Documentação do NetApp Backup and Recovery

NetApp Backup and Recovery

NetApp
October 07, 2025

Índice

Documentação do NetApp Backup and Recovery

Notas de lançamento

Novidades no NetApp Backup and Recovery

Saiba o que há de novo no NetApp Backup and Recovery.

06 de outubro de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

O BlueXP backup and recovery agora são NetApp Backup e Recovery

O BlueXP backup and recovery foi renomeado para NetApp Backup and Recovery.

BlueXP agora é NetApp Console

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

Para obter detalhes sobre o que mudou, consulte o"Notas de versão do NetApp Console."

Suporte à carga de trabalho do Hyper-V como uma visualização privada

Esta versão do NetApp Backup and Recovery apresenta suporte para descoberta e gerenciamento de cargas de trabalho do Hyper-V:

- Fazer backup e restaurar VMs em instâncias autônomas, bem como instâncias de cluster de failover (FCI)
- Proteja VMs armazenadas em compartilhamentos SMB3
- Proteção em massa no nível da máquina virtual
- Backups consistentes de VM e falhas
- Restaurar VMs do armazenamento primário, secundário e de objetos
- Pesquisar e restaurar backups de VM

Para obter detalhes sobre como proteger cargas de trabalho do Hyper-V, consulte "Visão geral das cargas de trabalho de proteção do Hyper-V" .

Suporte à carga de trabalho KVM como uma visualização privada

Esta versão do NetApp Backup and Recovery apresenta suporte para descoberta e gerenciamento de cargas de trabalho KVM:

- Fazer backup e restaurar imagens de VM qcow2 armazenadas em compartilhamentos NFS
- Fazer backup de pools de armazenamento
- Proteção de pool de armazenamento e VM em massa usando grupos de proteção
- Backups de VM consistentes e consistentes com falhas
- Pesquisar e restaurar backups de VM de armazenamento primário, secundário e de objetos

- Processo guiado para fazer backup e restaurar VMs baseadas em KVM e dados de VM

Para obter detalhes sobre como proteger cargas de trabalho KVM, consulte "Visão geral das cargas de trabalho de proteção do KVM" .

Melhorias na pré-visualização do Kubernetes

A versão de pré-visualização das cargas de trabalho do Kubernetes apresenta os seguintes aprimoramentos:

- Suporte à arquitetura de backup Fan Out 3-2-1
- Suporte para ONTAP S3 como destino de backup
- Novo painel do Kubernetes para gerenciamento mais fácil
- A configuração aprimorada de controle de acesso baseado em função (RBAC) inclui suporte para as seguintes funções:
  - Superadministrador de Backup e Recuperação
  - Administrador de backup e recuperação
  - Administração de restauração de backup e recuperação
  - Visualizador de backup e recuperação
- Suporte para distribuição do SUSE Rancher Kubernetes
- Suporte a vários buckets: agora você pode proteger os volumes dentro de um sistema com vários buckets por sistema em diferentes provedores de nuvem

Para obter detalhes sobre como proteger cargas de trabalho do Kubernetes, consulte "Visão geral das cargas de trabalho do Protect Kubernetes" .

Suporte à carga de trabalho do Oracle Database como uma visualização privada

Esta versão do NetApp Backup and Recovery apresenta suporte para descoberta e gerenciamento de cargas de trabalho do Oracle Database:

- Descubra bancos de dados Oracle autônomos
- Crie políticas de proteção somente para dados ou backups de dados e logs
- Proteja os bancos de dados Oracle com um esquema de backup 3-2-1
- Configurar retenção de backup
- Montar e desmontar backups do ARCHIVELOG
- Bancos de dados virtualizados
- Pesquisar e restaurar backups de banco de dados
- Suporte ao painel Oracle

Para obter detalhes sobre como proteger cargas de trabalho do Oracle Database, consulte "Visão geral das cargas de trabalho do Protect Oracle" .

25 de agosto de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Suporte para proteção de cargas de trabalho VMware na visualização

Esta versão adiciona suporte de pré-visualização para proteger cargas de trabalho do VMware. Faça backup de VMs e datastores VMware de sistemas ONTAP locais para Amazon Web Services e StorageGRID.

> A documentação sobre a proteção de cargas de trabalho do VMware é fornecida como uma prévia da tecnologia. Com esta oferta de visualização, a NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da disponibilidade geral.

"Saiba mais sobre como proteger cargas de trabalho do VMware com o NetApp Backup and Recovery" .

A indexação de alto desempenho para AWS, Azure e GCP está geralmente disponível

Em fevereiro de 2025, anunciamos a prévia da indexação de alto desempenho (Indexed Catalog v2) para AWS, Azure e GCP. Este recurso agora está disponível para o público em geral (GA). Em junho de 2025, fornecemos isso a todos os *novos* clientes por padrão. Com esta versão, o suporte está disponível para *todos* os clientes. A indexação de alto desempenho melhora o desempenho das operações de backup e restauração para cargas de trabalho protegidas no armazenamento de objetos.

Ativado por padrão:

- Se você for um novo cliente, a indexação de alto desempenho será habilitada por padrão.
- Se você já for cliente, poderá habilitar a reindexação acessando a seção Restaurar da interface do usuário.

12 de agosto de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

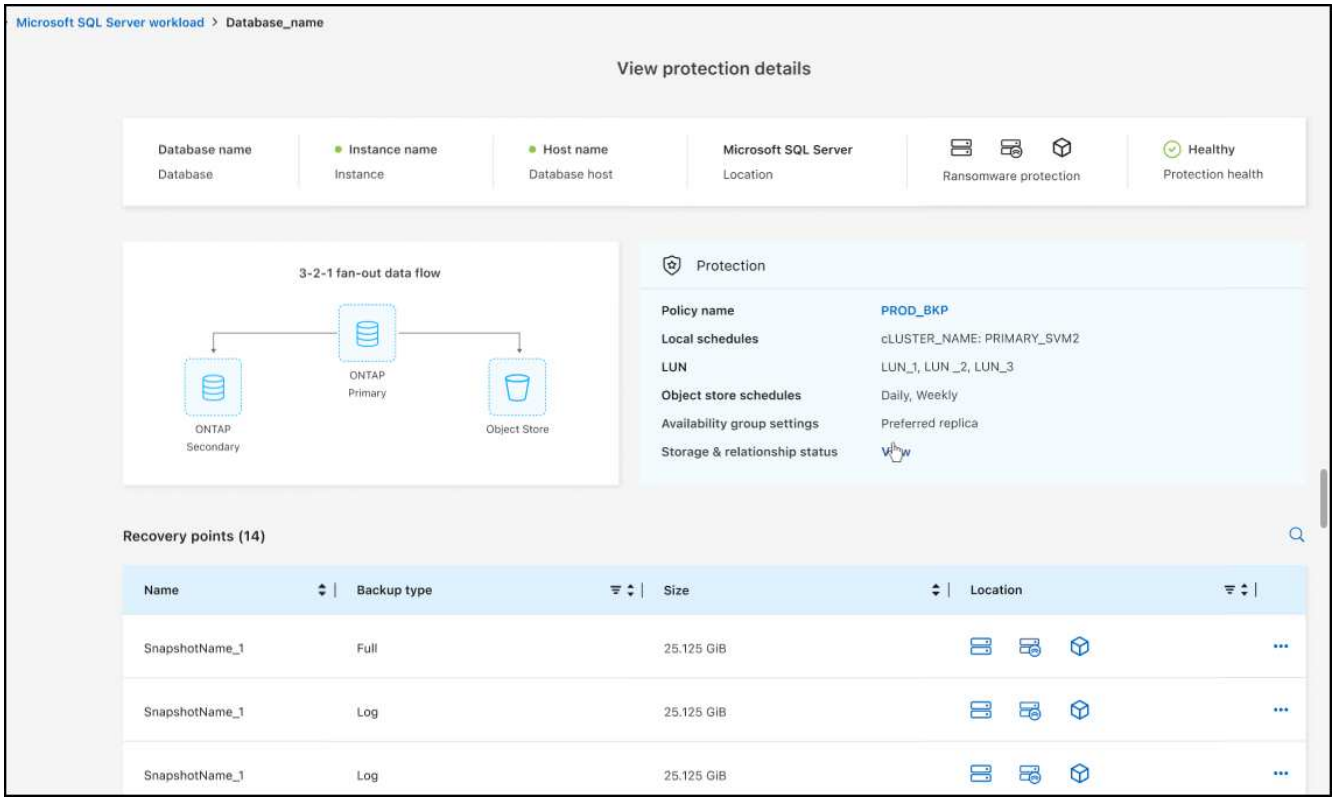
Carga de trabalho do Microsoft SQL Server com suporte em Disponibilidade Geral (GA)

O suporte à carga de trabalho do Microsoft SQL Server agora está disponível de modo geral (GA) no NetApp Backup and Recovery. Organizações que usam um ambiente MSSQL no ONTAP, Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP agora podem aproveitar este novo serviço de backup e recuperação para proteger seus dados.

Esta versão inclui os seguintes aprimoramentos no suporte à carga de trabalho do Microsoft SQL Server em relação à versão de visualização anterior:

- * Sincronização ativa do SnapMirror **: Esta versão agora oferece suporte à sincronização ativa do SnapMirror (também conhecida como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos executem failover transparente usando uma cópia secundária. O NetApp Backup and Recovery agora oferece suporte à proteção de bancos de dados do Microsoft SQL Server em uma configuração de sincronização ativa do SnapMirror e Metrocluster. As informações aparecem na seção *Status de armazenamento e relacionamento** da página Detalhes de proteção. As informações de relacionamento são exibidas na seção atualizada **Configurações secundárias** da página Política.

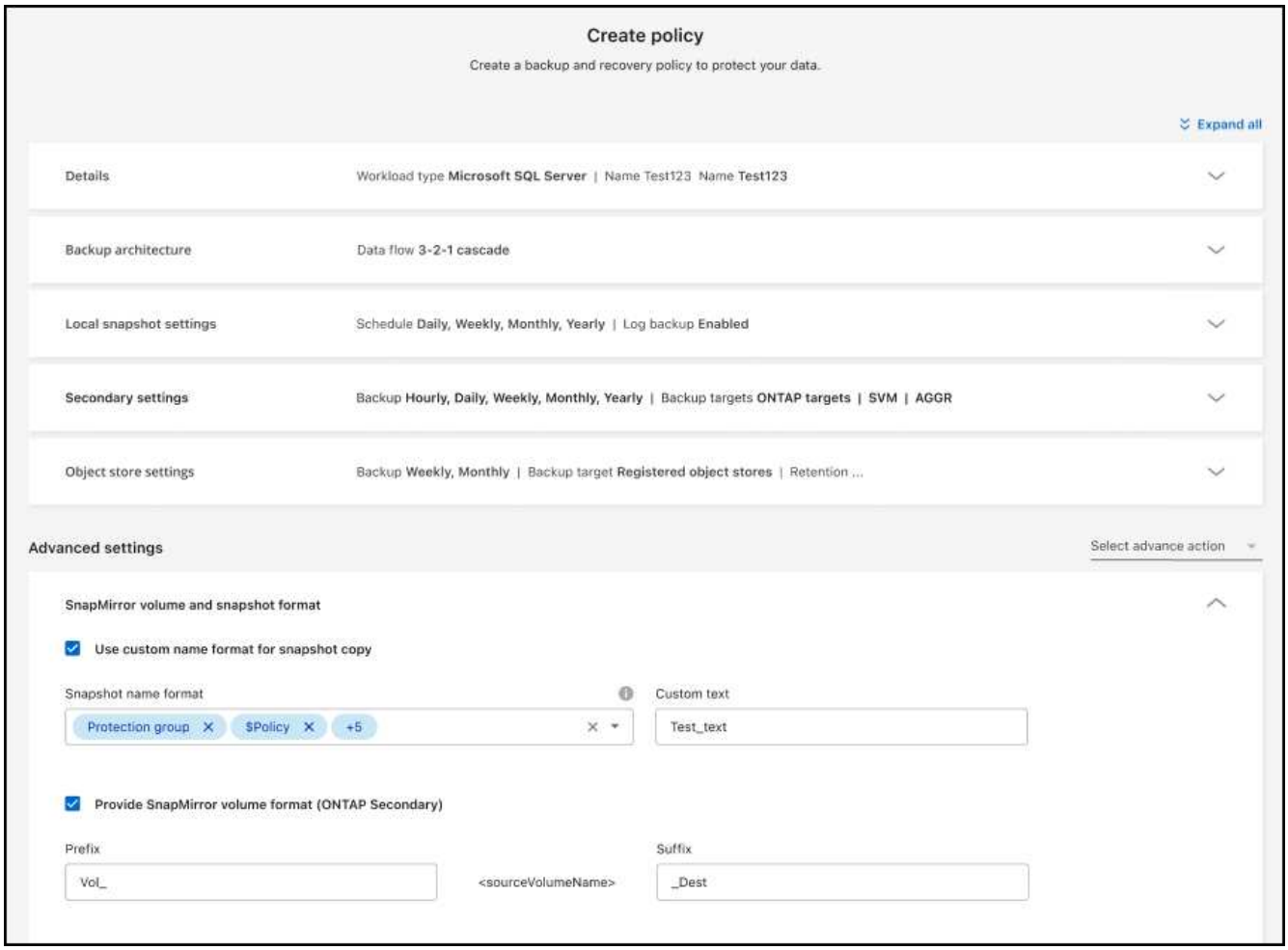
  Consulte "Use políticas para proteger suas cargas de trabalho" .



- **Suporte a vários buckets**: agora você pode proteger os volumes dentro de um ambiente de trabalho com até 6 buckets por ambiente de trabalho em diferentes provedores de nuvem.
- **Atualizações de licenciamento e avaliação gratuita** para cargas de trabalho do SQL Server: agora você pode usar o modelo de licenciamento existente do NetApp Backup and Recovery para proteger cargas de trabalho do SQL Server. Não há requisito de licenciamento separado para cargas de trabalho do SQL Server.

  Para mais detalhes, consulte "Configurar licenciamento para NetApp Backup and Recovery" .

- **Nome de instantâneo personalizado**: agora você pode usar seu próprio nome de instantâneo em uma política que controla os backups para cargas de trabalho do Microsoft SQL Server. Insira essas informações na seção **Configurações avançadas** da página Política.

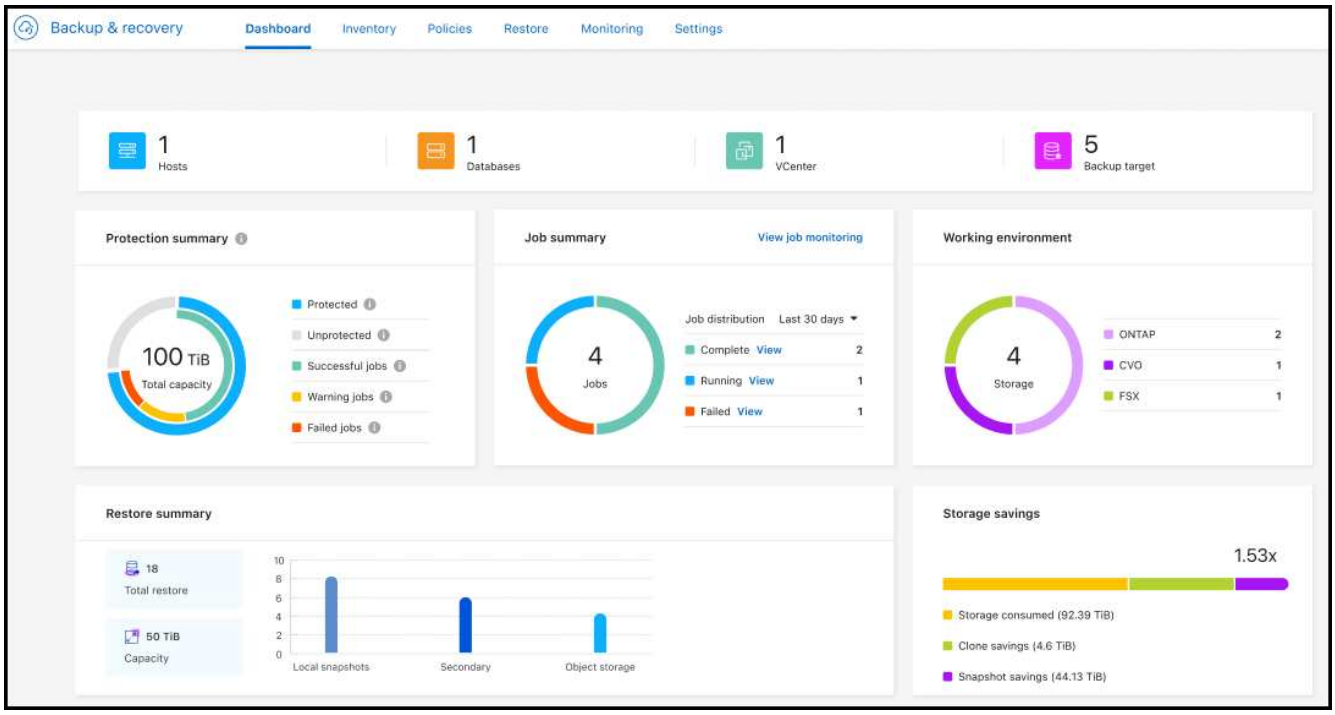


Consulte "Use políticas para proteger suas cargas de trabalho" .

- **Prefixo e sufixo do volume secundário**: você pode inserir um prefixo e sufixo personalizados na seção **Configurações avançadas** da página Política.
- **Identidade e acesso**: Agora você pode controlar o acesso dos usuários aos recursos.

  Consulte "Efetue login no NetApp Backup and Recovery" e "Acesso aos recursos do NetApp Backup and Recovery" .

- **Restaurar do armazenamento de objetos para um host alternativo**: Agora você pode restaurar do armazenamento de objetos para um host alternativo, mesmo que o armazenamento primário esteja inativo.
- **Dados de backup de log**: A página de detalhes de proteção do banco de dados agora mostra backups de log. Você pode ver a coluna Tipo de backup que mostra se o backup é completo ou de log.
- **Painel aprimorado**: O painel agora mostra economias de armazenamento e clone.



Melhorias na carga de trabalho do volume ONTAP

- *Restauração de várias pastas para volumes ONTAP *: Até agora, você podia restaurar uma pasta ou vários arquivos de uma vez usando o recurso Navegar e restaurar. O NetApp Backup and Recovery agora oferece a capacidade de selecionar várias pastas ao mesmo tempo usando o recurso Procurar e restaurar.
- **Visualizar e gerenciar backups de volumes excluídos**: O NetApp Backup and Recovery Dashboard agora oferece uma opção para mostrar e gerenciar volumes excluídos do ONTAP. Com isso, você pode visualizar e excluir backups de volumes que não existem mais no ONTAP.
- **Forçar exclusão de backups**: Em alguns casos extremos, você pode querer que o NetApp Backup and Recovery não tenha mais acesso aos backups. Isso pode acontecer, por exemplo, se o serviço não tiver mais acesso ao bucket de backup ou se os backups forem protegidos pelo DataLock, mas você não os quiser mais. Anteriormente, não era possível excluí-los sozinho e era necessário ligar para o Suporte da NetApp . Com esta versão, você pode usar a opção para forçar a exclusão de backups (em níveis de volume e ambiente de trabalho).

> Use esta opção com cuidado e somente em casos de extrema necessidade de limpeza. O NetApp Backup and Recovery não terá mais acesso a esses backups, mesmo que eles não sejam excluídos do armazenamento de objetos. Você precisará ir ao seu provedor de nuvem e excluir manualmente os backups.

Consulte "Proteja cargas de trabalho ONTAP" .

28 de julho de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Suporte à carga de trabalho do Kubernetes como uma prévia

Esta versão do NetApp Backup and Recovery apresenta suporte para descoberta e gerenciamento de cargas de trabalho do Kubernetes:

- Descubra o Red Hat OpenShift e os clusters Kubernetes de código aberto, apoiados pelo NetApp ONTAP, sem compartilhar arquivos kubeconfig.
- Descubra, gerencie e proteja aplicativos em vários clusters do Kubernetes usando um plano de controle unificado.
- Descarregue operações de movimentação de dados para backup e recuperação de aplicativos Kubernetes para o NetApp ONTAP.
- Orquestre backups de aplicativos locais e baseados em armazenamento de objetos.
- Faça backup e restaure aplicativos inteiros e recursos individuais em qualquer cluster do Kubernetes.
- Trabalhe com contêineres e máquinas virtuais em execução no Kubernetes.
- Crie backups consistentes com o aplicativo usando ganchos e modelos de execução.

Para obter detalhes sobre como proteger cargas de trabalho do Kubernetes, consulte "Visão geral das cargas de trabalho do Protect Kubernetes" .

14 de julho de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Painel de volume ONTAP aprimorado

Em abril de 2025, lançamos uma prévia de um Painel de Volume ONTAP aprimorado que é muito mais rápido e eficiente.

Este painel foi projetado para ajudar clientes corporativos com um grande número de cargas de trabalho. Mesmo para clientes com 20.000 volumes, o novo painel carrega em <10 segundos.

Após uma prévia bem-sucedida e ótimos comentários dos clientes, agora estamos tornando-a a experiência padrão para todos os nossos clientes. Esteja pronto para um painel incrivelmente rápido.

Para obter detalhes, consulte "Visualizar a saúde da proteção no Painel" .

Suporte à carga de trabalho do Microsoft SQL Server como uma prévia de tecnologia pública

Esta versão do NetApp Backup and Recovery fornece uma interface de usuário atualizada que permite gerenciar cargas de trabalho do Microsoft SQL Server usando uma estratégia de proteção 3-2-1, familiar no NetApp Backup and Recovery. Com esta nova versão, você pode fazer backup dessas cargas de trabalho no armazenamento primário, replicá-las no armazenamento secundário e fazer backup delas no armazenamento de objetos na nuvem.

Você pode se inscrever para a prévia preenchendo este formulário "Formulário de inscrição de pré-visualização" .

> Esta documentação sobre a proteção de cargas de trabalho do Microsoft SQL Server é fornecida como uma prévia da tecnologia. Com esta oferta de prévia, a NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da disponibilidade geral.

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações:

- **Recurso de backup 3-2-1**: Esta versão integra recursos do SnapCenter , permitindo que você gerencie e proteja seus recursos do SnapCenter com uma estratégia de proteção de dados 3-2-1 na interface do

usuário do NetApp Backup and Recovery.

- **Importar do SnapCenter**: Você pode importar dados e políticas de backup do SnapCenter para o NetApp Backup and Recovery.
- **Uma interface de usuário redesenhada** proporciona uma experiência mais intuitiva para gerenciar suas tarefas de backup e recuperação.
- **Destinos de backup**: Você pode adicionar buckets em ambientes Amazon Web Services (AWS), Microsoft Azure Blob Storage, StorageGRID e ONTAP S3 para usar como destinos de backup para suas cargas de trabalho do Microsoft SQL Server.
- **Suporte de carga de trabalho**: Esta versão permite que você faça backup, restaure, verifique e clone bancos de dados e grupos de disponibilidade do Microsoft SQL Server. (Suporte para outras cargas de trabalho será adicionado em versões futuras.)
- **Opções de restauração flexíveis**: Esta versão permite que você restaure bancos de dados para locais originais e alternativos em caso de corrupção ou perda acidental de dados.
- **Cópias de produção instantâneas**: gere cópias de produção com eficiência de espaço para desenvolvimento, testes ou análises em minutos, em vez de horas ou dias.
- Esta versão inclui a capacidade de criar relatórios detalhados.

Para obter detalhes sobre como proteger cargas de trabalho do Microsoft SQL Server, consulte"Visão geral da proteção de cargas de trabalho do Microsoft SQL Server" .

09 de junho de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Atualizações de suporte ao catálogo indexado

Em fevereiro de 2025, introduzimos o recurso de indexação atualizado (Catálogo Indexado v2) que você usa durante o método Pesquisar e Restaurar para restaurar dados. A versão anterior melhorou significativamente o desempenho de indexação de dados em ambientes locais. Com esta versão, o catálogo de indexação agora está disponível nos ambientes Amazon Web Services, Microsoft Azure e Google Cloud Platform (GCP).

Se você for um novo cliente, o Catálogo Indexado v2 será habilitado por padrão para todos os novos ambientes. Se você já for cliente, poderá reindexar seu ambiente para aproveitar o Catálogo Indexado v2.

Como você habilita a indexação?

Antes de poder usar o método Pesquisar e Restaurar para restaurar dados, você precisa habilitar a "Indexação" em cada ambiente de trabalho de origem do qual você planeja restaurar volumes ou arquivos. Selecione a opção **Ativar indexação** quando estiver executando uma pesquisa e restauração.

O Catálogo Indexado pode então rastrear cada volume e arquivo de backup, tornando suas pesquisas rápidas e eficientes.

Para obter mais informações, consulte "Habilitar indexação para Pesquisa e Restauração" .

Pontos de extremidade de link privado e pontos de extremidade de serviço do Azure

Normalmente, o NetApp Backup and Recovery estabelece um ponto de extremidade privado com o provedor de nuvem para lidar com tarefas de proteção. Esta versão apresenta uma configuração opcional que permite habilitar ou desabilitar o NetApp Backup and Recovery para criar automaticamente um endpoint privado. Isso pode ser útil se você quiser mais controle sobre o processo de criação de endpoint privado.

Você pode habilitar ou desabilitar esta opção ao habilitar a proteção ou iniciar o processo de restauração.

Se você desabilitar essa configuração, será necessário criar manualmente o endpoint privado para que o NetApp Backup and Recovery funcione corretamente. Sem a conectividade adequada, talvez você não consiga executar tarefas de backup e recuperação com sucesso.

Suporte para SnapMirror para ressincronização em nuvem no ONTAP S3

A versão anterior introduziu suporte para SnapMirror para Cloud Resync (SM-C Resync). O recurso simplifica a proteção de dados durante a migração de volume em ambientes NetApp . Esta versão adiciona suporte para SM-C Resync no ONTAP S3, bem como outros provedores compatíveis com S3, como Wasabi e MinIO.

Traga seu próprio bucket para o StorageGRID

Ao criar arquivos de backup no armazenamento de objetos para um ambiente de trabalho, por padrão, o NetApp Backup and Recovery cria o contêiner (bucket ou conta de armazenamento) para os arquivos de backup na conta de armazenamento de objetos que você configurou. Anteriormente, você podia substituir isso e especificar seu próprio contêiner para Amazon S3, Azure Blob Storage e Google Cloud Storage. Com esta versão, agora você pode trazer seu próprio contêiner de armazenamento de objetos StorageGRID .

Ver "Crie seu próprio contêiner de armazenamento de objetos" .

13 de maio de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Ressincronização do SnapMirror para a Nuvem para migrações de volume

O recurso SnapMirror to Cloud Resync simplifica a proteção de dados e a continuidade durante migrações de volume em ambientes NetApp . Quando um volume é migrado usando o SnapMirror Logical Replication (LRSE), de uma implantação NetApp local para outra, ou para uma solução baseada em nuvem, como o Cloud Volumes ONTAP ou o Cloud Volumes Service, o SnapMirror para o Cloud Resync garante que os backups em nuvem existentes permaneçam intactos e operacionais.

Esse recurso elimina a necessidade de uma operação de redefinição de linha de base demorada e que exige muitos recursos, permitindo que as operações de backup continuem após a migração. Esse recurso é valioso em cenários de migração de carga de trabalho, oferecendo suporte a FlexVols e FlexGroups, e está disponível a partir da versão 9.16.1 do ONTAP .

Ao manter a continuidade do backup em todos os ambientes, o SnapMirror to Cloud Resync aumenta a eficiência operacional e reduz a complexidade do gerenciamento de dados híbridos e multinuvem.

Para obter detalhes sobre como executar a operação de ressincronização, consulte "Migrar volumes usando o SnapMirror para o Cloud Resync" .

Suporte para armazenamento de objetos MinIO de terceiros (visualização)

O NetApp Backup and Recovery agora estende seu suporte a armazenamentos de objetos de terceiros com foco principal no MinIO. Este novo recurso de visualização permite que você aproveite qualquer armazenamento de objetos compatível com S3 para suas necessidades de backup e recuperação.

Com esta versão de pré-visualização, esperamos garantir uma integração robusta com armazenamentos de objetos de terceiros antes que a funcionalidade completa seja lançada. Você é incentivado a explorar esse novo recurso e fornecer feedback para ajudar a melhorar o serviço.

Este recurso não deve ser usado em produção.

Limitações do modo de visualização

Embora esse recurso esteja em versão prévia, há certas limitações:

- Traga seu próprio balde (BYOB) não é suportado.
- A ativação do DataLock na política não é suportada.
- A ativação do modo de arquivamento na política não é suportada.
- Somente ambientes ONTAP locais são suportados.
- O MetroCluster não é suportado.
- Opções para habilitar criptografia em nível de bucket não são suportadas.

Começando

Para começar a usar este recurso de visualização, você deve habilitar um sinalizador no agente do Console. Você pode então inserir os detalhes de conexão do seu armazenamento de objetos de terceiros MinIO no fluxo de trabalho de proteção escolhendo Armazenamento de objetos **Compatível com terceiros** na seção de backup.

16 de abril de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Melhorias na interface do usuário

Esta versão melhora sua experiência simplificando a interface:

- A remoção da coluna Agregado das tabelas Volumes, juntamente com as colunas Política de Snapshot, Política de Backup e Política de Replicação da tabela Volume no Painel V2, resulta em um layout mais simplificado.
- Excluir ambientes de trabalho não ativados da lista suspensa torna a interface menos confusa, a navegação mais eficiente e o carregamento mais rápido.
- Embora a classificação na coluna Tags esteja desabilitada, você ainda pode visualizar as tags, garantindo que informações importantes permaneçam facilmente acessíveis.
- A remoção de rótulos nos ícones de proteção contribui para uma aparência mais limpa e diminui o tempo de carregamento.
- Durante o processo de ativação do ambiente de trabalho, uma caixa de diálogo exibe um ícone de carregamento para fornecer feedback até que o processo de descoberta seja concluído, aumentando a transparência e a confiança nas operações do sistema.

Painel de Volume Aprimorado (Visualização)

O Volume Dashboard agora carrega em menos de 10 segundos, proporcionando uma interface muito mais rápida e eficiente. Esta versão de pré-visualização está disponível para clientes selecionados, oferecendo a eles uma prévia dessas melhorias.

Suporte para armazenamento de objetos Wasabi de terceiros (visualização)

O NetApp Backup and Recovery agora estende seu suporte a armazenamentos de objetos de terceiros, com foco principal no Wasabi. Este novo recurso de visualização permite que você aproveite qualquer armazenamento de objetos compatível com S3 para suas necessidades de backup e recuperação.

Começando com Wasabi

Para começar a usar o armazenamento de terceiros como um armazenamento de objetos, você deve habilitar um sinalizador no agente do Console. Em seguida, você pode inserir os detalhes de conexão do seu armazenamento de objetos de terceiros e integrá-lo aos seus fluxos de trabalho de backup e recuperação.

Passos

1. Conecte-se via SSH ao seu conector.
2. Acesse o contêiner do servidor cbs do NetApp Backup and Recovery:

```
docker exec -it cloudmanager_cbs sh
```

3. Abra o `default.json` arquivo dentro do `config` pasta via VIM ou qualquer outro editor:

```
vi default.json
```

4. Modificar `allow-s3-compatible` : falso para `allow-s3-compatible` : verdadeiro.
5. Salve as alterações.
6. Saia do contêiner.
7. Reinicie o contêiner do servidor cbs do NetApp Backup and Recovery.

Resultado

Depois que o contêiner estiver LIGADO novamente, abra a interface do usuário do NetApp Backup and Recovery. Ao iniciar um backup ou editar uma estratégia de backup, você verá o novo provedor "Compatível com S3" listado junto com outros provedores de backup da AWS, Microsoft Azure, Google Cloud, StorageGRID e ONTAP S3.

Limitações do modo de visualização

Embora esse recurso esteja em versão prévia, considere as seguintes limitações:

- Traga seu próprio balde (BYOB) não é suportado.
- Não há suporte para habilitar o DataLock em uma política.
- Não há suporte para habilitar o modo de arquivamento em uma política.
- Somente ambientes ONTAP locais são suportados.
- O MetroCluster não é suportado.
- Opções para habilitar criptografia em nível de bucket não são suportadas.

Durante esta prévia, incentivamos você a explorar esse novo recurso e fornecer feedback sobre a integração com armazenamentos de objetos de terceiros antes que a funcionalidade completa seja implementada.

17 de março de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Navegação de instantâneos SMB

Esta atualização do NetApp Backup and Recovery resolveu um problema que impedia os clientes de navegar em snapshots locais em um ambiente SMB.

Atualização do ambiente AWS GovCloud

Esta atualização do NetApp Backup and Recovery corrigiu um problema que impedia a interface do usuário de se conectar a um ambiente AWS GovCloud devido a erros de certificado TLS. O problema foi resolvido usando o nome do host do agente do Console em vez do endereço IP.

Limites de retenção da política de backup

Anteriormente, a interface de usuário do NetApp Backup and Recovery limitava os backups a 999 cópias, enquanto a CLI permitia mais. Agora, você pode anexar até 4.000 volumes a uma política de backup e incluir 1.018 volumes não anexados a uma política de backup. Esta atualização inclui validações adicionais que impedem que esses limites sejam excedidos.

Ressincronização do SnapMirror Cloud

Esta atualização garante que a ressincronização do SnapMirror Cloud não possa ser iniciada a partir do NetApp Backup and Recovery para versões ONTAP não suportadas após um relacionamento do SnapMirror ter sido excluído.

21 de fevereiro de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Indexação de alto desempenho

O NetApp Backup and Recovery apresenta um recurso de indexação atualizado que torna a indexação de dados no sistema de origem mais eficiente. O novo recurso de indexação inclui atualizações na interface do usuário, desempenho aprimorado do método Pesquisar e Restaurar para restauração de dados, atualizações nos recursos de pesquisa global e melhor escalabilidade.

Aqui está uma análise das melhorias:

- **Consolidação de pastas**: A versão atualizada agrupa pastas usando nomes que incluem identificadores específicos, tornando o processo de indexação mais suave.
- **Compactação de arquivos Parquet**: A versão atualizada reduz o número de arquivos usados para indexar cada volume, simplificando o processo e eliminando a necessidade de um banco de dados extra.
- **Escalar com mais sessões**: A nova versão adiciona mais sessões para lidar com tarefas de indexação, acelerando o processo.
- **Suporte para múltiplos contêineres de índice**: A nova versão usa múltiplos contêineres para gerenciar e distribuir melhor as tarefas de indexação.
- **Fluxo de trabalho de indexação dividido**: A nova versão divide o processo de indexação em duas partes, aumentando a eficiência.
- **Concorrência aprimorada**: A nova versão torna possível excluir ou mover diretórios ao mesmo tempo,

acelerando o processo de indexação.

Quem se beneficia com esse recurso?

O novo recurso de indexação está disponível para todos os novos clientes.

Como você habilita a indexação?

Antes de poder usar o método Pesquisar e Restaurar para restaurar dados, você precisa habilitar a "Indexação" em cada sistema de origem do qual planeja restaurar volumes ou arquivos. Isso permite que o Catálogo Indexado rastreie cada volume e cada arquivo de backup, tornando suas pesquisas rápidas e eficientes.

Habilite a indexação no ambiente de trabalho de origem selecionando a opção "Habilitar indexação" quando estiver executando uma Pesquisa e Restauração.

Para mais informações, consulte a documentação "como restaurar dados ONTAP usando Pesquisar e Restaurar" .

Escala suportada

O novo recurso de indexação oferece suporte ao seguinte:

- Eficiência de pesquisa global em menos de 3 minutos
- Até 5 bilhões de arquivos
- Até 5000 volumes por cluster
- Até 100 mil instantâneos por volume
- O tempo máximo para indexação de linha de base é inferior a 7 dias. O tempo real variará dependendo do seu ambiente.

Melhorias no desempenho da pesquisa global

Esta versão também inclui melhorias no desempenho da pesquisa global. Agora você verá indicadores de progresso e resultados de pesquisa mais detalhados, incluindo a contagem de arquivos e o tempo gasto na pesquisa. Contêineres dedicados para pesquisa e indexação garantem que pesquisas globais sejam concluídas em menos de cinco minutos.

Observe estas considerações relacionadas à pesquisa global:

- O novo índice não é executado em snapshots rotulados como horários.
- O novo recurso de indexação funciona apenas em snapshots em FlexVols e não em snapshots em FlexGroups.

