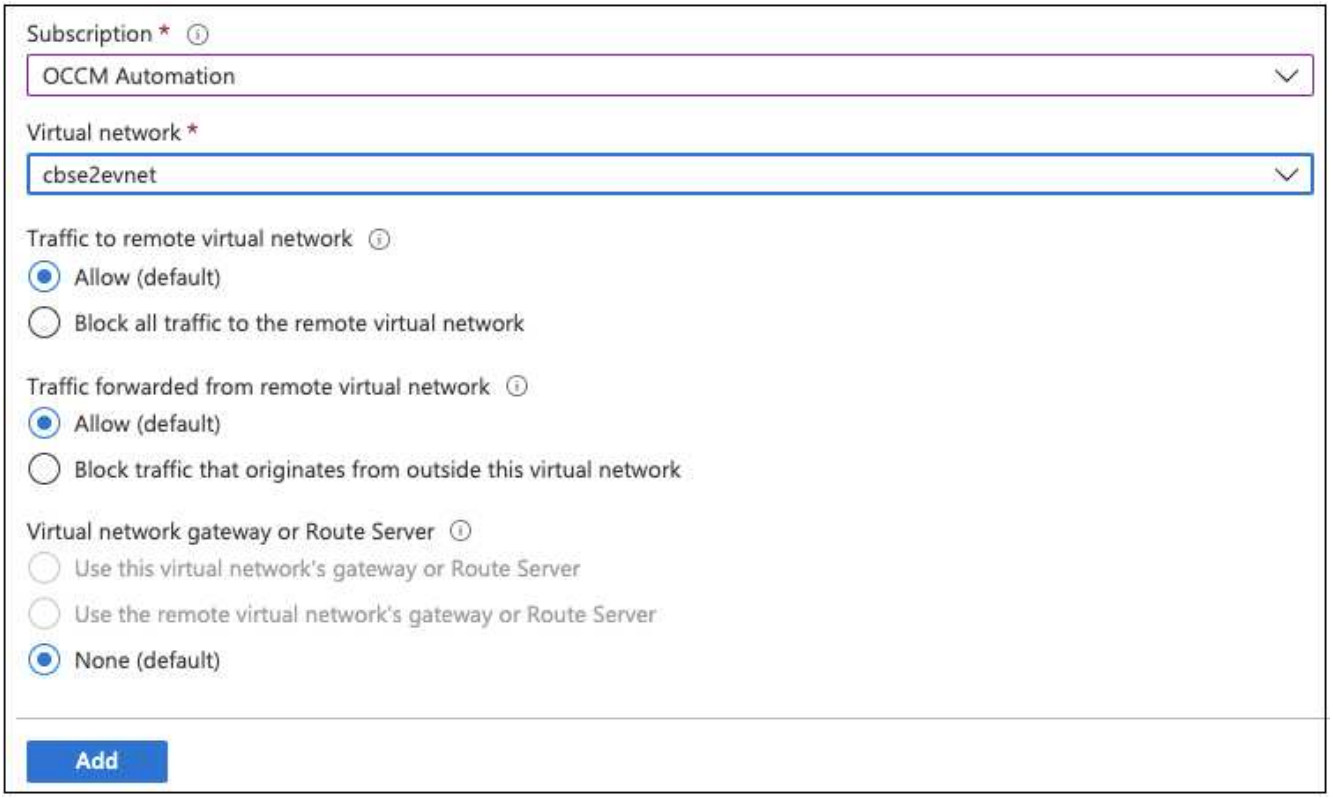
Configure o peering VNet entre contas

Observe que se você quiser que o BlueXP gerencie seu sistema Cloud Volumes ONTAP em uma conta/região diferente, então você precisa configurar o peering VNet. O peering VNet não é necessário para a conetividade da conta de armazenamento.

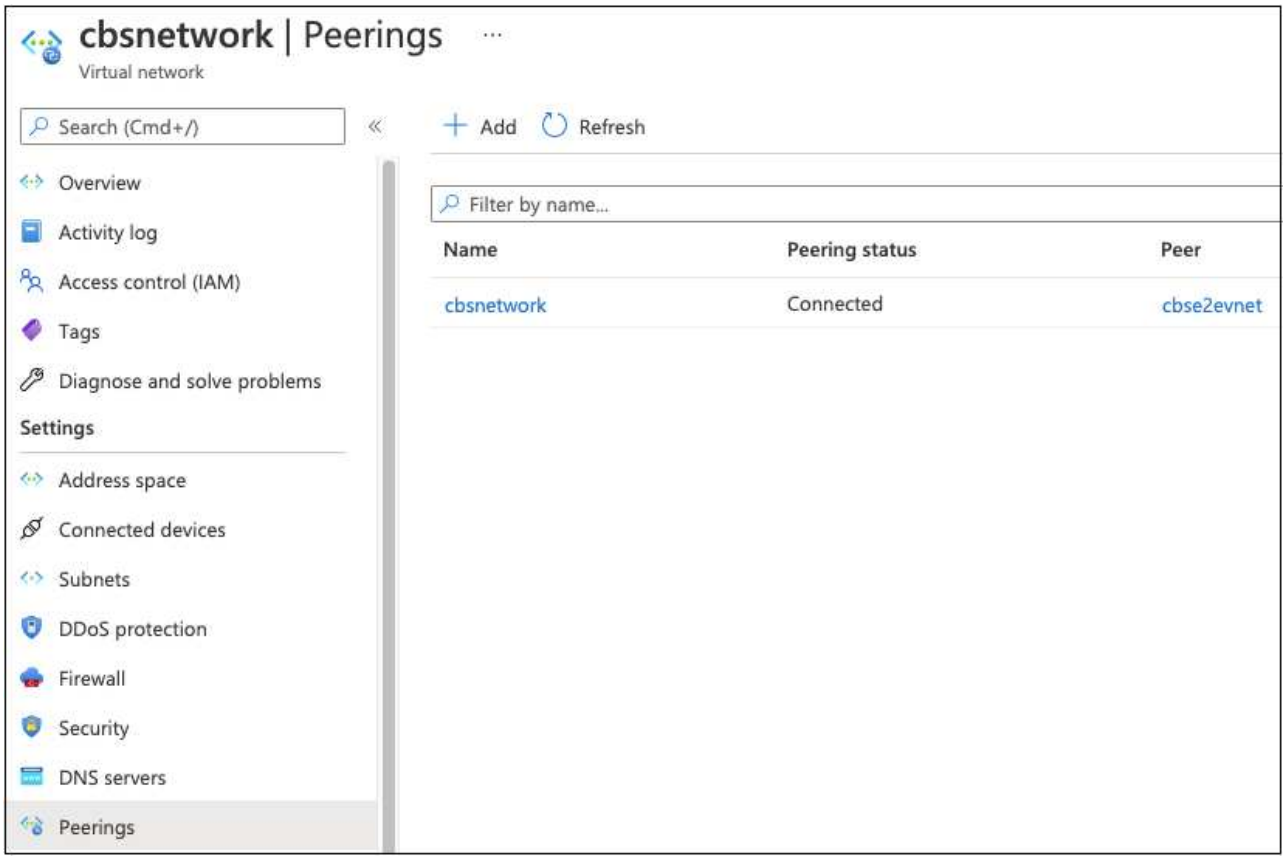
1. Inicie sessão no portal do Azure e, a partir de casa, selecione redes virtuais.
2. Selecione a subscrição que está a utilizar como subscrição 1 e clique no VNet onde pretende configurar o peering.