13 de fevereiro de 2025

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Versão prévia do NetApp Backup and Recovery

Esta versão de pré-visualização do NetApp Backup and Recovery fornece uma interface de usuário atualizada que permite gerenciar cargas de trabalho do Microsoft SQL Server usando uma estratégia de proteção 3-2-1, familiar no NetApp Backup and Recovery. Com esta nova versão, você pode fazer backup dessas cargas de trabalho no armazenamento primário, replicá-las no armazenamento secundário e fazer backup delas no armazenamento de objetos na nuvem.

Esta documentação é fornecida como uma prévia da tecnologia. Com esta oferta de visualização, a NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da disponibilidade geral.

Esta versão do NetApp Backup and Recovery Preview 2025 inclui as seguintes atualizações.

- Uma interface de usuário redesenhada que oferece uma experiência mais intuitiva para gerenciar suas tarefas de backup e recuperação.
- A versão de visualização permite que você faça backup e restaure bancos de dados do Microsoft SQL Server. (Suporte para outras cargas de trabalho será adicionado em versões futuras.)
- Esta versão integra os recursos do SnapCenter , permitindo que você gerencie e proteja seus recursos do SnapCenter com uma estratégia de proteção de dados 3-2-1 na interface do usuário do NetApp Backup and Recovery.
- Esta versão permite importar cargas de trabalho do SnapCenter para o NetApp Backup and Recovery.

22 de novembro de 2024

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Modos de proteção SnapLock Compliance e SnapLock Enterprise

O NetApp Backup and Recovery agora pode fazer backup de volumes FlexVol e FlexGroup locais configurados usando os modos de proteção SnapLock Compliance ou SnapLock Enterprise . Seus clusters devem estar executando o ONTAP 9.14 ou superior para esse suporte. O backup de volumes FlexVol usando o modo SnapLock Enterprise é suportado desde a versão 9.11.1 do ONTAP . Versões anteriores do ONTAP não oferecem suporte para backup de volumes de proteção SnapLock .

Veja a lista completa de volumes suportados no "Saiba mais sobre o NetApp Backup and Recovery" .

Indexação para processo de Pesquisa e Restauração na página Volumes

Antes de poder usar a Pesquisa e Restauração, você precisa habilitar a "Indexação" em cada sistema de origem do qual deseja restaurar dados de volume. Isso permite que o Catálogo Indexado rastreie os arquivos de backup de cada volume. A página Volumes agora mostra o status de indexação:

- Indexado: Os volumes foram indexados.
- Em andamento
- Não indexado
- Indexação pausada
- Erro
- Não habilitado

27 de setembro de 2024

Esta versão do NetApp Backup and Recovery inclui as seguintes atualizações.

Suporte ao Podman no RHEL 8 ou 9 com Navegar e Restaurar

O NetApp Backup and Recovery agora oferece suporte a restaurações de arquivos e pastas no Red Hat Enterprise Linux (RHEL) versões 8 e 9 usando o mecanismo Podman. Isso se aplica ao método Navegar e

Restaurar do NetApp Backup and Recovery.

A versão 3.9.40 do agente do console oferece suporte a determinadas versões do Red Hat Enterprise Linux 8 e 9 para qualquer instalação manual do software do agente do console em um host RHEL 8 ou 9, independentemente do local, além dos sistemas operacionais mencionados no "requisitos do host" . Essas versões mais recentes do RHEL exigem o mecanismo Podman em vez do mecanismo Docker. Anteriormente, o NetApp Backup and Recovery tinha duas limitações ao usar o mecanismo Podman. Essas limitações foram removidas.

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

Indexação de catálogo mais rápida melhora a Pesquisa e Restauração

Esta versão inclui um índice de catálogo aprimorado que conclui a indexação de base muito mais rápido. A indexação mais rápida permite que você use o recurso Pesquisar e Restaurar mais rapidamente.

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

Limitações conhecidas com o NetApp Backup and Recovery para volumes ONTAP

Plataformas, dispositivos ou recursos que não funcionam ou não funcionam bem com esta versão estão listados aqui. Leia estas limitações com atenção.

- O NetApp Backup and Recovery pode fazer backup do Cloud Volumes ONTAP em um armazenamento de objetos nas regiões da AWS China (incluindo Pequim e Ningxia); no entanto, talvez seja necessário modificar manualmente as políticas de identidade e acesso primeiro.

  Para obter detalhes sobre como criar um agente de console na AWS, consulte "Instalando um agente de console na AWS" .

  Para mais detalhes, consulte a postagem do blog "Blog de recursos de backup e recuperação da NetApp , maio de 2023" .

- O NetApp Backup and Recovery não oferece suporte às regiões do Microsoft Azure China.

  Para obter detalhes sobre como criar um agente de console no Azure, consulte "Instalando um agente de console no Azure" .

- O NetApp Backup and Recovery não oferece suporte a backups de volumes FlexCache .

Limitações de replicação para volumes ONTAP

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

  Não há limitação para volumes FlexVol - você pode selecionar todos os volumes FlexVol no seu sistema e atribuir as mesmas políticas de backup.

- A seguinte funcionalidade é suportada em "Replicação NetApp" , mas não ao usar o recurso de replicação do NetApp Backup and Recovery:
  - Não há suporte para uma configuração em cascata onde a replicação ocorre do volume A para o volume B e do volume B para o volume C. O suporte inclui a replicação do volume A para o volume B.

- Não há suporte para replicação de dados de e para o FSx para sistemas ONTAP .
- Não há suporte para criar uma replicação única de um volume.

- Ao criar replicações de sistemas ONTAP locais, se a versão do ONTAP no sistema Cloud Volumes ONTAP de destino for 9.8, 9.9 ou 9.11, somente políticas de mirror-vault serão permitidas.

Limitações de backup para objeto para volumes ONTAP

- Ao fazer backup de dados, o NetApp Backup and Recovery não manterá o NetApp Volume Encryption (NVE). Isso significa que os dados criptografados no volume NVE serão descriptografados enquanto os dados estiverem sendo transferidos para o destino e a criptografia não será mantida.

  Para obter uma explicação sobre esses tipos de criptografia, consultehttps://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html["Visão geral da configuração da criptografia de volume do NetApp"^] .

- Se snapshots de retenção de longo prazo forem habilitados em um volume de destino do SnapMirror usando o agendamento na política do SnapMirror , os snapshots serão criados diretamente no volume de destino. Nesse caso, você não deve fazer backup desses volumes usando o NetApp Backup and Recovery porque esses instantâneos não serão movidos para o armazenamento de objetos.
- Ao fazer backup de dados, o NetApp Backup and Recovery não manterá o NetApp Volume Encryption (NVE). Isso significa que os dados criptografados no volume NVE serão descriptografados enquanto os dados estiverem sendo transferidos para o destino e a criptografia não será mantida.

  Para obter uma explicação sobre esses tipos de criptografia, consultehttps://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html["Visão geral da configuração da criptografia de volume do NetApp"^] .

- Se snapshots de retenção de longo prazo forem habilitados em um volume de destino do SnapMirror usando o agendamento na política do SnapMirror , os snapshots serão criados diretamente no volume de destino. Nesse caso, você não deve fazer backup desses volumes usando o NetApp Backup and Recovery porque esses instantâneos não serão movidos para o armazenamento de objetos.
- 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 editá-la para criar até 4.000 backups.
- Ao fazer backup de volumes de proteção de dados (DP):
  - Relacionamentos com os rótulos do SnapMirror `app_consistent` e `all_source_snapshot` não será feito 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 NetApp Backup and Recovery faça backup deles.
- Os backups de volume do FlexGroup não podem ser movidos para armazenamento de arquivamento.
- Os backups de volume do FlexGroup podem usar proteção DataLock e Ransomware se o cluster estiver executando o ONTAP 9.13.1 ou superior.
- O backup de volume SVM-DR é suportado com as seguintes restrições:
  - Os backups são suportados somente pelo ONTAP secundário.
  - A política de Snapshot aplicada ao volume deve ser uma das políticas reconhecidas pelo NetApp Backup and Recovery, 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 mostrado na lista de

volumes que podem ser submetidos a backup.

    - O SVM-DR e o backup e a recuperação de volume funcionam de forma totalmente independente quando o backup é feito da origem ou do destino. A única restrição é que o SVM-DR não replica o relacionamento de nuvem do SnapMirror . No cenário de DR, quando o SVM fica online no local secundário, você deve atualizar manualmente o relacionamento da nuvem do SnapMirror .

- Suporte ao MetroCluster :
    - Ao usar o ONTAP 9.12.1 GA ou superior, o backup é suportado quando conectado ao sistema primário. Toda a configuração de backup é transferida para o sistema secundário para que os backups na nuvem continuem automaticamente após a troca. Você não precisa configurar o backup no sistema secundário (na verdade, você está impedido de fazer isso).
    - Ao usar o ONTAP 9.12.0 e versões anteriores, o backup é suportado apenas no sistema secundário do ONTAP .
    - Backups de volumes FlexGroup não são suportados no momento.
- O backup de volume ad-hoc usando o botão **Fazer backup agora** não é suportado em volumes de proteção de dados.
- Configurações SM-BC não são suportadas.
- O ONTAP não oferece suporte ao fan-out de relacionamentos do SnapMirror de um único volume para vários armazenamentos de objetos; portanto, essa configuração não é suportada pelo NetApp Backup and Recovery.
- O modo WORM/Compliance em um armazenamento de objetos é suportado no Amazon S3, Azure e StorageGRID no momento. Isso é conhecido como recurso DataLock e deve ser gerenciado usando as configurações do NetApp Backup and Recovery, não usando a interface do provedor de nuvem.

Restaurar limitações para volumes ONTAP

Essas limitações se aplicam aos métodos Pesquisar e Restaurar e Navegar e Restaurar para restaurar arquivos e pastas, a menos que sejam especificamente indicados.

- O Browse & Restore pode restaurar até 100 arquivos individuais por vez.
- O Search & Restore pode restaurar 1 arquivo por vez.
- Ao usar o ONTAP 9.13.0 ou superior, o Browse & Restore e o Search & Restore podem restaurar uma pasta junto com todos os arquivos e subpastas dentro dela.

  Ao usar uma versão do ONTAP superior à 9.11.1, mas anterior à 9.13.0, a operação de restauração pode restaurar apenas a pasta selecionada e os arquivos nela contidos - nenhuma subpasta ou arquivo em subpastas será restaurado.

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

- A restauração de diretório/pasta é suportada para dados que residem no armazenamento de arquivo somente quando o cluster está executando o ONTAP 9.13.1 e superior.
- A restauração de diretório/pasta é suportada para dados protegidos usando DataLock somente quando o cluster está executando o ONTAP 9.13.1 e superior.
- Atualmente, a restauração de diretórios/pastas não é suportada por replicações e/ou snapshots locais.
- A restauração de volumes FlexGroup para volumes FlexVol ou de volumes FlexVol para volumes FlexGroup não é suportada.
- O arquivo que está sendo restaurado deve estar usando o mesmo idioma do 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 backup de um volume DP e decidir quebrar o relacionamento do SnapMirror com esse volume, não será possível restaurar os arquivos para esse volume, a menos que você também exclua o relacionamento do SnapMirror ou inverta a direção do SnapMirror .
- Limitações da restauração rápida:
  - O local de destino deve ser um sistema Cloud Volumes ONTAP usando ONTAP 9.13.0 ou superior.
  - Não é compatível com backups localizados em armazenamento arquivado.
  - Os volumes FlexGroup são suportados somente se o sistema de origem do qual o backup em nuvem foi criado estiver executando o ONTAP 9.12.1 ou superior.
  - Os volumes SnapLock são suportados somente se o sistema de origem do qual o backup em nuvem foi criado estiver executando o ONTAP 9.11.0 ou superior.

Limitações conhecidas do NetApp Backup and Recovery para cargas de trabalho do Microsoft SQL Server

Plataformas, dispositivos ou recursos que não funcionam ou não funcionam bem com esta versão estão listados aqui. Leia estas limitações com atenção.

Suporte ao ciclo de vida do clone

- A clonagem do armazenamento de objetos não é suportada.
- Operações de clonagem em massa não são suportadas para clones sob demanda.
- A escolha de grupos I não é suportada.
- A escolha de opções de QOS (taxa de transferência máxima) não é suportada.

Somente modo de implantação padrão

Esta versão do NetApp Backup and Recovery funciona apenas no modo de implantação padrão, não nos modos restrito ou privado.

Restrição de nome de cluster do Windows

O nome do cluster do Windows não pode conter um caractere de sublinhado (_).

Problemas de migração do SnapCenter

A migração de recursos do SnapCenter para o NetApp Backup and Recovery tem as seguintes limitações.

Para obter detalhes sobre como as políticas do SnapCenter migram para as políticas de backup e recuperação do NetApp , consulte"Políticas no SnapCenter comparadas com aquelas no NetApp Backup and Recovery" .

Limitações do grupo de recursos

Se todos os recursos em um grupo de recursos estiverem protegidos e um desses recursos também estiver protegido fora do grupo de recursos, a migração do SnapCenter será bloqueada.

Solução alternativa: proteja o recurso em um grupo de recursos ou sozinho, mas não em ambos.

Recursos com várias políticas usando a mesma camada de agendamento não são suportados

Não é possível atribuir várias políticas que usam o mesmo nível de agendamento (por exemplo, por hora, diariamente, semanalmente, etc.) a um recurso. O NetApp Backup and Recovery não importará esses recursos do SnapCenter.

Solução alternativa: Anexe apenas uma política usando a mesma camada de agendamento a um recurso.

As políticas horárias devem começar no início da hora

Se você tiver uma política do SnapCenter que se repete a cada hora, mas não usa intervalos no início da hora, o NetApp Backup and Recovery não importará o recurso. Por exemplo, políticas com agendamentos de 1:30, 2:30, 3:30, etc. não são suportadas, enquanto políticas com agendamentos de 1:00, 2:00, 3:00, etc. são suportadas.

Solução alternativa: use uma política que se repita em intervalos de 1 hora, começando no início da hora.

Políticas diárias e mensais vinculadas a um recurso não são suportadas

Se uma política do SnapCenter for repetida em intervalos de um dia e de um mês, o NetApp Backup and Recovery não importará a política.

Por exemplo, você não pode anexar uma política diária (com menos ou igual a 7 dias ou mais de 7 dias) a um recurso e também anexar uma política mensal ao mesmo recurso.

Solução alternativa: use uma política que utilize um intervalo diário ou mensal, mas não ambos.

Políticas de backup sob demanda não migradas

O NetApp Backup and Recovery não importa políticas de backup sob demanda do SnapCenter.

Políticas de backup somente de log não migradas

O NetApp Backup and Recovery não importa políticas de backup somente de log do SnapCenter. Se uma política do SnapCenter incluir backups somente de log, o NetApp Backup and Recovery não importará o recurso.

Solução alternativa: use uma política no SnapCenter que use mais do que apenas backups somente de log.

Mapeamento de host

O SnapCenter não tem clusters de armazenamento de mapas ou SVMs para os recursos dos hosts, mas o NetApp Backup and Recovery tem. O cluster ONTAP local ou SVM não será mapeado para um host nas versões de visualização do NetApp Backup and Recovery. Além disso, o NetApp Console não oferece suporte a SVMs.

Solução alternativa: antes de importar recursos do SnapCenter, crie um sistema no NetApp Backup and Recovery para todos os sistemas de armazenamento ONTAP locais registrados no SnapCenter local. Em seguida, importe os recursos desse cluster do SnapCenter para o NetApp Backup and Recovery.

Horários não em intervalos de 15 minutos

Se você tiver uma programação de política do SnapCenter que começa em um determinado horário e se repete em intervalos diferentes de 15 minutos, o NetApp Backup and Recovery não importará a programação.

Solução alternativa: use o SnapCenter para ajustar a política para que ela seja repetida em intervalos de 15 minutos.

Suporte limitado para software de gerenciamento de virtualização

Ao proteger cargas de trabalho do KVM, o NetApp Backup and Recovery não oferece suporte à descoberta de cargas de trabalho do KVM quando um software de gerenciamento de virtualização, como Apache CloudStack ou Red Hat OpenShift Virtualization, está em uso.

Limitações conhecidas do NetApp Backup and Recovery para cargas de trabalho VMware

Plataformas, dispositivos ou recursos que não funcionam ou não funcionam bem com esta versão estão listados aqui. Leia estas limitações com atenção.

As seguintes ações não são suportadas na versão de pré-visualização das cargas de trabalho do VMware no NetApp Backup and Recovery:

- Monte
- Desmontar
- Restaurar para local alternativo
- Restaurar VMDK
- Anexar VMDK
- Desanexar VMDK
- Suporte vVol
- Suporte NVMe
- Integração de e-mail
- Editar política
- Editar grupo de proteção
- Suporte ao controle de acesso baseado em função (RBAC)

Limitações conhecidas com o NetApp Backup and Recovery para cargas de trabalho do Hyper-V

Plataformas, dispositivos ou recursos que não funcionam ou não funcionam bem com esta versão estão listados aqui. Leia estas limitações com atenção.

As seguintes ações não são suportadas na versão de visualização privada das cargas de trabalho do Hyper-V no NetApp Backup and Recovery:

- Criar grupos de recursos

- Discos de abrangência (em vários compartilhamentos CIFS)
- Proteja VMs em SAN
- Restaurar do armazenamento de objetos
- Proteja hosts Hyper-V agrupados usando o System Center Virtual Machine Manager (SCVMM)

Limitações conhecidas do NetApp Backup and Recovery para cargas de trabalho KVM

Plataformas, dispositivos ou recursos que não funcionam ou não funcionam bem com esta versão estão listados aqui. Leia estas limitações com atenção.

As seguintes ações e configurações não são suportadas na versão de visualização privada das cargas de trabalho do KVM no NetApp Backup and Recovery:

Ações não suportadas

As seguintes ações não são suportadas na versão de visualização privada:

- Clonar, montar ou desmontar VMs
- Restaurar VMs para um local alternativo
- Proteja VMs armazenadas em SAN
- Proteger aplicativos
- Backup ou restauração de armazenamentos de objetos
- Editar grupos de proteção
- Crie grupos de proteção usando VMs de vários hosts KVM
- Crie backups definidos pelo usuário (somente backups iniciados no NetApp Console são suportados)

Configurações não suportadas

As seguintes configurações não são suportadas:

- Controle de acesso baseado em função (RBAC)
- Discos diretamente conectados ao host KVM
- Discos distribuídos por vários pontos de montagem ou compartilhamentos NFS
- Formato de disco RAW
- Tipos de pool de armazenamento diferentes de NetFS (somente NetFS é suportado)

Limitações conhecidas com o NetApp Backup and Recovery para cargas de trabalho Oracle

Plataformas, dispositivos ou recursos que não funcionam ou não funcionam bem com esta versão estão listados aqui. Leia estas limitações com atenção.

As seguintes ações não são suportadas na versão de visualização privada das cargas de trabalho do Oracle

Database no NetApp Backup and Recovery:

- Backup offline
- Clone
- Configuração ASM
- Protegendo bancos de dados armazenados em SAN

O Oracle Database é suportado apenas como uma implantação autônoma usando NFS na versão de visualização privada das cargas de trabalho do Oracle.

Começar

Saiba mais sobre o NetApp Backup and Recovery

O NetApp Backup and Recovery é um serviço de dados que fornece proteção de dados eficiente, segura e econômica para todas as suas cargas de trabalho ONTAP , incluindo volumes, bancos de dados, máquinas virtuais e cargas de trabalho do Kubernetes.

O suporte para backup e recuperação já está integrado em todos os sistemas ONTAP , portanto não há necessidade de hardware adicional, licenças de software ou gateways de mídia. Isso torna as operações de backup simples e econômicas. O console NetApp simplifica a implementação de qualquer estratégia de backup, incluindo todo o espectro de variantes de backup 3-2-1, sem a necessidade de vários gerentes de recursos ou pessoal especializado.

> A documentação sobre a proteção de cargas de trabalho VMware, KVM, Hyper-V e Kubernetes é fornecida como uma prévia da tecnologia. Com esta oferta de visualização, a NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da disponibilidade geral.

O que você pode fazer com o NetApp Backup and Recovery

Use o NetApp Backup and Recovery para atingir os seguintes objetivos:

- * Cargas de trabalho de volume ONTAP *:
  - Crie snapshots locais, replique para armazenamento secundário e faça backup de volumes ONTAP de sistemas ONTAP locais ou Cloud Volumes ONTAP para armazenamento de objetos em sua conta de nuvem pública ou privada.
  - Crie backups incrementais permanentes em nível de bloco que são armazenados em outro cluster ONTAP e no armazenamento de objetos na nuvem.
  - Use o NetApp Backup and Recovery junto com o SnapCenter.
  - Consulte "Proteger volumes ONTAP" .
- **Cargas de trabalho do Microsoft SQL Server**:
  - Faça backup de instâncias e bancos de dados do Microsoft SQL Server do ONTAP local, Cloud Volumes ONTAP ou Amazon FSx for NetApp ONTAP.
  - Restaurar bancos de dados do Microsoft SQL Server.
  - Clonar bancos de dados do Microsoft SQL Server.
  - Use o NetApp Backup and Recovery sem o SnapCenter.
  - Consulte "Proteja as cargas de trabalho do Microsoft SQL Server" .
- **Cargas de trabalho VMware (visualização com nova interface de usuário sem o SnapCenter Plug-in for VMware vSphere)**:
  - Proteja suas VMs e armazenamentos de dados VMware com o NetApp Backup and Recovery.
  - Faça backup de cargas de trabalho do VMware no Amazon Web Services S3 ou StorageGRID (para visualização).
  - Restaure dados do VMware da nuvem para o vCenter local.

    - Use o NetApp Backup and Recovery sem o SnapCenter Plug-in for VMware vSphere.
    - Consulte "Proteja as cargas de trabalho do VMware" .
- **Cargas de trabalho VMware (com SnapCenter Plug-in for VMware vSphere)**:
    - Faça backup de VMs e armazenamentos de dados no Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform e StorageGRID e restaure as VMs de volta para o host SnapCenter Plug-in for VMware vSphere local.
    - Restaure dados de VM da nuvem para o vCenter local com o NetApp Backup and Recovery. Você pode restaurar a VM exatamente no mesmo local de onde o backup foi feito ou em um local alternativo.
    - Use o NetApp Backup and Recovery junto com o SnapCenter Plug-in for VMware vSphere.
    - Consulte "Proteja as cargas de trabalho do VMware" .
- **Cargas de trabalho KVM (visualização)**:
    - Fazer backup e restaurar máquinas virtuais
    - Fazer backup de pools de armazenamento KVM
    - Use grupos de proteção para gerenciar tarefas de backup
    - Consulte "Proteja cargas de trabalho KVM" .
- **Cargas de trabalho do Hyper-V (visualização)**:
    - Fazer backup e restaurar máquinas virtuais
    - Use grupos de proteção para gerenciar tarefas de backup
    - Consulte "Proteja as cargas de trabalho do Hyper-V" .
- **Cargas de trabalho Oracle (visualização)**:
    - Fazer backup e restaurar bancos de dados e logs
    - Use grupos de proteção para gerenciar tarefas de backup
    - Crie políticas para gerenciar backups de banco de dados e logs
    - Protegendo um banco de dados com uma arquitetura de backup 3-2-1
    - Configurar retenção de backup
    - Montar e desmontar backups do ARCHIVELOG
    - Consulte "Proteja as cargas de trabalho do Oracle" .
- **Cargas de trabalho do Kubernetes (visualização)**:
    - Gerencie e proteja seus aplicativos e recursos do Kubernetes em um só lugar.
    - Use políticas de proteção para estruturar seus backups incrementais.
    - Restaure aplicativos e recursos para os mesmos clusters e namespaces ou para clusters diferentes.
    - Use o NetApp Backup and Recovery sem o SnapCenter.
    - Consulte "Proteja as cargas de trabalho do Kubernetes" .

Benefícios de usar o NetApp Backup and Recovery

O NetApp Backup and Recovery oferece os seguintes benefícios:

- **Eficiente**: o NetApp Backup and Recovery executa replicação incremental contínua em nível de bloco, o que reduz significativamente a quantidade de dados replicados e armazenados. Isso ajuda a minimizar o

tráfego de rede e os custos de armazenamento.

- **Seguro**: o NetApp Backup and Recovery criptografa dados em trânsito e em repouso e usa protocolos de comunicação seguros para proteger seus dados.
- **Custo-benefício**: o NetApp Backup and Recovery usa os níveis de armazenamento de menor custo disponíveis na sua conta na nuvem, o que ajuda a reduzir custos.
- **Automatizado**: o NetApp Backup and Recovery gera backups automaticamente com base em uma programação predefinida, o que ajuda a garantir que seus dados estejam protegidos.
- **Flexível**: o NetApp Backup and Recovery permite que você restaure dados no mesmo sistema ou em sistemas diferentes, o que proporciona flexibilidade na recuperação de dados.

Custo

A NetApp não cobra pelo uso da versão de teste. No entanto, você é responsável pelos custos associados aos recursos de nuvem que utiliza, como custos de armazenamento e transferência de dados.

Há dois tipos de custos associados ao uso do recurso de backup para objeto do NetApp Backup and Recovery com sistemas ONTAP :

- Taxas de recursos
- Taxas de serviço

Não há custo para criar cópias de instantâneos ou volumes replicados, além do espaço em disco necessário para armazenar as cópias de instantâneos e os volumes replicados.

Custos de recursos

As taxas 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.

- Para fazer backup em armazenamento de objetos, você paga ao seu provedor de nuvem pelos custos de armazenamento de objetos.

  Como o NetApp Backup and Recovery preserva a eficiência de armazenamento do volume de origem, você paga os custos de armazenamento de objetos do provedor de nuvem pelos dados *após* as eficiências do ONTAP (para a menor quantidade de dados após a aplicação da desduplicação e da compactação).

- Para restaurar dados usando o Search & Restore, certos recursos são provisionados pelo seu provedor de nuvem, e há um custo por TiB associado à quantidade de dados verificados pelas suas solicitações de pesquisa. (Esses recursos não são necessários para Navegar e Restaurar.)
  - Na AWS, "Amazona Atena" e "Cola AWS" os recursos são implantados em um novo bucket S3.
  - No Azure, um "Espaço de trabalho do Azure Synapse" e "Armazenamento do Azure Data Lake" são provisionados em sua conta de armazenamento para armazenar e analisar seus dados.
- No Google, um novo bucket é implantado e o "Serviços do Google Cloud BigQuery" são provisionados em nível de conta/projeto. endif::gcp[]
  - Se você planeja restaurar dados de volume de um arquivo de backup que foi movido para um armazenamento de objetos de arquivamento, haverá uma taxa adicional de recuperação por GiB e uma taxa por solicitação do provedor de nuvem.
  - Se você planeja verificar se há ransomware em um arquivo de backup durante o processo de restauração de dados de volume (se você habilitou o DataLock e o Ransomware Resilience para seus

backups na nuvem), você também incorrerá em custos extras de saída do seu provedor de nuvem.

Taxas de serviço

As taxas de serviço são pagas à NetApp e cobrem tanto o custo de *criação* de backups no armazenamento de objetos quanto de *restauração* de volumes ou arquivos desses backups. Você paga somente pelos dados que protege no armazenamento de objetos, calculado pela capacidade lógica de origem utilizada (*antes* das eficiências do ONTAP) dos volumes ONTAP que são copiados para o armazenamento de objetos. Essa capacidade também é conhecida como Terabytes Front-End (FETB).

Para o Microsoft SQL Server, serão aplicadas taxas quando você inicia a replicação de instantâneos para um destino ONTAP secundário ou armazenamento de objetos.

Existem três maneiras de pagar pelo serviço de Backup:

- A primeira opção é assinar com 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 oLicenciamento seção para detalhes.

Licenciamento

O NetApp Backup and Recovery está disponível como teste gratuito. Você pode usar o serviço sem uma chave de licença por um tempo limitado.

O NetApp Backup and Recovery está disponível com os seguintes modelos de consumo:

- **Traga sua própria licença (BYOL)**: uma licença adquirida da NetApp que pode ser usada com qualquer provedor de nuvem.
- **Pague conforme o uso (PAYGO)**: Uma assinatura por hora do marketplace do seu provedor de nuvem.
- **Anual**: Um contrato anual do marketplace do seu provedor de nuvem.

Uma licença de backup é necessária apenas para backup e restauração do armazenamento de objetos. A criação de cópias de snapshot e volumes replicados não requer licença.

Traga sua própria licença

O BYOL é baseado em prazo (1, 2 ou 3 anos) e em capacidade em incrementos de 1 TiB. Você paga à NetApp para usar o serviço por um período de tempo, digamos 1 ano, e por uma capacidade máxima, digamos 10 TiB.

Você receberá um número de série que deverá ser inserido no NetApp Console para habilitar o serviço. Quando qualquer um dos limites for atingido, você precisará renovar a licença. A licença Backup BYOL se aplica a todos os sistemas de origem associados à sua organização ou conta do NetApp Console.

"Aprenda a configurar licenças" .

Assinatura pré-paga

O NetApp Backup and Recovery oferece licenciamento baseado no consumo em um modelo de pagamento conforme o uso. Após assinar pelo marketplace do seu provedor de nuvem, você paga por GiB pelos dados armazenados em backup — não há pagamento inicial. Você é cobrado pelo seu provedor de nuvem por meio de sua fatura mensal.

Observe que um teste gratuito de 30 dias está disponível quando você se inscreve inicialmente com uma assinatura PAYGO.

Contrato anual

Ao usar a AWS, dois contratos anuais estão disponíveis por 1, 2 ou 3 anos:

- Um plano "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.
- Um plano "CVO Professional" que permite combinar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para Cloud Volumes ONTAP Volumes cobrados nesta licença (a capacidade de backup não é contabilizada na licença). endif::aws[]

Ao usar o Azure, dois contratos anuais estão disponíveis por 1, 2 ou 3 anos:

- Um plano "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.
- Um plano "CVO Professional" que permite combinar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para Cloud Volumes ONTAP Volumes cobrados nesta licença (a capacidade de backup não é contabilizada na licença). endif::azure[]

Ao usar o GCP, você pode solicitar uma oferta privada da NetApp e, em seguida, selecionar o plano ao assinar no Google Cloud Marketplace durante a ativação do NetApp Backup and Recovery. endif::gcp[]

Fontes de dados, sistemas e destinos de backup suportados

Fontes de dados de carga de trabalho suportadas

O NetApp Backup and Recovery protege as seguintes cargas de trabalho:

- Volumes ONTAP
- Instâncias e bancos de dados do Microsoft SQL Server para NFS físico, VMware Virtual Machine File System (VMFS) e VMware Virtual Machine Disk (VMDK)
- VMs e datastores VMware
- Cargas de trabalho KVM (visualização)
- Cargas de trabalho do Hyper-V (visualização)
- Cargas de trabalho do Kubernetes (visualização)

Sistemas suportados

- ONTAP SAN local (protocolo iSCSI) e NAS (usando protocolos NFS e CIFS) com ONTAP versão 9.8 e superior
- Cloud Volumes ONTAP 9.8 ou superior para AWS (usando SAN e NAS)
- Cloud Volumes ONTAP 9.8 ou superior para Microsoft Azure (usando SAN e NAS)
- Amazon FSx for NetApp ONTAP

Destinos de backup suportados

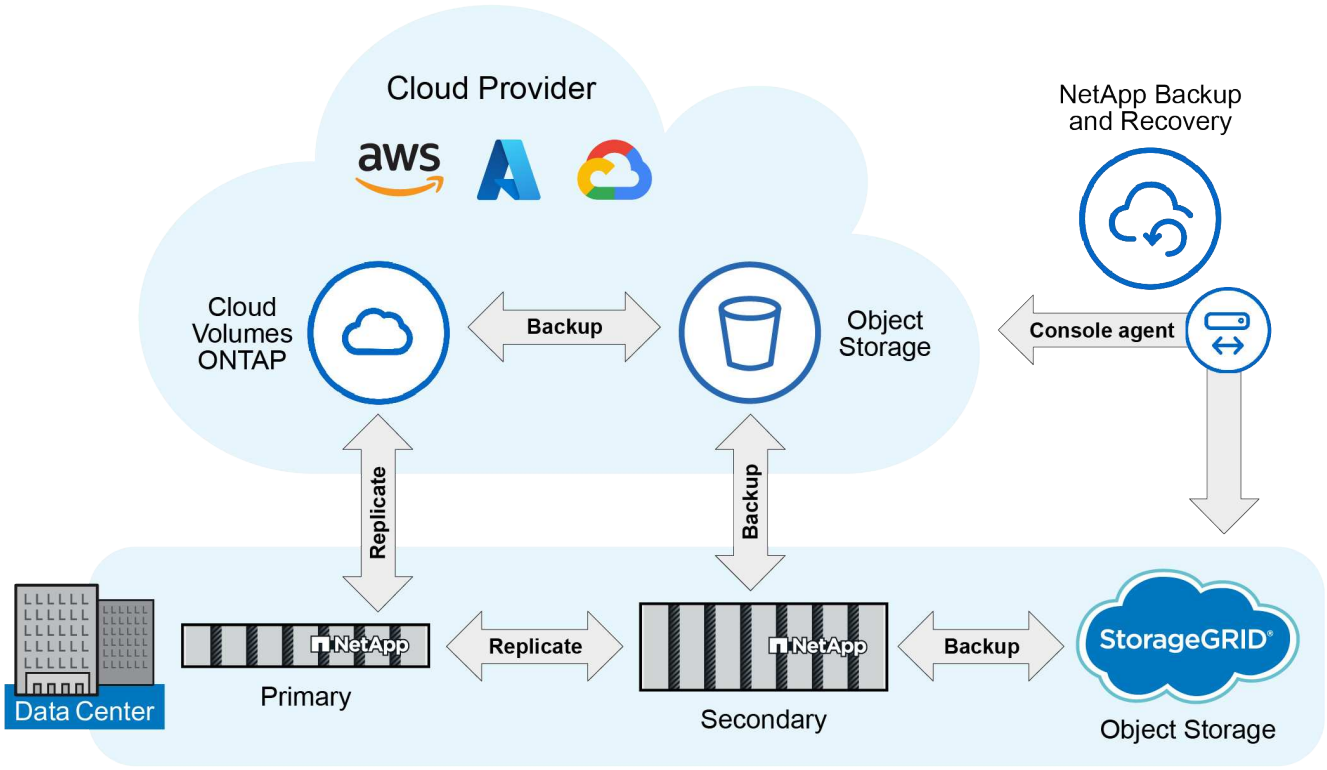
- Amazon Web Services (AWS) S3
- Microsoft Azure Blob (não disponível para cargas de trabalho VMware na versão de visualização)
- StorageGRID

- ONTAP S3 (não disponível para cargas de trabalho VMware na versão de visualização)

Como funciona o NetApp Backup and Recovery

Quando você ativa o NetApp Backup and Recovery, o serviço executa um backup completo dos seus dados. Após o backup inicial, todos os backups adicionais são incrementais. Isso mantém o tráfego de rede no mínimo.

A imagem a seguir mostra o relacionamento entre os componentes.



O armazenamento primário para o objeto também é suportado, não apenas do armazenamento secundário para o armazenamento de objetos.

Onde os backups residem em locais de armazenamento de objetos

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

- Na AWS, o NetApp Console permite que o "Recurso de bloqueio de acesso público do Amazon S3" no bucket S3. endif::aws[]
- No Azure, o NetApp Console usa um grupo de recursos novo ou existente com uma conta de armazenamento para o contêiner Blob. o Console "bloqueia o acesso público aos seus dados de blob" por padrão. endif::azure[]
- No StorageGRID, o Console usa uma conta de armazenamento existente para o bucket de armazenamento de objetos.

- No ONTAP S3, o Console usa uma conta de usuário existente para o bucket S3.

As cópias de backup estão associadas à sua organização do NetApp Console

As cópias de backup são associadas à organização do NetApp Console na qual o agente do Console reside. "Saiba mais sobre identidade e acesso do NetApp Console" .

Se você tiver vários agentes do Console na mesma organização do NetApp Console, cada agente do Console exibirá a mesma lista de backups.

Termos que podem ajudar você com o NetApp Backup and Recovery

Você pode se beneficiar ao entender alguma terminologia relacionada à proteção.

- **Proteção**: Proteção no NetApp Backup and Recovery significa garantir que snapshots e backups imutáveis ocorram regularmente em um domínio de segurança diferente usando políticas de proteção.
- **Carga de trabalho**: uma carga de trabalho no NetApp Backup and Recovery pode incluir volumes ONTAP , instâncias e bancos de dados do Microsoft SQL Server; VMs e datastores do VMware; ou clusters e aplicativos do Kubernetes.