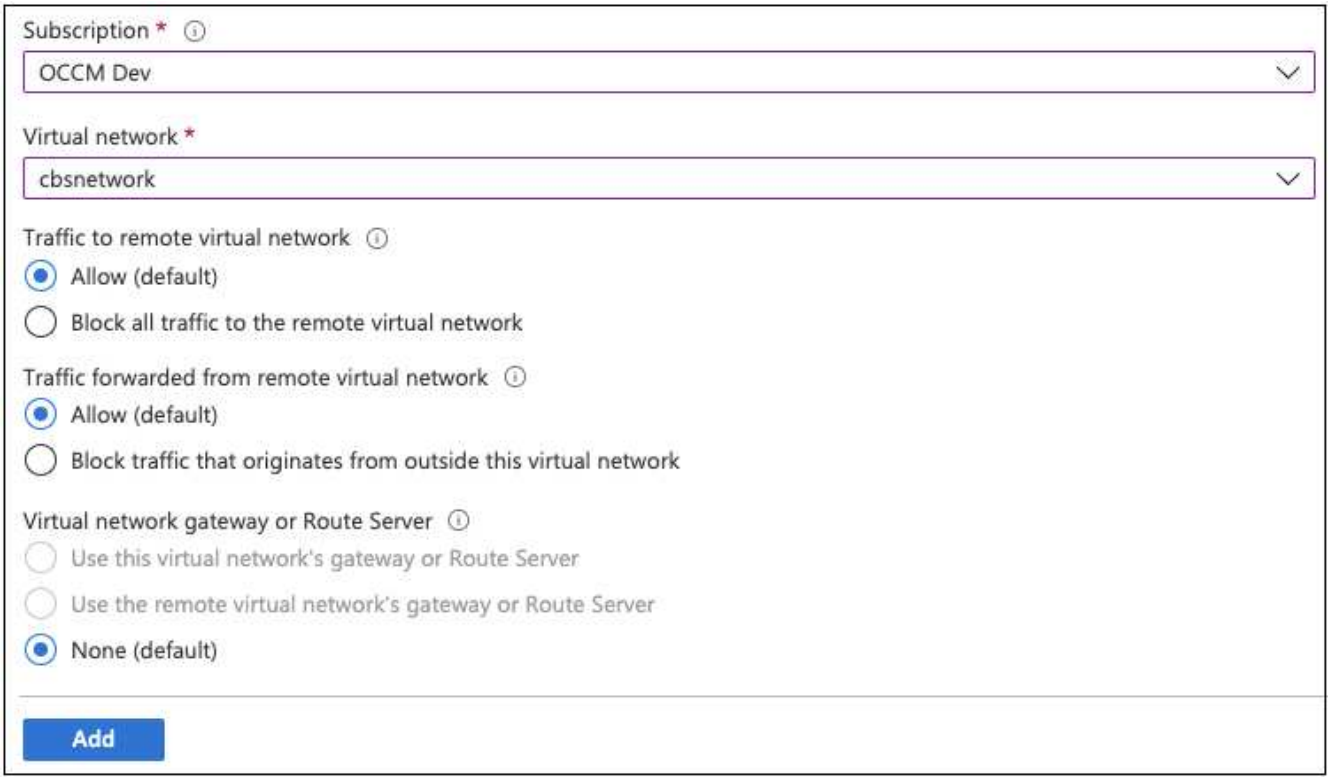
3. Selecione **cbsnetwork** e, no painel esquerdo, clique em **Peerings** e, em seguida, clique em **Add**.



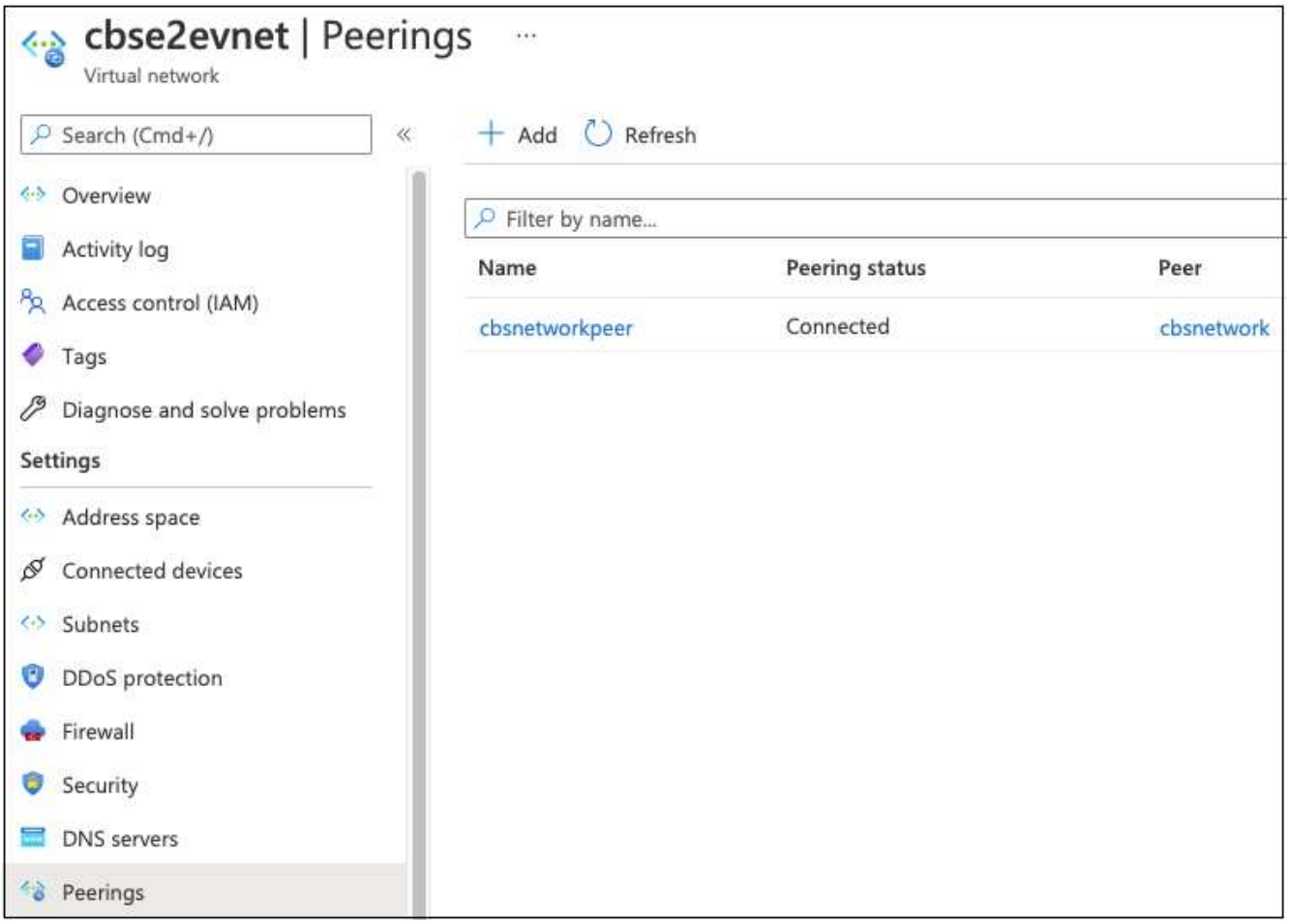
4. Insira as seguintes informações na página de peering e clique em **Add**.
   - Nome do link de peering para esta rede: Você pode dar qualquer nome para identificar a conexão de peering.
   - Nome do link de peering de rede virtual remota: Insira um nome para identificar o VNet remoto.
   - Mantenha todas as seleções como valores padrão.
   - Em subscrição, selecione a subscrição 2.
   - Rede virtual, selecione a rede virtual na subscrição 2 à qual pretende configurar o peering.



5. Execute as mesmas etapas na assinatura 2 VNet e especifique os detalhes da assinatura e do VNet remoto da assinatura 1.



As configurações de peering são adicionadas.