Pré-requisitos do NetApp Backup and Recovery

Comece a usar o NetApp Backup and Recovery verificando a prontidão do seu ambiente operacional, do agente do NetApp Console e da conta do NetApp Console. Para usar o NetApp Backup and Recovery, você precisará destes pré-requisitos.

Pré-requisito para ONTAP 9.8 e posterior

Uma licença ONTAP One deve ser habilitada na instância ONTAP local.

Pré-requisitos para backups no armazenamento de objetos

Para usar o armazenamento de objetos como destinos de backup, você precisa de uma conta no AWS S3, Microsoft Azure Blob, StorageGRID ou ONTAP e as permissões de acesso apropriadas configuradas.

- "Proteja seus dados de volume ONTAP"

Requisitos para proteger cargas de trabalho do Microsoft SQL Server

Para usar o NetApp Backup and Recovery para cargas de trabalho do Microsoft SQL Server, você precisa dos seguintes pré-requisitos de sistema host, espaço e dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Item	Requisitos
Versões do Microsoft SQL Server	A versão 2012 e posteriores são suportadas pelo VMware Virtual Machine File System (VMFS) e pelo VMware Virtual Machine Disk (VMDK) NFS.
Versão do SnapCenter Server	O SnapCenter Server versão 5.0 ou superior é necessário se você for importar seus dados existentes do SnapCenter para o NetApp Backup and Recovery. Se você já tem o SnapCenter, primeiro verifique se atendeu aos pré-requisitos antes de importar do SnapCenter. Ver "Pré-requisitos para importar recursos do SnapCenter" .
RAM mínima para o plug-in no host do SQL Server	1 GB
Espaço mínimo de instalação e log para o plug-in no host do SQL Server	5 GB Aloque espaço em disco suficiente e monitore o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de backups realizados e da frequência das operações de proteção de dados. Se não houver espaço suficiente, os logs não serão criados para as operações.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell 7.4.2 Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Requisitos para proteger cargas de trabalho do VMware

Você precisa de requisitos específicos para descobrir e proteger suas cargas de trabalho do VMware.

Suporte de software

- Os armazenamentos de dados NFS e VMFS são suportados. Os vVols não são suportados.
- Versões NFS suportadas: NFS 3 e NFS 4.1
- Versões do VMware ESXi Server suportadas: 7.0U1 e superior
- Versões do VMware vCenter vSphere suportadas: 7.0U1 e superior
- Endereços IP: IPv4 e IPv6
- VMware TLS: 1.2, 1.3

Requisitos de conexão e porta para proteger cargas de trabalho do VMware

Tipo de porta	Porta pré-configurada
Porta do servidor VMware ESXi	443 (HTTPS), bidirecional. O recurso Restauração de arquivo convidado usa esta porta.
Porta do VMware vSphere vCenter Server	Se estiver protegendo VMs vVol, você deverá usar a porta 443.
Cluster de armazenamento ou porta de VM de armazenamento	443 (HTTPS), bidirecional. 80 (HTTP), bidirecional. Esta porta é usada para comunicação entre o dispositivo virtual e a VM de armazenamento ou o cluster que contém a VM de armazenamento.

Requisitos de controle de acesso baseado em função (RBAC) para proteger cargas de trabalho do VMware

A conta de administrador do vCenter deve ter os privilégios necessários do vCenter.

Para obter uma lista de privilégios do vCenter necessários, consulte "Privilégios necessários do SnapCenter Plug-in for VMware vSphere vCenter" .

Requisitos para proteger cargas de trabalho KVM

Você precisa de requisitos específicos para descobrir e proteger máquinas virtuais KVM.

- Uma distribuição Linux moderna executando a versão do kernel 5.14.0-503.22.1.el9_5.x86_64 (longo prazo) ou posterior
- Certifique-se de que o tráfego de entrada para a porta 22 seja permitido do agente do Console para o host KVM
- QEMU Guest Agent versão 9.0.0 ou posterior
- libvirt versão 10.5.0 ou posterior

Requisitos para proteger cargas de trabalho Oracle

Garanta que seu ambiente atenda aos requisitos específicos para descobrir e proteger recursos Oracle.

- Banco de dados Oracle:
  - O Oracle 19C e 21C são suportados em uma implantação autônoma.
  - O Oracle Database deve ser implantado no armazenamento NetApp ONTAP primário ou secundário.
- Suporte de armazenamento de objetos:
  - Armazenamento de Objetos do Azure
  - Amazon AWS
  - NetApp StorageGRID
  - ONTAP S3

Requisitos para proteger aplicativos Kubernetes

Você precisa de requisitos específicos para descobrir recursos do Kubernetes e proteger seus aplicativos Kubernetes.

Para requisitos do NetApp Console, consulteNo console NetApp .

- Um sistema ONTAP primário (ONTAP 9.16.1 ou posterior)
- Um cluster do Kubernetes - As distribuições e versões do Kubernetes suportadas incluem:
  - Anthos On-Prem (VMware) e Anthos em bare metal 1.16
  - Kubernetes 1.27 - 1.33
  - OpenShift 4.10 - 4.18
  - Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
  - Suse Rancher
- NetApp Trident 24.10 ou posterior
- NetApp Trident Protect 25.07 ou posterior (instalado durante a descoberta da carga de trabalho do Kubernetes)
- NetApp Trident Protect Connector 25.07 ou posterior (instalado durante a descoberta da carga de trabalho do Kubernetes)
  - Certifique-se de que a porta TCP 443 não esteja filtrada na direção de saída entre o cluster Kubernetes, o Trident Protect Connector e o proxy Trident Protect.

Requisitos para proteger cargas de trabalho do Hyper-V

Certifique-se de que sua instância do Hyper-V atenda aos requisitos específicos para descobrir e proteger máquinas virtuais.

- Requisitos de software para o host Hyper-V:
  - Edições do Microsoft Hyper-V 2019, 2022 e 2025
  - Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes)
  - PowerShell 7.4.2 ou posterior
  - Certifique-se de que o tráfego HTTPS bidirecional seja permitido para as seguintes portas nas configurações do Firewall do Windows:
    - 8144 (Plug-in NetApp para Hyper-V)
    - 8145 (Plug-in NetApp para Windows)
- Requisitos de hardware para o host Hyper-V:
  - Hosts autônomos e agrupados pela FCI são suportados
  - Mínimo de 1 GB de RAM para o plug-in NetApp Hyper-V no host Hyper-V
  - 5 GB de espaço mínimo para instalação e log do plug-in no host Hyper-V

> Certifique-se de alocar espaço em disco suficiente no host Hyper-V para a pasta de logs e monitore regularmente seu uso. O espaço necessário depende da frequência com que ocorrem backups e operações de proteção de dados. Se não houver espaço suficiente, os logs não serão gerados.

- Requisitos de configuração do NetApp ONTAP :
  - Um sistema ONTAP primário (ONTAP 9.14.1 ou posterior)
  - Para implantações do Hyper-V usando compartilhamentos CIFS para armazenar dados de máquina virtual, certifique-se de que a propriedade de compartilhamento de disponibilidade contínua esteja

habilitada no sistema ONTAP . Consulte o "Documentação do ONTAP" para obter instruções.

No console NetApp

Certifique-se de que o NetApp Console atenda aos seguintes requisitos.

- Um usuário do Console deve ter a função e os privilégios necessários para executar operações em cargas de trabalho do Microsoft SQL Server e do Kubernetes. Para descobrir os recursos, você precisa ter a função de Superadministrador do NetApp Backup and Recovery. Ver"Acesso baseado em função do NetApp Backup and Recovery aos recursos" para obter detalhes sobre as funções e permissões necessárias para executar operações no NetApp Backup and Recovery.
- Uma organização do Console com pelo menos um agente do Console ativo que se conecta a clusters ONTAP locais ou ao Cloud Volumes ONTAP.
- Pelo menos um sistema de console com um cluster NetApp ONTAP local ou Cloud Volumes ONTAP .
- Um agente de console

  Consulte "Aprenda a configurar um agente de console" e "requisitos padrão do NetApp Console" .

  - A versão de visualização requer o sistema operacional Ubuntu 22.04 LTS para o agente do Console.

Configurar o NetApp Console

O próximo passo é configurar o Console e o NetApp Backup and Recovery.

Análise "requisitos padrão do NetApp Console" .

Criar um agente de console

Você deve entrar em contato com sua equipe de produtos da NetApp para experimentar este serviço. Então, quando você usar o agente do Console, ele incluirá os recursos apropriados para o serviço.

Para criar um agente do Console no NetApp Console antes de usar o serviço, consulte a documentação do Console que descreve "como criar um agente de console" .

Onde instalar o agente do Console

Para concluir uma operação de restauração, o agente do Console pode ser instalado nos seguintes locais:

- Para o Amazon S3, o agente do Console pode ser implantado em suas instalações.
- Para o Azure Blob, o agente do Console pode ser implantado em suas instalações.
- Para o StorageGRID, o agente do Console deve ser implantado em suas instalações; com ou sem acesso à Internet.
- Para o ONTAP S3, o agente do Console pode ser implantado em suas instalações (com ou sem acesso à Internet) ou em um ambiente de provedor de nuvem

Referências a "sistemas ONTAP locais" incluem sistemas FAS e AFF .

Configurar licenciamento para NetApp Backup and Recovery

Você pode licenciar o NetApp Backup and Recovery comprando uma assinatura de

pagamento conforme o uso (PAYGO) ou anual do mercado para * NetApp Intelligent Services * do seu provedor de nuvem ou comprando uma licença "traga sua própria licença" (BYOL) da NetApp. Uma licença válida é necessária para ativar o NetApp Backup and Recovery em um sistema, criar backups dos seus dados de produção e restaurar dados de backup em um sistema de produção.

Algumas notas antes de continuar lendo:

- Se você já assinou a assinatura pré-paga (PAYGO) no marketplace do seu provedor de nuvem para um sistema Cloud Volumes ONTAP , você também estará automaticamente inscrito no NetApp Backup and Recovery. Você não precisará assinar novamente.
- A licença BYOL (Bring Your Own License) do NetApp Backup and Recovery é uma licença flutuante que você pode usar em todos os sistemas associados à sua organização ou conta do NetApp Console. 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 assine também 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 no StorageGRID, você precisa de uma licença BYOL, mas não há custo para espaço de armazenamento do provedor de nuvem.

"Saiba mais sobre os custos relacionados ao uso do NetApp Backup and Recovery."

Teste gratuito de 30 dias

Um teste gratuito de 30 dias do NetApp Backup and Recovery está disponível se você assinar uma assinatura paga conforme o uso no marketplace do seu provedor de nuvem para * NetApp Intelligent Services*. O teste gratuito começa no momento em que você assina a listagem do mercado. Observe que se você pagar pela assinatura do marketplace ao implantar um sistema Cloud Volumes ONTAP e iniciar seu teste gratuito do NetApp Backup and Recovery 10 dias depois, você terá 20 dias restantes para usar o teste gratuito.

Quando o teste gratuito terminar, você será transferido automaticamente para a assinatura PAYGO sem interrupção. Se você decidir não continuar usando o NetApp Backup and Recovery, basta"cancelar o registro do NetApp Backup and Recovery do sistema" antes do término do teste e você não será cobrado.

Encerrar o teste gratuito

Se quiser continuar usando o NetApp Backup and Recovery após o término do teste gratuito, você deverá configurar uma assinatura paga. Você pode fazer isso na interface do NetApp Console navegando até a seção de cobrança e selecionando um plano de assinatura que atenda às suas necessidades. Se não quiser continuar usando o NetApp Backup and Recovery, você pode encerrar o teste gratuito.

Quando você encerra o teste gratuito sem assinar um plano pago, seus dados são excluídos automaticamente 60 dias após o término do teste gratuito. Opcionalmente, você pode fazer com que o sistema exclua seus dados imediatamente.

Passos

1. Na página inicial do NetApp Backup and Recovery, selecione **Ver avaliação gratuita**.
2. Selecione **Encerrar teste gratuito**.
3. Selecione **Excluir dados imediatamente após encerrar meu teste gratuito** para excluir seus dados

imediatamente.

4. Digite **fim do teste** na caixa.
5. Selecione **Fim** para confirmar.

Use uma assinatura PAYGO do NetApp Backup and Recovery

No pagamento conforme o uso, você pagará ao seu provedor de nuvem pelos custos de armazenamento de objetos e pelos custos de licenciamento de backup da NetApp por hora em uma única assinatura. Você deve assinar o * NetApp Intelligent Services * no Marketplace mesmo se tiver uma avaliação gratuita ou se trouxer sua própria licença (BYOL):

- A assinatura garante que não haverá interrupção do serviço após o término do teste gratuito. Quando o período de teste terminar, você será cobrado por hora, de acordo com a quantidade de dados dos quais fizer 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 por meio da sua assinatura paga conforme o uso. Por exemplo, se você tiver uma licença BYOL de 10 TiB, toda a capacidade além de 10 TiB será cobrada por meio da assinatura PAYGO.

Você não será cobrado pela sua assinatura pré-paga durante o período de teste gratuito ou se não tiver excedido sua licença BYOL.

Existem alguns planos PAYGO para NetApp Backup and Recovery:

- Um pacote "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.
- Um pacote "CVO Professional" que permite agrupar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a capacidade de backup não é contabilizada na capacidade licenciada). Esta opção não permite que você faça backup de dados ONTAP locais.

  Observe que esta opção também requer uma assinatura PAYGO de backup e recuperação, mas nenhuma cobrança será cobrada para sistemas Cloud Volumes ONTAP qualificados.

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

Use estes links para assinar o NetApp Backup and Recovery no marketplace do seu provedor de nuvem:

- AWS: "Acesse a oferta do Marketplace para NetApp Intelligent Services para obter detalhes sobre preços" .endif::aws[]
- Azul: "Acesse a oferta do Marketplace para NetApp Intelligent Services para obter detalhes sobre preços" .endif::azure[]
- Google Cloud: "Acesse a oferta do Marketplace para NetApp Intelligent Services para obter detalhes sobre preços" .endif::gcp[]

Use um contrato anual

Pague pelo NetApp Backup and Recovery anualmente adquirindo um contrato anual. Eles estão disponíveis em prazos de 1, 2 ou 3 anos.

Se você tiver um contrato anual de um marketplace, todo o consumo do NetApp Backup and Recovery será

cobrado desse contrato. Você não pode misturar e combinar um contrato de mercado anual com um BYOL.

Ao usar a AWS, há dois contratos anuais disponíveis na "Página do AWS Marketplace" para sistemas Cloud Volumes ONTAP e ONTAP locais:

- Um plano "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.

  Se você quiser usar esta opção, configure sua assinatura na página do Marketplace e então "associe a assinatura às suas credenciais da AWS" . Observe que você também precisará pagar pelos seus sistemas Cloud Volumes ONTAP usando esta assinatura de contrato anual, pois você pode atribuir apenas uma assinatura ativa às suas credenciais da AWS no Console.

- Um plano "CVO Professional" que permite combinar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a capacidade de backup não é contabilizada na capacidade licenciada). Esta opção não permite que você faça backup de dados ONTAP locais.

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

  Se quiser usar essa opção, você pode configurar o contrato anual ao criar um sistema Cloud Volumes ONTAP e o Console solicitará que você assine o AWS Marketplace. endif::aws[]

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

- Um plano "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.

  Se você quiser usar esta opção, configure sua assinatura na página do Marketplace e então "associar a assinatura às suas credenciais do Azure" . Observe que você também precisará pagar pelos seus sistemas Cloud Volumes ONTAP usando esta assinatura de contrato anual, pois você pode atribuir apenas uma assinatura ativa às suas credenciais do Azure no Console.

- Um plano "CVO Professional" que permite combinar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para o sistema Cloud Volumes ONTAP usando a licença (a capacidade de backup não é contabilizada na capacidade licenciada). Esta opção não permite que você faça backup de dados ONTAP locais.

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

  Se quiser usar essa opção, você pode configurar o contrato anual ao criar um sistema Cloud Volumes ONTAP e o Console solicitará que você assine o Azure Marketplace. endif::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 a NetApp compartilhar a oferta privada com você, você poderá selecionar o plano anual ao assinar no Google Cloud Marketplace durante a ativação do NetApp Backup and Recovery. endif::gcp[]

Use uma licença BYOL do NetApp Backup and Recovery

As licenças "traga sua própria" da NetApp oferecem prazos de 1, 2 ou 3 anos. Você paga somente pelos dados que protege, calculados pela capacidade lógica utilizada (*antes* de quaisquer eficiências) dos volumes ONTAP de origem que estão sendo copiados. Essa capacidade também é conhecida como Terabytes Front-End (FETB).

A licença BYOL NetApp Backup and Recovery é uma licença flutuante em que a capacidade total é compartilhada entre todos os sistemas associados à sua organização ou conta do NetApp Console. Para sistemas ONTAP , você pode obter uma estimativa aproximada da capacidade necessária executando o comando CLI `volume show -fields logical-used-by-afs` para os volumes que você planeja fazer backup.

Se você não tiver uma licença BYOL do NetApp Backup and Recovery, clique no ícone de bate-papo no canto inferior direito do Console para adquirir uma.

Opcionalmente, se você tiver uma licença baseada em nó não atribuída para o Cloud Volumes ONTAP que não será usada, você poderá convertê-la em uma licença do NetApp Backup and Recovery com a mesma equivalência em dólares e a mesma data de expiração. "Clique aqui para mais detalhes" .

Use o NetApp Console para gerenciar licenças BYOL. Você pode adicionar novas licenças, atualizar licenças existentes e visualizar o status da licença no Console.

"Saiba mais sobre como adicionar licenças" .

Configure destinos de backup antes de usar o NetApp Backup and Recovery

Antes de usar o NetApp Backup and Recovery, execute algumas etapas para configurar destinos de backup.

Antes de começar, revise"pré-requisitos" para garantir que seu ambiente esteja pronto.

Preparar o destino do backup

Prepare um ou mais dos seguintes destinos de backup:

- NetApp StorageGRID.

  Consulte "Descubra o StorageGRID" .

  Consulte "Documentação do StorageGRID" para obter detalhes sobre StorageGRID.

- Serviços Web da Amazon. Consulte "Documentação do Amazon S3" .

  Faça o seguinte para preparar a AWS como um destino de backup:

  - Crie uma conta na AWS.
  - Configure as permissões do S3 na AWS, listadas na próxima seção.
  - Para obter detalhes sobre como gerenciar seu armazenamento AWS no Console, consulte "Gerencie seus buckets do Amazon S3" .

- Microsoft Azure.

- Consulte "Documentação do Azure NetApp Files" .
- Crie uma conta no Azure.
- Configurar "Permissões do Azure" no Azure.
- Para obter detalhes sobre como gerenciar seu armazenamento do Azure no Console, consulte "Gerencie suas contas de armazenamento do Azure" .

Depois de configurar as opções no próprio destino de backup, você o configurará posteriormente como um destino de backup no NetApp Backup and Recovery. Para obter detalhes sobre como configurar o destino do backup no NetApp Backup and Recovery, consulte"Descubra alvos de backup" .

Configurar permissões do S3

Você precisará configurar dois conjuntos de permissões do AWS S3:

- Permissões para o agente do Console criar e gerenciar o bucket do S3.
- Permissões para o cluster ONTAP local para que ele possa ler e gravar dados no bucket S3.

Passos

1. Certifique-se de que o agente do Console tenha as permissões necessárias. Para mais detalhes, veja "Permissões de política do NetApp Console" .

   Ao criar backups nas regiões da AWS China, você precisa alterar o nome do 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. Ao ativar o serviço, o assistente de backup solicitará que você insira uma chave de acesso e uma chave secreta. Essas credenciais são passadas ao cluster ONTAP para que o ONTAP possa fazer backup e restaurar dados no bucket S3. Para isso, você precisará criar um usuário do IAM com as seguintes permissões.

   Consulte o "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"
        }
    ]
}
```

Efetue login no NetApp Backup and Recovery

Use o NetApp Console para efetuar login no NetApp Backup and Recovery.

O NetApp Backup and Recovery usa o gerenciamento de identidade e acesso para controlar o acesso que cada usuário tem a ações específicas.

Para obter detalhes sobre as ações que cada função pode executar, consulte"Funções de usuário do NetApp Backup and Recovery" .

Para efetuar login no NetApp Console, você pode usar suas credenciais do site de suporte da NetApp ou pode se inscrever para um login no NetApp Console usando seu e-mail e uma senha. "Saiba mais sobre como fazer login" .

Função necessária do NetApp Console Superadministrador de backup e recuperação ou função de administrador de restauração de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Para adicionar um agente do Console, você precisa ter a função de administrador da organização ou de superadministrador do Backup and Recovery.

Passos

1. Abra um navegador da web e vá para o "Console NetApp" .

   A página de login do NetApp Console é exibida.

2. Efetue login no Console.
3. Na navegação à esquerda do Console, selecione **Proteção** > **Backup e Recuperação**.
   - Se esta for a primeira vez que você faz login neste serviço e ainda não adicionou um sistema à página **Sistemas**, a página inicial "Bem-vindo ao novo NetApp Backup and Recovery" será exibida e mostrará uma opção para adicionar um sistema. Para obter detalhes sobre como adicionar um sistema à página **Sistemas**, consulte "Introdução ao modo padrão do NetApp Console" .
   - Se esta for a primeira vez que você faz login neste serviço e já tiver adicionado um sistema à página **Sistemas**, mas não tiver descoberto nenhum recurso, a página inicial "Bem-vindo ao novo NetApp Backup and Recovery" será exibida e mostrará uma opção para **Descobrir recursos**.
4. Se você ainda não fez isso, selecione a opção **Descobrir e gerenciar**. <<<<<<< CABEÇA
   - Para cargas de trabalho do Microsoft SQL Server, consulte"Descubra as cargas de trabalho do Microsoft SQL Server" .
   - Para cargas de trabalho VMware, consulte"Descubra as cargas de trabalho da VMware" .
   - Para cargas de trabalho KVM, consulte"Descubra cargas de trabalho KVM" .
   - Para cargas de trabalho do Hyper-V, consulte"Descubra as cargas de trabalho do Hyper-V" .
   - Para cargas de trabalho do Kubernetes, consulte"Descubra as cargas de trabalho do Kubernetes" .

+ * Para cargas de trabalho do Microsoft SQL Server, consulte"Descubra as cargas de trabalho do Microsoft SQL Server" . * Para cargas de trabalho VMware, consulte"Descubra as cargas de trabalho da VMware" . * Para cargas de trabalho KVM, consulte"Descubra cargas de trabalho KVM" . * Para cargas de trabalho Oracle, consulte"Descubra as cargas de trabalho da Oracle" . * Para cargas de trabalho do Kubernetes, consulte"Descubra as cargas de trabalho do Kubernetes" .

>>>>>>> 6b2aaa82d1d2ec0ac72303b380f289e4a01ba4c6

Descubra alvos de backup externos no NetApp Backup and Recovery

Conclua algumas etapas para descobrir ou adicionar manualmente destinos de backup externos no NetApp Backup and Recovery.

Descubra um alvo de backup

Antes de usar o NetApp Backup and Recovery, você deve configurar seus destinos de backup do Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage ou StorageGRID.

Você pode descobrir esses alvos automaticamente ou adicioná-los manualmente.

Forneça as credenciais necessárias para acessar o sistema de conta de armazenamento. Essas credenciais são usadas para descobrir as cargas de trabalho que você deseja fazer backup.

Antes de começar

Para adicionar um destino de backup externo, pelo menos uma carga de trabalho precisa ser descoberta.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione a aba **Destinos de backup externo**.
3. Selecione **Descobrir destino de backup**.
4. Selecione um dos tipos de destino de backup: **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* ou * ONTAP S3*.
5. Na seção **Escolher local das credenciais**, escolha o local onde as credenciais residem e, em seguida, escolha como associá-las.
6. Selecione **Avançar**.
7. Insira as informações de credenciais. As informações variam dependendo do tipo de destino de backup selecionado e do local das credenciais escolhido.
   - Para AWS:
     - **Nome da credencial**: insira o nome da credencial da AWS.
     - **Chave de acesso**: Digite o segredo da AWS.
     - **Chave secreta**: Insira a chave secreta da AWS.
   - Para o Azure:
     - **Nome da credencial**: insira o nome da credencial do Armazenamento de Blobs do Azure.

- **Segredo do cliente**: insira o segredo do cliente do Armazenamento de Blobs do Azure.
- **ID do aplicativo (cliente)**: selecione o ID do aplicativo do Armazenamento de Blobs do Azure.
- **ID do locatário do diretório**: insira o ID do locatário do Armazenamento de Blobs do Azure.

◦ Para StorageGRID:

- **Nome da credencial**: insira o nome da credencial do StorageGRID .
- **FQDN do nó de gateway**: insira um nome de FQDN para StorageGRID.
- **Porta**: Insira o número da porta para StorageGRID.
- **Chave de acesso**: Insira a chave de acesso do StorageGRID S3.
- **Chave secreta**: Insira a chave secreta do StorageGRID S3.

◦ Para ONTAP S3:

- **Nome da credencial**: insira o nome da credencial do ONTAP S3.
- **FQDN do nó do gateway**: insira um nome FQDN para o ONTAP S3.
- **Porta**: Digite o número da porta para o ONTAP S3.
- **Chave de acesso**: Digite a chave de acesso do ONTAP S3.
- **Chave secreta**: Digite a chave secreta do ONTAP S3.

8. Selecione **Descobrir**.

Adicionar um bucket para um destino de backup

Em vez de o NetApp Backup and Recovery descobrir buckets automaticamente, você pode adicionar manualmente um bucket a um destino de backup externo.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione **Destinos de backup externos**.
3. Selecione o alvo e à direita, selecione **Ações*** ••• **ícone e selecione *Adicionar bucket**.
4. Insira as informações do bucket. As informações variam dependendo do tipo de destino de backup selecionado.

◦ Para AWS:

- **Nome do bucket**: insira o nome do bucket S3. O prefixo "netapp-backup" é um prefixo obrigatório e é adicionado automaticamente ao nome fornecido.
- **Conta AWS**: Insira o nome da conta AWS.
- **Região do bucket**: insira a região da AWS para o bucket.
- **Habilitar bloqueio de objeto S3**: selecione esta opção para habilitar o bloqueio de objeto S3 para o bucket. O S3 Object Lock impede que objetos sejam excluídos ou substituídos por um período de retenção especificado, fornecendo uma camada adicional de proteção de dados. Você pode habilitar isso somente quando estiver criando um bucket e não poderá desativá-lo mais tarde.
  - **Modo de governança**: selecione esta opção para habilitar o modo de governança para o bucket de bloqueio de objeto do S3. O modo de governança permite que você proteja objetos de serem excluídos ou substituídos pela maioria dos usuários, mas permite que certos usuários alterem as configurações de retenção.
  - **Modo de conformidade**: selecione esta opção para habilitar o modo de conformidade para o

bucket de bloqueio de objeto do S3. O modo de conformidade impede que qualquer usuário, incluindo o usuário root, altere as configurações de retenção ou exclua objetos até que o período de retenção expire.

- **Controle de versão**: selecione esta opção para habilitar o controle de versão para o bucket S3. O controle de versão permite que você mantenha várias versões de objetos no bucket, o que pode ser útil para fins de backup e recuperação.
- **Tags**: Selecione tags para o bucket S3. Tags são pares de chave-valor que podem ser usados para organizar e gerenciar seus recursos do S3.
- **Criptografia**: Selecione o tipo de criptografia para o bucket S3. As opções são chaves gerenciadas pelo AWS S3 ou chaves do AWS Key Management Service. Se você selecionar chaves do AWS Key Management Service, deverá fornecer o ID da chave.

◦ Para o Azure:

- **Assinatura**: Selecione o nome do contêiner do Azure Blob Storage.
- **Grupo de recursos**: selecione o nome do grupo de recursos do Azure.
- **Detalhes da instância**:
  - **Nome da conta de armazenamento**: insira o nome do contêiner do Armazenamento de Blobs do Azure.
  - **Região do Azure**: insira a região do Azure para o contêiner.
  - **Tipo de desempenho**: selecione o tipo de desempenho padrão ou premium para o contêiner do Azure Blob Storage, indicando o nível de desempenho necessário.
  - **Criptografia**: Selecione o tipo de criptografia para o contêiner do Azure Blob Storage. As opções são chaves gerenciadas pela Microsoft ou chaves gerenciadas pelo cliente. Se você selecionar chaves gerenciadas pelo cliente, deverá fornecer o nome do cofre de chaves e o nome da chave.

◦ Para StorageGRID:

- **Nome do destino do backup**: Selecione o nome do bucket do StorageGRID .
- **Nome do bucket**: insira o nome do bucket do StorageGRID .
- **Região**: insira a região StorageGRID para o bucket.
- **Habilitar controle de versão**: selecione esta opção para habilitar o controle de versão para o bucket StorageGRID . O controle de versão permite que você mantenha várias versões de objetos no bucket, o que pode ser útil para fins de backup e recuperação.
- **Bloqueio de objeto**: selecione esta opção para habilitar o bloqueio de objeto para o bucket StorageGRID . O bloqueio de objetos impede que objetos sejam excluídos ou substituídos por um período de retenção especificado, fornecendo uma camada adicional de proteção de dados. Você pode habilitar isso somente quando estiver criando um bucket e não poderá desativá-lo mais tarde.
- **Capacidade**: insira a capacidade do bucket StorageGRID . Esta é a quantidade máxima de dados que podem ser armazenados no bucket.

◦ Para ONTAP S3:

- **Nome do destino do backup**: Selecione o nome do bucket ONTAP S3.
- **Nome de destino do bucket**: insira o nome do bucket ONTAP S3.
- **Capacidade**: insira a capacidade do bucket ONTAP S3. Esta é a quantidade máxima de dados que podem ser armazenados no bucket.
- **Habilitar controle de versão**: selecione esta opção para habilitar o controle de versão para o bucket ONTAP S3. O controle de versão permite que você mantenha várias versões de objetos no

bucket, o que pode ser útil para fins de backup e recuperação.

- **Bloqueio de objeto**: selecione esta opção para habilitar o bloqueio de objeto para o bucket ONTAP S3. O bloqueio de objetos impede que objetos sejam excluídos ou substituídos por um período de retenção especificado, fornecendo uma camada adicional de proteção de dados. Você pode habilitar isso somente quando estiver criando um bucket e não poderá desativá-lo mais tarde.

5. Selecione **Adicionar**.

Alterar credenciais para um destino de backup

Insira as credenciais necessárias para acessar o destino de backup.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione **Destinos de backup externos**.
3. Selecione o alvo e à direita, selecione **Ações*** **ícone e selecione *Alterar credenciais**.
4. Insira as novas credenciais para o destino de backup. As informações variam dependendo do tipo de destino de backup selecionado.
5. Selecione **Concluído**.

Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery

Você pode alternar entre as diferentes cargas de trabalho do NetApp Backup and Recovery.

Mudar para uma carga de trabalho diferente

Você pode alternar para uma carga de trabalho diferente na interface do usuário do NetApp Backup and Recovery.

Passos

1. Na navegação à esquerda do Console, selecione **Proteção** > **Backup e Recuperação**.
2. No canto superior direito da página, selecione a lista suspensa **Alternar carga de trabalho**.
3. Selecione a carga de trabalho para a qual você deseja alternar.

   A página é atualizada e mostra a carga de trabalho selecionada.

Configurar as configurações de backup e recuperação do NetApp

Depois de configurar o NetApp Console, defina as configurações de backup e recuperação. Adicione credenciais para recursos de host, importe recursos do SnapCenter , configure diretórios de log e defina configurações do VMware vCenter. Conclua estas etapas antes de fazer backup ou recuperar dados.

- Adicionar credenciais para recursos do hostpara os hosts Windows e SQL Server que você importou do

SnapCenter e adicione credenciais. (Somente cargas de trabalho do Microsoft SQL Server)

- Manter as configurações do VMware vCenter .
- Importar e gerenciar recursos do host SnapCenter . (Somente cargas de trabalho do Microsoft SQL Server)
- Configurar diretórios de log em instantâneos para hosts Windows .

Função necessária do NetApp Console Superadministrador de backup e recuperação, administrador de backup de backup e recuperação, administrador de restauração de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Adicionar credenciais para recursos do host

Adicione credenciais para recursos de host para importar do SnapCenter. O NetApp Backup and Recovery usa essas credenciais para descobrir cargas de trabalho e aplicar políticas de backup.

Se você não tiver credenciais, crie-as com permissões para acessar e gerenciar cargas de trabalho do host.

Você precisa configurar os seguintes tipos de credenciais:

- Credenciais do Microsoft SQL Server
- Credenciais do host do SnapCenter Windows

Passos

1. No menu NetApp Backup and Recovery, selecione **Configurações**.
2. Selecione a seta para baixo para **Credenciais**.
3. Selecione **Adicionar novas credenciais**.
4. Insira informações para as credenciais. Campos diferentes aparecem dependendo do modo de autenticação selecionado. Selecione as Informações **i** para obter mais informações sobre os campos.
   - **Nome das credenciais**: Insira um nome para as credenciais.
   - **Modo de autenticação**: Selecione **Windows** ou **Microsoft SQL**.

   Você precisa inserir credenciais para o Windows e o Microsoft SQL Server, então precisará adicionar dois conjuntos de credenciais.

5. Se você selecionou **Windows**:
   - **Agente do console**: insira o endereço IP do agente do console.
   - **Domínio e nome de usuário**: insira o NetBIOS ou o FQDN do domínio e o nome de usuário para as credenciais.
   - **Senha**: Digite a senha para as credenciais.
6. Se você selecionou **Microsoft SQL**:
   - **Host**: Selecione um endereço de host do SQL Server descoberto.
   - **Instância do SQL Server**: Selecione uma instância do SQL Server descoberta.
7. Selecione **Adicionar**.

Editar credenciais para recursos do host

Mais tarde, você pode editar a senha dos recursos do host importados do SnapCenter.

Passos

1. No menu NetApp Backup and Recovery, selecione **Configurações**.
2. Selecione a seta para baixo para expandir a seção **Credenciais**.
3. Selecione o ícone Ações ••• > **Editar credenciais**.
   - **Senha**: Digite a senha para as credenciais.
4. Selecione **Salvar**.

Manter as configurações do VMware vCenter

Forneça credenciais do VMware vCenter para descobrir cargas de trabalho para backup. Se você não tiver credenciais, crie-as com permissões para acessar e gerenciar as cargas de trabalho do VMware vCenter Server.

Passos

1. No menu NetApp Backup and Recovery, selecione **Configurações**.
2. Selecione a seta para baixo para expandir a seção **VMware vCenter**.
3. Selecione **Adicionar vCenter**.
4. Insira as informações do VMware vCenter Server.
   - **FQDN ou endereço IP do vCenter**: insira um nome FQDN ou o endereço IP do VMware vCenter Server.
   - **Nome de usuário** e **Senha**: Digite o nome de usuário e a senha do VMware vCenter Server.
   - **Porta**: Digite o número da porta para o VMware vCenter Server.
   - **Protocolo**: Selecione **HTTP** ou **HTTPS**.
5. Selecione **Adicionar**.

Importar e gerenciar recursos do host SnapCenter

Se você usou o SnapCenter anteriormente para fazer backup de seus recursos, poderá importar e gerenciar esses recursos no NetApp Backup and Recovery. Esta opção permite importar informações do servidor SnapCenter para registrar vários servidores Snapcenter e descobrir cargas de trabalho do banco de dados.

Este é um processo de duas partes:

- Importar recursos do aplicativo e do host do SnapCenter Server
- Gerenciar recursos selecionados do host SnapCenter

Importar recursos do aplicativo e do host do SnapCenter Server

Esta primeira etapa importa recursos de host do SnapCenter e exibe esses recursos na página Inventário de backup e recuperação do NetApp . Nesse ponto, os recursos ainda não são gerenciados pelo NetApp Backup and Recovery.

Após importar os recursos do host do SnapCenter , o NetApp Backup and Recovery não assume o gerenciamento de proteção. Para fazer isso, você deve selecionar explicitamente gerenciar esses recursos no NetApp Backup and Recovery.

Passos

1. No menu NetApp Backup and Recovery, selecione **Configurações**.
2. Selecione a seta para baixo para expandir a seção **Importar do SnapCenter**.
3. Selecione **Importar do SnapCenter** para importar os recursos do SnapCenter .
4. Insira * Credenciais do aplicativo SnapCenter *:
   a. * FQDN ou endereço IP do SnapCenter *: insira o FQDN ou endereço IP do próprio aplicativo SnapCenter .
   b. **Porta**: insira o número da porta para o SnapCenter Server.
   c. **Nome de usuário** e **Senha**: Digite o nome de usuário e a senha do SnapCenter Server.
   d. **Agente de console**: Selecione o agente de console para o SnapCenter.
5. Insira * Credenciais do host do servidor SnapCenter *:
   a. **Credenciais existentes**: Se você selecionar esta opção, poderá usar as credenciais existentes que você já adicionou. Digite o nome das credenciais.
   b. **Adicionar novas credenciais**: Se você não tiver credenciais de host do SnapCenter existentes, poderá adicionar novas credenciais. Digite o nome das credenciais, o modo de autenticação, o nome de usuário e a senha.
6. Selecione **Importar** para validar suas entradas e registrar o SnapCenter Server.

   Se o SnapCenter Server já estiver registrado, você poderá atualizar os detalhes de registro existentes.

Resultado

A página Inventário mostra os recursos importados do SnapCenter .

Gerenciar recursos do host SnapCenter

Depois de importar os recursos do SnapCenter , gerencie esses recursos de host no NetApp Backup and Recovery. Depois de selecionar o gerenciamento desses recursos importados, o NetApp Backup and Recovery pode fazer backup e recuperar os recursos que você está importando do SnapCenter. Você não precisa mais gerenciar esses recursos no SnapCenter Server.

Passos

1. Depois de importar os recursos do SnapCenter , na página Inventário exibida, selecione os recursos do SnapCenter que você importou e que deseja que o NetApp Backup and Recovery gerencie a partir de agora.
2. Selecione o ícone Ações ••• > **Gerenciar** para gerenciar os recursos.
3. Selecione **Gerenciar no NetApp Console**.

   A página Inventário mostra **Gerenciado** sob o nome do host para indicar que os recursos do host selecionados agora são gerenciados pelo NetApp Backup and Recovery.

Editar recursos importados do SnapCenter

Mais tarde, você pode reimportar os recursos do SnapCenter ou editar os recursos importados do SnapCenter para atualizar os detalhes de registro.

Você pode alterar apenas os detalhes da porta e da senha do SnapCenter Server.

Passos

1. No menu NetApp Backup and Recovery, selecione **Configurações**.
2. Selecione a seta para baixo para **Importar do SnapCenter**.

   A página Importar do SnapCenter mostra todas as importações anteriores.

3. Selecione o ícone Ações ••• > **Editar** para atualizar os recursos.
4. Atualize a senha e os detalhes da porta do SnapCenter , conforme necessário.
5. Selecione **Importar**.

Configurar diretórios de log em instantâneos para hosts Windows

Antes de criar políticas para hosts Windows, você deve configurar diretórios de log em instantâneos para hosts Windows. Os diretórios de log são usados para armazenar os logs gerados durante o processo de backup.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Na página Inventário, selecione uma carga de trabalho e, em seguida, selecione o ícone Ações ••• > **Ver detalhes** para exibir os detalhes da carga de trabalho.
3. Na página Detalhes do inventário que mostra o Microsoft SQL Server, selecione a guia Hosts.
4. Na página de detalhes do inventário, selecione um host e selecione o ícone Ações ••• > **Configurar diretório de log**.
5. Navegue ou insira o caminho para o diretório de log.
6. Selecione **Salvar**.

Use o NetApp Backup e Recovery

Visualize a integridade da proteção no Painel de Backup e Recuperação do NetApp

Monitorar a integridade de suas cargas de trabalho garante que você esteja ciente dos problemas com a proteção da carga de trabalho e possa tomar medidas para resolvê-los. Veja o status dos seus backups e restaurações no Painel de Backup e Recuperação da NetApp . Você pode revisar o resumo do sistema, o resumo da proteção, o resumo do trabalho, o resumo da restauração e muito mais.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, administrador de backup e recuperação, administrador de restauração de backup e recuperação, administrador de clone de backup e recuperação ou função de visualizador de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Painel**.
    - Número de hosts ou VMs descobertos
    - Número de clusters do Kubernetes descobertos
    - Número de destinos de backup no armazenamento de objetos
    - Número de vCenters
    - Número de clusters de armazenamento no ONTAP

Ver o resumo da proteção

Revise as seguintes informações no resumo de proteção:

- O número total de bancos de dados, VMs e armazenamentos de dados protegidos e desprotegidos.

  Um banco de dados protegido é aquele que tem uma política de backup atribuída. Um banco de dados desprotegido é aquele que não tem uma política de backup atribuída a ele.

- O número de backups que foram bem-sucedidos, apresentaram um aviso ou falharam.
- A capacidade total descoberta pelo serviço de backup e a capacidade protegida versus desprotegida. Passe o mouse sobre o ícone **"i"** para ver os detalhes.

Ver o resumo do trabalho

Revise o total de trabalhos concluídos, em execução ou com falha no Resumo do trabalho.

Passos

1. Para cada distribuição de trabalho, altere um filtro para mostrar o resumo de tarefas com falha, em execução e concluídas com base no número de dias, por exemplo, os últimos 30 dias, os últimos 7 dias, as últimas 24 horas ou o último 1 ano.
2. Veja detalhes dos trabalhos com falha, em execução e concluídos selecionando **Exibir monitoramento**

de trabalhos.

Ver o resumo da restauração

Revise as seguintes informações no resumo da restauração:

- O número total de trabalhos de restauração realizados
- A quantidade total de capacidade que foi restaurada
- O número de trabalhos de restauração executados no armazenamento local, secundário e de objetos. Passe o mouse sobre o gráfico para ver os detalhes.

Crie e gerencie políticas para governar backups no NetApp Backup and Recovery

No NetApp Backup and Recovery, crie suas próprias políticas que controlam a frequência do backup, o horário em que o backup é feito e o número de arquivos de backup que são retidos.

Algumas dessas opções e seções de configuração não estão disponíveis para todas as cargas de trabalho.

Se você importar recursos do SnapCenter, poderá encontrar algumas diferenças entre as políticas usadas no SnapCenter e aquelas usadas no NetApp Backup and Recovery. Ver "Diferenças de política entre SnapCenter e NetApp Backup and Recovery" .

Você pode atingir os seguintes objetivos relacionados às políticas:

- Criar uma política de instantâneo local
- Crie uma política para replicação para armazenamento secundário
- Crie uma política para configurações de armazenamento de objetos
- Configurar configurações avançadas de política
- Editar políticas (não disponível para cargas de trabalho de visualização do VMware)
- Excluir políticas

Ver políticas

1. No menu NetApp Backup and Recovery, selecione **Políticas**.
2. Revise os detalhes desta política.
    - **Carga de trabalho**: Exemplos incluem Microsoft SQL Server, Volumes, VMware, KVM, Hyper-V ou Kubernetes.
    - **Tipo de backup**: Exemplos incluem backup completo e backup de log.
    - **Arquitetura**: Exemplos incluem snapshot local, fan-out, cascateamento, disco para disco e disco para armazenamento de objetos.
    - **Recursos protegidos**: mostra quantos recursos do total de recursos naquela carga de trabalho estão protegidos.
    - **Proteção contra ransomware**: mostra se a política inclui bloqueio de snapshot no snapshot local,

bloqueio de snapshot no armazenamento secundário ou bloqueio de DataLock no armazenamento de objetos.

Criar uma política

Você pode criar políticas que controlam seus snapshots locais, replicações para armazenamento secundário e backups para armazenamento de objetos. Parte da sua estratégia 3-2-1 envolve a criação de uma cópia instantânea das instâncias, bancos de dados, aplicativos ou VMs no sistema de armazenamento **primário**.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, administrador de backup de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Antes de começar

Se você planeja replicar para armazenamento secundário e deseja usar o bloqueio de snapshot em snapshots locais ou em armazenamento secundário ONTAP remoto, primeiro precisa inicializar o relógio de conformidade ONTAP no nível do cluster. Este é um requisito para habilitar o bloqueio de snapshot na política.

Para obter instruções sobre como fazer isso, consulte "Inicializar o relógio de conformidade no ONTAP" .

Para obter informações sobre bloqueio de instantâneo em geral, consulte "Bloqueio de instantâneo no ONTAP" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Políticas**.
2. Na página Políticas, selecione **Criar nova política**.
3. Na página Políticas, forneça as seguintes informações.
    - Seção **Detalhes**:
        - Tipo de carga de trabalho: selecione a carga de trabalho que usará a política.
        - Insira um nome de política.

          Para uma lista de caracteres a serem evitados, veja a dica de foco.

        - Selecione um agente do Console na lista **Agente**.
    - Seção **Arquitetura de backup**: Selecione a seta para baixo e escolha o fluxo de dados para o backup, como fan-out 3-2-1, cascata 3-2-1 ou disco para disco.
        - **3-2-1 fanout**: Armazenamento primário (disco) para armazenamento secundário (disco) para nuvem (armazenamento de objetos). Cria várias cópias de dados em diferentes sistemas de armazenamento, como configurações de ONTAP para ONTAP e de ONTAP para armazenamento de objetos. Este pode ser um armazenamento de objetos de hiperescala em nuvem ou um armazenamento de objetos privado — StorageGRID. Essas configurações ajudam a alcançar proteção ideal de dados e recuperação de desastres.

          Esta opção não está disponível para o Amazon FSx for NetApp ONTAP.

          Para cargas de trabalho do VMware, isso configura o snapshot local nos armazenamentos de dados ou VMs no primário e replica do armazenamento em disco primário para o armazenamento em disco secundário, bem como replica do primário para o armazenamento de objetos na nuvem.

- **Cascata 3-2-1**: (Não disponível para cargas de trabalho do Kubernetes) Armazenamento primário (disco) para armazenamento secundário (disco) e armazenamento primário (disco) para armazenamento em nuvem (armazenamento de objetos). Este pode ser um armazenamento de objetos de hiperescala em nuvem ou um armazenamento de objetos privado — StorageGRID. Isso cria uma cadeia de replicação de dados em vários sistemas para garantir redundância e confiabilidade.

  Esta opção não está disponível para o Amazon FSx for NetApp ONTAP.

Para cargas de trabalho do VMware, isso configura o snapshot local nos datastores ou VMs no armazenamento primário e uma cascata do armazenamento em disco primário para o armazenamento em disco secundário e, depois, para o armazenamento de objetos na nuvem.

- **Disco para disco**: (Não disponível para cargas de trabalho do Kubernetes) Armazenamento primário (disco) para armazenamento secundário (disco). A estratégia de proteção de dados ONTAP para ONTAP replica dados entre dois sistemas ONTAP para garantir alta disponibilidade e recuperação de desastres. Isso normalmente é obtido usando o SnapMirror, que suporta replicação síncrona e assíncrona. Este método garante que seus dados sejam continuamente atualizados e estejam disponíveis em vários locais, fornecendo proteção robusta contra perda de dados.

  Para cargas de trabalho do VMware, isso configura o snapshot local nos datastores ou VMwares no sistema de armazenamento primário e, em seguida, replica os dados do sistema de armazenamento em disco primário para o sistema de armazenamento em disco secundário.

- **Armazenamento de disco para objeto**: Armazenamento primário (disco) para nuvem (armazenamento de objeto). Isso replica dados de um sistema ONTAP para um sistema de armazenamento de objetos, como AWS S3, Azure Blob Storage ou StorageGRID. Isso normalmente é obtido usando o SnapMirror Cloud, que fornece backups incrementais permanentes transferindo apenas blocos de dados alterados após a transferência de linha de base inicial. Este pode ser um armazenamento de objetos de hiperescala em nuvem ou um armazenamento de objetos privado — StorageGRID. Este método é ideal para retenção e arquivamento de dados a longo prazo, oferecendo uma solução econômica e escalável para proteção de dados.

  Para cargas de trabalho VMWare, isso configura o snapshot local nos datastores ou VMs no primário e a replicação do armazenamento em disco primário para o armazenamento de objetos na nuvem.

- **Fanout de disco para disco**: (Não disponível para cargas de trabalho do Kubernetes) Armazenamento primário (disco) para armazenamento secundário (disco) e armazenamento primário (disco) para armazenamento secundário (disco).

  Você pode configurar várias configurações secundárias para a opção de fanout de disco para disco.

Para cargas de trabalho do VMware, isso configura o armazenamento em disco primário para o armazenamento em disco secundário e replica o armazenamento em disco primário para o armazenamento em disco secundário.

- **Instantâneos locais**: instantâneo local no volume selecionado (Microsoft SQL Server). Os snapshots locais são um componente essencial das estratégias de proteção de dados, capturando o estado dos seus dados em momentos específicos. Isso cria cópias somente leitura, em um ponto específico no tempo, dos volumes de produção onde suas cargas de trabalho estão sendo executadas. O snapshot

consome espaço de armazenamento mínimo e incorre em sobrecarga de desempenho insignificante porque registra somente alterações em arquivos desde o último snapshot. Você pode usar instantâneos locais para recuperar dados perdidos ou corrompidos, bem como para criar backups para fins de recuperação de desastres.

Para cargas de trabalho do VMware, isso configura o snapshot local nos datastores ou VMs no sistema de armazenamento primário.

Criar uma política de instantâneo local

Forneça informações para o instantâneo local.

- Selecione a opção **Adicionar agendamento** para selecionar o agendamento ou agendamentos de instantâneos. Você pode ter no máximo 5 agendamentos.
- **Frequência do instantâneo**: selecione a frequência: horária, diária, semanal, mensal ou anual. A frequência anual não está disponível para cargas de trabalho do Kubernetes.
- **Retenção de instantâneos**: insira o número de instantâneos a serem mantidos.
- **Habilitar backup de log**: (Aplica-se somente a cargas de trabalho do Microsoft SQL Server e do Oracle Database.) Habilite esta opção para fazer backup de logs e definir a frequência e a retenção dos backups de logs. Para fazer isso, você já deve ter configurado um backup de log. Ver "Configurar diretórios de log" .
  - **Remover logs de arquivo após backup**: (somente cargas de trabalho do Oracle Database) Se os backups de log estiverem habilitados, você pode opcionalmente habilitar esse recurso para limitar por quanto tempo o Backup e Recuperação mantém os logs de arquivo do Oracle. Você pode escolher o período de retenção e também onde o Backup and Recovery deve excluir os logs de arquivamento.
- **Provedor**: (somente cargas de trabalho do Kubernetes) Selecione o provedor de armazenamento que hospeda os recursos do aplicativo Kubernetes.

Crie uma política para configurações secundárias (replicação para armazenamento secundário)

Forneça informações para a replicação para armazenamento secundário. As informações de agendamento das configurações de instantâneo local aparecem para você nas configurações secundárias. Essas configurações não estão disponíveis para cargas de trabalho do Kubernetes.

- **Backup**: Selecione a frequência: horária, diária, semanal, mensal ou anual.
- **Destino do backup**: Selecione o sistema de destino no armazenamento secundário para o backup.
- **Retenção**: Insira o número de snapshots a serem mantidos.
- **Ativar bloqueio de instantâneos**: selecione se deseja ativar instantâneos à prova de violação.
- **Período de bloqueio do snapshot**: insira o número de dias, meses ou anos que você deseja bloquear o snapshot.
- **Transferência para o secundário**:
  - A opção * Agendamento de transferência ONTAP - Em linha* é selecionada por padrão e indica que os instantâneos são transferidos para o sistema de armazenamento secundário imediatamente. Você não precisa agendar o backup.
  - Outras opções: Se você escolher uma transferência diferida, as transferências não serão imediatas e você poderá definir um cronograma.
- * Relacionamento secundário do SnapMirror e do SnapVault SMAS*: use relacionamentos secundários do SnapMirror e do SnapVault SMAS para cargas de trabalho do SQL Server.

Crie uma política para configurações de armazenamento de objetos

Forneça informações para o backup no armazenamento de objetos. Essas configurações são chamadas de "Configurações de backup" para cargas de trabalho do Kubernetes.

Os campos que aparecem diferem dependendo do provedor e da arquitetura selecionada.

Crie uma política para armazenamento de objetos da AWS

Insira informações nestes campos:

- **Provedor**: Selecione **AWS**.
- **Conta AWS**: Selecione a conta AWS.
- **Destino de backup**: selecione um destino de armazenamento de objetos S3 registrado. Certifique-se de que o destino esteja acessível dentro do seu ambiente de backup.
- **IPspace**: Selecione o IPspace a ser usado para as operações de backup. Isso é útil se você tiver vários IPspaces e quiser controlar qual deles será usado para backups.
- **Configurações de agendamento**: selecione o agendamento que foi definido para os instantâneos locais. Você pode remover uma programação, mas não pode adicionar uma porque as programações são definidas de acordo com as programações de instantâneos locais.
- **Cópias de retenção**: insira o número de instantâneos a serem mantidos.
- **Executar em**: Escolha o agendamento de transferência ONTAP para fazer backup de dados no armazenamento de objetos.
- **Coloque seus backups em camadas do armazenamento de objetos para o armazenamento de arquivamento**: se você optar por colocar os backups em camadas para o armazenamento de arquivamento (por exemplo, AWS Glacier), selecione a opção de camada e o número de dias para arquivamento.
- **Habilitar verificação de integridade**: (Não disponível para cargas de trabalho do Kubernetes) Selecione se deseja habilitar verificações de integridade (bloqueio de instantâneo) no armazenamento de objetos. Isso garante que os backups sejam válidos e possam ser restaurados com sucesso. A frequência de verificação de integridade é definida como 7 dias por padrão. Para proteger seus backups de serem modificados ou excluídos, selecione a opção **Verificação de integridade**. A verificação ocorre apenas no instantâneo mais recente. Você pode habilitar ou desabilitar verificações de integridade no snapshot mais recente.

Crie uma política para armazenamento de objetos do Microsoft Azure

Insira informações nestes campos:

- **Provedor**: Selecione **Azure**.
- **Assinatura do Azure**: Selecione a assinatura do Azure entre as descobertas.
- **Grupo de recursos do Azure**: selecione o grupo de recursos do Azure entre os descobertos.
- **Destino de backup**: Selecione um destino de armazenamento de objeto registrado. Certifique-se de que o destino esteja acessível dentro do seu ambiente de backup.
- **IPspace**: Selecione o IPspace a ser usado para as operações de backup. Isso é útil se você tiver vários IPspaces e quiser controlar qual deles será usado para backups.
- **Configurações de agendamento**: selecione o agendamento que foi definido para os instantâneos locais. Você pode remover uma programação, mas não pode adicionar uma porque as programações são

definidas de acordo com as programações de instantâneos locais.

- **Cópias de retenção**: insira o número de instantâneos a serem mantidos.
- **Executar em**: Escolha o agendamento de transferência ONTAP para fazer backup de dados no armazenamento de objetos.
- **Coloque seus backups em camadas do armazenamento de objetos para o armazenamento de arquivamento**: se você optar por colocar os backups em camadas para o armazenamento de arquivamento, selecione a opção de camada e o número de dias para arquivamento.
- **Habilitar verificação de integridade**: (Não disponível para cargas de trabalho do Kubernetes) Selecione se deseja habilitar verificações de integridade (bloqueio de instantâneo) no armazenamento de objetos. Isso garante que os backups sejam válidos e possam ser restaurados com sucesso. A frequência de verificação de integridade é definida como 7 dias por padrão. Para proteger seus backups de serem modificados ou excluídos, selecione a opção **Verificação de integridade**. A verificação ocorre apenas no instantâneo mais recente. Você pode habilitar ou desabilitar verificações de integridade no snapshot mais recente.

Crie uma política para armazenamento de objetos StorageGRID

Insira informações nestes campos:

- **Provedor**: Selecione * StorageGRID*.
- * Credenciais do StorageGRID *: Selecione as credenciais do StorageGRID entre as descobertas. Essas credenciais são usadas para acessar o sistema de armazenamento de objetos StorageGRID e foram inseridas na opção Configurações.
- **Destino de backup**: selecione um destino de armazenamento de objetos S3 registrado. Certifique-se de que o destino esteja acessível dentro do seu ambiente de backup.
- **IPspace**: Selecione o IPspace a ser usado para as operações de backup. Isso é útil se você tiver vários IPspaces e quiser controlar qual deles será usado para backups.
- **Configurações de agendamento**: selecione o agendamento que foi definido para os instantâneos locais. Você pode remover uma programação, mas não pode adicionar uma porque as programações são definidas de acordo com as programações de instantâneos locais.
- **Cópias de retenção**: insira o número de instantâneos a serem mantidos para cada frequência.
- **Cronograma de transferência para armazenamento de objetos**: (Não disponível para cargas de trabalho do Kubernetes) Escolha o cronograma de transferência ONTAP para fazer backup de dados no armazenamento de objetos.
- **Habilitar verificação de integridade**: (Não disponível para cargas de trabalho do Kubernetes) Selecione se deseja habilitar verificações de integridade (bloqueio de instantâneo) no armazenamento de objetos. Isso garante que os backups sejam válidos e possam ser restaurados com sucesso. A frequência de verificação de integridade é definida como 7 dias por padrão. Para proteger seus backups de serem modificados ou excluídos, selecione a opção **Verificação de integridade**. A verificação ocorre apenas no instantâneo mais recente. Você pode habilitar ou desabilitar verificações de integridade no snapshot mais recente.
- **Coloque seus backups em camadas do armazenamento de objetos para o armazenamento de arquivamento**: (Não disponível para cargas de trabalho do Kubernetes) Se você optar por dividir os backups em camadas para o armazenamento de arquivamento, selecione a opção de camada e o número de dias para arquivamento.

Configurar configurações avançadas na política

Opcionalmente, você pode configurar configurações avançadas na política. Essas configurações estão

disponíveis para todas as arquiteturas de backup, incluindo snapshots locais, replicação para armazenamento secundário e backups para armazenamento de objetos. Essas configurações não estão disponíveis para cargas de trabalho do Kubernetes. As configurações avançadas disponíveis serão diferentes dependendo da carga de trabalho selecionada na parte superior da página, portanto, as configurações avançadas descritas aqui podem não se aplicar a todas as cargas de trabalho. Configurações avançadas não estão disponíveis ao configurar uma política para cargas de trabalho do Kubernetes.

Passos

1. No menu NetApp Backup and Recovery, selecione **Políticas**.
2. Na página Políticas, selecione **Criar nova política**.
3. Na seção **Política > Configurações avançadas**, selecione o menu **Selecionar ação avançada** para escolher em uma lista de configurações avançadas.
4. Habilite qualquer uma das configurações que você deseja visualizar ou alterar e selecione **Aceitar**.
5. Forneça as seguintes informações:
   - **Backup somente cópia**: (Aplica-se somente a cargas de trabalho do Microsoft SQL Server) Escolha o backup somente cópia (um tipo de backup do Microsoft SQL Server) se precisar fazer backup de seus recursos usando outro aplicativo de backup.
   - **Configurações do grupo de disponibilidade**: (Aplica-se somente a cargas de trabalho do Microsoft SQL Server) Selecione réplicas de backup preferenciais ou especifique uma réplica específica. Essa configuração é útil se você tiver um grupo de disponibilidade do SQL Server e quiser controlar qual réplica será usada para backups.
   - **Taxa máxima de transferência**: Para não definir um limite no uso da largura de banda, selecione **Ilimitado**. Se você quiser limitar a taxa de transferência, selecione **Limitado** e selecione a largura de banda de rede entre 1 e 1.000 Mbps alocada para carregar backups no armazenamento de objetos. Por padrão, o ONTAP pode usar uma quantidade ilimitada de largura de banda para transferir os dados de backup de volumes no sistema para o armazenamento de objetos. Se você perceber que o tráfego de backup está afetando as cargas de trabalho normais dos usuários, considere diminuir a quantidade de largura de banda da rede usada durante a transferência.
   - **Repetições de backup**: (Não aplicável a cargas de trabalho VMware) Para repetir a tarefa em caso de falha ou interrupção, selecione **Ativar repetições de tarefa durante falha**. Insira o número máximo de tentativas de snapshot e backup, bem como o intervalo de tempo para novas tentativas. A recontagem deve ser inferior a 10. Esta configuração é útil se você quiser garantir que o trabalho de backup seja repetido em caso de falha ou interrupção.

     Se a frequência do snapshot for definida como 1 hora, o atraso máximo, juntamente com a contagem de novas tentativas, não deverá exceder 45 minutos.

   - **Habilitar snapshot consistente com VM**: (Aplica-se somente a cargas de trabalho VMware) Selecione se deseja habilitar snapshots consistentes com VM. Isso garante que os instantâneos recém-criados sejam consistentes com o estado da máquina virtual no momento do instantâneo. Isso é útil para garantir que os backups possam ser restaurados com sucesso e que os dados estejam em um estado consistente. Isso não se aplica a instantâneos existentes.
   - **Verificação de ransomware**: selecione se deseja habilitar a verificação de ransomware em cada bucket. Isso requer bloqueio do DataLock no armazenamento de objetos. Insira a frequência da verificação em dias. Esta opção se aplica ao armazenamento de objetos da AWS e do Microsoft Azure. Observe que esta opção pode incorrer em custos adicionais, dependendo do provedor de nuvem.
   - **Verificação de backup**: (Não aplicável a cargas de trabalho VMware) Selecione se deseja habilitar a verificação de backup e se deseja que ela seja feita imediatamente ou mais tarde. Esse recurso

garante que os backups sejam válidos e possam ser restaurados com sucesso. Recomendamos que você habilite esta opção para garantir a integridade dos seus backups. Por padrão, a verificação de backup é executada no armazenamento secundário, se o armazenamento secundário estiver configurado. Se o armazenamento secundário não estiver configurado, a verificação de backup será executada a partir do armazenamento primário.

Além disso, configure as seguintes opções:

- Verificação **Diária**, **Semanal**, **Mensal** ou **Anual**: Se você escolher **Mais tarde** como verificação de backup, selecione a frequência da verificação de backup. Isso garante que os backups sejam verificados regularmente quanto à integridade e possam ser restaurados com sucesso.
- **Etiquetas de backup**: insira uma etiqueta para o backup. Este rótulo é usado para identificar o backup no sistema e pode ser útil para rastrear e gerenciar backups.
- **Verificação de consistência do banco de dados**: (Não aplicável a cargas de trabalho do VMware) Selecione se deseja habilitar verificações de consistência do banco de dados. Esta opção garante que os bancos de dados estejam em um estado consistente antes do backup ser feito, o que é crucial para garantir a integridade dos dados.
- **Verificar backups de log**: (Não aplicável a cargas de trabalho do VMware) Selecione se deseja verificar os backups de log. Selecione o servidor de verificação. Se você escolher disco para disco ou 3-2-1, selecione também o local de armazenamento de verificação. Esta opção garante que os backups de log sejam válidos e possam ser restaurados com sucesso, o que é importante para manter a integridade dos seus bancos de dados.

◦ **Rede**: Selecione a interface de rede a ser usada para as operações de backup. Isso é útil se você tiver várias interfaces de rede e quiser controlar qual delas será usada para backups.

- **IPspace**: Selecione o IPspace a ser usado para as operações de backup. Isso é útil se você tiver vários IPspaces e quiser controlar qual deles será usado para backups.
- **Configuração de endpoint privado**: Se você estiver usando um endpoint privado para seu armazenamento de objetos, selecione a configuração de endpoint privado a ser usada para as operações de backup. Isso é útil se você quiser garantir que os backups sejam transferidos com segurança por uma conexão de rede privada.

◦ **Notificação**: Selecione se deseja habilitar notificações por e-mail para operações de backup. Isso é útil se você quiser ser notificado quando uma operação de backup for iniciada, concluída ou falhar.

◦ **Discos independentes**: (Aplica-se somente a cargas de trabalho do VMware) Marque esta opção para incluir no backup quaisquer armazenamentos de dados com discos independentes que contenham dados temporários. Um disco independente é um disco de VM que não está incluído em snapshots do VMware.

◦ * Formato de volume e instantâneo do SnapMirror *: Opcionalmente, insira seu próprio nome de instantâneo em uma política que controla os backups para cargas de trabalho do Microsoft SQL Server. Insira o formato e o texto personalizado. Se você optar por fazer backup no armazenamento secundário, também poderá adicionar um prefixo e sufixo de volume do SnapMirror .

Editar uma política

Você pode editar a arquitetura de backup, a frequência de backup, a política de retenção e outras configurações de uma política.

Este recurso não está disponível para cargas de trabalho do VMware Preview.

Você pode adicionar outro nível de proteção ao editar uma política, mas não pode remover um nível de proteção. Por exemplo, se a política estiver protegendo apenas instantâneos locais, você poderá adicionar

replicação ao armazenamento secundário ou backups ao armazenamento de objetos. Se você tiver snapshots e replicação locais, poderá adicionar armazenamento de objetos. No entanto, se você tiver snapshots locais, replicação e armazenamento de objetos, não poderá remover um desses níveis.

Se estiver editando uma política que faz backup no armazenamento de objetos, você pode habilitar o arquivamento.

Se você importou recursos do SnapCenter, poderá encontrar algumas diferenças entre as políticas usadas no SnapCenter e aquelas usadas no NetApp Backup and Recovery. Ver "Diferenças de política entre SnapCenter e NetApp Backup and Recovery" .

Função necessária do NetApp Console

Superadministrador de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No NetApp Console, acesse **Proteção** > **Backup e Recuperação**.
2. Selecione a opção **Políticas**.
3. Selecione a política que você deseja editar.
4. Selecione as **Ações*** ••• **ícone e selecione *Editar**.

Excluir uma política