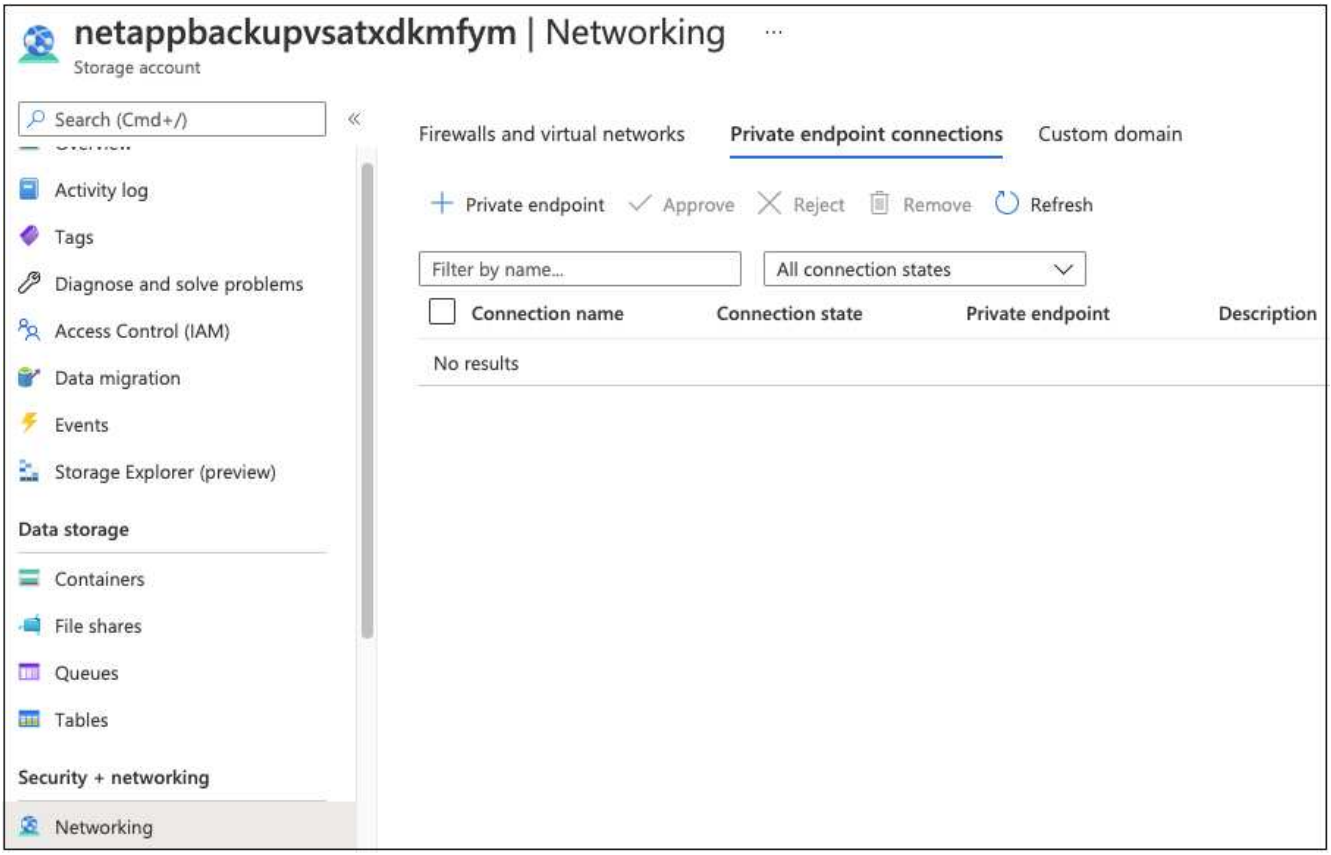
Crie um endpoint privado para a conta de armazenamento

Agora você precisa criar um endpoint privado para a conta de armazenamento. Neste exemplo, a conta de storage é criada na assinatura 1 e o sistema Cloud Volumes ONTAP está sendo executado na assinatura 2.

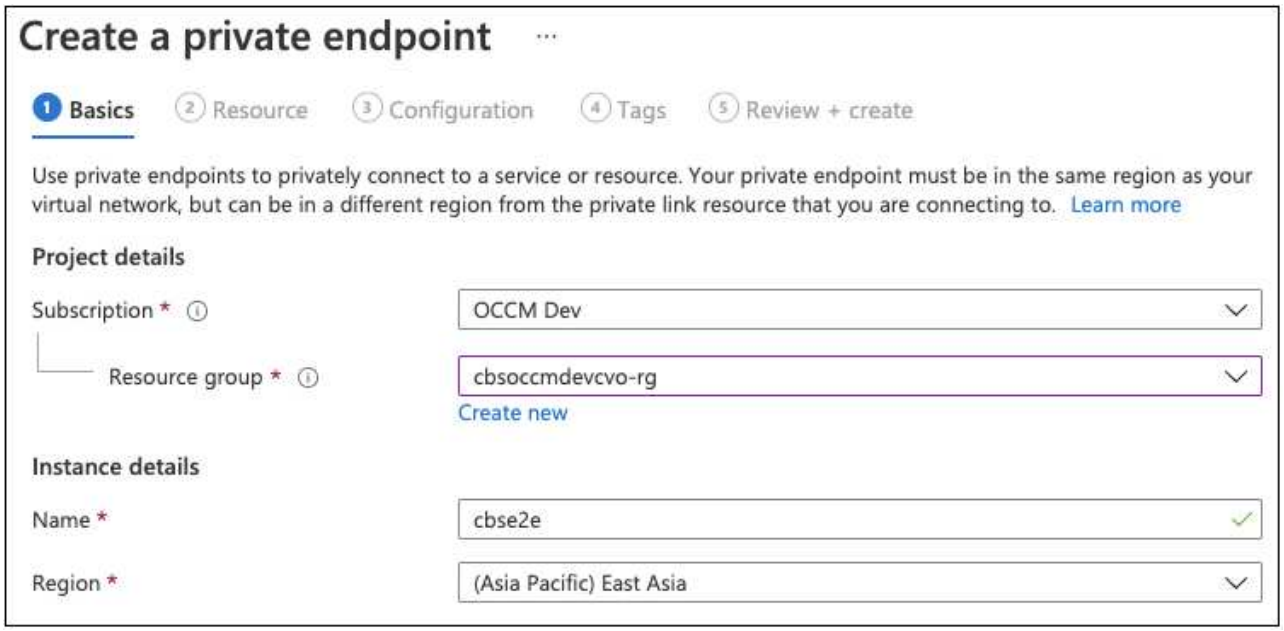
Você precisa de permissão de colaborador de rede para executar a seguinte ação.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

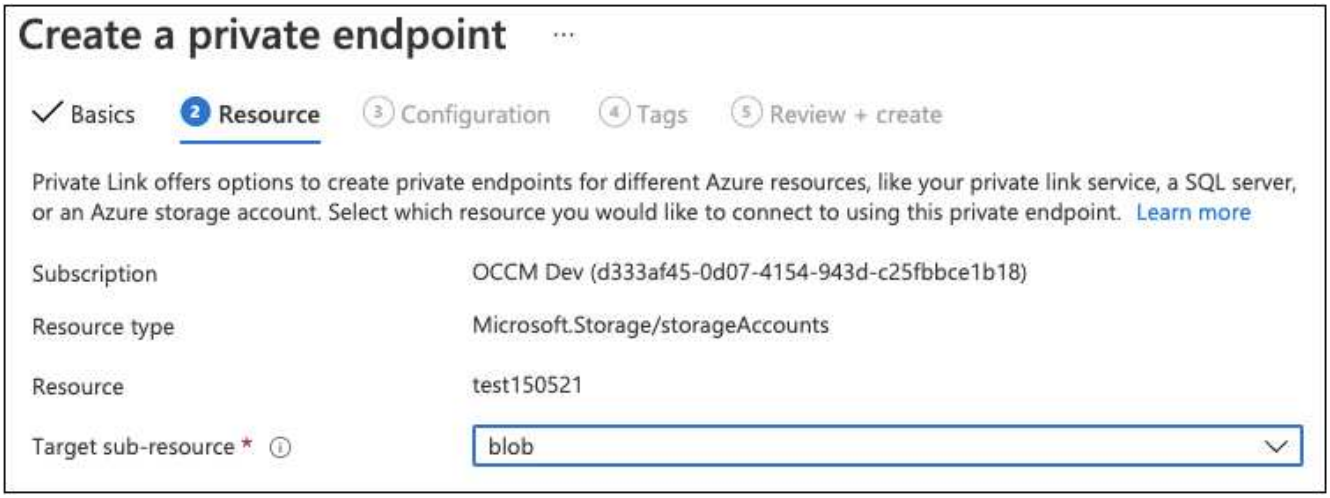
1. Vá para a conta de armazenamento > rede > conexões de endpoint privado e clique em * endpoint privado*.



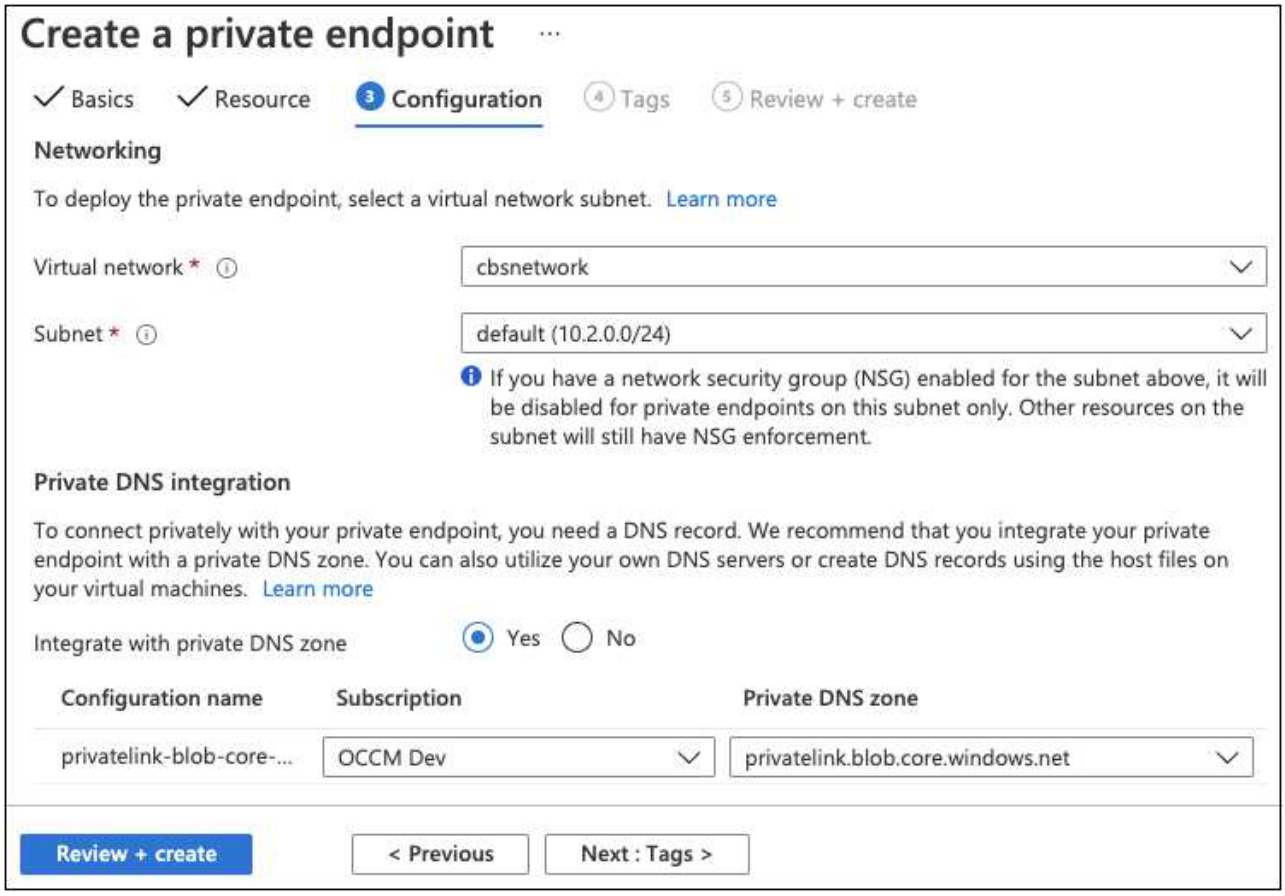
2. Na página Private Endpoint *Basics*:
   - Selecione a subscrição 2 (onde o BlueXP Connector e o sistema Cloud Volumes ONTAP são implantados) e o grupo de recursos.
   - Introduza um nome de endpoint.
   - Selecione a região.



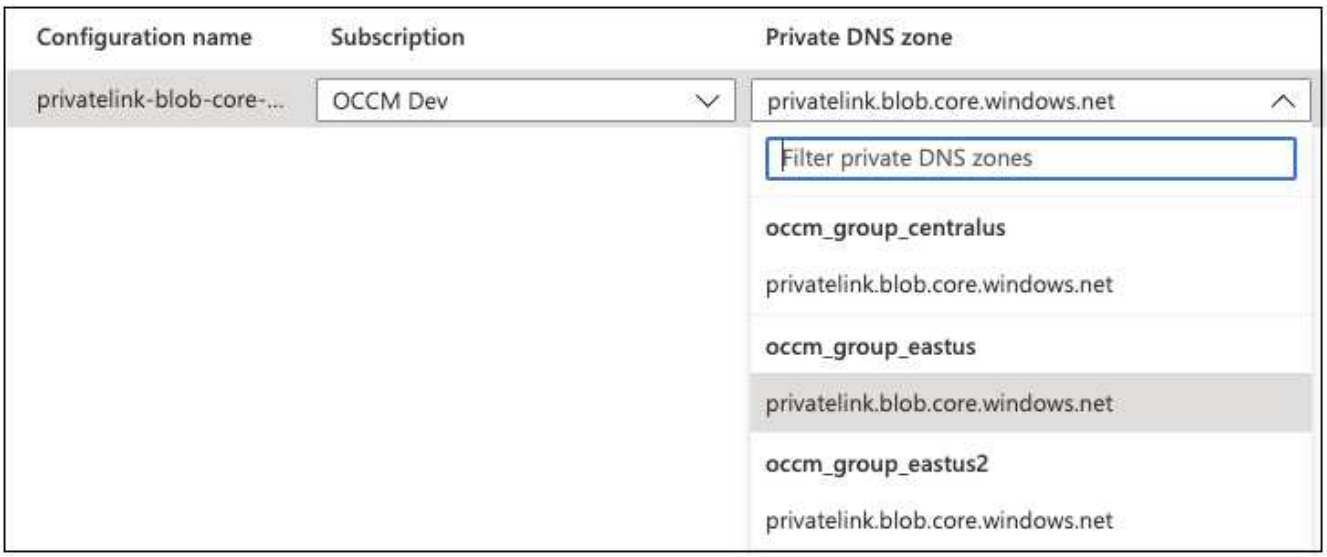
3. Na página *Resource*, selecione Target sub-resource como **blob**.



4. Na página Configuração:
   - Selecione a rede virtual e a sub-rede.
   - Clique no botão de opção **Yes** para "integrar com a zona DNS privada".



5. Na lista zona DNS privada, certifique-se de que a zona privada está selecionada na região correta e clique em **Rever e criar**.



Agora, a conta de armazenamento (na assinatura 1) tem acesso ao sistema Cloud Volumes ONTAP que está sendo executado na assinatura 2.

6. Tente novamente ativar o backup e a recuperação do BlueXP no sistema Cloud Volumes ONTAP e, desta vez, ele deve ser bem-sucedido.

Restaure os dados de recuperação e backup do BlueXP em um local escuro

Ao usar o backup e a recuperação do BlueXP em um site sem acesso à Internet, conhecido como *modo privado*, o backup e os dados de configuração de recuperação do BlueXP são copiados para o bucket do StorageGRID ou ONTAP S3, onde seus backups estão sendo armazenados. Se você tiver um problema com o sistema host do BlueXP Connector no futuro, poderá implantar um novo conetor e restaurar os dados críticos de backup e recuperação do BlueXP .

Observe que quando você usa o backup e a recuperação do BlueXP em um ambiente SaaS em que o BlueXP Connector é implantado em seu fornecedor de nuvem ou em seu próprio sistema de host que tem acesso à Internet, todos os dados importantes de configuração de backup e recuperação do BlueXP são protegidos na nuvem. Se você tiver um problema com o conetor, basta criar um novo conetor e adicionar seus ambientes de trabalho e os detalhes do backup serão restaurados automaticamente.

Existem 2 tipos de dados que são copiados:

- Banco de dados de backup e recuperação do BlueXP - contém uma lista de todos os volumes, arquivos de backup, políticas de backup e informações de configuração.
- Arquivos de catálogo indexados - contém índices detalhados que são usados para a funcionalidade de pesquisa e restauração que tornam suas pesquisas muito rápidas e eficientes ao procurar dados de volume que você deseja restaurar.

O backup desses dados é feito uma vez por dia, à meia-noite, e um máximo de 7 cópias de cada arquivo é retido. Se o conetor estiver gerenciando vários ambientes de trabalho do ONTAP locais, os arquivos de backup e recuperação do BlueXP estarão localizados no bucket do ambiente de trabalho que foi ativado primeiro.

Nenhum volume de dados é incluído no banco de dados de backup e recuperação do BlueXP ou nos arquivos de catálogo indexado.

Restaure os dados de backup e recuperação do BlueXP para um novo conetor

Se o seu conector no local apresentar uma falha catastrófica, você precisará instalar um novo conector e restaurar os dados de backup e recuperação do BlueXP para o novo conector.