Você pode excluir uma política se não precisar mais dela.

Não é possível excluir uma política associada a uma carga de trabalho.

Passos

1. No Console, vá para **Proteção** > **Backup e Recuperação**.
2. Selecione a opção **Políticas**.
3. Selecione a política que você deseja excluir.
4. Selecione as **Ações*** ••• **ícone e selecione *Excluir**.
5. Confirme a ação e selecione **Excluir**.

Proteja cargas de trabalho de volume ONTAP

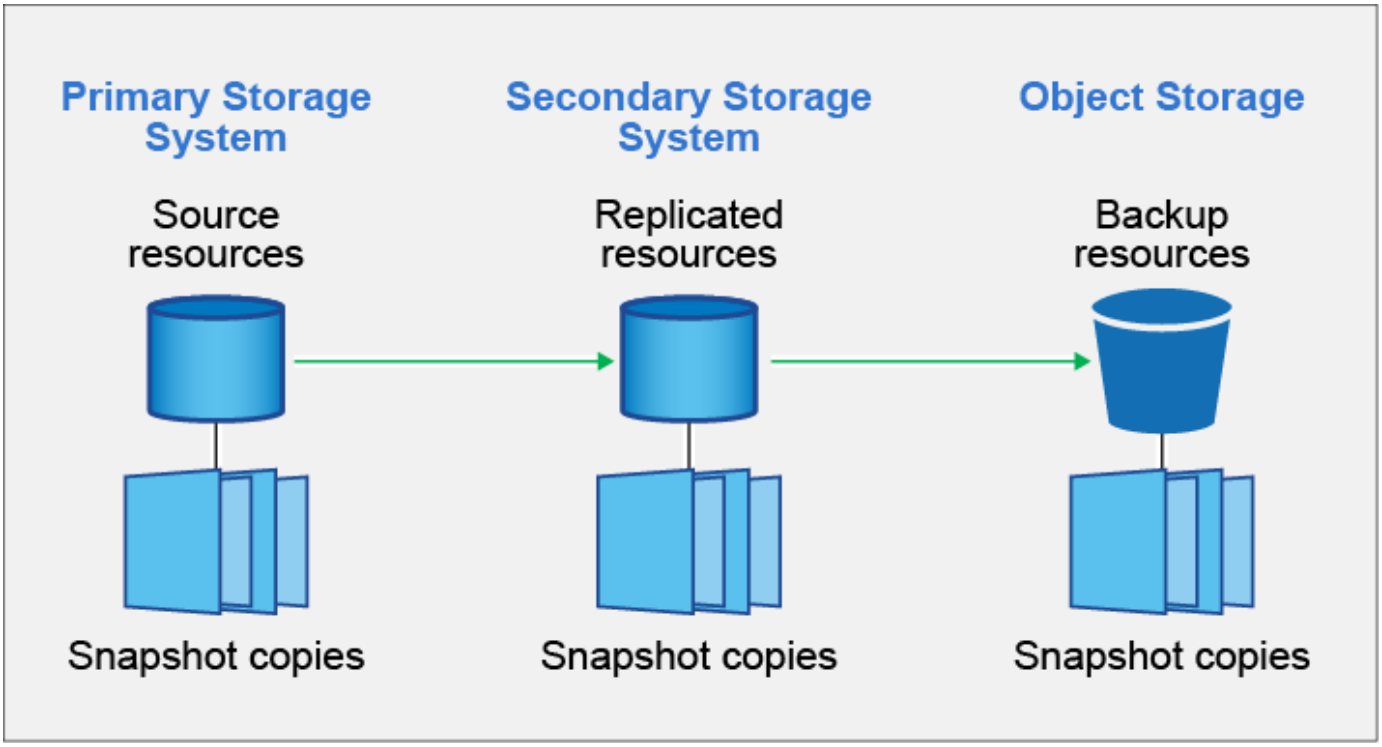
Proteja os dados do seu volume ONTAP usando o NetApp Backup and Recovery

O NetApp Backup and Recovery fornece recursos de backup e restauração para proteção e arquivamento de longo prazo dos dados do seu volume ONTAP . Você pode implementar uma estratégia 3-2-1, na qual você tem 3 cópias dos seus dados de origem em 2 sistemas de armazenamento diferentes, além de 1 cópia na nuvem.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

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

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



O NetApp Backup and Recovery utiliza a tecnologia de replicação de dados SnapMirror da NetApp para garantir que todos os backups estejam totalmente sincronizados, criando cópias de instantâneos e transferindo-as para os locais de backup.

Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados fornecem proteção multicamadas contra ameaças de segurança cibernética internas e externas.
- Vários tipos de mídia garantem a viabilidade de failover no caso de falha física ou lógica de um tipo de mídia.
- A cópia no local facilita restaurações rápidas, com as cópias externas prontas para o caso de a cópia no local ser 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 sistema ou para um sistema diferente.

Características

Recursos de replicação:

- Replique dados entre sistemas de armazenamento ONTAP para dar suporte a backup e recuperação de desastres.

- Garanta a confiabilidade do seu ambiente de DR com alta disponibilidade.
- Criptografia ONTAP nativa em voo 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 autocurativa em caso de falha de transferência.
- Quando comparado a "Replicação NetApp" , a replicação no NetApp Backup and Recovery inclui os seguintes recursos:
  - Replique vários volumes FlexVol de uma vez para um sistema secundário.
  - Restaure um volume replicado para o sistema de origem ou para um sistema diferente usando a interface do usuário.

Ver"Limitações de replicação para volumes ONTAP" para obter uma lista de recursos de replicação que não estão disponíveis com o NetApp Backup and Recovery para volumes ONTAP .

Recursos de backup para objeto:

- Faça backup de cópias independentes dos seus volumes de dados em armazenamento 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 de ponto de recuperação exclusivos.
- Crie uma política de backup a ser aplicada a todos os volumes futuros criados no cluster.
- Crie arquivos de backup imutáveis para que eles fiquem bloqueados e protegidos durante o período de retenção.
- Verifique os arquivos de backup em busca de possíveis ataques de ransomware e remova/substitua backups infectados automaticamente.
- Coloque arquivos de backup mais antigos em camadas para armazenamento de arquivo para economizar custos.
- Exclua o relacionamento de backup para que você possa arquivar volumes de origem desnecessários e, ao mesmo tempo, manter os backups de volume.
- Faça backup de nuvem para nuvem e de sistemas locais para nuvem pública ou privada.
- Os dados de backup são protegidos com criptografia AES de 256 bits em repouso e conexões TLS 1.2 HTTPS 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 dados de um ponto específico no tempo a partir de cópias locais do Snapshot, volumes replicados ou volumes de backup no armazenamento de objetos.
- Restaurar um volume, uma pasta ou arquivos individuais para o sistema de origem ou para um sistema diferente.
- Restaure dados para um sistema usando uma assinatura/conta diferente ou que esteja em uma região diferente.
- Execute uma *restauração rápida* de um volume do 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 nível de bloco, colocando os dados diretamente no local especificado, preservando as ACLs originais.
- Navegue e pesquise catálogos de arquivos para fácil seleção de pastas e arquivos individuais para restauração de arquivo único.

Sistemas suportados para operações de backup e restauração

O NetApp Backup and Recovery oferece suporte a sistemas ONTAP e provedores de nuvem pública e privada.

Regiões suportadas

O NetApp Backup and Recovery é compatível com o Cloud Volumes ONTAP em muitas regiões da Amazon Web Services, Microsoft Azure e Google Cloud.

"Saiba mais usando o Mapa de Regiões Globais"

Destinos de backup suportados

O NetApp Backup and Recovery permite que você faça backup de volumes ONTAP dos seguintes sistemas de origem para os seguintes sistemas secundários e armazenamento de objetos em provedores de nuvem pública e privada. Cópias de instantâneos residem no sistema de origem.

Sistema de origem	Sistema secundário (Replicação)	Armazenamento de objeto de destino (backup) ifdef::aws[]
Cloud Volumes ONTAP na AWS	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Amazon S3 endif::aws[] ifdef::azure[]
Cloud Volumes ONTAP no Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Blob do Azure endif::azure[] ifdef::gcp[]
Cloud Volumes ONTAP no Google	Cloud Volumes ONTAP no sistema Google On-premises ONTAP	Armazenamento em nuvem do Google endif::gcp[]
Sistema ONTAP local	Sistema Cloud Volumes ONTAP 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

Você pode restaurar dados do ONTAP de um arquivo de backup que reside em um sistema secundário (um volume replicado) ou em um armazenamento de objetos (um arquivo de backup) para os seguintes sistemas. Cópias de instantâneos residem no sistema de origem e podem ser restauradas somente no mesmo sistema.

Localização do arquivo de backup		Sistema de destino
Armazenamento de Objetos (Backup)	**Sistema Secundário (Replicação)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Cloud Volumes ONTAP no sistema ONTAP local da AWS endif::aws[] ifdef::azure[]

Localização do arquivo de backup		Sistema de destino
Blob do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure endif::azure[] ifdef::gcp[]
Armazenamento em nuvem do Google	Cloud Volumes ONTAP no sistema Google On-premises ONTAP	Cloud Volumes ONTAP no sistema ONTAP local do Google endif::gcp[]
NetApp StorageGRID	Sistema ONTAP local Cloud Volumes ONTAP	Sistema ONTAP local
ONTAP S3	Sistema ONTAP local Cloud Volumes ONTAP	Sistema ONTAP local

Observe que as referências a "sistemas ONTAP locais" incluem sistemas FAS, AFF e ONTAP Select .

Volumes suportados

O NetApp Backup and Recovery oferece suporte aos seguintes tipos de volumes:

- Volumes de leitura e gravação FlexVol
- Volumes FlexGroup (requer ONTAP 9.12.1 ou posterior)
- Volumes SnapLock Enterprise (requer ONTAP 9.11.1 ou posterior)
- SnapLock Compliance para volumes locais (requer ONTAP 9.14 ou posterior)
- Volumes de destino de proteção de dados (DP) do SnapMirror

O NetApp Backup and Recovery não oferece suporte a backups de volumes FlexCache .

Veja as seções sobre"Limitações de backup e restauração para volumes ONTAP" para requisitos e limitações adicionais.

Custo

Há dois tipos de custos associados ao uso do NetApp Backup and Recovery com sistemas ONTAP : taxas de recursos e taxas de serviço. Ambas as cobranças são para a parte de backup do objeto do serviço.

Não há custo para criar cópias de Snapshot ou volumes replicados, além do espaço em disco necessário para armazenar as cópias de Snapshot e os volumes replicados.

Custos de recursos

As taxas 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.

- Para fazer backup em armazenamento de objetos, você paga ao seu provedor de nuvem pelos custos de armazenamento de objetos.

  Como o NetApp Backup and Recovery preserva a eficiência de armazenamento do volume de origem, você paga os custos de armazenamento de objetos do provedor de nuvem pelos dados *após* as eficiências do ONTAP (para a menor quantidade de dados após a aplicação da desduplicação e da compactação).

- Para restaurar dados usando o Search & Restore, certos recursos são provisionados pelo seu provedor de nuvem, e há um custo por TiB associado à quantidade de dados verificados pelas suas solicitações de pesquisa. (Esses recursos não são necessários para Navegar e Restaurar.)
  - Na AWS, "Amazona Atena" e "Cola AWS" os recursos são implantados em um novo bucket S3.
  - No Azure, um "Espaço de trabalho do Azure Synapse" e "Armazenamento do Azure Data Lake" são provisionados em sua conta de armazenamento para armazenar e analisar seus dados.
- No Google, um novo bucket é implantado e o "Serviços do Google Cloud BigQuery" são provisionados em nível de conta/projeto.
- Se você planeja restaurar dados de volume de um arquivo de backup que foi movido para um armazenamento de objetos de arquivamento, haverá uma taxa adicional de recuperação por GiB e uma taxa por solicitação do provedor de nuvem.
- Se você planeja verificar se há ransomware em um arquivo de backup durante o processo de restauração de dados de volume (se você tiver habilitado o DataLock e o Ransomware Resilience para seus backups na nuvem), você também incorrerá em custos extras de saída do seu provedor de nuvem.

Taxas de serviço

As taxas de serviço são pagas à NetApp e cobrem tanto o custo de *criação* de backups no armazenamento de objetos quanto de *restauração* de volumes ou arquivos desses backups. Você paga somente pelos dados que protege no armazenamento de objetos, calculado pela capacidade lógica de origem utilizada (*antes* das eficiências do ONTAP) dos volumes ONTAP que são copiados para o armazenamento de objetos. Essa capacidade também é conhecida como Terabytes Front-End (FETB).

Há três maneiras de pagar pelo serviço de Backup. A primeira opção é assinar com 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.

Licenciamento

O NetApp Backup and Recovery está disponível com os seguintes modelos de consumo:

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

Uma licença de backup é necessária apenas para backup e restauração do armazenamento de objetos. A criação de cópias de snapshot e volumes replicados não requer licença.

Traga sua própria licença

O BYOL é baseado em prazo (1, 2 ou 3 anos) e em capacidade em incrementos de 1 TiB. Você paga à NetApp para usar o serviço por um período de tempo, digamos 1 ano, e por uma capacidade máxima, digamos 10 TiB.

Você receberá um número de série que deverá ser inserido no NetApp Console para habilitar o serviço. Quando qualquer um dos limites for atingido, você precisará renovar a licença. A licença Backup BYOL se aplica a todos os sistemas de origem associados à sua organização ou conta do NetApp Console.

"Aprenda a gerenciar suas licenças BYOL" .

Assinatura pré-paga

O NetApp Backup and Recovery oferece licenciamento baseado no consumo em um modelo de pagamento conforme o uso. Após assinar pelo marketplace do seu provedor de nuvem, você paga por GiB pelos dados armazenados em backup — não há pagamento inicial. Você é cobrado pelo seu provedor de nuvem por meio de sua fatura mensal.

"Aprenda a configurar uma assinatura pré-paga" .

Observe que um teste gratuito de 30 dias está disponível quando você se inscreve inicialmente com uma assinatura PAYGO.

Contrato anual

Ao usar a AWS, dois contratos anuais estão disponíveis para períodos de 1, 2 ou 3 anos:

- Um plano "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.
- Um plano "CVO Professional" que permite combinar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para Cloud Volumes ONTAP Volumes cobrados nesta licença (a capacidade de backup não é contabilizada na licença).

Ao usar o Azure, dois contratos anuais estão disponíveis para períodos de 1, 2 ou 3 anos:

- Um plano "Cloud Backup" que permite fazer backup de dados Cloud Volumes ONTAP e de dados ONTAP locais.
- Um plano "CVO Professional" que permite combinar o Cloud Volumes ONTAP e o NetApp Backup and Recovery. Isso inclui backups ilimitados para Cloud Volumes ONTAP Volumes cobrados nesta licença (a capacidade de backup não é contabilizada na licença).

Ao usar o GCP, você pode solicitar uma oferta privada da NetApp e, em seguida, selecionar o plano ao assinar no Google Cloud Marketplace durante a ativação do NetApp Backup and Recovery.

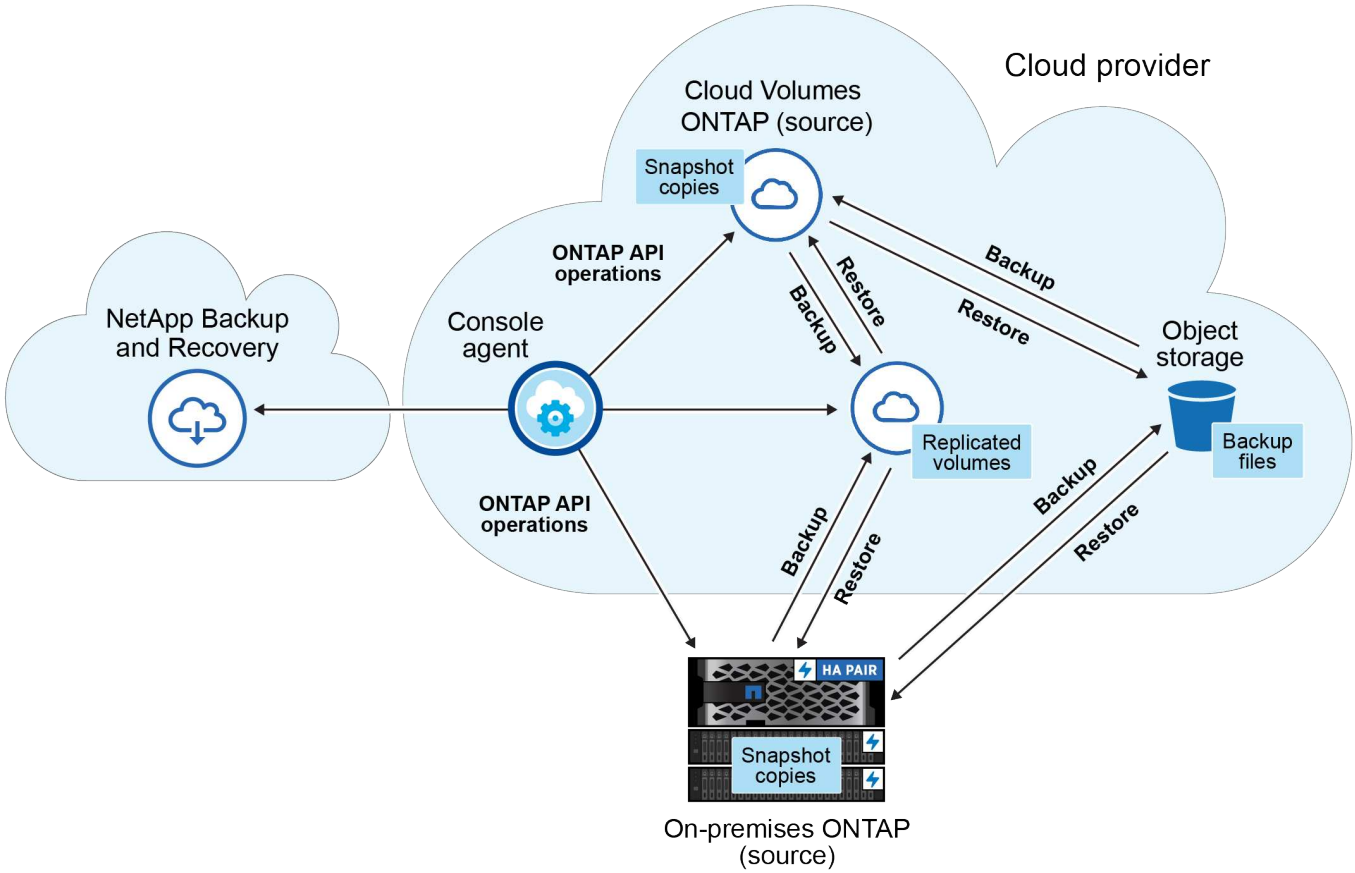
"Aprenda a configurar contratos anuais" .

Como funciona o NetApp Backup and Recovery

Quando você habilita o NetApp Backup and Recovery em um sistema Cloud Volumes ONTAP ou ONTAP local, o serviço executa um backup completo dos seus dados. Após o backup inicial, todos os backups adicionais são incrementais, o que significa que somente os blocos alterados e novos blocos são copiados. Isso mantém o tráfego de rede no mínimo. O backup para armazenamento de objetos é criado com base no "Tecnologia NetApp SnapMirror Cloud" .

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

A imagem a seguir mostra a relação entre cada componente:



Este diagrama mostra volumes sendo replicados para um sistema Cloud Volumes ONTAP , mas os volumes também podem ser replicados para um sistema ONTAP local.

Onde os backups residem

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

- *Cópias de instantâneo* residem no volume de origem no sistema de origem.
- Os *volumes replicados* residem no sistema de armazenamento secundário - um sistema Cloud Volumes ONTAP ou ONTAP local.
- *Cópias de backup* são armazenadas em um armazenamento de objetos que o Console cria na sua conta na nuvem. Há um armazenamento de objetos por cluster/sistema, e o Console nomeia o armazenamento de objetos da seguinte forma: "netapp-backup-clusteruuid". Certifique-se de não excluir este armazenamento de objetos.

+ ** Na AWS, o Console habilita o "Recurso de bloqueio de acesso público do Amazon S3" no bucket S3.

+ ** No Azure, o Console usa um grupo de recursos novo ou existente com uma conta de armazenamento para o contêiner de Blobs. O Console "bloqueia o acesso público aos seus dados de blob" por padrão.

+ ** No GCP, o Console usa um projeto novo ou existente com uma conta de armazenamento para o bucket do Google Cloud Storage.

+ ** No StorageGRID, o Console usa uma conta de locatário existente para o bucket S3.

+ ** No ONTAP S3, o Console usa uma conta de usuário existente para o bucket S3.

Se você quiser alterar o armazenamento de objetos de destino para um cluster no futuro, será

necessário"cancelar o registro do NetApp Backup and Recovery para o sistema" e, em seguida, habilite o NetApp Backup and Recovery usando as novas informações do provedor de nuvem.

Configurações de retenção e agendamento de backup personalizáveis

Quando você habilita o NetApp Backup and Recovery para um sistema, todos os volumes selecionados inicialmente são copiados usando as políticas selecionadas. Você pode selecionar políticas separadas para cópias de instantâneos, volumes replicados e arquivos de backup. Se desejar atribuir políticas de backup diferentes a determinados volumes que têm objetivos de ponto de recuperação (RPO) diferentes, você poderá criar políticas adicionais para esse cluster e atribuí-las aos outros volumes depois que o NetApp Backup and Recovery for ativado.

Você pode escolher uma combinação de backups por hora, diariamente, semanalmente, mensalmente e anualmente de todos os volumes. Para fazer backup no objeto, você também pode selecionar uma das políticas definidas pelo sistema que fornecem backups e retenção por 3 meses, 1 ano e 7 anos. As políticas de proteção de backup que você criou no cluster usando o ONTAP System Manager ou o ONTAP CLI também aparecerão como seleções. Isso inclui políticas criadas usando rótulos personalizados do SnapMirror .

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

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

> O período de retenção para backups de volumes de proteção de dados é o mesmo definido no relacionamento SnapMirror de origem. Você pode alterar isso se quiser usando a API.

Configurações de proteção de arquivo de backup

Se o seu cluster estiver usando o ONTAP 9.11.1 ou superior, você poderá proteger seus backups no armazenamento de objetos contra exclusão e ataques de ransomware. Cada política de backup fornece uma seção para *DataLock e Resiliência contra Ransomware* que pode ser aplicada aos seus arquivos de backup por um período de tempo específico - o *período de retenção*.

- *DataLock* protege seus arquivos de backup contra modificações ou exclusão.
- A *Proteção contra ransomware* 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 verificações agendadas de proteção contra ransomware são ativadas por padrão. A configuração padrão para a frequência de verificação é de 7 dias. A verificação ocorre apenas na cópia mais recente do Snapshot. As verificações agendadas podem ser desativadas para reduzir seus custos. Você pode habilitar ou desabilitar verificações agendadas de ransomware na cópia mais recente do Snapshot usando a opção na página Configurações avançadas. Se você habilitar, as verificações serão realizadas semanalmente por padrão. Você pode alterar essa programação para dias ou semanas ou desativá-la, economizando custos.

O período de retenção de backup é o mesmo que o período de retenção de agendamento de backup, mais um buffer máximo de 31 dias. Por exemplo, backups *semanais* com *5* cópias retidas 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 mais detalhes, consulte estas informações:

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

O DataLock não pode ser habilitado se você estiver hierarquizando backups para armazenamento de arquivamento.

Armazenamento de arquivo para arquivos de backup mais antigos

Ao usar determinado armazenamento em nuvem, você pode mover arquivos de backup mais antigos para uma classe de armazenamento/nível de acesso mais barato após um certo número de dias. Você também pode optar por enviar seus arquivos de backup para armazenamento de arquivo imediatamente, sem que eles sejam gravados no armazenamento em nuvem padrão. Observe que o armazenamento de arquivo não pode ser usado se você tiver habilitado o DataLock.

- Na AWS, os backups começam na classe de armazenamento *Padrão* e fazem a transição para a classe de armazenamento *Acesso Infrequente Padrão* após 30 dias.

  Se o seu cluster estiver usando o ONTAP 9.10.1 ou superior, você poderá optar por colocar backups mais antigos em camadas no armazenamento *S3 Glacier* ou *S3 Glacier Deep Archive* na interface de usuário do NetApp Backup and Recovery após um determinado número de dias para otimizar ainda mais os custos. "Saiba mais sobre o armazenamento de arquivo da AWS" .

- No Azure, os backups são associados à camada de acesso *Cool*.

  Se o seu cluster estiver usando o ONTAP 9.10.1 ou superior, você poderá optar por colocar backups mais antigos em camadas no armazenamento *Azure Archive* na interface do usuário do NetApp Backup and Recovery após um determinado número de dias para otimizar ainda mais os custos. "Saiba mais sobre o armazenamento de arquivamento do Azure" .

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

  Se o seu cluster estiver usando o ONTAP 9.12.1 ou superior, você poderá optar por colocar backups mais antigos em camadas no armazenamento *Archive* na interface do NetApp Backup and Recovery após um determinado número de dias para otimizar ainda mais os custos. "Saiba mais sobre o armazenamento de arquivo do Google" .

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

  Se o seu cluster local estiver usando o ONTAP 9.12.1 ou superior, e o seu sistema StorageGRID estiver usando o 11.4 ou superior, você poderá arquivar arquivos de backup mais antigos no armazenamento de arquivamento em nuvem pública após um determinado número de dias. O suporte atual é para níveis de armazenamento AWS S3 Glacier/S3 Glacier Deep Archive ou Azure Archive. "Saiba mais sobre como arquivar arquivos de backup do StorageGRID" .

Veja xref:./prev-ontap-policy-object-options.html] para obter detalhes sobre como arquivar arquivos de backup mais antigos.

Considerações sobre a política de níveis do FabricPool

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

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

  Esta operação pode causar um aumento único no custo de leitura dos dados do seu provedor de nuvem.

  - Os backups subsequentes são incrementais e não têm esse efeito.
  - Se a política de camadas for atribuída ao volume quando ele for criado inicialmente, você não verá esse problema.
- Considere o impacto dos backups antes de atribuir o `all` política de estratificação para volumes. Como os dados são hierarquizados imediatamente, o NetApp Backup and Recovery lerá os dados da camada de nuvem em vez da camada local. Como as operações de backup simultâneas compartilham o link de rede com o armazenamento de objetos na nuvem, pode ocorrer degradação do desempenho se os recursos da rede ficarem saturados. Nesse caso, talvez você queira configurar proativamente várias interfaces de rede (LIFs) para diminuir esse tipo de saturação de rede.

Planeje sua jornada de proteção com o NetApp Backup and Recovery

O NetApp Backup and Recovery permite que você crie até três cópias dos seus volumes de origem para proteger seus dados. Há muitas opções que você pode selecionar ao habilitar este serviço em seus volumes, então você deve revisar suas escolhas para estar preparado.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Analisaremos as seguintes opções:

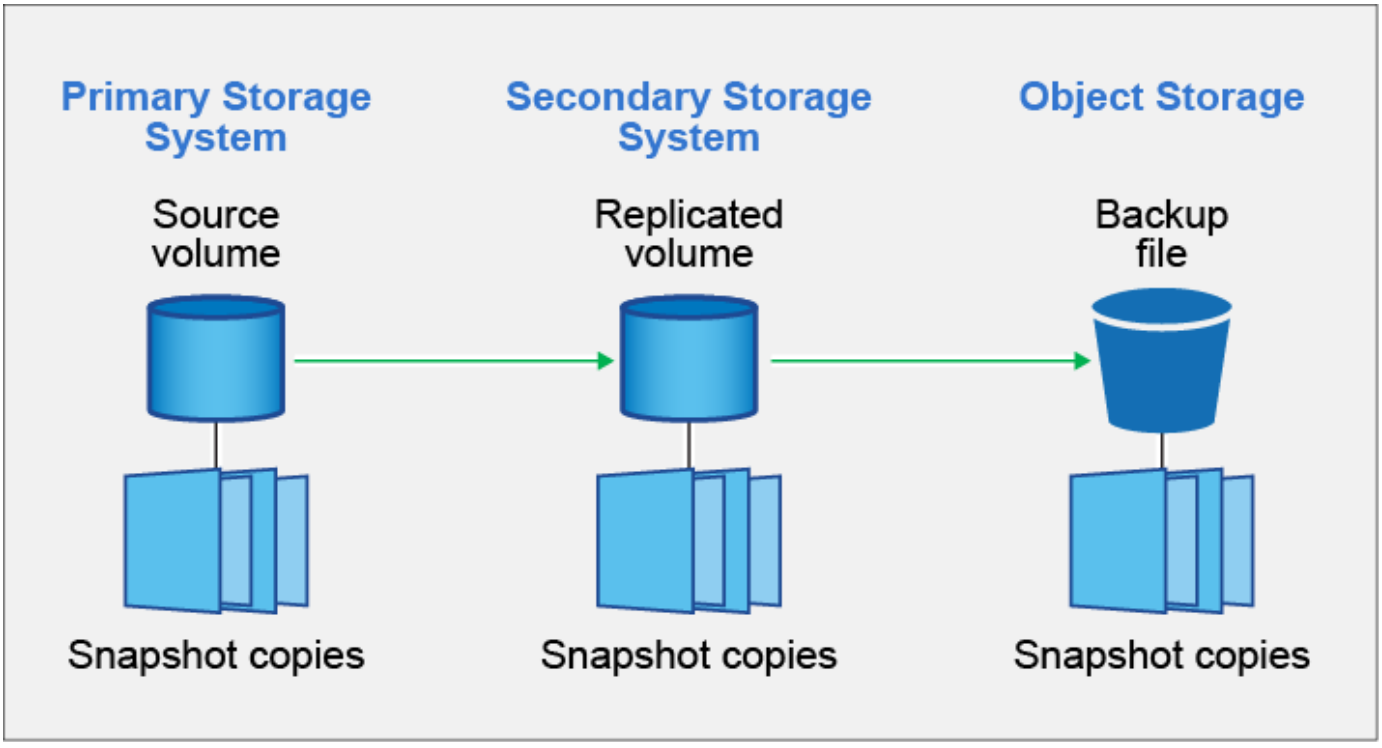
- Quais recursos de proteção você usará: cópias de snapshot, volumes replicados e/ou backup na nuvem
- Qual arquitetura de backup você usará: um backup em cascata ou em fan-out dos seus volumes
- Você usará as políticas de backup padrão ou precisará criar políticas personalizadas
- Você quer que o serviço crie os buckets de nuvem para você ou quer criar seus contêineres de armazenamento de objetos antes de começar
- Qual modo de implantação do agente do Console 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 sobre o que cada recurso faz e que tipo de proteção ele oferece.

Tipo de backup	Descrição
Instantâneo	Cria uma imagem somente leitura, em um determinado momento, de um volume dentro do volume de origem como uma cópia instantânea. Você pode usar a cópia instantânea para recuperar arquivos individuais ou restaurar todo o conteúdo de um volume.
Replicação	Cria uma cópia secundária dos seus dados em outro sistema de armazenamento ONTAP e atualiza continuamente os dados secundários. Seus dados são mantidos atualizados e permanecem disponíveis sempre que você precisar.
Backup em nuvem	Cria backups dos seus dados na nuvem para proteção e para fins de arquivamento de longo prazo. Se necessário, você pode restaurar um volume, uma pasta ou arquivos individuais do backup para o mesmo sistema ou para um sistema 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 instantânea é uma imagem somente leitura de um volume em um determinado momento. A imagem consome espaço de armazenamento mínimo e gera sobrecarga de desempenho insignificante porque registra apenas alterações nos arquivos desde que a última cópia instantânea foi feita. A cópia de instantâneo criada no seu 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 armazenamento ONTAP e fazer backup de arquivos na nuvem. Ou você pode escolher apenas criar volumes replicados ou arquivos de backup: a escolha é sua.

Para resumir, estes são os fluxos de proteção válidos que você pode criar para volumes no seu sistema ONTAP :

- Volume de origem → Cópia de instantâneo → Volume replicado → Arquivo de backup
- Volume de origem → Cópia de instantâneo → Arquivo de backup
- Volume de origem → Cópia de instantâneo → 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*. Transferências subsequentes contêm apenas cópias diferenciais dos dados de origem (o instantâneo).

Comparação dos diferentes métodos de backup

A tabela a seguir mostra uma comparação generalizada dos três métodos de backup. Embora o espaço de armazenamento de objetos normalmente seja mais barato do que o armazenamento 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 precisará restaurar dados dos arquivos de backup na nuvem.

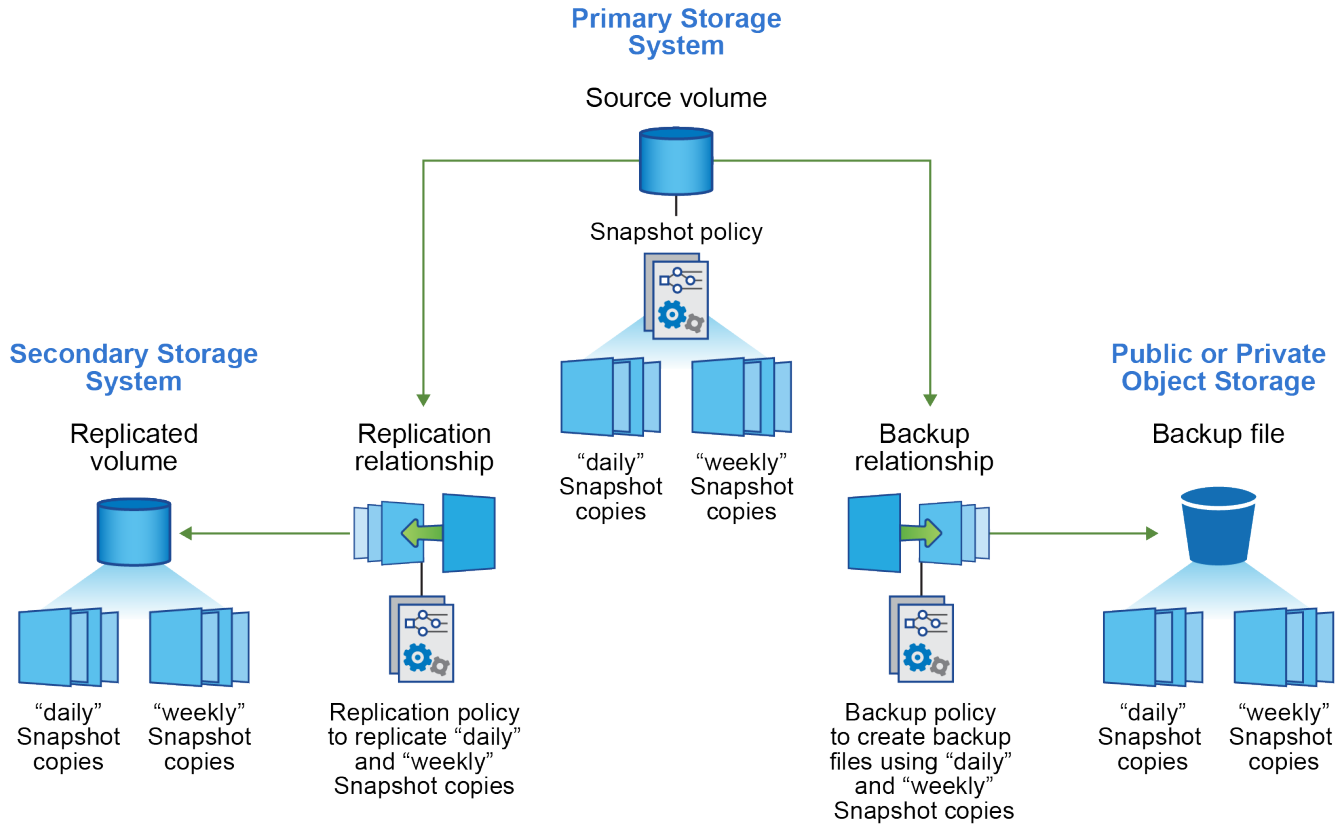
Além desses critérios, o armazenamento em nuvem oferece opções de segurança adicionais se você usar o recurso DataLock e Ransomware Resilience, além de economia de custos adicional ao selecionar classes de armazenamento de arquivamento para arquivos de backup mais antigos. "Saiba mais sobre a proteção do DataLock e do Ransomware e as configurações de armazenamento de arquivamento" .

Tipo de backup	Velocidade de backup	Custo de backup	Restaurar velocidade	Custo de restauração
Instantâneo	Alto	Baixo (espaço em disco)	Alto	Baixo
Replicação	Médio	Médio (espaço em disco)	Médio	Médio (rede)
Backup em nuvem	Baixo	Baixo (espaço do objeto)	Baixo	Alto (taxas do provedor)

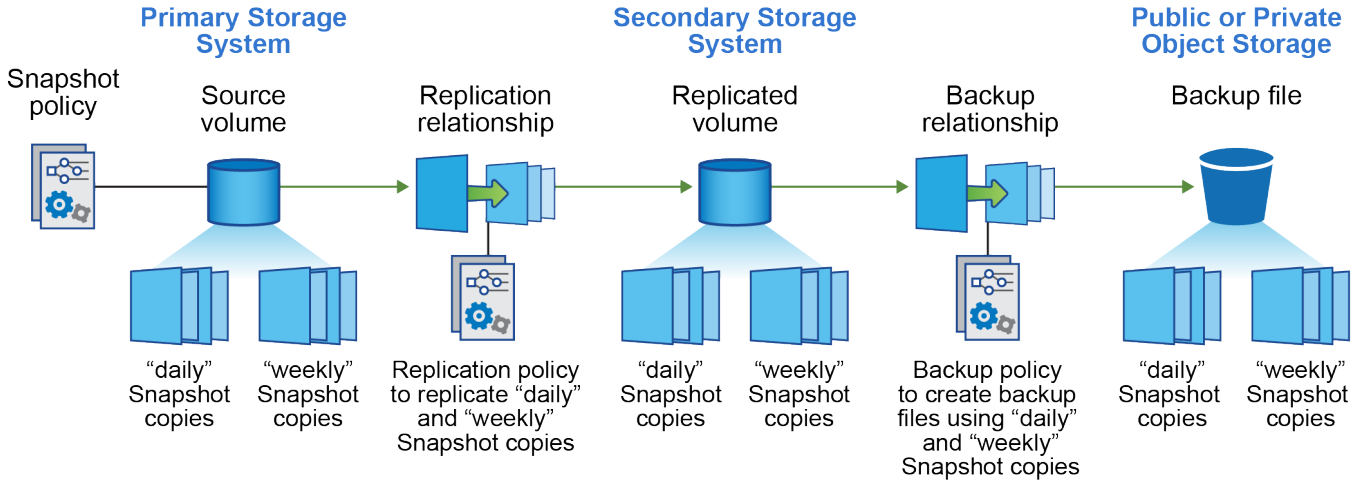
Qual arquitetura de backup você usará

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

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



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



Comparação das diferentes escolhas de arquitetura

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

Fan-out	Cascata
Pequeno impacto no desempenho do sistema de origem porque ele está enviando cópias instantâneas para dois sistemas distintos	Menor efeito no desempenho do sistema de armazenamento de origem porque ele envia a cópia do instantâneo apenas uma vez

Fan-out	Cascata
Mais fácil de configurar porque todas as políticas, redes e configurações ONTAP são feitas no sistema de origem	Requer alguma configuração de rede e ONTAP a ser feita também no sistema secundário.

Você usará as políticas padrão para snapshots, replicações e backups

Você pode usar as políticas padrão fornecidas pela NetApp para criar seus backups ou pode 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 sistema (Cloud Volumes ONTAP ou sistema ONTAP local). Se quiser usar uma política diferente das políticas existentes, você pode criá-la antes de começar ou enquanto usa o assistente de ativação.

- A política de snapshot padrão cria cópias de snapshot por hora, diariamente e semanalmente, retendo 6 cópias de snapshot por hora, 2 diariamente e 2 semanalmente.
- A política de replicação padrão replica cópias de instantâneos diárias e semanais, retendo 7 cópias de instantâneos diárias e 52 semanais.
- A política de backup padrão replica cópias de instantâneos diárias e semanais, retendo 7 cópias de instantâneos diárias e 52 semanais.

Se você criar políticas personalizadas para replicação ou backup, os rótulos das políticas (por exemplo, "diário" ou "semanal") deverão corresponder aos rótulos existentes nas suas políticas de instantâneo, ou os volumes replicados e os arquivos de backup não serão criados.

Você pode criar snapshot, replicação e backup para políticas de armazenamento de objetos na interface de usuário do NetApp Backup and Recovery. Veja a seção para"adicionando uma nova política de backup" para mais detalhes.

Além de usar o NetApp Backup and Recovery para criar políticas personalizadas, você pode usar o System Manager ou a Interface de Linha de Comando (CLI) do ONTAP :

- "Crie uma política de snapshot usando o System Manager ou o ONTAP CLI"
- "Crie uma política de replicação usando o System Manager ou o ONTAP CLI"

Observação: Ao usar o Gerenciador do Sistema, selecione **Assíncrono** como o tipo de política para políticas de replicação e selecione **Assíncrono** e **Fazer backup na nuvem** para políticas de backup em objetos.

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

Descrição da Política	Comando
Política de snapshot simples	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`

Descrição da Política	Comando
Backup simples para a 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`
Backup para 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 para nuvem com classe de armazenamento de arquivo	`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 armazenamento	`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 cofre podem ser usadas para backup em relacionamentos na nuvem.

Onde ficam 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 as políticas de backup não são projetadas da mesma forma porque as replicações emparelham dois sistemas de armazenamento ONTAP e o backup para objeto usa um provedor de armazenamento como destino.

- As políticas de instantâneo sempre residem no sistema de armazenamento primário.
- As políticas de replicação sempre residem no sistema de armazenamento secundário.
- As políticas de backup para objeto são criadas no sistema onde 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 de instantâneo	Política de replicação	Política de backup
Espalhar	Primário	Secundário	Primário
Cascata	Primário	Secundário	Secundário

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

fazer backup em políticas de objeto no sistema primário.

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

Você quer criar seu próprio contêiner de armazenamento de objetos

Ao criar arquivos de backup no armazenamento de objetos de um sistema, por padrão, o serviço de backup e recuperação cria o contêiner (bucket ou conta de armazenamento) para os arquivos de backup na conta de armazenamento de objetos que você configurou. O bucket AWS ou GCP é chamado "netapp-backup-<uuid>" por padrão. A conta de armazenamento de Blobs do Azure é chamada "netappbackup<uuid>".

Você pode criar o contêiner na conta do provedor de objetos se quiser usar um prefixo específico ou atribuir propriedades especiais. Se você quiser criar seu próprio contêiner, deverá criá-lo antes de iniciar o assistente de ativação. O NetApp Backup and Recovery pode usar qualquer bucket e compartilhar buckets. O assistente de ativação de backup descobrirá automaticamente seus contêineres provisionados para a conta e as credenciais selecionadas para que você possa selecionar o que deseja usar.

Você pode criar o bucket no Console ou no seu provedor de nuvem.

- "Crie buckets do Amazon S3 no console"
- "Crie contas de armazenamento de Blobs do Azure no Console"
- "Crie buckets do Google Cloud Storage no Console"

Se você planeja usar um prefixo de bucket diferente de "netapp-backup-xxxxxx", será necessário modificar as permissões do S3 para a função IAM do agente do console.

Configurações avançadas do bucket

Se você planeja mover arquivos de backup mais antigos para armazenamento de arquivo ou se planeja habilitar a proteção DataLock e Ransomware para bloquear seus arquivos de backup e verificá-los em busca de possível ransomware, você precisará criar o contêiner com determinadas configurações:

- O armazenamento de arquivamento em seus próprios buckets é suportado no armazenamento AWS S3 no momento ao usar o software ONTAP 9.10.1 ou superior em seus 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* (antigo S3 Glacier)
- A proteção contra DataLock e Ransomware é suportada no armazenamento da AWS ao usar o software ONTAP 9.11.1 ou superior em seus clusters, e no 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.

Qual modo de implantação do agente do console você está usando

Se você já estiver usando o Console para gerenciar seu armazenamento, um agente do Console já terá sido instalado. Se você planeja usar o mesmo agente do Console com o NetApp Backup and Recovery, está tudo

pronto. Se precisar usar um agente de console diferente, você precisará instalá-lo antes de iniciar a implementação de backup e recuperação.

O NetApp Console oferece vários modos de implantação que permitem que você use o Console de uma maneira que atenda aos seus requisitos comerciais e de segurança. O *modo padrão* aproveita a camada SaaS do Console para fornecer funcionalidade completa, enquanto o *modo restrito* e o *modo privado* estão disponíveis para organizações com restrições de conectividade.

"Saiba mais sobre os modos de implantação do NetApp Console" .

Suporte para sites com conectividade total à Internet

Quando o NetApp Backup and Recovery é usado em um site com conectividade total à Internet (também conhecido como *modo padrão* ou *modo SaaS*), você pode criar volumes replicados em qualquer sistema ONTAP local ou Cloud Volumes ONTAP gerenciado pelo Console e pode criar arquivos de backup no armazenamento de objetos em qualquer um dos provedores de nuvem suportados. "Veja a lista completa de destinos de backup suportados" .

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

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

Suporte para sites com conectividade de internet limitada

O NetApp Backup and Recovery pode ser usado em um local com conectividade de internet limitada (também conhecido como *modo restrito*) para fazer backup de dados de volume. Nesse caso, você precisará implantar o agente do Console na região da nuvem de destino.

- Você pode fazer backup de dados de sistemas ONTAP locais ou sistemas Cloud Volumes ONTAP instalados em regiões comerciais da AWS para o Amazon S3. "Faça backup dos dados do Cloud Volumes ONTAP no Amazon S3" .
- Você pode fazer backup de dados de sistemas ONTAP locais ou sistemas Cloud Volumes ONTAP instalados em regiões comerciais do Azure para o Azure Blob. "Faça backup dos dados do Cloud Volumes ONTAP no Azure Blob" .

Suporte para sites sem conectividade com a Internet

O NetApp Backup and Recovery pode ser usado em um site sem conectividade com a Internet (também conhecido como *modo privado* ou sites *escuros*) para fazer backup de dados de volume. Nesse caso, você precisará implantar o agente do Console em um host Linux no mesmo site.

O modo privado BlueXP (interface BlueXP legada) normalmente é usado com ambientes locais que não têm conexão com a Internet e com regiões de nuvem seguras, o que inclui AWS Secret Cloud, AWS Top Secret Cloud e Azure IL6. A NetApp continua a oferecer suporte a esses ambientes com a interface legada BlueXP . Para documentação do modo privado na interface BlueXP legada, consulte o "Documentação em PDF para o modo privado do BlueXP" .

- Você pode fazer backup de dados de sistemas ONTAP locais para sistemas NetApp StorageGRID locais. "Faça backup de dados ONTAP locais no StorageGRID" .
- Você pode fazer backup de dados de sistemas ONTAP locais para sistemas ONTAP locais ou sistemas Cloud Volumes ONTAP configurados para armazenamento de objetos S3. "Faça backup de dados ONTAP locais no ONTAP S3" . ifdef::aws[]

Gerencie políticas de backup para volumes ONTAP com o NetApp Backup and Recovery

Com o NetApp Backup and Recovery, use as políticas de backup padrão fornecidas pela NetApp para criar seus backups ou crie políticas personalizadas. As políticas controlam a frequência do backup, o horário em que o backup é feito e o número de arquivos de backup que são retidos.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

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 sistema (Cloud Volumes ONTAP ou sistema ONTAP local). Se quiser usar uma política diferente das políticas existentes, você pode criá-la antes ou enquanto usa o assistente de ativação.

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

O NetApp Backup and Recovery oferece três tipos de backups de dados ONTAP : snapshots, replicações e backups para armazenamento 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 de instantâneo	Local de armazenamento da política de replicação	Backup para local de armazenamento de política de objeto
Espalhar	Primário	Secundário	Primário
Cascata	Primário	Secundário	Secundário

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

- Interface do usuário do console NetApp
- Interface do usuário do gerenciador de sistema
- CLI ONTAP

Ao usar o Gerenciador do Sistema, selecione **Assíncrono** como o tipo de política para políticas de replicação e selecione **Assíncrono** e **Fazer backup na nuvem** para políticas de backup em objetos.

Exibir políticas para um sistema

1. Na interface do usuário do console, selecione **Volumes** > **Configurações de backup**.
2. Na página Configurações de backup, selecione o sistema, selecione **Ações*** ••• **ícone e selecione *Gerenciamento de políticas**.

   A página Gerenciamento de políticas é exibida. As políticas de instantâneo são exibidas por padrão.

3. Para visualizar outras políticas existentes no sistema, selecione **Políticas de replicação** ou **Políticas de backup**. Se as políticas existentes puderem ser usadas para seus planos de backup, está tudo pronto. Se você precisar ter uma apólice com características diferentes, você pode criar novas apólices nesta página.

Criar políticas

Você pode criar políticas que controlam suas cópias de instantâneos, replicações e backups para armazenamento de objetos:

- Crie uma política de snapshot antes de iniciar o snapshot
- 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 snapshot antes de iniciar o snapshot

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

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

Passos

1. Na interface do usuário do console, selecione **Volumes** > **Configurações de backup**.
2. Na página Configurações de backup, selecione o sistema, selecione **Ações*** ••• **ícone e selecione *Gerenciamento de políticas**.

   A página Gerenciamento de políticas é exibida.

3. Na página Políticas, selecione **Criar política** > **Criar política de instantâneo**.
4. Especifique o nome da política.
5. Selecione o agendamento ou agendamentos de snapshot. Você pode ter no máximo 5 rótulos. Ou crie uma programação.
6. Se você optar por criar uma programação:
   a. Selecione a frequência: horária, diária, semanal, mensal ou anual.
   b. Especifique os rótulos de instantâneo que indicam o agendamento e a retenção.
   c. Insira quando e com que frequência o instantâneo será tirado.
   d. Retenção: insira o número de snapshots 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 de replicação e backup para objeto.
   c. Crie a política de snapshot.
2. Cluster 2:
   a. Selecione Cluster 2 na página Política.
   b. Ignore a seção de política de snapshot.
   c. Configure as políticas de replicação e backup para objetos.

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 armazenamento 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 os rótulos do SnapMirror (máximo de 5) que indicam a retenção de cada rótulo.
4. Especifique o cronograma 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 no armazenamento de objetos.

Esta política de armazenamento reside em diferentes locais do sistema de armazenamento, dependendo da arquitetura de backup:

- Fan-out: Sistema de armazenamento primário
- Cascata: Sistema de armazenamento 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 os rótulos do SnapMirror (máximo de 5) que indicam a retenção de cada rótulo.
4. Especifique as configurações, incluindo o cronograma de transferência e quando arquivar backups.
5. (Opcional) Para mover arquivos de backup mais antigos para uma classe de armazenamento ou nível de acesso menos dispendioso após um determinado número de dias, selecione a opção **Arquivar** 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 arquivamento.

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

6. (Opcional) Para proteger seus backups contra modificações ou exclusão, selecione a opção **Proteção DataLock e Ransomware**.

   Se o seu cluster estiver usando o ONTAP 9.11.1 ou superior, você pode optar por proteger seus backups contra exclusão configurando o *DataLock* e a *proteção contra ransomware*.

   "Saiba mais sobre as configurações disponíveis do DataLock" .

7. Selecione **Criar**.

Editar uma política

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

Alterar a política de backup afeta todos os volumes que estão usando essa política.

Passos

1. Na página Gerenciamento de políticas, selecione a política, selecione **Ações*** ícone 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 **Salvar**.

Excluir uma política

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

Se uma política estiver associada a um volume e você quiser excluí-la, será necessário removê-la do volume primeiro.

Passos

1. Na página Gerenciamento de políticas, selecione a política, selecione **Ações*** ícone e selecione ***Excluir política de instantâneo**.
2. Selecione **Excluir**.

Encontre mais informações

Para obter instruções sobre como criar políticas usando o System Manager ou o ONTAP CLI, consulte o seguinte:

"Crie uma política de instantâneo usando o Gerenciador de sistemas" "Crie uma política de Snapshot usando o ONTAP CLI" "Crie uma política de replicação usando o Gerenciador do Sistema" "Crie uma política de replicação usando o ONTAP CLI" "Crie um backup para uma política de armazenamento de objetos usando o Gerenciador do Sistema" "Crie um backup para uma política de armazenamento de objetos usando o ONTAP CLI"

Opções de política de backup para objeto no NetApp Backup and Recovery

O NetApp Backup and Recovery permite que você crie políticas de backup com uma

variedade de configurações para seus sistemas ONTAP locais e Cloud Volumes ONTAP .

Essas configurações de política são relevantes somente para armazenamento de backup em objeto. Nenhuma dessas configurações afeta suas políticas de snapshot ou replicação.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Opções de agendamento de backup

O NetApp Backup and Recovery permite que você crie várias políticas de backup com agendamentos exclusivos para cada sistema (cluster). Você pode atribuir diferentes políticas de backup a volumes que tenham diferentes objetivos de ponto de recuperação (RPO).

Cada política de backup fornece uma seção para *Rótulos e retenção* que você pode aplicar aos seus arquivos de backup. Observe que a política de Snapshot aplicada ao volume deve ser uma das políticas reconhecidas pelo NetApp Backup and Recovery, ou os arquivos de backup não serão criados.

Há duas partes do cronograma: o rótulo e o valor de retenção:

- O **rótulo** define a frequência com que um arquivo de backup é criado (ou atualizado) a partir do volume. Você pode selecionar entre os seguintes tipos de etiquetas:
  - Você pode escolher um ou uma combinação de períodos de tempo **por hora**, **diário**, **semanal**, **mensal** e **anual**.
  - Você pode selecionar uma das políticas definidas pelo sistema que fornecem backup e retenção por 3 meses, 1 ano ou 7 anos.
  - Se você tiver criado políticas de proteção de backup personalizadas no cluster usando o ONTAP System Manager ou o ONTAP CLI, poderá selecionar uma dessas políticas.
- O valor **retenção** define quantos arquivos de backup para cada rótulo (período de tempo) são retidos. Quando o número máximo de backups for atingido em uma categoria ou intervalo, os backups mais antigos serão removidos para que você sempre tenha 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 7 backups **semanais** e 12 **mensais**:

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

Os backups anuais são excluídos automaticamente do sistema de origem após serem transferidos para o armazenamento de objetos. Esse comportamento padrão pode ser alterado na página Configurações avançadas do sistema.

Opções de proteção DataLock e Ransomware

O NetApp Backup and Recovery oferece suporte para proteção DataLock e Ransomware para seus backups

de volume. Esses recursos permitem que você bloqueie seus arquivos de backup e os verifique para detectar possíveis ransomwares 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 para um cluster.

Ambos os 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 aos 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 DataLock e Ransomware Resilience estiver habilitada, o bucket de nuvem provisionado como parte da ativação do NetApp Backup and Recovery terá o bloqueio de objetos e o controle de versão de objetos habilitados.

"Veja o blog de proteção DataLock e Ransomware para mais detalhes" .

Este recurso não fornece proteção para seus volumes de origem; apenas para os backups desses volumes de origem. Use alguns dos "proteções anti-ransomware fornecidas pela ONTAP" para proteger seus 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 NetApp Backup and Recovery para esse cluster. Mais tarde, você pode habilitar ou desabilitar a verificação de ransomware usando as Configurações avançadas do NetApp Backup and Recovery.
- Quando o Console 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

Com esse recurso, você pode bloquear os snapshots da nuvem replicados via SnapMirror para a nuvem e também habilitar o recurso para detectar um ataque de ransomware e recuperar uma cópia consistente do snapshot no armazenamento de objetos. Este recurso é compatível com AWS, Azure e StorageGRID.

O DataLock protege seus arquivos de backup contra modificações ou exclusão por um determinado período de tempo - também chamado de *armazenamento imutável*. Essa funcionalidade usa tecnologia do provedor de armazenamento de objetos para "bloqueio de objetos".

Os provedores de nuvem usam uma Data de Retenção Até (RUD), que é calculada com base no Período de Retenção de Snapshot. O Período de Retenção de Snapshot é calculado com base no rótulo e na contagem de retenção definidos na política de backup.

O Período mínimo de retenção de instantâneos é de 30 dias. Vejamos alguns exemplos de como isso funciona:

- Se você escolher o rótulo **Diário** com Contagem de retenção 20, o Período de retenção do instantâneo será de 20 dias, cujo padrão é o mínimo de 30 dias.
- Se você escolher o rótulo **Semanal** com Contagem de retenção 4, o Período de retenção do instantâneo será de 28 dias, cujo padrão é o mínimo de 30 dias.
- Se você escolher o rótulo **Mensal** com Contagem de retenção 3, o Período de retenção do instantâneo será de 90 dias.
- Se você escolher o rótulo **Anual** com Contagem de retenção 1, o Período de retenção do instantâneo será de 365 dias.

O que é Retenção até a Data (RUD) e como ela é calculada?

A data de retenção (RUD) é determinada com base no período de retenção do instantâneo. A data de retenção é calculada somando o período de retenção do instantâneo e um buffer.

- Buffer é o Buffer para Tempo de Transferência (3 dias) + Buffer para Otimização de Custos (28 dias), totalizando 31 dias.
- A data mínima de retenção é de 30 dias + buffer de 31 dias = 61 dias.

Aqui estão alguns exemplos:

- Se você criar um agendamento de backup mensal com 12 retenções, seus backups serão bloqueados por 12 meses (mais 31 dias) antes de serem excluídos (substituídos pelo próximo arquivo de backup).
- 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" são mantidos por 61 dias (30 dias mais 31 dias de buffer),
  - Os backups "7 semanais" são mantidos por 11 semanas (7 semanas mais 31 dias) e
  - Os backups "de 12 meses" são mantidos por 12 meses (mais 31 dias).
- Se você criar um agendamento de backup por hora com 24 retenções, poderá pensar que os backups ficarão bloqueados por 24 horas. Entretanto, como isso é menos que o mínimo de 30 dias, cada backup será bloqueado e retido por 61 dias (30 dias mais 31 dias de buffer).

Os backups antigos são excluídos após o término do Período de Retenção do DataLock, não após o período de retenção da política de backup.

A configuração de retenção do DataLock substitui a configuração de retenção de política da sua política de backup. Isso pode afetar seus custos de armazenamento, pois seus arquivos de backup serão salvos no armazenamento de objetos por um período de tempo mais longo.

Habilitar proteção contra DataLock e Ransomware

Você pode habilitar a proteção DataLock e Ransomware ao criar uma política. Você não pode habilitar, modificar ou desabilitar isso depois que a política for criada.

1. Ao criar uma política, expanda a seção **DataLock e Resiliência contra Ransomware**.
2. Escolha uma das seguintes opções:
   - **Nenhum**: A proteção DataLock e a resiliência contra ransomware estão desabilitadas.
   - **Desbloqueado**: A proteção DataLock e a resiliência contra ransomware estão ativadas. Usuários com permissões específicas podem substituir ou excluir arquivos de backup protegidos durante o período de retenção.
   - **Bloqueado**: A proteção DataLock e a resiliência contra ransomware estão ativadas. Nenhum usuário pode substituir ou excluir arquivos de backup protegidos durante o período de retenção. Isso satisfaz a conformidade regulatória total.

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

O que é proteção contra ransomware

A proteção contra ransomware verifica seus arquivos de backup em busca de evidências de um ataque de ransomware. A detecção de ataques de ransomware é realizada usando uma comparação de soma de