Há 4 tarefas que você precisará executar para retornar seu sistema de backup e recuperação do BlueXP a um estado de funcionamento:

- Instale um novo conetor BlueXP
- Restaure o banco de dados de backup e recuperação do BlueXP
- Restaure os arquivos de Catálogo indexado
- Redescubra todos os seus sistemas ONTAP locais e sistemas StorageGRID para a IU do BlueXP

Depois de verificar se o sistema está de volta em uma ordem de funcionamento, recomendamos que você crie novos arquivos de backup.

O que você vai precisar

Você precisará acessar o banco de dados mais recente e indexar backups a partir do bucket do StorageGRID ou do ONTAP S3 onde seus arquivos de backup estão sendo armazenados:

- Backup e recuperação do BlueXP arquivo de banco de dados MySQL

  Esse arquivo está localizado no seguinte local no bucket `netapp-backup-<GUID>/mysql_backup/`, e é `CBS_DB_Backup_<day>_<month>_<year>.sql` nomeado .

- Arquivo zip de backup de catálogo indexado

  Esse arquivo está localizado no seguinte local no bucket `netapp-backup-<GUID>/catalog_backup/`, e é `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` nomeado .

Instale um novo conetor em um novo host Linux no local

Ao instalar um novo conetor BlueXP , certifique-se de que transfere a mesma versão do software que tinha instalado no conetor original. Alterações periódicas na estrutura do banco de dados de backup e recuperação do BlueXP podem tornar as versões de software mais recentes incompatíveis com os backups originais do banco de dados. Você pode "Atualize o software Connector para a versão mais atual depois de restaurar a base de dados de cópia de segurança".

1. "Instale o BlueXP Connector em um novo host Linux no local"
2. Faça login no BlueXP usando as credenciais de usuário admin que você acabou de criar.

Restaure o banco de dados de backup e recuperação do BlueXP

1. Copie o backup do MySQL do local de backup para o novo host do conetor. Vamos usar o nome de arquivo de exemplo "CBS_DB_Backup_23_05_2023.sql" abaixo.
2. Copie o backup para o contentor MySQL docker usando um dos seguintes comandos, dependendo se você está usando um contentor Docker ou Podman:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Digite o shell do contentor MySQL usando um dos seguintes comandos, dependendo se você está usando um contentor Docker ou Podman:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. No shell do contentor, implante o "env".
5. Você precisará da senha do MySQL DB, então copie o valor da chave "MYSQL_root_PASSWORD".
6. Restaure o banco de dados MySQL de backup e recuperação do BlueXP usando o seguinte comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verifique se o banco de dados MySQL de backup e recuperação do BlueXP foi restaurado corretamente usando os seguintes comandos SQL:

```
mysql -u root -p cloud_backup
```

Introduza a palavra-passe.

```
mysql> show tables;
mysql> select * from volume;
```

Verifique se os volumes mostrados são os mesmos que os existentes no ambiente original.

Restaure os arquivos de Catálogo indexado

1. Copie o arquivo zip de backup do Catálogo indexado (usaremos o nome de arquivo de exemplo "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") do local de backup para o novo host do conetor na pasta "/opt/Application/NetApp/CBS".
2. Descompacte o arquivo "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" usando o seguinte comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Execute o comando **ls** para se certificar de que a pasta "catalogdb1" foi criada com as subpastas "alterações" e "instantâneos" abaixo.

Descubra os clusters do ONTAP e os sistemas StorageGRID

1. "Descubra todos os ambientes de trabalho do ONTAP no local" que estavam disponíveis em seu ambiente anterior. Isso inclui o sistema ONTAP que você usou como um servidor S3.
2. "Descubra os seus sistemas StorageGRID".

Configure os detalhes do ambiente do StorageGRID

Adicione os detalhes do sistema StorageGRID associados aos ambientes de trabalho do ONTAP conforme eles foram configurados na configuração do conetor original usando o "APIs da BlueXP ".

Você precisará executar estas etapas para cada sistema ONTAP que estiver fazendo backup de dados no StorageGRID.

1. Extraia o token de autorização usando a seguinte API oauth/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'User-Agent:
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100101 Firefox/108.0'
-H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H
'Accept-Encoding: gzip, deflate' -H 'Content-Type: application/json' -d
'{"username":admin@netapp.com,"password":"Netapp@123","grant_type":"pass
word"}
> '
```

   Esta API retornará uma resposta como a seguinte. Você pode recuperar o token de autorização como mostrado abaixo.


```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```


2. Extraia o ID do ambiente de trabalho e o ID do X-Agent usando a API de alocação/externo/recurso.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Esta API retornará uma resposta como a seguinte. O valor sob o "resourceIdentifier" denota o *WorkingEnvironment ID* e o valor sob "agentId" denota *x-Agent-id*.

3. Atualize o banco de dados de backup e recuperação do BlueXP com os detalhes do sistema StorageGRID associado aos ambientes de trabalho. Certifique-se de inserir o nome de domínio totalmente qualificado do StorageGRID, bem como a chave de acesso e a chave de armazenamento, conforme mostrado abaixo:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Verifique as configurações de backup e recuperação do BlueXP

1. Selecione cada ambiente de trabalho do ONTAP e clique em **Exibir backups** ao lado do serviço de backup e recuperação no painel direito.

   Você deve ser capaz de ver todos os backups que foram criados para seus volumes.

2. No Painel de Restauro, na secção pesquisar e Restaurar, clique em **Definições de Indexação**.

   Certifique-se de que os ambientes de trabalho que tinham a catalogação indexada ativada anteriormente permanecem ativados.

3. Na página pesquisar e Restaurar, execute algumas pesquisas de catálogo para confirmar que a restauração do Catálogo indexado foi concluída com êxito.

Reinicie o serviço de backup e recuperação do BlueXP

Pode haver situações em que você precisará reiniciar o serviço de backup e recuperação do BlueXP .

A funcionalidade de backup e recuperação do BlueXP está integrada ao BlueXP Connector. Você precisará seguir diferentes etapas iniciais para reiniciar o serviço, dependendo se você implantou o conetor na nuvem ou se instalou o conetor manualmente em um sistema Linux.

Passos

1. Conete-se ao sistema Linux no qual o conetor está sendo executado.

Localização do conetor	Procedimento
Implantação de nuvem	Siga as instruções para "Conexão à máquina virtual Connector Linux" dependendo do provedor de nuvem que você está usando.
Instalação manual	Faça login no sistema Linux.

2. Digite o comando para reiniciar o serviço.

Localização do conetor	Comando Docker	Podman comando
Implantação de nuvem	`docker restart cloudmanager_cbs`	`podman restart cloudmanager cbs`
Instalação manual com acesso à Internet	`docker restart cloudmanager_cbs`	`podman restart cloudmanager cbs`
Instalação manual sem acesso à Internet	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`

Conhecimento e apoio

Registre-se para obter suporte

O Registro de suporte é necessário para receber suporte técnico específico da BlueXP e de suas soluções e serviços de storage. O Registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP.

O Registro para suporte não ativa o suporte do NetApp para um serviço de arquivos de provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP para esse produto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

Visão geral do Registro de suporte

Existem duas formas de Registro para ativar o direito de suporte:

- Registar o número de série da sua conta BlueXP (o número de série 960xxxxxxxx de 20 dígitos localizado na página recursos de suporte no BlueXP).

  Isso serve como seu ID de assinatura de suporte único para qualquer serviço no BlueXP . Cada assinatura de suporte no nível de conta do BlueXP deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no mercado do seu provedor de nuvem (estes são números de série de 20 dígitos 909201xxxxxxxx).

  Esses números de série são comumente referidos como *PAYGO serial numbers* e são gerados pelo BlueXP no momento da implantação do Cloud Volumes ONTAP.

Registrar ambos os tipos de números de série permite recursos como abrir tickets de suporte e geração automática de casos. O Registro é concluído adicionando contas do site de suporte da NetApp (NSS) ao BlueXP , conforme descrito abaixo.

Registre o BlueXP para obter suporte ao NetApp

Para se Registrar para obter suporte e ativar o direito de suporte, um usuário em sua organização (ou conta) do BlueXP deve associar uma conta do site de suporte da NetApp ao login do BlueXP . A forma como você se Registra no suporte da NetApp depende se você já tem uma conta do site de suporte da NetApp (NSS).

Cliente existente com uma conta NSS

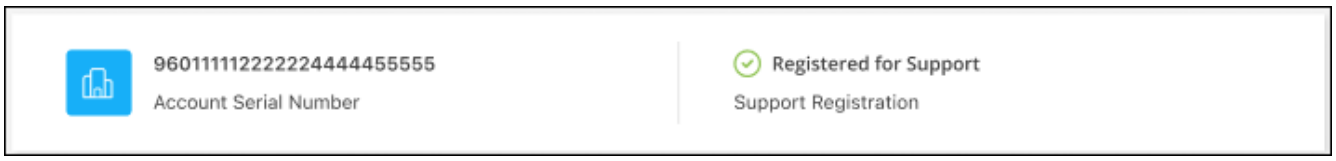
Se você é um cliente da NetApp com uma conta NSS, você simplesmente precisa se Registrar para obter suporte através do BlueXP .

Passos

1. No canto superior direito do console BlueXP , selecione o ícone Configurações e selecione **credenciais**.
2. Selecione **credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do site de suporte da NetApp (NSS).
4. Para confirmar que o processo de Registro foi bem-sucedido, selecione o ícone Ajuda e selecione **suporte**.

   A página **recursos** deve mostrar que sua organização do BlueXP está registrada para suporte.



   Observe que outros usuários do BlueXP não verão esse mesmo status de Registro de suporte se não tiverem associado uma conta do site de suporte da NetApp ao login do BlueXP . No entanto, isso não significa que sua organização do BlueXP não esteja registrada para suporte. Desde que um usuário na organização tenha seguido esses passos, sua organização foi registrada.

Cliente existente, mas sem conta NSS

Se você já é um cliente NetApp com licenças e números de série existentes, mas *no* conta NSS, você precisa criar uma conta NSS e associá-la ao seu login no BlueXP .

Passos

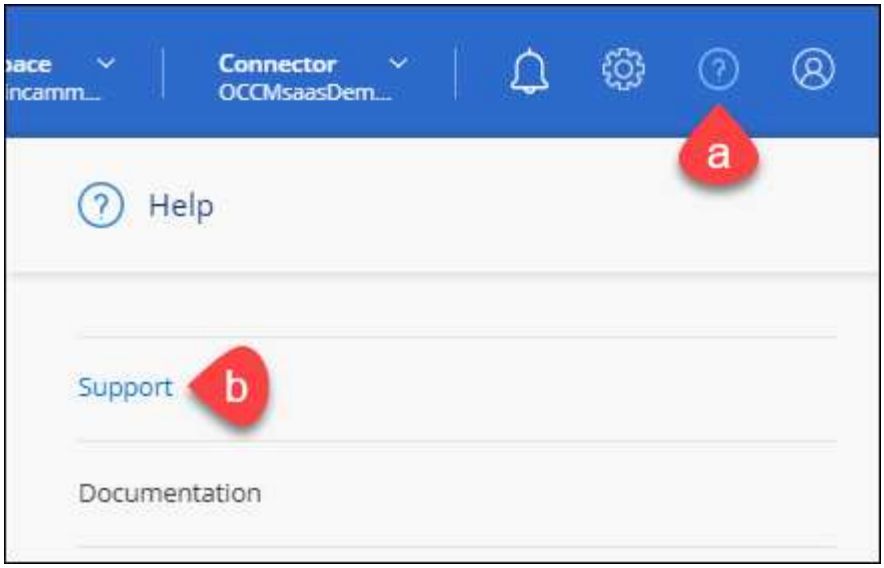
1. Crie uma conta do site de suporte da NetApp preenchendo o. "Formulário de Registro do usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
   b. Certifique-se de copiar o número de série da conta BlueXP (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento da conta.
2. Associe a sua nova conta NSS ao seu login no BlueXP executando as etapas em Cliente existente com uma conta NSS.

Novo na NetApp

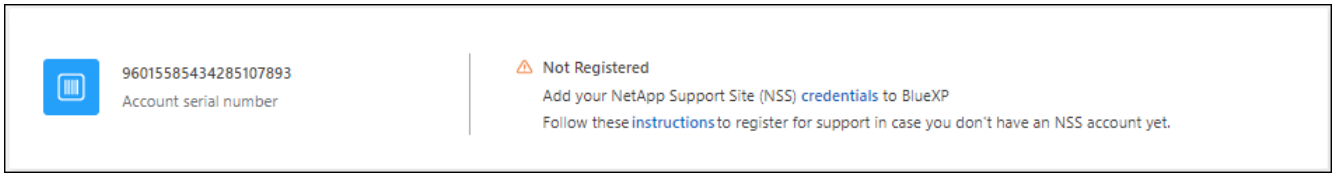
Se você é novo no NetApp e não tem uma conta NSS, siga cada passo abaixo.

Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.



2. Localize o número de série da ID da conta na página Registro de suporte.



3. Navegue "Site de Registro de suporte da NetApp" e selecione **não sou um Cliente NetApp registado**.
4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).
5. No campo **linha de produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de cobrança aplicável.
6. Copie o número de série da sua conta a partir da etapa 2 acima, complete a verificação de segurança e confirme se leu a Política de Privacidade de dados globais da NetApp.

   Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Certifique-se de verificar suas pastas de spam se o e-mail de validação não chegar em poucos minutos.

7. Confirme a ação a partir do e-mail.

   A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta do site de suporte da NetApp.

8. Crie uma conta do site de suporte da NetApp preenchendo o. "Formulário de Registro do usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o nível de usuário apropriado, que normalmente é **Cliente NetApp/Usuário final**.
   b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isto irá acelerar o processamento.

Depois de terminar

O NetApp deve entrar em Contato com você durante esse processo. Este é um exercício de integração única para novos usuários.

Depois de ter sua conta do site de suporte da NetApp, associe a conta ao login do BlueXP , executando as

etapas em Cliente existente com uma conta NSS.

Associar credenciais NSS para suporte ao Cloud Volumes ONTAP

A associação das credenciais do site de suporte da NetApp à sua organização do BlueXP é necessária para ativar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

  Fornecer sua conta NSS é necessário para ativar o suporte para o seu sistema e para obter acesso aos recursos de suporte técnico da NetApp.

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer a sua conta NSS para que o BlueXP possa carregar a sua chave de licença e ativar a subscrição para o período que adquiriu. Isso inclui atualizações automáticas para renovações de prazo.

- Atualizar o software Cloud Volumes ONTAP para a versão mais recente

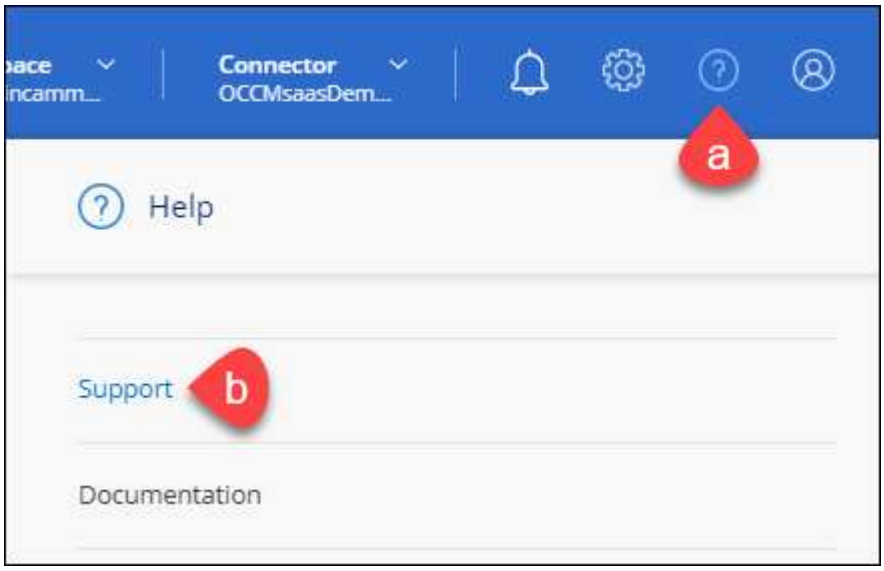
Associar credenciais NSS à sua organização do BlueXP é diferente da conta NSS associada a um login de usuário do BlueXP .