verificação. Se um possível ransomware for identificado em um novo arquivo de backup em comparação ao arquivo de backup anterior, esse arquivo de backup mais recente será substituído pelo arquivo de backup mais recente que não mostre nenhum sinal de ataque de ransomware. (O arquivo que foi identificado como tendo um ataque de ransomware é excluído 1 dia após ter sido substituído.)

As varreduras ocorrem nas seguintes situações:

- As verificações em objetos de backup na nuvem são iniciadas logo após eles serem transferidos para o armazenamento de objetos na nuvem. A verificação não é realizada no arquivo de backup quando ele é gravado pela primeira vez no armazenamento em nuvem, mas quando o próximo arquivo de backup é gravado.
- As verificações de ransomware podem ser iniciadas quando o backup é selecionado para o processo de restauração.
- As varreduras podem ser realizadas sob demanda a qualquer momento.

Como funciona o processo de recuperação?

Quando um ataque de ransomware é detectado, o serviço usa a API REST do Integrity Checker do agente do Active Data Console para iniciar o processo de recuperação. A versão mais antiga dos objetos de dados é a fonte da verdade e é transformada na versão atual como parte do processo de recuperação.

Vamos ver como isso funciona:

- No caso de um ataque de ransomware, o serviço tenta substituir ou excluir o objeto no bucket.
- Como o armazenamento em nuvem permite controle de versão, ele cria automaticamente uma nova versão do objeto de backup. Se um objeto for excluído com o controle de versão ativado, ele será marcado como excluído, mas ainda poderá ser recuperado. Se um objeto for substituído, versões anteriores serão armazenadas e marcadas.
- Quando uma verificação de ransomware é iniciada, as somas de verificação são validadas para ambas as versões do objeto e comparadas. Se as somas de verificação forem inconsistentes, um possível ransomware foi detectado.
- O processo de recuperação envolve reverter para a última cópia boa conhecida.

Sistemas suportados e provedores de armazenamento de objetos

Você pode habilitar a proteção DataLock e Ransomware em volumes ONTAP dos seguintes sistemas ao usar o armazenamento de objetos nos seguintes provedores de nuvem pública e privada.

Sistema de origem	Destino do arquivo de backup ifdef::aws[]
Cloud Volumes ONTAP na AWS	Amazon S3 endif::aws[] ifdef::azure[]
Cloud Volumes ONTAP no Azure	Blob do Azure endif::azure[] ifdef::gcp[]
Cloud Volumes ONTAP no Google Cloud	Google Cloud endif::gcp[]
Sistema ONTAP local	ifdef::aws[] Amazon S3 endif::aws[] ifdef::azure[] Azure Blob endif::azure[] ifdef::gcp[] Google Cloud endif::gcp[] NetApp StorageGRID

Requisitos

- Para AWS:

- Seus clusters devem executar o ONTAP 9.11.1 ou superior
- O agente do Console pode ser implantado na nuvem ou em suas instalações
- As seguintes permissões do S3 devem fazer parte da função do IAM que fornece permissões ao agente do Console. Eles residem na seção "backupS3Policy" do recurso "arn:aws:s3:::netapp-backup-*":

  Permissões do AWS S3

  - s3:ObterTag deVersão do Objeto
  - s3:GetBucketObjectLockConfiguration
  - s3:ObterVersãoDoObjetoAcl
  - s3:PutObjectTagging
  - s3:ExcluirObjeto
  - s3:ExcluirMarcaçãoDeObjeto
  - s3:ObterRetençãoDeObjeto
  - s3:ExcluirMarcaçãoDeVersãoDoObjeto
  - s3:ColocarObjeto
  - s3:ObterObjeto
  - s3:PutBucketObjectLockConfiguração
  - s3:ObterConfiguração do Ciclo de Vida
  - s3:Obter marcação de balde
  - s3:ExcluirVersãoDoObjeto
  - s3:ListBucketVersões
  - s3:ListBucket
  - s3:PutBucketTagging
  - s3:ObterMarcaçãoDeObjeto
  - s3:PutBucketVersionamento
  - s3:PutObjectVersionTagging
  - s3:GetBucketVersionamento
  - s3:ObterBucketAcl
  - s3:Ignorar Governança Retenção
  - s3:PutObjectRetention
  - s3:ObterLocalização do Balde
  - s3:ObterVersãoDoObjeto

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

- Para o Azure:
  - Seus clusters devem executar o ONTAP 9.12.1 ou superior

    - O agente do Console pode ser implantado na nuvem ou em suas instalações
- Para o Google Cloud:
    - Seus clusters devem estar executando o ONTAP 9.17.1 ou superior
    - O agente do Console pode ser implantado na nuvem ou em suas instalações
- Para StorageGRID:
    - Seus clusters devem executar o ONTAP 9.11.1 ou superior
    - Seus sistemas StorageGRID devem estar executando 11.6.0.3 ou superior
    - O agente do Console 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 agente do Console:

Permissões do StorageGRID S3

- s3:ObterTag deVersão do Objeto
- s3:GetBucketObjectLockConfiguration
- s3:ObterVersãoDoObjetoAcl
- s3:PutObjectTagging
- s3:ExcluirObjeto
- s3:ExcluirMarcaçãoDeObjeto
- s3:ObterRetençãoDeObjeto
- s3:ExcluirMarcaçãoDeVersãoDoObjeto
- s3:ColocarObjeto
- s3:ObterObjeto
- s3:PutBucketObjectLockConfiguração
- s3:ObterConfiguração do Ciclo de Vida
- s3:Obter marcação de balde
- s3:ExcluirVersãoDoObjeto
- s3:ListBucketVersões
- s3:ListBucket
- s3:PutBucketTagging
- s3:ObterMarcaçãoDeObjeto
- s3:PutBucketVersionamento
- s3:PutObjectVersionTagging
- s3:GetBucketVersionamento
- s3:ObterBucketAcl
- s3:PutObjectRetention
- s3:ObterLocalização do Balde
- s3:ObterVersãoDoObjeto

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 NetApp Backup and Recovery deve ser usada para todas as políticas de backup desse cluster.
- Não é possível usar vários modos DataLock em um único cluster.
- Se você habilitar o DataLock, todos os backups de volume serão bloqueados. Não é possível misturar backups de volumes bloqueados e não bloqueados para um único cluster.
- A proteção contra DataLock e Ransomware é aplicável para novos backups de volume usando uma política de backup com proteção contra DataLock e Ransomware habilitada. Você pode habilitar ou desabilitar esses recursos posteriormente usando a opção Configurações avançadas.

- Os volumes 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 custos extras, você pode desabilitar as verificações agendadas de ransomware. Isso permite que você personalize suas configurações de segurança e evite incorrer em custos do provedor de nuvem.

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

Você pode escolher diferentes níveis de proteção:

- **DataLock *sem* varreduras de ransomware**: Fornece proteção para dados de backup no armazenamento de destino que pode estar no modo de Governança ou Conformidade.
  - **Modo de governança**: Oferece flexibilidade aos administradores para substituir ou excluir dados protegidos.
  - **Modo de conformidade**: Oferece indelével completo até que o período de retenção expire. Isso ajuda a atender aos requisitos de segurança de dados mais rigorosos de ambientes altamente regulamentados. Os dados não podem ser substituídos ou modificados durante seu ciclo de vida, fornecendo o mais alto nível de proteção para suas cópias de backup.

    O Microsoft Azure usa um modo de bloqueio e desbloqueio.

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

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

Além disso, você pode obter estimativas de custo associadas ao DataLock visitando o "Calculadora de custo total de propriedade (TCO) do NetApp Backup and Recovery" .

Opções de armazenamento de arquivo

Ao usar o armazenamento em nuvem AWS, Azure ou Google, você pode mover arquivos de backup mais antigos para uma classe de armazenamento de arquivamento ou nível de acesso mais barato após um determinado número de dias. Você também pode optar por enviar seus arquivos de backup para armazenamento de arquivo imediatamente, sem que eles sejam gravados no armazenamento em nuvem padrão. Basta digitar **0** como "Arquivar após 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 precisará restaurar dados de arquivos de backup antes de decidir arquivá-los.

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

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

- Na AWS, os backups começam na classe de armazenamento *Padrão* e fazem a transição para a classe de armazenamento *Acesso Infrequente Padrão* após 30 dias.

  Se o seu cluster estiver usando o ONTAP 9.10.1 ou superior, você poderá colocar backups mais antigos em camadas no armazenamento *S3 Glacier* ou *S3 Glacier Deep Archive*. "Saiba mais sobre o armazenamento de arquivo da AWS" .

  - Se você não selecionar nenhuma camada de arquivamento em sua primeira política de backup ao ativar o NetApp Backup and Recovery, o *S3 Glacier* será sua única opção de arquivamento para políticas futuras.
  - Se você selecionar *S3 Glacier* na sua primeira política de backup, poderá mudar para a camada *S3 Glacier Deep Archive* para futuras políticas de backup para esse cluster.
  - Se você selecionar *S3 Glacier Deep Archive* na sua primeira política de backup, essa camada será a única camada de arquivamento disponível para futuras políticas de backup para esse cluster.
- No Azure, os backups são associados à camada de acesso *Cool*.

  Se o seu cluster estiver usando o ONTAP 9.10.1 ou superior, você poderá colocar backups mais antigos em camadas no armazenamento *Azure Archive*. "Saiba mais sobre o armazenamento de arquivamento do Azure" .

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

  Se o seu cluster local estiver usando o ONTAP 9.12.1 ou superior, você poderá optar por colocar backups mais antigos em camadas no armazenamento *Archive* na interface do usuário do NetApp Backup and Recovery após um determinado número de dias para otimizar ainda mais os custos. "Saiba mais sobre o armazenamento de arquivo do Google" .

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

  Se o seu cluster local estiver usando o ONTAP 9.12.1 ou superior, e o seu sistema StorageGRID estiver usando o 11.4 ou superior, você poderá arquivar arquivos de backup mais antigos no armazenamento de arquivamento em nuvem pública.

+ ** Para AWS, você pode fazer backups em camadas no armazenamento AWS *S3 Glacier* ou *S3 Glacier Deep Archive*. "Saiba mais sobre o armazenamento de arquivo da AWS" .

+ ** Para o Azure, você pode colocar backups mais antigos em camadas no armazenamento *Azure Archive*. "Saiba mais sobre o armazenamento de arquivamento do Azure" .

Gerenciar opções de armazenamento de backup para objeto nas Configurações avançadas do NetApp Backup and Recovery

Você pode alterar as configurações de armazenamento de backup para objeto no nível do cluster definidas ao ativar o NetApp Backup and Recovery 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 armazenamento de objetos, se cópias históricas do Snapshot são exportadas como arquivos de backup e habilitar ou desabilitar verificações de ransomware para um sistema.

Essas configurações estão disponíveis somente para armazenamento de backup em objeto. Nenhuma dessas configurações afeta suas configurações de Snapshot ou replicação.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Você pode alterar as seguintes opções na página Configurações avançadas:

- Alterando a largura de banda de rede alocada para carregar backups no armazenamento de objetos usando a opção Max Transfer Rate ifdef::aws[]
- Alterar se cópias históricas do Snapshot são exportadas como arquivos de backup e incluídas nos arquivos de backup de linha de base inicial para volumes futuros
- Alterar se os snapshots "anuais" são removidos do sistema de origem
- Habilitar ou desabilitar varreduras de ransomware para um sistema, incluindo varreduras agendadas

Exibir configurações de backup em nível de cluster

Você pode visualizar as configurações de backup em nível de cluster para cada sistema.

Passos

1. No menu Console, selecione **Proteção > Backup e recuperação**.
2. Na aba **Volumes**, selecione **Configurações de backup**.
3. Na página *Configurações de backup*, clique em ••• para o sistema e selecione **Configurações avançadas**.

   A página *Configurações avançadas* exibe as configurações atuais do sistema.

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 no destino do provedor de nuvem onde os backups residem.

Alterar a largura de banda de rede disponível para fazer upload de backups para armazenamento de objetos

Quando você ativa o NetApp Backup and Recovery para um sistema, por padrão, o ONTAP pode usar uma

quantidade ilimitada de largura de banda para transferir os dados de backup de volumes no sistema para o armazenamento de objetos. Se você perceber que o tráfego de backup está afetando as cargas de trabalho normais dos usuários, você pode limitar a quantidade de largura de banda de rede usada durante a transferência usando a opção Taxa máxima de transferência na página Configurações avançadas.

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, clique em ••• para o sistema e selecione **Configurações avançadas**.
3. Na página Configurações avançadas, expanda a seção **Taxa máxima de transferência**.
4. Escolha um valor entre 1 e 1.000 Mbps como taxa máxima de transferência.
5. Selecione o botão de opção **Limitado** e insira a largura de banda máxima que pode ser usada ou selecione **Ilimitado** para indicar que não há limite.
6. Selecione **Aplicar**.

Esta configuração não afeta a largura de banda alocada para quaisquer outros relacionamentos de replicação que possam ser configurados para volumes no sistema.

Alterar se cópias históricas de instantâneos são exportadas como arquivos de backup

Se houver cópias de instantâneos locais para volumes que correspondam ao rótulo de agendamento de backup que você está usando neste sistema (por exemplo, diário, semanal, etc.), você poderá exportar esses instantâneos históricos para o armazenamento de objetos como arquivos de backup. Isso permite que você inicialize seus backups na nuvem movendo cópias de instantâneos mais antigas para a cópia de backup de base.

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

Passos

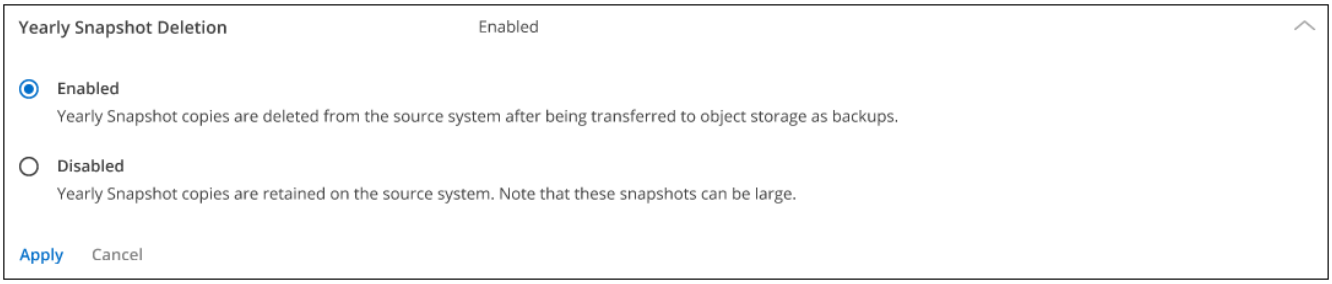
1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, clique em ••• para o sistema e selecione **Configurações avançadas**.
3. Na página Configurações avançadas, expanda a seção **Exportar cópias de instantâneos existentes**.
4. Selecione se deseja que cópias existentes do Snapshot sejam exportadas.
5. Selecione **Aplicar**.

Alterar se os snapshots "anuais" são removidos do sistema de origem

Quando você seleciona o rótulo de backup "anual" para uma política de backup para qualquer um dos seus volumes, a cópia do Snapshot criada é muito grande. Por padrão, esses instantâneos 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 anual de instantâneos.

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, clique em ••• para o sistema e selecione **Configurações avançadas**.
3. Na página Configurações avançadas, expanda a seção **Exclusão anual de instantâneos**.



4. Selecione **Desativado** para manter os instantâneos anuais no sistema de origem.
5. Selecione **Aplicar**.

Habilitar ou desabilitar verificações de ransomware

As verificações de proteção contra ransomware são ativadas por padrão. A configuração padrão para a frequência de verificação é de 7 dias. A verificação ocorre apenas na cópia mais recente do instantâneo. Você pode habilitar ou desabilitar verificações de ransomware na cópia mais recente do snapshot usando a opção na página Configurações avançadas. Se você habilitar, as verificações serão realizadas a cada 7 dias por padrão.

Para obter detalhes sobre as opções de DataLock e Ransomware Resilience, consulte"Opções de resiliência do DataLock e do Ransomware" .

Você pode alterar essa programação para dias ou semanas ou desativá-la, economizando custos.

A ativação de verificações de ransomware incorrerá em custos extras, dependendo do provedor de nuvem.

As verificações agendadas de ransomware são executadas apenas na cópia mais recente do snapshot.

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

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

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, clique em••• para o sistema e selecione **Configurações avançadas**.
3. Na página Configurações avançadas, expanda a seção **Verificação de ransomware**.
4. Habilitar ou desabilitar **Verificação de ransomware**.
5. Selecione **Verificação agendada de ransomware**.
6. Opcionalmente, altere a verificação padrão semanal para dias ou semanas.
7. Defina a frequência em dias ou semanas em que a verificação deve ser executada.
8. Selecione **Aplicar**.

Faça backup dos dados do Cloud Volumes ONTAP no Amazon S3 com o NetApp Backup and Recovery

Conclua algumas etapas no NetApp Backup and Recovery para começar a fazer backup de dados de volume dos seus sistemas Cloud Volumes ONTAP para o Amazon S3.

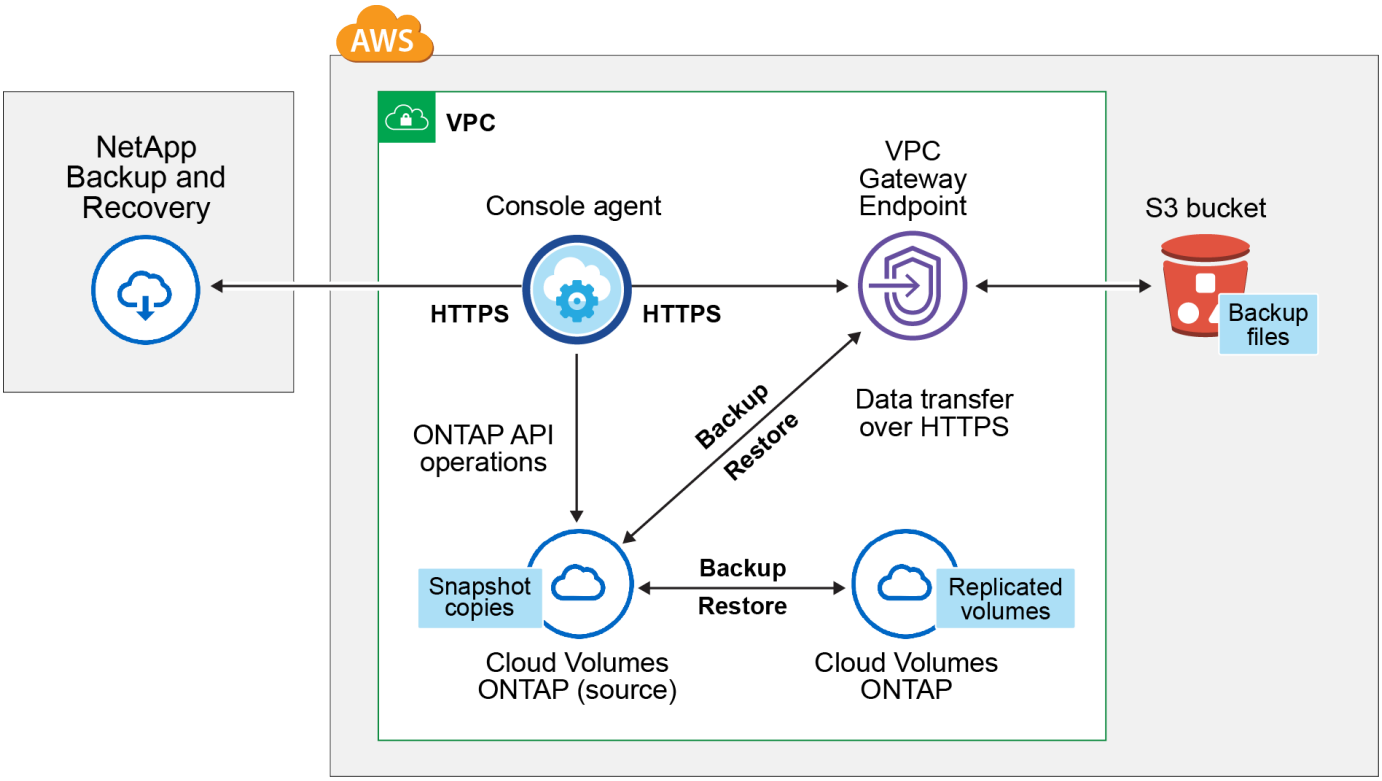
NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Verifique o suporte para sua configuração

Leia os seguintes requisitos para garantir que você tenha uma configuração compatível antes de começar a fazer backup de volumes no 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 também a conexão pública ou privada.



O ponto de extremidade do gateway VPC já deve existir na sua VPC. "Saiba mais sobre endpoints de gateway" .

Versões ONTAP suportadas

Mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior é recomendado.

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 de criptografia gerenciadas já configuradas. "Veja como usar suas próprias chaves" .

Verificar requisitos de licença

Para o licenciamento PAYGO do NetApp Backup and Recovery, uma assinatura do Console está disponível no AWS Marketplace que permite implantações do Cloud Volumes ONTAP e do NetApp Backup and Recovery. Você precisa "assinar esta assinatura do NetApp Console" antes de habilitar o NetApp Backup and Recovery. O faturamento do NetApp Backup and Recovery é feito por meio desta assinatura.

Para um contrato anual que permite fazer backup de dados do Cloud Volumes ONTAP e de dados do ONTAP local, você precisa assinar o "Página do AWS Marketplace" e então "associe a assinatura às suas credenciais da AWS" .

Para um contrato anual que permite agrupar o Cloud Volumes ONTAP e o NetApp Backup and Recovery, você deve configurar o contrato anual ao criar um sistema Cloud Volumes ONTAP . Esta opção não permite que você faça backup de dados locais.

Para o licenciamento BYOL do NetApp Backup and Recovery, você precisa do número de série da NetApp que lhe permite usar o serviço durante a duração e a capacidade da licença. "Aprenda a gerenciar suas licenças BYOL" . Você deve usar uma licença BYOL quando o agente do Console e o sistema Cloud Volumes ONTAP forem implantados em um site escuro.

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

Prepare seu agente de console

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

- "Saiba mais sobre os agentes do Console"
- "Implantar um agente de console na AWS no modo padrão (acesso total à Internet)"
- "Instalar o agente do Console no modo restrito (acesso de saída limitado)"

Verifique ou adicione permissões ao agente do Console

A função do IAM que fornece permissões ao Console deve incluir permissões do S3 da versão mais recente "Política de console" . Se a política não contiver todas essas permissões, consulte o "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 do 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 Cloud Volumes ONTAP

Quando o sistema Cloud Volumes ONTAP estiver executando o software ONTAP 9.12.1 ou superior, a função do IAM que fornece permissões ao sistema deve incluir um novo conjunto de permissões S3 especificamente para o NetApp Backup and Recovery da versão mais recente. "Política Cloud Volumes ONTAP" .

Se você criou o sistema Cloud Volumes ONTAP usando o Console 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 suportadas

O NetApp Backup and Recovery é compatível com todas as regiões da AWS, incluindo as regiões AWS GovCloud.

Configuração necessária para criar backups em uma conta AWS diferente

Por padrão, os backups são criados usando a mesma conta usada para seu 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 agente do Console.
- Adicione as credenciais da conta de destino da AWS no Console. "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 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" .

Verifique os requisitos de rede ONTAP para replicar volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o NetApp Backup and Recovery, certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede ONTAP local

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

  Como você pode replicar para o Cloud Volumes ONTAP ou para 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 do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: especificamente, regras para ICMP e portas 11104 e 11105. Essas regras estão incluídas no grupo de segurança predefinido.
- Para replicar dados entre dois sistemas Cloud Volumes ONTAP em sub-redes diferentes, as sub-redes devem ser roteadas juntas (essa é a configuração padrão).

Habilitar backup e recuperação do NetApp em Cloud Volumes ONTAP

Habilitar o NetApp Backup and Recovery é fácil. As etapas variam um pouco dependendo se você tem um sistema Cloud Volumes ONTAP existente ou um novo.

Habilitar o NetApp Backup and Recovery em um novo sistema

O NetApp Backup and Recovery é habilitado por padrão no assistente do sistema. Certifique-se de manter a opção ativada.

Ver "Lançamento do Cloud Volumes ONTAP na AWS" para obter requisitos e detalhes para criar seu sistema Cloud Volumes ONTAP .

Passos

1. Na página **Sistemas** do Console, selecione **Adicionar sistema**, escolha o provedor de nuvem e selecione **Adicionar novo**. Selecione **Criar Cloud Volumes ONTAP**.
2. Selecione **Amazon Web Services** como o provedor de nuvem e, em seguida, escolha um único nó ou sistema HA.
3. Preencha a página Detalhes e Credenciais.
4. Na página Serviços, deixe o serviço habilitado e selecione **Continuar**.
5. Preencha as páginas do assistente para implantar o sistema.

Resultado

O NetApp Backup and Recovery está habilitado no sistema. Depois de criar volumes nesses sistemas Cloud Volumes ONTAP , inicie o NetApp Backup and Recovery e"ative o backup em cada volume que você deseja proteger" .

Habilitar o NetApp Backup and Recovery em um sistema existente

Habilite o NetApp Backup and Recovery em um sistema existente a qualquer momento diretamente do Console.

Passos

1. Na página **Sistemas** do Console, selecione o cluster e selecione **Ativar** ao lado de Backup e recuperação no painel direito.

   Se o destino do Amazon S3 para seus backups existir como um cluster na página **Sistemas**, você poderá arrastar o cluster para o sistema Amazon S3 para iniciar o assistente de configuração.

Ative backups em seus volumes ONTAP

Ative backups a qualquer momento diretamente do seu sistema local.

Um assistente guia você pelas seguintes etapas principais:

- Selecione os volumes dos quais deseja fazer backup
- Defina a estratégia de backup
- Revise suas seleções

Você também podeMostrar os comandos da API na etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para sistemas futuros.

Inicie o assistente

Passos

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

   - Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar > Volumes de backup** ao lado de Backup e recuperação no painel direito.

     Se o destino da AWS para seus backups existir como um sistema na página **Sistemas** do Console,

você poderá arrastar o cluster ONTAP para o armazenamento de objetos da AWS.

- Selecione **Volumes** na barra Backup e Recuperação. Na aba Volumes, selecione **Ações*** **opção de ícone e selecione *Ativar backup** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos habilitado).

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

2. Continue com as seguintes opções:
   - Se você já tem um agente do Console, está tudo pronto. Basta selecionar **Avançar**.
   - Se você ainda não tiver um agente do Console, a opção **Adicionar um agente do Console** será exibida. Consulte Prepare seu agente de console .

Selecione os volumes dos quais deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem um ou mais dos seguintes: política de instantâneo, política de replicação, política de backup em objeto.

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

- Você pode ativar um backup somente em um único volume FlexGroup por vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock . Todos os volumes devem ter o SnapLock Enterprise habilitado ou o SnapLock desabilitado.

Passos

Se os volumes escolhidos já tiverem políticas de snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que você 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 podem ser selecionados apenas um de cada vez). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e depois marque a caixa na linha de título.
   - Para fazer backup de volumes individuais, marque a caixa de cada volume.
2. Selecione **Avançar**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Se você deseja uma ou todas as opções de backup: instantâneos locais, replicação e backup para armazenamento 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 substituídas.

- 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 backup no armazenamento de objetos, instantâneos locais deverão ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP .
   - **Backup**: Faz backup de volumes no armazenamento de objetos.
2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascata**: As informações fluem do sistema de armazenamento primário para o secundário e do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do sistema de armazenamento primário para o secundário *e* do primário para o armazenamento de objetos.

     Para obter detalhes sobre essas arquiteturas, consulte"Planeje sua jornada de proteção" .
3. **Instantâneo local**: escolha uma política de instantâneo existente ou crie uma nova.

   Para criar uma política personalizada antes de ativar o instantâneo, consulte"Criar uma política" .

   Para criar uma política, selecione **Criar nova política** e faça o seguinte:
   - Digite o nome da política.
   - Selecione até cinco programações, normalmente com frequências diferentes.
   - Selecione **Criar**.
4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o sistema de destino e o SVM. Opcionalmente, selecione o(s) agregado(s) de destino e o prefixo ou sufixo que serão adicionados ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma.

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

     Para criar uma política, selecione **Criar nova política** e faça o seguinte:
     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Selecione **Criar**.
5. **Fazer backup no objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Provedor**: 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 daquela onde o sistema Cloud Volumes ONTAP reside.

  Se quiser usar uma conta AWS diferente para seus backups, você deve adicionar as credenciais da conta AWS de destino no Console e adicionar as permissões "s3:PutBucketPolicy" e "s3:PutBucketOwnershipControls" à função do IAM que fornece permissões ao Console.

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

  Crie um novo bucket ou selecione um existente.

- **Chave de criptografia**: Se você criou um novo bucket, insira as informações da chave de criptografia fornecidas pelo provedor. Escolha se você usará as chaves de criptografia padrão da AWS ou escolherá suas próprias chaves gerenciadas pelo cliente na sua conta da AWS para gerenciar a criptografia dos 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 escolher um bucket existente, as informações de criptografia já estarão disponíveis, então você não precisa inseri-las 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 o backup, consulte"Criar uma política" .

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

  - Digite o nome da política.
  - Selecione até cinco programações, normalmente com frequências diferentes.
  - Para políticas de backup para objeto, defina as configurações de DataLock e Resiliência de Ransomware. Para obter detalhes sobre DataLock e Ransomware Resilience, consulte"Configurações de política de backup para objeto" .
  - Selecione **Criar**.

- **Exportar cópias de Snapshot existentes para armazenamento de objetos como cópias de backup**: Se houver cópias de Snapshot locais para volumes neste sistema que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este sistema (por exemplo, diário, semanal, etc.), este 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 **Avançar**.

Revise suas seleções

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

Passos

1. Na página Revisão, revise suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos da política de instantâneo com os rótulos da política de replicação e backup**. Isso cria instantâneos com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O NetApp Backup and Recovery começa 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 armazenamento primário. Transferências subsequentes contêm cópias diferenciais dos dados do sistema de armazenamento primário contidos em cópias de 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 pela 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.

Você também pode monitorar o status dos trabalhos de backup e restauração usando o"Página de monitoramento de tarefas" .

Mostrar os comandos da API

Talvez você queira exibir e, opcionalmente, copiar os comandos de API usados no assistente Ativar backup e recuperação. Talvez você queira fazer isso para automatizar a ativação de backup em sistemas futuros.

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**.

Faça backup dos dados do Cloud Volumes ONTAP no armazenamento de Blobs do Azure com o NetApp Backup and Recovery

Conclua algumas etapas no NetApp Backup and Recovery para começar a fazer backup de dados de volume dos seus sistemas Cloud Volumes ONTAP para o armazenamento de Blobs do Azure.

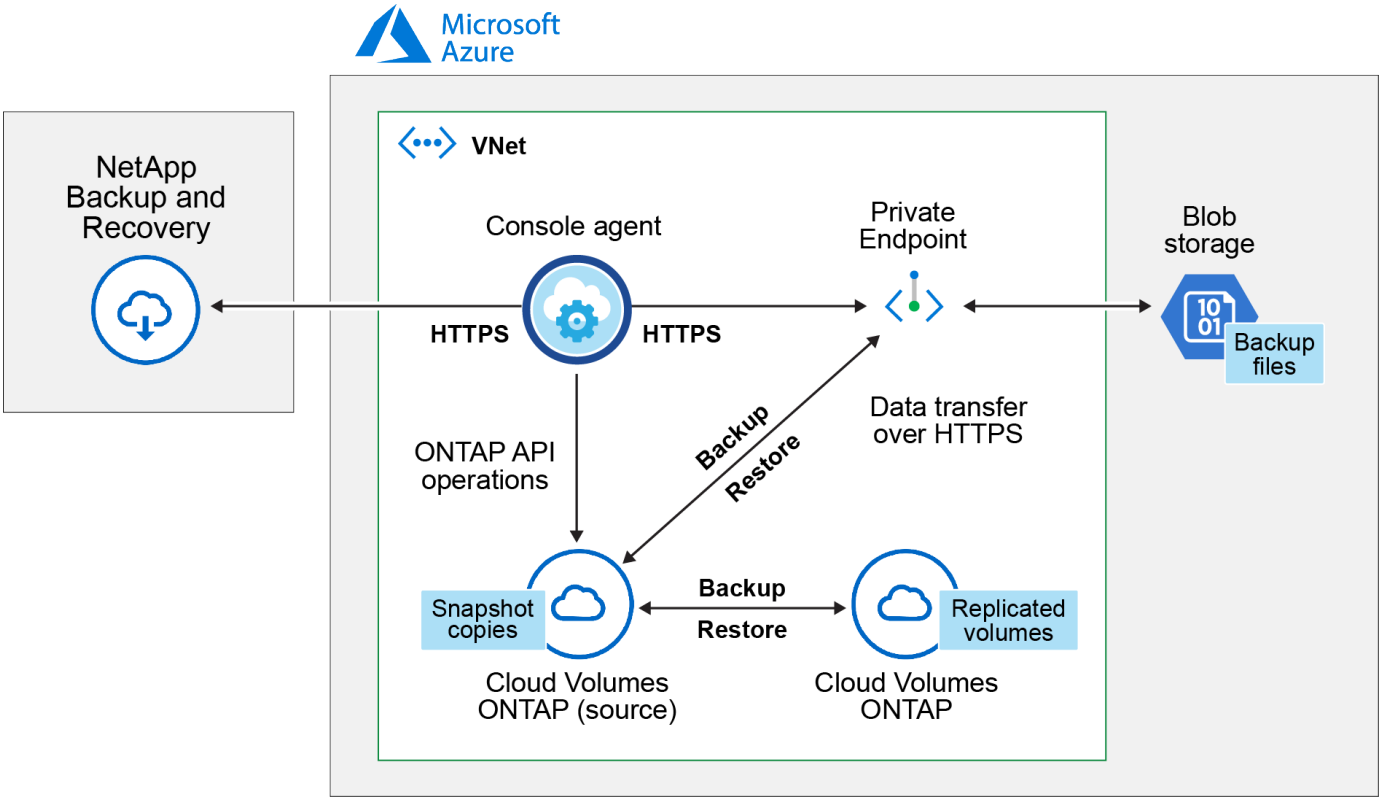
NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Verifique o suporte para sua configuração

Leia os seguintes requisitos para garantir que você tenha uma configuração compatível antes de começar a fazer backup de volumes no armazenamento de Blobs do Azure.

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 também a conexão pública ou privada.



Versões ONTAP suportadas

Mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior é recomendado.

Regiões do Azure com suporte

O NetApp Backup and Recovery tem suporte em todas as regiões do Azure, incluindo regiões governamentais do Azure.

Por padrão, o NetApp Backup and Recovery provisiona o contêiner Blob com redundância local (LRS) para otimização de custos. Você pode alterar essa configuração para Redundância de zona (ZRS) depois que o NetApp Backup and Recovery for ativado se quiser garantir que seus dados sejam replicados entre diferentes zonas. Veja as instruções da Microsoft para "alterando como 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 seu sistema Cloud Volumes ONTAP .

Verificar requisitos de licença

Para o licenciamento PAYGO do NetApp Backup and Recovery, é necessária uma assinatura pelo Azure Marketplace antes de habilitar o NetApp Backup and Recovery. O faturamento do NetApp Backup and Recovery é feito por meio desta assinatura. "Você pode se inscrever na página Detalhes e credenciais do assistente do sistema" .

Para o licenciamento BYOL do NetApp Backup and Recovery, você precisa do número de série da NetApp que lhe permite usar o serviço durante a duração e a capacidade da licença. "Aprenda a gerenciar suas licenças BYOL" . Você deve usar uma licença BYOL quando o agente do Console 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 serão localizados.

Prepare seu agente de console

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

- "Saiba mais sobre os agentes do Console"
- "Implantar um agente de console no Azure no modo padrão (acesso total à Internet)"
- "Instalar o agente do Console no modo restrito (acesso de saída limitado)"

Verifique ou adicione permissões ao agente do Console

Para usar a funcionalidade de pesquisa e restauração do NetApp Backup and Recovery, você precisa ter permissões específicas na função do agente do Console para que ele possa acessar a conta do Azure Synapse Workspace e do Data Lake Storage. Veja as permissões abaixo e siga as etapas se precisar modificar a política.

Antes de começar

- Você deve registrar o Provedor de Recursos do Azure Synapse Analytics (chamado "Microsoft.Synapse") com sua Assinatura. "Veja como registrar este provedor de recursos para sua assinatura" . Você deve ser o **Proprietário** ou **Colaborador** da Assinatura para registrar o provedor de recursos.
- A porta 1433 deve estar aberta para comunicação entre o agente do Console e os serviços do Azure Synapse SQL.

Passos

1. Identifique a função atribuída à máquina virtual do agente do Console:
   a. No portal do Azure, abra o serviço de máquinas virtuais.
   b. Selecione a máquina virtual do agente do Console.
   c. Em Configurações, selecione **Identidade**.
   d. Selecione **Atribuições de função do Azure**.
   e. Anote a função personalizada atribuída à máquina virtual do agente do Console.
2. Atualizar a função personalizada:
   a. No portal do Azure, abra sua assinatura do Azure.
   b. Selecione **Controle de acesso (IAM) > Funções**.
   c. Selecione as reticências (**…**) para a função personalizada e selecione **Editar**.
   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 para a política"

e. Selecione **Revisar + atualizar** e depois selecione **Atualizar**.

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 padrão gerenciadas pela Microsoft. Nesse caso, você precisará ter a Assinatura do Azure, o nome do Key Vault e a Chave. "Veja como usar suas próprias chaves" .

O NetApp Backup and Recovery oferece suporte às *políticas de acesso do Azure*, ao modelo de permissão *controle de acesso baseado em função do Azure* (Azure RBAC) e ao *Modelo de segurança de hardware gerenciado* (HSM) (consulte "O que é o HSM gerenciado do Azure Key Vault?").

Crie sua conta de armazenamento de Blobs do Azure

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" .

Verifique os requisitos de rede ONTAP para replicar volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o NetApp Backup and Recovery, certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede ONTAP local

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

  Como você pode replicar para o Cloud Volumes ONTAP ou para 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 do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: especificamente, regras para ICMP e portas 11104 e 11105. Essas regras estão incluídas no grupo de segurança predefinido.
- Para replicar dados entre dois sistemas Cloud Volumes ONTAP em sub-redes diferentes, as sub-redes devem ser roteadas juntas (essa é a configuração padrão).

Habilitar backup e recuperação do NetApp em Cloud Volumes ONTAP

Habilitar o NetApp Backup and Recovery é fácil. As etapas variam um pouco dependendo se você tem um sistema Cloud Volumes ONTAP existente ou um novo.

Habilitar o NetApp Backup and Recovery em um novo sistema

O NetApp Backup and Recovery é habilitado por padrão no assistente do sistema. Certifique-se de manter a opção ativada.

Ver "Iniciando o Cloud Volumes ONTAP no Azure" para obter requisitos e detalhes para criar seu sistema Cloud Volumes ONTAP .

Se você quiser escolher o nome do grupo de recursos, **desative** o NetApp Backup and Recovery ao implantar o Cloud Volumes ONTAP.

Passos

1. Na página **Sistemas** do Console, selecione **Adicionar sistema**, escolha o provedor de nuvem e selecione **Adicionar novo**. Selecione **Criar Cloud Volumes ONTAP**.
2. Selecione **Microsoft Azure** como o provedor de nuvem e, em seguida, escolha um único nó ou sistema HA.
3. Na página Definir Credenciais do Azure, insira o nome das credenciais, a ID do cliente, o segredo do cliente e a ID do diretório e selecione **Continuar**.
4. Preencha a página Detalhes e credenciais, certifique-se de que uma assinatura do Azure Marketplace esteja ativa e selecione **Continuar**.
5. Na página Serviços, deixe o serviço habilitado e selecione **Continuar**.
6. Preencha as páginas do assistente para implantar o sistema.

Resultado

O NetApp Backup and Recovery está habilitado no sistema. Depois de criar volumes nesses sistemas Cloud Volumes ONTAP , inicie o NetApp Backup and Recovery e"ative o backup em cada volume que você deseja proteger" .

Habilitar o NetApp Backup and Recovery em um sistema existente

Ative o NetApp Backup and Recovery a qualquer momento diretamente do sistema.

Passos

1. Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar** ao lado de Backup e Recuperação no painel direito.

   Se o destino do Blob do Azure para seus backups existir como um sistema na página **Sistemas** do Console, você poderá arrastar o cluster para o sistema Blob do Azure para iniciar o assistente de configuração.

2. Preencha as páginas do assistente para implantar o NetApp Backup and Recovery.
3. Quando você quiser iniciar backups, continue comAtive backups em seus volumes ONTAP .

Ative backups em seus volumes ONTAP

Ative backups a qualquer momento diretamente do seu sistema local.

Um assistente guia você pelas seguintes etapas principais:

- Selecione os volumes dos quais deseja fazer backup
- Defina a estratégia de backup
- Revise suas seleções

Você também podeMostrar os comandos da API na etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para sistemas futuros.

Inicie o assistente

Passos

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

   - Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar > Volumes de backup** ao lado de Backup e recuperação no painel direito.

     Se o destino do Azure para seus backups existir como um sistema na página **Sistemas**, você poderá arrastar o cluster ONTAP para o armazenamento de objetos do Azure Blob.

   - Selecione **Volumes** na barra Backup e Recuperação. Na aba Volumes, selecione **Ações*** ícone e selecione *Ativar backup** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos habilitado).

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

2. Continue com as seguintes opções:

   - Se você já tem um agente do Console, está tudo pronto. Basta selecionar **Avançar**.
   - Se você ainda não tiver um agente do Console, a opção **Adicionar um agente do Console** será exibida. Consulte Prepare seu agente de console .

Selecione os volumes dos quais deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem um ou mais dos seguintes: política de instantâneo, política de replicação, política de backup para objeto.

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

- Você pode ativar um backup somente em um único volume FlexGroup por vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock . Todos os volumes devem ter o SnapLock Enterprise habilitado ou o SnapLock desabilitado.

Passos

Se os volumes escolhidos já tiverem políticas de snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que você 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 do FlexVol . (Os volumes do FlexGroup podem ser selecionados apenas um de cada vez.) Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e depois marque a caixa na linha de título.
   - Para fazer backup de volumes individuais, marque a caixa de cada volume.

2. Selecione **Avançar**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Se você deseja uma ou todas as opções de backup: instantâneos locais, replicação e backup para armazenamento 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 substituídas.

- 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 backup no armazenamento de objetos, instantâneos locais deverão ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP .
   - **Backup**: Faz backup de volumes no armazenamento de objetos.
2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascata**: As informações fluem do sistema de armazenamento primário para o secundário e do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do sistema de armazenamento primário para o secundário *e* do primário para o armazenamento de objetos.

     Para obter detalhes sobre essas arquiteturas, consulte"Planeje sua jornada de proteção" .
3. **Instantâneo local**: escolha uma política de instantâneo existente ou crie uma.

   > Para criar uma política personalizada antes de ativar o instantâneo, consulte"Criar uma política" .

   Para criar uma política, selecione **Criar nova política** e faça o seguinte:
   - Digite o nome da política.
   - Selecione até cinco programações, normalmente com frequências diferentes.
   - Selecione **Criar**.
4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o sistema de destino e o SVM. Opcionalmente, selecione o(s) agregado(s) de destino e o prefixo ou sufixo que serão adicionados 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, consulte"Criar uma política" .

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

- Digite o nome da política.
- Selecione até cinco programações, normalmente com frequências diferentes.
- Selecione **Criar**.

5. **Fazer backup no objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Provedor**: Selecione **Microsoft Azure**.
   - **Configurações do provedor**: insira os detalhes do provedor.

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

     Crie uma nova conta de armazenamento ou selecione uma existente.

     Insira a assinatura do Azure usada para armazenar os backups. Esta pode ser uma assinatura diferente daquela em que o sistema Cloud Volumes ONTAP reside.

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

     Se você quiser proteger seus arquivos de backup contra modificações ou exclusão, certifique-se de que a conta de armazenamento foi criada com armazenamento imutável habilitado usando um período de retenção de 30 dias.

     Se você quiser colocar arquivos de backup mais antigos no Armazenamento de Arquivos do Azure para otimizar ainda mais os custos, certifique-se de que a conta de armazenamento tenha 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 você usará as chaves de criptografia padrão do Azure ou escolherá suas próprias chaves gerenciadas pelo cliente na sua conta do Azure para gerenciar a criptografia dos seus dados.

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

     Se você escolheu uma conta de armazenamento existente da Microsoft, as informações de criptografia já estão disponíveis, então você não precisa inseri-las agora.

   - **Rede**: Escolha o espaço IP e se você usará um ponto de extremidade privado. O Private Endpoint está desabilitado por padrão.
     i. O IPspace no cluster ONTAP onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet.
     ii. Opcionalmente, escolha se você usará um ponto de extremidade privado do Azure que você configurou anteriormente. "Saiba mais sobre como usar um ponto de extremidade privado do Azure" .

- **Política de backup**: selecione uma política de armazenamento de backup para objeto existente.

  Para criar uma política personalizada antes de ativar o backup, consulte"Criar uma política" .

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

  - Digite o nome da política.
  - Para políticas de backup para objeto, defina as configurações de DataLock e Resiliência de Ransomware. Para obter detalhes sobre DataLock e Ransomware Resilience, consulte"Configurações de política de backup para objeto" .
  - Selecione até cinco programações, normalmente com frequências diferentes.
  - Selecione **Criar**.

- **Exportar cópias de snapshot existentes para armazenamento de objetos como cópias de backup**: Se houver cópias de snapshot locais para volumes neste sistema que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este sistema (por exemplo, diário, semanal, etc.), este 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 **Avançar**.

Revise suas seleções

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

Passos

1. Na página Revisão, revise suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos da política de instantâneo com os rótulos da política de replicação e backup**. Isso cria instantâneos com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O NetApp Backup and Recovery começa 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 armazenamento primário. Transferências subsequentes contêm cópias diferenciais dos dados de armazenamento primário contidos em cópias de Snapshot.

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

Um contêiner de armazenamento de Blobs é criado no grupo de recursos que você inseriu, e os arquivos de backup são armazenados lá.

Por padrão, o NetApp Backup and Recovery provisiona o contêiner Blob com redundância local (LRS) para otimização de custos. Você pode alterar esta configuração para Redundância de zona (ZRS) se quiser garantir que seus dados sejam replicados entre diferentes zonas. Veja as instruções da Microsoft para "alterando como sua conta de armazenamento é replicada" .

O Painel de Backup de Volume é exibido para que você possa monitorar o estado dos backups.

Você também pode monitorar o status dos trabalhos de backup e restauração usando o"Página de

monitoramento de tarefas" .

Mostrar os comandos da API

Talvez você queira exibir e, opcionalmente, copiar os comandos de API usados no assistente Ativar backup e recuperação. Talvez você queira fazer isso para automatizar a ativação de backup em sistemas futuros.

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 vem a seguir?

- 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 backups e muito mais.
- Você pode "gerenciar configurações de backup em nível de cluster" . Isso inclui alterar as chaves de armazenamento que o ONTAP usa para acessar o armazenamento em nuvem, alterar a largura de banda de rede disponível para carregar backups no armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Você também pode"restaurar volumes, pastas ou arquivos individuais de um arquivo de backup" para um sistema Cloud Volumes ONTAP na AWS ou para um sistema ONTAP local.

Faça backup dos dados do Cloud Volumes ONTAP no Google Cloud Storage com o NetApp Backup and Recovery

Conclua algumas etapas no NetApp Backup and Recovery para começar a fazer backup de dados de volume dos seus sistemas Cloud Volumes ONTAP para o Google Cloud Storage.

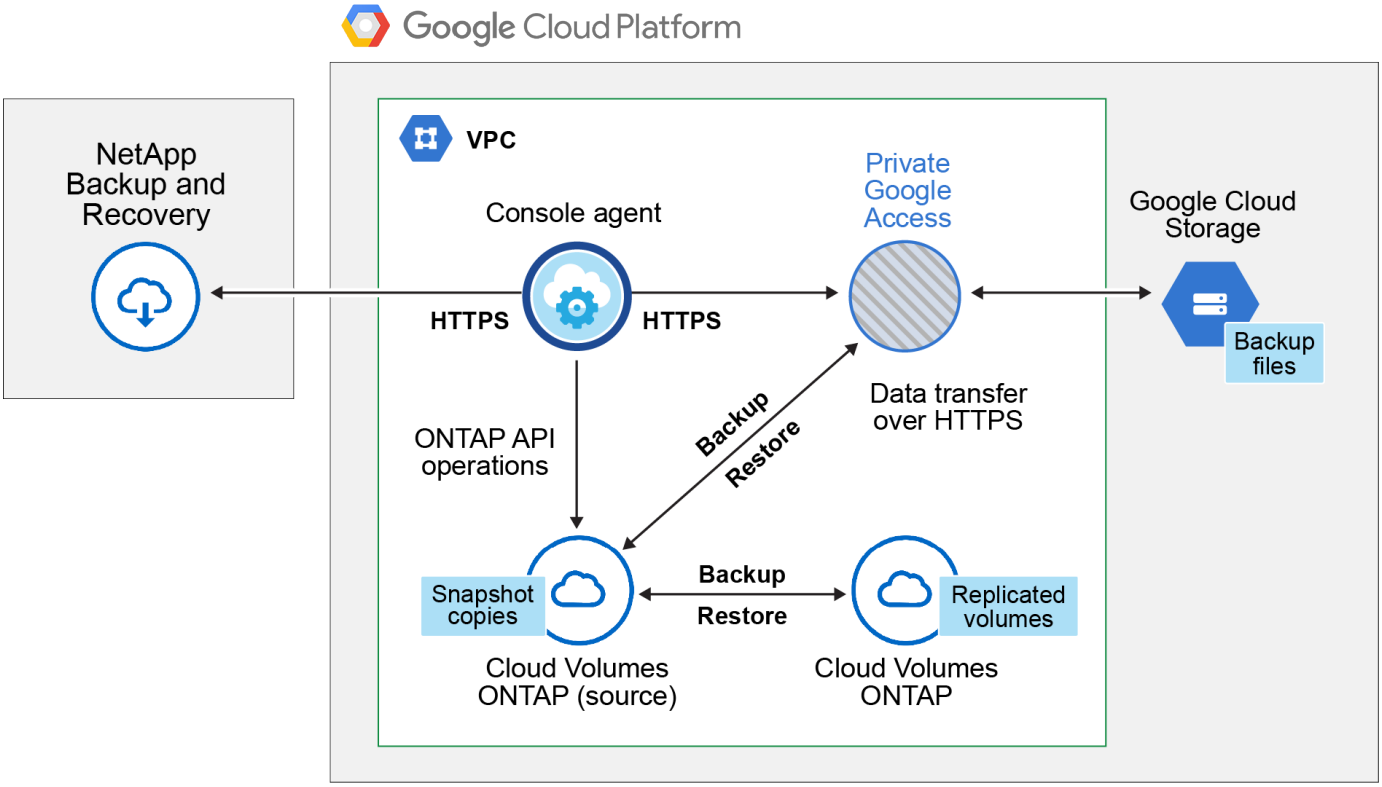
NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Verifique o suporte para sua configuração

Leia os seguintes requisitos para garantir que você tenha uma configuração compatível antes de começar a fazer 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 também a conexão pública ou privada.



Versões ONTAP suportadas

Mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior é recomendado.

Regiões GCP suportadas

O NetApp Backup and Recovery é suportado em todas as regiões do GCP.

Conta de serviço do GCP

Você precisa ter uma conta de serviço no seu projeto do Google Cloud que tenha a função personalizada. "Aprenda a criar uma conta de serviço" .

A função de administrador de armazenamento não é mais necessária para a conta de serviço que permite que o NetApp Backup and Recovery acesse os buckets do Google Cloud Storage.

Verificar requisitos de licença

Para o licenciamento PAYGO do NetApp Backup and Recovery, uma assinatura do Console está disponível no Google Marketplace que permite implantações do Cloud Volumes ONTAP e do NetApp Backup and Recovery. Você precisa "assinar esta assinatura do Console" antes de habilitar o NetApp Backup and Recovery. O faturamento do NetApp Backup and Recovery é feito por meio desta assinatura. "Você pode se inscrever na página Detalhes e credenciais do assistente do sistema" .

Para o licenciamento BYOL do NetApp Backup and Recovery, você precisa do número de série da NetApp que lhe permite usar o serviço durante a duração e a capacidade da licença. "Aprenda a gerenciar suas licenças BYOL" .

E você precisa ter uma assinatura do Google para o espaço de armazenamento onde seus backups serão localizados.

Prepare seu agente de console

O agente do Console deve ser instalado em uma região do Google com acesso à Internet.

- "Saiba mais sobre os agentes do Console"
- "Implantar um agente de console no Google Cloud"

Verifique ou adicione permissões ao agente do Console

Para usar a funcionalidade "Pesquisar e restaurar" do NetApp Backup and Recovery, você precisa ter permissões específicas na função do agente do Console para que ele possa acessar o serviço Google Cloud BigQuery. Veja as permissões abaixo e siga as etapas se precisar modificar a política.

Passos

1. No "Console do Google Cloud" , vá para a página **Funções**.
2. Usando a lista suspensa na parte superior da página, selecione o projeto ou a organização que contém a função que você 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 criptografar dados em vez de usar as chaves de criptografia padrão gerenciadas pelo Google. Chaves entre regiões e entre projetos são suportadas, então você pode escolher um projeto para um bucket que seja diferente do projeto da chave CMEK. Se você planeja 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 agente do Console:

```
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 no seu projeto. Veja o "Documentação do Google Cloud: Habilitando APIs" para mais detalhes.

Considerações sobre CMEK:

- Tanto chaves HSM (com suporte de hardware) quanto chaves geradas por software são suportadas.
- Chaves do Cloud KMS recém-criadas ou importadas são suportadas.
- Somente chaves regionais são suportadas; chaves globais não são suportadas.
- Atualmente, apenas a finalidade "Criptografar/descriptografar simetricamente" é suportada.
- O agente de serviço associado à conta de armazenamento recebe a função IAM "Criptografador/Descriptografador CryptoKey (roles/cloudkms.cryptoKeyEncrypterDecrypter)" do NetApp Backup and Recovery.

Crie seus próprios baldes

Por padrão, o serviço cria buckets para você. Se 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" .

Verifique os requisitos de rede ONTAP para replicar volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o NetApp Backup and Recovery, certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede ONTAP local

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

  Como você pode replicar para o Cloud Volumes ONTAP ou para 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 do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: especificamente, regras para ICMP e portas 11104 e 11105. Essas regras estão incluídas no grupo de segurança predefinido.

- Para replicar dados entre dois sistemas Cloud Volumes ONTAP em sub-redes diferentes, as sub-redes devem ser roteadas juntas (essa é a configuração padrão).

Habilitar backup e recuperação do NetApp em Cloud Volumes ONTAP

As etapas para habilitar o NetApp Backup and Recovery variam um pouco dependendo se você tem um sistema Cloud Volumes ONTAP existente ou um novo.

Habilitar o NetApp Backup and Recovery em um novo sistema

O NetApp Backup and Recovery pode ser ativado quando você conclui o assistente do sistema 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 desligar o sistema e adicionar a conta de serviço ao Cloud Volumes ONTAP no console do GCP.

Ver "Lançamento do Cloud Volumes ONTAP na GCP" para obter requisitos e detalhes para criar seu sistema Cloud Volumes ONTAP .

Passos

1. Na página **Sistemas** do Console, selecione **Adicionar sistema**, escolha o provedor de nuvem e selecione **Adicionar novo**. Selecione **Criar Cloud Volumes ONTAP**.
2. **Escolha um local**: Selecione **Google Cloud Platform**.
3. **Escolha o 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 agente do Console reside).
   b. Especifique o nome do cluster.
   c. Habilite a opção **Conta de serviço** e selecione a Conta de serviço que tem a função de administrador de armazenamento predefinida. Isso é necessário para habilitar backups e camadas.
   d. Especifique as credenciais.

      Certifique-se de que uma assinatura do GCP Marketplace esteja ativa.
5. **Serviços**: Deixe o NetApp Backup and Recovery ativado e clique em **Continuar**.
6. Preencha as páginas do assistente para implantar o sistema conforme descrito em "Lançamento do Cloud Volumes ONTAP na GCP" .

Resultado

O NetApp Backup and Recovery está habilitado no sistema. Depois de criar volumes nesses sistemas Cloud Volumes ONTAP , inicie o NetApp Backup and Recovery e"ative o backup em cada volume que você deseja proteger" .

Habilitar o NetApp Backup and Recovery em um sistema existente

Você pode habilitar o NetApp Backup and Recovery a qualquer momento diretamente do sistema.

Passos

1. Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar** ao lado de Backup e Recuperação no painel direito.

Se o destino do Google Cloud Storage para seus backups existir como um sistema na página **Sistemas** do Console, você poderá arrastar o cluster para o sistema Google Cloud Storage para iniciar o assistente de configuração.