Essas credenciais do NSS estão associadas ao ID específico da organização do BlueXP . Os utilizadores que pertencem à organização BlueXP podem aceder a estas credenciais a partir de **suporte > Gestão NSS**.

- Se você tiver uma conta no nível do cliente, pode adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, você pode adicionar uma ou mais contas NSS, mas elas não podem ser adicionadas ao lado de contas de nível de cliente.

Passos

1. No canto superior direito do console do BlueXP , selecione o ícone Ajuda e selecione **suporte**.



2. Selecione **NSS Management > Add NSS Account** (Gestão NSS > Adicionar conta NSS*).
3. Quando for solicitado, selecione **continuar** para ser redirecionado para uma página de login da Microsoft.

   O NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação

específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no site de suporte da NetApp para executar o processo de autenticação.

   Essas ações permitem que o BlueXP use sua conta NSS para tarefas como downloads de licenças, verificação de atualização de software e futuros Registros de suporte.

   Observe o seguinte:

   - A conta NSS tem de ser uma conta ao nível do cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS no nível do cliente.
   - Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS no nível do cliente e existir uma conta no nível do parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, uma vez que já existem utilizadores NSS de tipo diferente."

   O mesmo acontece se você tiver contas NSS pré-existentes no nível do cliente e tentar adicionar uma conta no nível do parceiro.

   - Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

     Este é um ID gerado pelo sistema que mapeia para o seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail no ••• menu.

   - Se você precisar atualizar seus tokens de credenciais de login, há também uma opção **Atualizar credenciais** ••• no menu.

     Usando esta opção, você solicita que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será postada para alertá-lo sobre isso.

Obtenha ajuda

A NetApp oferece suporte ao BlueXP e seus serviços de nuvem de várias maneiras. Amplas opções gratuitas de suporte autônomo estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. O seu registo de suporte inclui suporte técnico remoto através de Bilheteira na Web.

Obtenha suporte para um serviço de arquivos do provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo de provedor de nuvem, sua infraestrutura ou qualquer solução usando o serviço, consulte "obter ajuda" na documentação do BlueXP para esse produto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service para Google Cloud"

Para receber suporte técnico específico da BlueXP e de suas soluções e serviços de storage, use as opções de suporte descritas abaixo.

Use opções de suporte autônomo

Estas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

  A documentação do BlueXP que você está visualizando no momento.

- "Base de conhecimento"

  PESQUISE na base de conhecimento do BlueXP para encontrar artigos úteis para solucionar problemas.

- "Comunidades"

  Junte-se à comunidade BlueXP para seguir as discussões em curso ou criar novas.

Crie um caso com o suporte do NetApp

Além das opções de suporte autônomo acima, você pode trabalhar com um especialista de suporte da NetApp para resolver quaisquer problemas depois de ativar o suporte.

Antes de começar

- Para usar o recurso **criar um caso**, primeiro você deve associar suas credenciais do site de suporte da NetApp ao login do BlueXP . "Saiba como gerenciar credenciais associadas ao seu login no BlueXP".
- Se você estiver abrindo um caso para um sistema ONTAP com um número de série, sua conta NSS deve estar associada ao número de série desse sistema.

Passos

1. No BlueXP , selecione **Ajuda > suporte**.
2. Na página **recursos**, escolha uma das opções disponíveis em suporte técnico:

   a. Selecione **Ligue para nós** se quiser falar com alguém no telefone. Você será direcionado para uma página no NetApp.com que lista os números de telefone que você pode ligar.

   b. Selecione **criar um caso** para abrir um ticket com um especialista em suporte da NetApp:

      - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, BlueXP quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do serviço.
      - **Ambiente de trabalho**: Se aplicável ao armazenamento, selecione **Cloud Volumes ONTAP** ou **no local** e, em seguida, o ambiente de trabalho associado.

        A lista de ambientes de trabalho está dentro do escopo da organização (ou conta) do BlueXP , do projeto (ou da área de trabalho) e do conetor que você selecionou no banner superior do serviço.

      - **Prioridade do caso**: Escolha a prioridade para o caso, que pode ser baixa, média, alta ou Crítica.

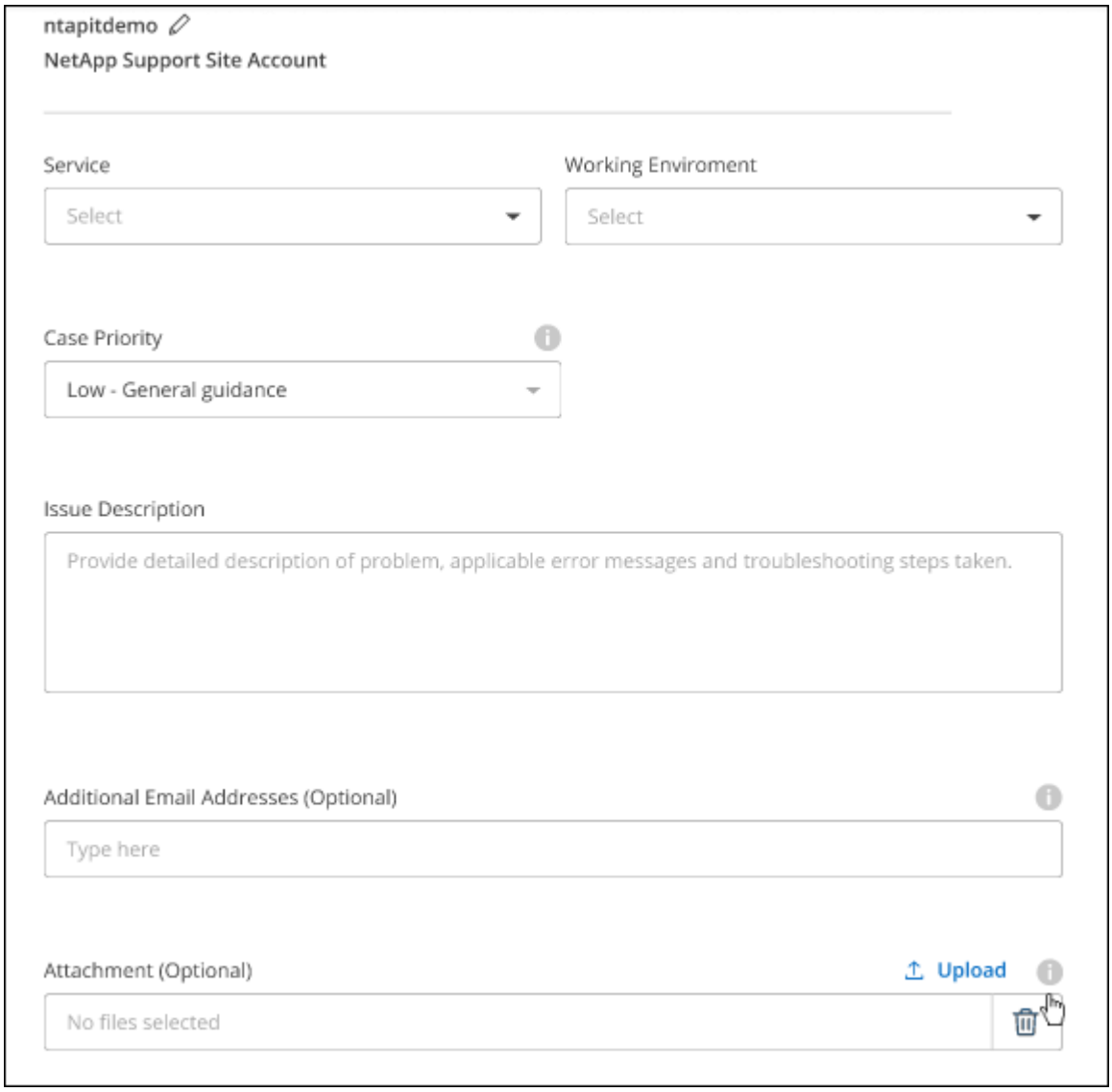
        Para saber mais detalhes sobre essas prioridades, passe o Mouse sobre o ícone de informações ao lado do nome do campo.

      - **Descrição do problema**: Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
      - **Endereços de e-mail adicionais**: Insira endereços de e-mail adicionais se você quiser que outra

pessoa saiba sobre esse problema.

- **Anexo (Opcional)**: Carregue até cinco anexos, um de cada vez.

  Os anexos estão limitados a 25 MB por ficheiro. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Depois de terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp irá rever o seu caso e voltar para você em breve.

Para obter um histórico de seus casos de suporte, você pode selecionar **Configurações > linha do tempo** e procurar ações chamadas "criar caso de suporte". Um botão à direita permite expandir a ação para ver detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

"Você não está autorizado a criar um caso contra o serviço selecionado"

Esse erro pode significar que a conta NSS e a empresa de Registro com a qual está associada não são a mesma empresa de Registro para o número de série da conta BlueXP (ou seja. 960xxxx) ou o número de

série do ambiente de trabalho. Pode procurar assistência utilizando uma das seguintes opções:

- Use o chat no produto
- Envie um caso não técnico em https://mysupport.netapp.com/site/help

Gerenciar seus casos de suporte (prévia)

Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do BlueXP . Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

O gerenciamento de casos está disponível como uma prévia. Planejamos refinar essa experiência e adicionar melhorias nos próximos lançamentos. Por favor, envie-nos feedback usando o chat no produto.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
  - A vista à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta do usuário NSS que você forneceu.
  - A visualização à direita mostra o total de casos abertos nos últimos 3 meses ao nível da sua empresa com base na sua conta NSS de utilizador.

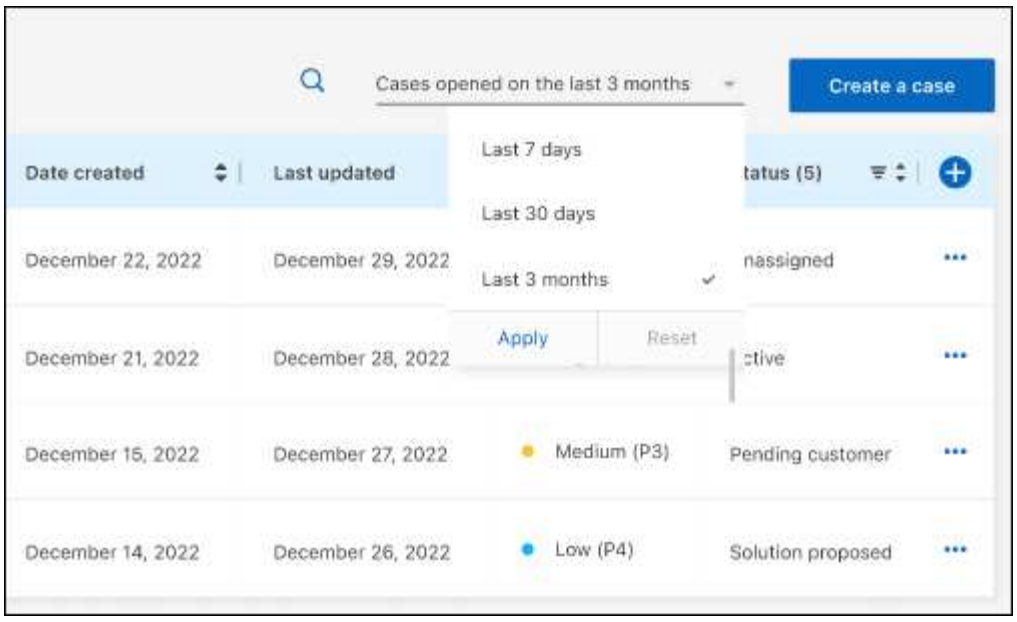
  Os resultados na tabela refletem os casos relacionados à exibição selecionada.
- Você pode adicionar ou remover colunas de interesse e pode filtrar o conteúdo de colunas como prioridade e Status. Outras colunas fornecem apenas capacidades de ordenação.

  Veja os passos abaixo para obter mais detalhes.
- Em um nível por caso, oferecemos a capacidade de atualizar notas de caso ou fechar um caso que ainda não esteja no status fechado ou pendente fechado.

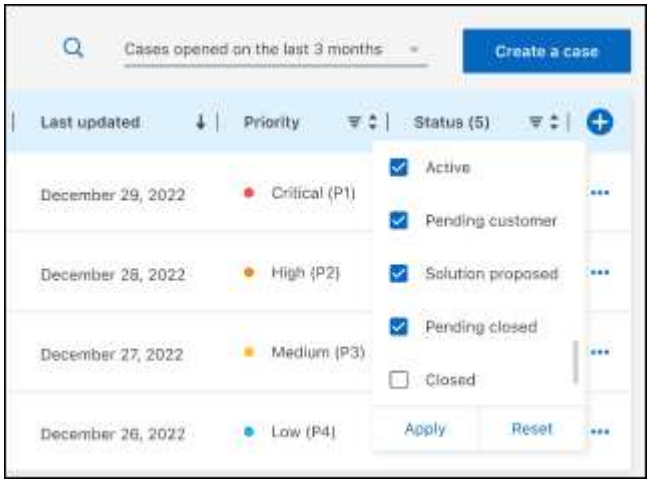
Passos

1. No BlueXP , selecione **Ajuda > suporte**.
2. Selecione **Gerenciamento de casos** e, se for solicitado, adicione sua conta NSS ao BlueXP .

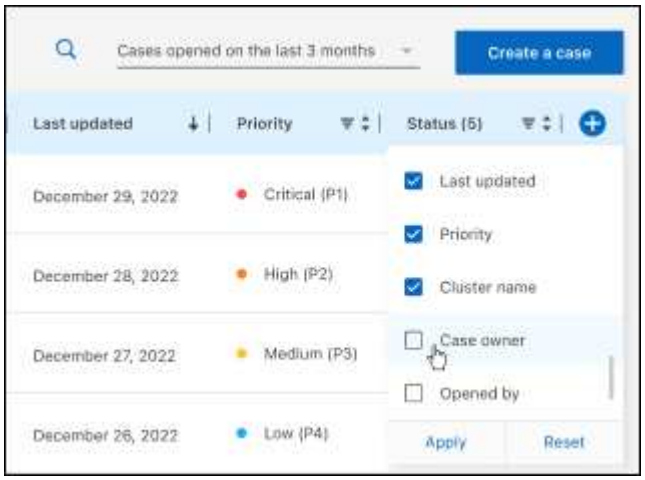
   A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à conta de usuário do BlueXP . Esta é a mesma conta NSS que aparece na parte superior da página **NSS Management**.
3. Opcionalmente, modifique as informações exibidas na tabela:
   - Em **casos da organização**, selecione **Exibir** para ver todos os casos associados à sua empresa.
   - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um intervalo de tempo diferente.



- Filtre o conteúdo das colunas.



- Altere as colunas que aparecem na tabela selecionando e escolhendo as colunas que você deseja exibir.

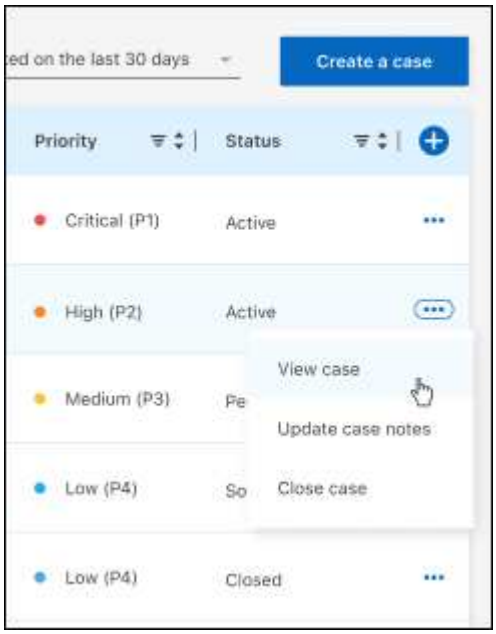


4. Gerencie um caso existente •••selecionando e selecionando uma das opções disponíveis:

   - **Ver caso**: Veja detalhes completos sobre um caso específico.
   - * Atualizar notas de caso*: Forneça detalhes adicionais sobre o seu problema ou selecione **carregar arquivos** para anexar até um máximo de cinco arquivos.

     Os anexos estão limitados a 25 MB por ficheiro. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

   - * Fechar caso*: Forneça detalhes sobre por que você está fechando o caso e selecione **Fechar caso**.



Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

"https://www.netapp.com/company/legal/copyright/"

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.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

- "Aviso para BlueXP"
- "Aviso para backup e recuperação do BlueXP "
- "Aviso para restauração de arquivo único"

Informações sobre direitos autorais

Informações sobre marcas comerciais