Prepare o Google Cloud Storage como seu destino de backup

Preparar o Google Cloud Storage como seu destino de backup envolve as seguintes etapas:

- Configurar permissões.
- (Opcional) Crie seus próprios buckets. (O serviço criará buckets para você, se desejar.)
- (Opcional) Configurar chaves gerenciadas pelo cliente para criptografia de dados

Configurar permissões

Você precisa fornecer chaves de acesso de armazenamento para uma conta de serviço que tenha permissões específicas usando uma função personalizada. Uma conta de serviço permite que o NetApp Backup and Recovery autentique e acesse 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 "Console do Google Cloud" , vá para a página **Funções**.
2. "Criar 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 de contas de serviço" .
4. Selecione seu projeto de nuvem.
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 a esta conta de serviço acesso 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 você ainda não tiver feito isso, selecione **Habilitar acesso de 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 você acabou de criar e clique em **Criar chave**.

   Você precisará inserir as chaves no NetApp Backup and Recovery mais tarde, ao configurar o serviço de backup.

Crie seus próprios baldes

Por padrão, o serviço cria buckets para você. Ou, se 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 criptografar dados em vez de usar as chaves de criptografia padrão gerenciadas pelo Google. Chaves entre regiões e entre projetos são suportadas, então você pode escolher um projeto para um bucket que seja diferente do projeto da chave CMEK.

Se você planeja 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 agente do Console:

```
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 no seu projeto. Veja o "Documentação do Google Cloud: Habilitando APIs" para mais detalhes.

Considerações sobre CMEK:

- Tanto chaves HSM (com suporte de hardware) quanto chaves geradas por software são suportadas.
- Chaves do Cloud KMS recém-criadas ou importadas são suportadas.
- Somente chaves regionais são suportadas, chaves globais não são suportadas.
- Atualmente, apenas a finalidade "Criptografar/descriptografar simetricamente" é suportada.
- O agente de serviço associado à conta de armazenamento recebe a função IAM "Criptografador/Descriptografador CryptoKey (roles/cloudkms.cryptoKeyEncrypterDecrypter)" do NetApp Backup and Recovery.

Ative backups em seus volumes ONTAP

Ative backups a qualquer momento diretamente do seu sistema local.

Um assistente guia você pelas seguintes etapas principais:

- Selecione os volumes dos quais deseja fazer backup
- Defina a estratégia de backup
- Revise suas seleções

Você também pode Mostrar os comandos da API na etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para sistemas futuros.

Inicie o assistente

Passos

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

   - Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar > Volumes de backup** ao lado de Backup e recuperação no painel direito.

     Se o destino do GCP para seus backups existir como um sistema na página **Sistemas** do Console, você poderá arrastar o cluster ONTAP para o armazenamento de objetos do GCP.

   - Selecione **Volumes** na barra Backup e Recuperação. Na aba Volumes, selecione **Ações*** ••• **ícone e selecione *Ativar backup** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos habilitado).

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

2. Continue com as seguintes opções:

   - Se você já tem um agente do Console, está tudo pronto. Basta selecionar **Avançar**.
   - Se você ainda não tiver um agente do Console, a opção **Adicionar um agente do Console** será exibida. Consulte Prepare seu agente de console .

Selecione os volumes dos quais deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem um ou mais dos seguintes: política de instantâneo, política de replicação, política de backup em objeto.

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

- Você pode ativar um backup somente em um único volume FlexGroup por vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock . Todos os volumes devem ter o SnapLock Enterprise habilitado ou o SnapLock desabilitado.

Passos

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

1. Na página Selecionar volumes, selecione o volume ou volumes que você 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 podem ser selecionados apenas um de cada vez). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e depois marque a caixa na linha de título.
   - Para fazer backup de volumes individuais, marque a caixa de cada volume.
2. Selecione **Avançar**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Se você deseja uma ou todas as opções de backup: instantâneos locais, replicação e backup para armazenamento 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 substituídas.

- 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 backup no armazenamento de objetos, instantâneos locais deverão ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP .
   - **Backup**: Faz backup de volumes no armazenamento de objetos.
2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascata**: As informações fluem do sistema de armazenamento primário para o secundário e do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do sistema de armazenamento primário para o secundário *e* do primário para o armazenamento de objetos.

     Para obter detalhes sobre essas arquiteturas, consulte"Planeje sua jornada de proteção" .
3. **Instantâneo local**: escolha uma política de instantâneo existente ou crie uma.

   > Para criar uma política personalizada antes de ativar o backup, consulte"Criar uma política" .

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

- Digite o nome da política.
- Selecione até cinco programações, normalmente com frequências diferentes.
- Para políticas de backup para objeto, configure o Datalock e o Ransomware Resilience. Para obter detalhes sobre Datalock e Resiliência de Ransomware, consulte"Configurações de política de backup para objeto" .
- Selecione **Criar**.

4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o sistema de destino e o SVM. Opcionalmente, selecione o(s) agregado(s) de destino e o prefixo ou sufixo que serão adicionados 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, consulte"Criar uma política" .

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

     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Selecione **Criar**.
5. **Fazer backup no objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Provedor**: 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 escolherá suas próprias chaves gerenciadas pelo cliente na sua conta do Google para gerenciar a criptografia 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 um bucket existente do Google Cloud, as informações de criptografia já estão disponíveis, então não é necessário inseri-las 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 o backup, consulte"Criar uma política" .

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

     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.

        - Selecione **Criar**.
    - **Exportar cópias de Snapshot existentes para armazenamento de objetos como cópias de backup**: Se houver cópias de Snapshot locais para volumes neste sistema que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este sistema (por exemplo, diário, semanal, etc.), este 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 **Avançar**.

Revise suas seleções

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

Passos

1. Na página Revisão, revise suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos da política de instantâneo com os rótulos da política de replicação e backup**. Isso cria instantâneos com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O NetApp Backup and Recovery começa 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 armazenamento primário. Transferências subsequentes contêm cópias diferenciais dos dados do sistema de armazenamento primário contidos em cópias de Snapshot.

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

Um bucket do Google Cloud Storage é criado 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.

Os backups são associados à classe de armazenamento *Padrão* por padrão. Você pode usar as classes de armazenamento de menor custo *Nearline*, *Coldline* ou *Archive*. No entanto, você configura a classe de armazenamento por meio do Google, não por meio da interface do usuário do NetApp Backup and Recovery. Veja o tópico do Google "Alterando a classe de armazenamento padrão de um bucket" para mais detalhes.

O Painel de Backup de Volume é exibido para que você possa monitorar o estado dos backups.

Você também pode monitorar o status dos trabalhos de backup e restauração usando o"Página de monitoramento de tarefas" .

Mostrar os comandos da API

Talvez você queira exibir e, opcionalmente, copiar os comandos de API usados no assistente Ativar backup e recuperação. Talvez você queira fazer isso para automatizar a ativação de backup em sistemas futuros.

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 vem a seguir?

- 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 backups e muito mais.
- Você pode "gerenciar configurações de backup em nível de cluster" . Isso inclui alterar as chaves de armazenamento que o ONTAP usa para acessar o armazenamento em nuvem, alterar a largura de banda de rede disponível para carregar backups no armazenamento de objetos, alterar a configuração de backup automático para volumes futuros e muito mais.
- Você também pode"restaurar volumes, pastas ou arquivos individuais de um arquivo de backup" para um sistema Cloud Volumes ONTAP na AWS ou para um sistema ONTAP local.

Faça backup de dados ONTAP locais no Amazon S3 com o NetApp Backup and Recovery

Conclua algumas etapas no NetApp Backup and Recovery para começar a fazer backup de dados de volume dos seus sistemas ONTAP locais para um sistema de armazenamento secundário e para o armazenamento em nuvem do Amazon S3.

Os "sistemas ONTAP locais" incluem sistemas FAS, AFF e ONTAP Select .

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

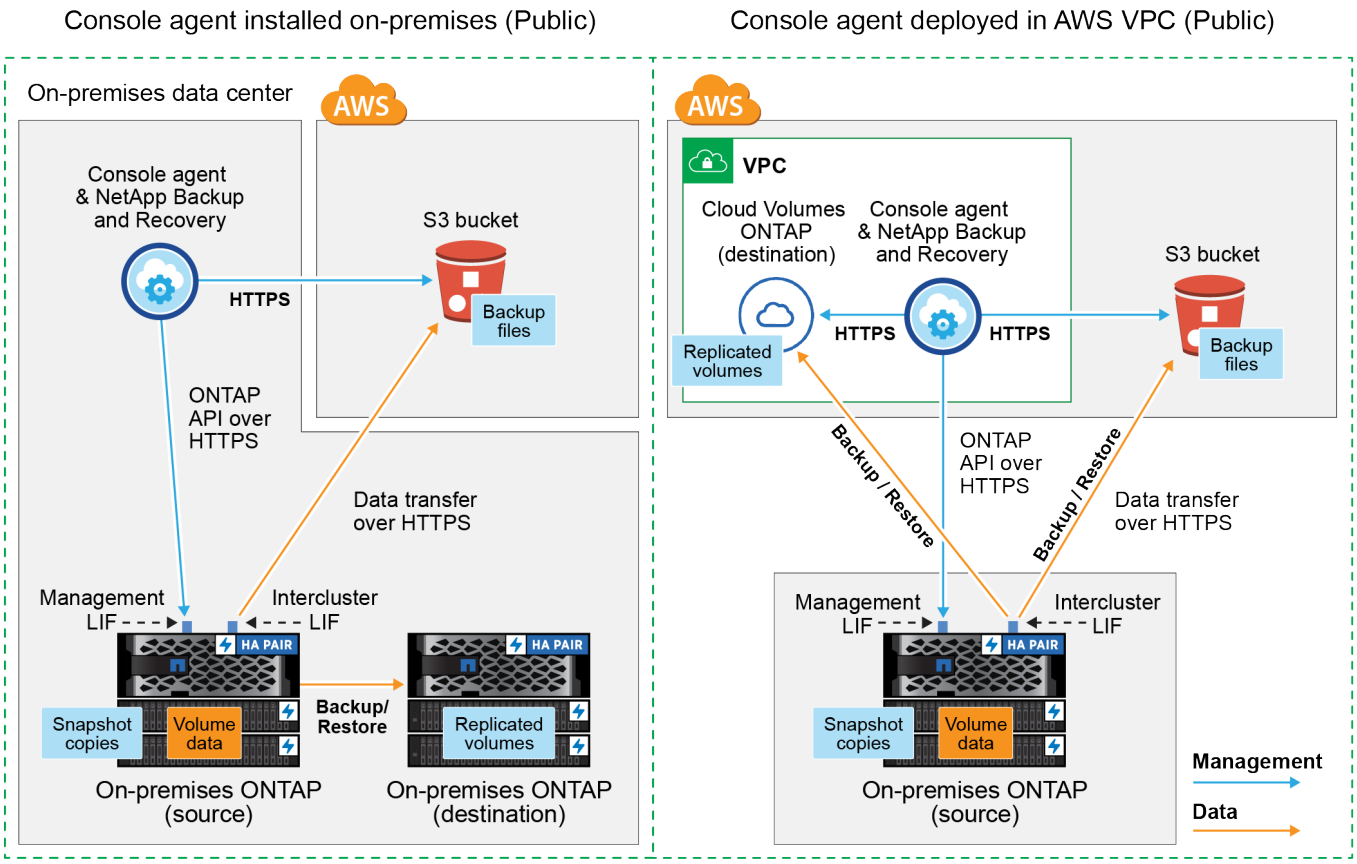
Identifique o método de conexão

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o AWS S3.

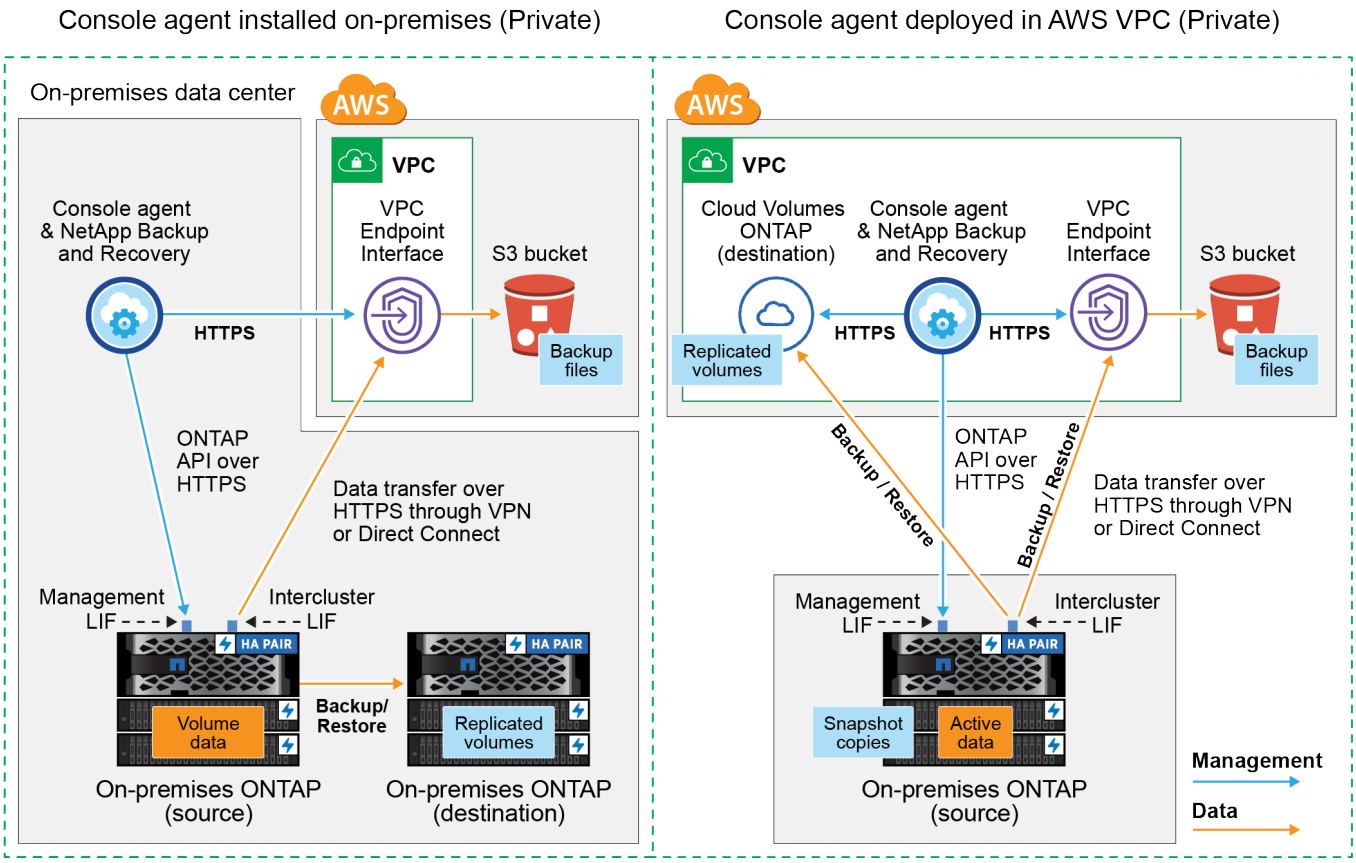
- **Conexão pública** - Conecte diretamente o sistema ONTAP ao AWS S3 usando um endpoint S3 público.
- **Conexão privada** - Use uma VPN ou AWS Direct Connect e direcione o tráfego por meio de uma interface de endpoint VPC que usa um endereço IP privado.

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

O diagrama a seguir mostra o método **conexão pública** e as conexões que você precisa preparar entre os componentes. Você pode usar um agente do Console instalado em suas instalações ou um agente do Console implantado na VPC da AWS.



O diagrama a seguir mostra o método de **conexão privada** e as conexões que você precisa preparar entre os componentes. Você pode usar um agente do Console instalado em suas instalações ou um agente do Console implantado na VPC da AWS.



Prepare seu agente de console

O agente do Console é o software principal para a funcionalidade do NetApp Console. Um agente do Console é necessário para fazer backup e restaurar seus dados ONTAP .

Criar ou alternar agentes do Console

Se você já tiver um agente do Console implantado no seu AWS VPC ou em suas instalações, está tudo pronto.

Caso contrário, você precisará criar um agente do Console em um desses locais para fazer backup dos dados do ONTAP no armazenamento do AWS S3. Você não pode usar um agente do Console implantado em outro provedor de nuvem.

- "Saiba mais sobre os agentes do Console"
- "Instalar um agente de console na AWS"
- "Instale um agente de console em suas instalações"
- "Instalar um agente de console em uma região AWS GovCloud"

  O NetApp Backup and Recovery é suportado nas regiões GovCloud quando o agente do Console é implantado na nuvem, não quando ele é instalado em suas instalações. Além disso, você deve implantar o agente do Console do AWS Marketplace. Não é possível implantar o agente do Console em uma região governamental a partir do site do NetApp Console SaaS.

Preparar os requisitos de rede do agente do console

Certifique-se de que os seguintes requisitos de rede sejam atendidos:

- Certifique-se de que a rede onde o agente do Console está instalado habilite as seguintes conexões:
  - Uma conexão HTTPS pela porta 443 para o NetApp Backup and Recovery e para o seu armazenamento de objetos S3("veja a lista de pontos de extremidade")
  - Uma conexão HTTPS pela porta 443 para seu LIF de gerenciamento de cluster ONTAP
  - Regras adicionais de grupo de segurança de entrada e saída são necessárias para implantações da AWS e AWS GovCloud. Ver "Regras para o agente do Console na AWS" para mais detalhes.
- Se você tiver uma conexão Direct Connect ou VPN do seu cluster ONTAP para o VPC e quiser que a comunicação entre o agente do Console e o S3 permaneça na sua rede interna da AWS (uma conexão **privada**), será necessário habilitar uma interface de endpoint do VPC para o S3. Configure seu sistema para uma conexão privada usando uma interface de endpoint VPC .

Verificar requisitos de licença

Você precisará verificar os requisitos de licença para a AWS e o NetApp Console:

- Antes de ativar o NetApp Backup and Recovery para seu cluster, você precisará assinar uma oferta do NetApp Console Marketplace com pagamento conforme o uso (PAYGO) da AWS ou comprar e ativar uma licença BYOL do NetApp Backup and Recovery da NetApp. Essas licenças são para sua conta e podem ser usadas em vários sistemas.
  - Para o licenciamento PAYGO do NetApp Backup and Recovery, você precisará de uma assinatura do "Oferta do NetApp Console do AWS Marketplace" . O faturamento do NetApp Backup and Recovery é feito por meio desta assinatura.
  - Para o licenciamento BYOL do NetApp Backup and Recovery, você precisará do número de série da NetApp que lhe permitirá usar o serviço durante a duração e a capacidade da licença.
- Você precisa ter uma assinatura da AWS para o espaço de armazenamento de objetos onde seus backups estarão localizados.

Regiões suportadas

Você pode criar backups de sistemas locais para o Amazon S3 em todas as regiões, incluindo regiões AWS GovCloud. Você especifica a região onde os backups serão armazenados ao configurar o serviço.

Prepare seus clusters ONTAP

Você precisará preparar seu sistema ONTAP local de origem e quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP .

Preparar seus clusters ONTAP envolve as seguintes etapas:

- Descubra seus sistemas ONTAP no NetApp Console
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos
- Verifique os requisitos de rede ONTAP para replicar volumes

Descubra seus sistemas ONTAP no NetApp Console

Tanto o sistema ONTAP local de origem quanto quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP devem estar disponíveis na página **Sistemas** do NetApp Console.

Você precisará saber o endereço IP de gerenciamento do cluster e a senha da conta de usuário administrador para adicionar o cluster. "Aprenda como descobrir um cluster" .

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP sejam atendidos:

- Mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior é recomendado.
- Uma licença do SnapMirror (incluída como parte do Pacote Premium ou Pacote de Proteção de Dados).

  Observação: O "Hybrid Cloud Bundle" não é necessário ao usar o NetApp Backup and Recovery.

  Aprenda como "gerencie suas licenças de cluster" .
- A hora e o fuso horário estão definidos corretamente. Aprenda como "configure o tempo do seu cluster" .
- Se você for replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar os dados.

  "Ver versões ONTAP compatíveis para relacionamentos SnapMirror" .

Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos

Você deve configurar os seguintes requisitos no sistema que se conecta ao armazenamento de objetos.

- Para uma arquitetura de backup em fan-out, configure as seguintes configurações no sistema *primário*.
- Para uma arquitetura de backup em cascata, configure as seguintes configurações no sistema *secundário*.

Os seguintes requisitos de rede de cluster ONTAP são necessários:

- O cluster requer uma conexão HTTPS de entrada do agente do Console para o LIF de gerenciamento do cluster.
- Um LIF intercluster é necessário em cada nó ONTAP que hospeda os volumes dos quais você deseja fazer backup. Esses LIFs intercluster devem ser capazes de acessar o armazenamento de objetos.

  O cluster inicia uma conexão HTTPS de saída pela porta 443 dos LIFs entre clusters para o armazenamento do Amazon S3 para operações de backup e restauração. O ONTAP lê e grava dados de e para o armazenamento de objetos — o armazenamento de objetos nunca inicia, ele apenas responde.
- Os LIFs intercluster devem ser associados ao *IPspace* que o ONTAP deve usar para se conectar ao armazenamento de objetos. "Saiba mais sobre IPspaces" .

  Ao configurar o NetApp Backup and Recovery, você será solicitado a informar o IPspace a ser usado. Você deve escolher o IPspace ao qual esses LIFs estão associados. Pode ser o IPspace "padrão" ou um IPspace personalizado que você criou.

  Se você estiver usando um IPspace diferente do "Padrão", talvez seja necessário criar uma rota estática para obter acesso ao armazenamento de objetos.

  Todos os LIFs intercluster dentro do IPspace devem ter acesso ao armazenamento de objetos. Se você

não puder configurar isso para o IPspace atual, será necessário criar um IPspace dedicado onde todos os LIFs intercluster tenham acesso ao armazenamento de objetos.

- Os servidores DNS devem ter sido configurados para a VM de armazenamento onde os volumes estão localizados. Veja como "configurar serviços DNS para o SVM" .
- Atualize as regras de firewall, se necessário, para permitir conexões do NetApp Backup and Recovery do ONTAP para o armazenamento de objetos pela porta 443 e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS pela porta 53 (TCP/UDP).
- Se você estiver usando um endpoint de interface VPC privada na AWS para a conexão S3, para que o HTTPS/443 seja usado, você precisará carregar o certificado de endpoint S3 no cluster ONTAP . Configure seu sistema para uma conexão privada usando uma interface de endpoint VPC . *[Certifique-se de que seu cluster ONTAP tenha permissões para acessar o bucket S3.

Verifique os requisitos de rede ONTAP para replicar volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o NetApp Backup and Recovery, certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede ONTAP local

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

  Como você pode replicar para o Cloud Volumes ONTAP ou para 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 do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: especificamente, regras para ICMP e portas 11104 e 11105. Essas regras estão incluídas no grupo de segurança predefinido.

Prepare o Amazon S3 como seu destino de backup

Preparar o Amazon S3 como seu destino de backup envolve as seguintes etapas:

- Configure as permissões do S3.
- (Opcional) Crie seus próprios buckets S3. (O serviço criará buckets para você, se desejar.)
- (Opcional) Configure chaves da AWS gerenciadas pelo cliente para criptografia de dados.
- (Opcional) Configure seu sistema para uma conexão privada usando uma interface de endpoint VPC.

Configurar permissões do S3

Você precisará configurar dois conjuntos de permissões:

- Permissões para o agente do Console criar e gerenciar o bucket do S3.
- Permissões para o cluster ONTAP local para que ele possa ler e gravar dados no bucket S3.

Passos

1. Certifique-se de que o agente do Console tenha as permissões necessárias. Para mais detalhes, veja "Permissões de política do NetApp Console" .

   Ao criar backups nas regiões da AWS China, você precisa alterar o nome do 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. Ao ativar o serviço, o assistente de backup solicitará que você insira uma chave de acesso e uma chave secreta. Essas credenciais são passadas ao cluster ONTAP para que o ONTAP possa fazer backup e restaurar dados no bucket S3. Para isso, você precisará criar um usuário do IAM com as seguintes permissões.

   Consulte o "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 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, deverá usar o nome de bucket "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.

"Ação": ["S3:ListBucket" "S3:GetBucketLocation"] "Recurso": "arn:aws:s3:::*", "Efeito": "Permitir" }, { "Ação": ["S3:GetObject", "S3:PutObject", "S3:DeleteObject", "S3:ListAllMyBuckets", "S3:PutObjectTagging", "S3:GetObjectTagging", "S3:RestoreObject", "S3:GetBucketObjectLockConfiguration", "S3:GetObjectRetention", "S3:PutBucketObjectLockConfiguration", "S3:PutObjectRetention"] "Recurso": "arn:aws:s3:::*",

Configurar chaves da 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 seu cluster local e o bucket do S3, está tudo pronto, pois 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, será necessário ter as chaves gerenciadas de criptografia já configuradas antes de iniciar o assistente do NetApp Backup and Recovery.

"Veja como usar suas próprias chaves de criptografia da Amazon com o Cloud Volumes ONTAP" .

"Veja como usar suas próprias chaves de criptografia da Amazon com o NetApp Backup and Recovery" .

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 agente do Console e não há mais nada que você precise fazer.

Se você quiser ter uma conexão mais segura pela internet do seu data center local para a VPC, há uma opção para selecionar uma conexão AWS PrivateLink no assistente de ativação de backup. É necessário se você planeja usar uma VPN ou AWS Direct Connect para conectar seu sistema local por meio de uma interface de endpoint VPC que usa um endereço IP privado.

Passos

1. Crie uma configuração de endpoint de interface usando o console do Amazon VPC ou a linha de comando. "Consulte os detalhes sobre o uso do AWS PrivateLink para Amazon S3" .
2. Modifique a configuração do grupo de segurança associado ao agente do Console. Você deve alterar a política para "Personalizada" (de "Acesso Total") e deveadicione as permissões S3 da política de backup como mostrado anteriormente.

   Se você estiver usando a porta 80 (HTTP) para comunicação com o ponto de extremidade privado, está tudo pronto. Agora você pode habilitar o NetApp Backup and Recovery no cluster.

   Se estiver usando a porta 443 (HTTPS) para comunicação com o endpoint privado, você deverá copiar o

certificado do endpoint VPC S3 e adicioná-lo ao seu cluster ONTAP , conforme mostrado nas próximas 4 etapas.

3. Obtenha o nome DNS do endpoint no Console da AWS.
4. Obtenha o certificado do endpoint S3 da VPC. Você faz isso por "efetuar login na VM que hospeda o agente do Console" e executando o seguinte comando. Ao inserir o nome DNS do endpoint, adicione "bucket" no 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. Da saída deste comando, copie os dados do certificado S3 (todos os dados entre, e incluindo, as tags BEGIN / END CERTIFICATE):

```
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. Efetue login na CLI do cluster ONTAP e aplique o certificado que você copiou usando o seguinte comando (substitua pelo nome da sua própria VM de armazenamento):

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

Ative backups em seus volumes ONTAP

Ative backups a qualquer momento diretamente do seu sistema local.

Um assistente guia você pelas seguintes etapas principais:

- Selecione os volumes dos quais deseja fazer backup
- Defina a estratégia de backup
- Revise suas seleções

Você também podeMostrar os comandos da API na etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para sistemas futuros.

Inicie o assistente

Passos

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

   - Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar > Volumes de backup** ao lado de Backup e recuperação no painel direito.

     Se o destino do Amazon S3 para seus backups existir como um sistema na página **Sistemas** do Console, você poderá arrastar o cluster ONTAP para o armazenamento de objetos do Amazon S3.

   - Selecione **Volumes** na barra Backup e recuperação. Na aba Volumes, selecione **Ações*** ícone e selecione *Ativar backup** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos habilitado).

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

2. Continue com as seguintes opções:

   - Se você já tem um agente do Console, está tudo pronto. Basta selecionar **Avançar**.
   - Se você ainda não tiver um agente do Console, a opção **Adicionar um agente do Console** será exibida. Consulte Prepare seu agente de console .

Selecione os volumes dos quais deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem um ou mais dos seguintes: política de instantâneo, política de replicação, política de backup em objeto.

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

- Você pode ativar um backup somente em um único volume FlexGroup por vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock . Todos os volumes devem ter o SnapLock Enterprise habilitado ou o SnapLock desabilitado.

Passos

Se os volumes escolhidos já tiverem políticas de snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que você 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 podem ser selecionados apenas um de cada vez). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e depois marque a caixa na linha de título.
   - Para fazer backup de volumes individuais, marque a caixa de cada volume.

2. Selecione **Avançar**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Se você deseja uma ou todas as opções de backup: instantâneos locais, replicação e backup para armazenamento 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 substituídas.

- 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 backup no armazenamento de objetos, instantâneos locais deverão ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP .
   - **Backup**: Faz backup de volumes no armazenamento de objetos.
2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascata**: As informações fluem do armazenamento primário para o secundário, para o armazenamento de objetos, e do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do primário para o secundário *e* do primário para o armazenamento de objetos.

     Para obter detalhes sobre essas arquiteturas, consulte"Planeje sua jornada de proteção" .
3. **Instantâneo local**: escolha uma política de instantâneo existente ou crie uma política.

   > Para criar uma política personalizada antes de ativar o instantâneo, consulte"Criar uma política" .
4. Para criar uma política, selecione **Criar nova política** e faça o seguinte:
   - Digite o nome da política.
   - Selecione até cinco programações, normalmente com frequências diferentes.
     - Para políticas de backup para objeto, defina as configurações de DataLock e Resiliência de Ransomware. Para obter detalhes sobre DataLock e Ransomware Resilience, consulte"Configurações de política de backup para objeto" .
   - Selecione **Criar**.
5. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o sistema de destino e o SVM. Opcionalmente, selecione o(s) agregado(s) de destino e o prefixo ou sufixo que serão adicionados 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, consulte"Criar uma política" .

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

  - Digite o nome da política.
  - Selecione até cinco programações, normalmente com frequências diferentes.
  - Selecione **Criar**.

6. **Fazer backup no objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Provedor**: 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 são para o usuário do IAM que você criou para dar ao cluster ONTAP acesso ao bucket S3.

   - **Bucket**: Escolha um bucket S3 existente ou crie um novo. Consulte "Adicionar buckets S3" .
   - **Chave de criptografia**: Se você criou um novo bucket S3, insira as informações da chave de criptografia fornecidas pelo provedor. Escolha se você usará as chaves de criptografia padrão do Amazon S3 ou escolherá suas próprias chaves gerenciadas pelo cliente na sua conta da AWS para gerenciar a criptografia dos seus dados.

     Se você escolher um bucket existente, as informações de criptografia já estarão disponíveis, então você não precisa inseri-las agora.

   - **Rede**: Escolha o espaço IP e se você usará um ponto de extremidade privado. O Private Endpoint está desabilitado por padrão.
     i. O IPspace no cluster ONTAP onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet.
     ii. Opcionalmente, escolha se você usará um AWS PrivateLink que você configurou anteriormente. "Veja detalhes sobre o uso do 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 o backup, consulte"Criar uma política" .

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

     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Selecione **Criar**.
   - **Exportar cópias de snapshot existentes para armazenamento de objetos como cópias de backup**: Se houver cópias de snapshot locais para volumes neste sistema que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este sistema (por exemplo, diário, semanal, etc.), este prompt adicional será exibido. Marque esta caixa para que todos os instantâneos históricos sejam copiados para o armazenamento de objetos como arquivos de backup

para garantir a proteção mais completa para seus volumes.

7. Selecione **Avançar**.

Revise suas seleções

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

Passos

1. Na página Revisão, revise suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos da política de instantâneo com os rótulos da política de replicação e backup**. Isso cria instantâneos com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O NetApp Backup and Recovery começa 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 armazenamento primário. Transferências subsequentes contêm cópias diferenciais dos dados primários contidos nas cópias do Snapshot.

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

O bucket S3 é criado na conta de serviço indicada pela chave de acesso S3 e pela 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.

Você também pode monitorar o status dos trabalhos de backup e restauração usando o"Página de monitoramento de tarefas" .

Mostrar os comandos da API

Talvez você queira exibir e, opcionalmente, copiar os comandos de API usados no assistente Ativar backup e recuperação. Talvez você queira fazer isso para automatizar a ativação de backup em sistemas futuros.

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**.

Faça backup de dados ONTAP locais no armazenamento de Blobs do Azure com o NetApp Backup and Recovery

Conclua algumas etapas no NetApp Backup and Recovery para começar a fazer backup de dados de volume dos seus sistemas ONTAP locais para um sistema de armazenamento secundário e para o armazenamento de Blobs do Azure.

Os "sistemas ONTAP locais" incluem sistemas FAS, AFF e ONTAP Select .

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

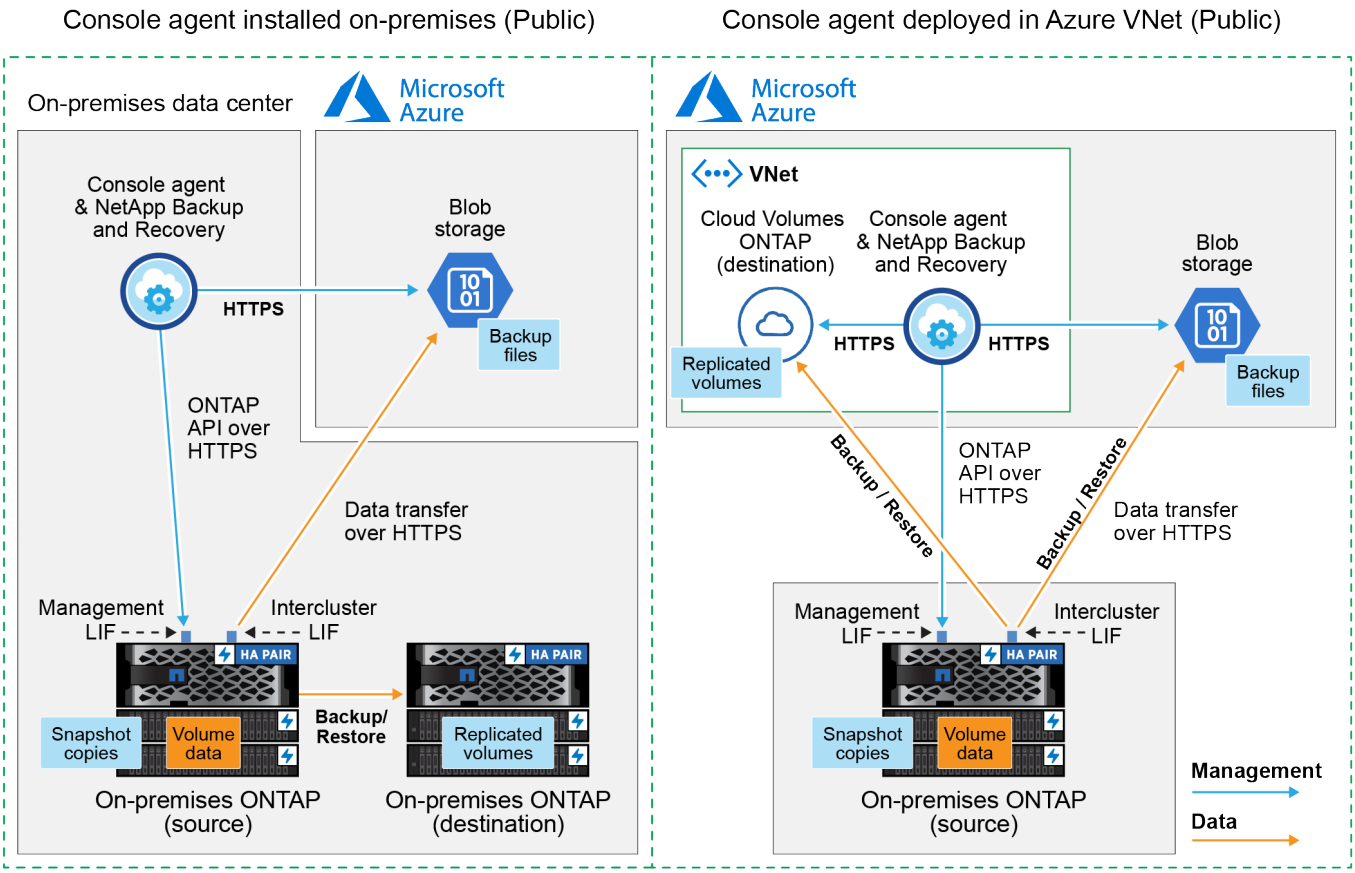
Identifique o método de conexão

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o Azure Blob.

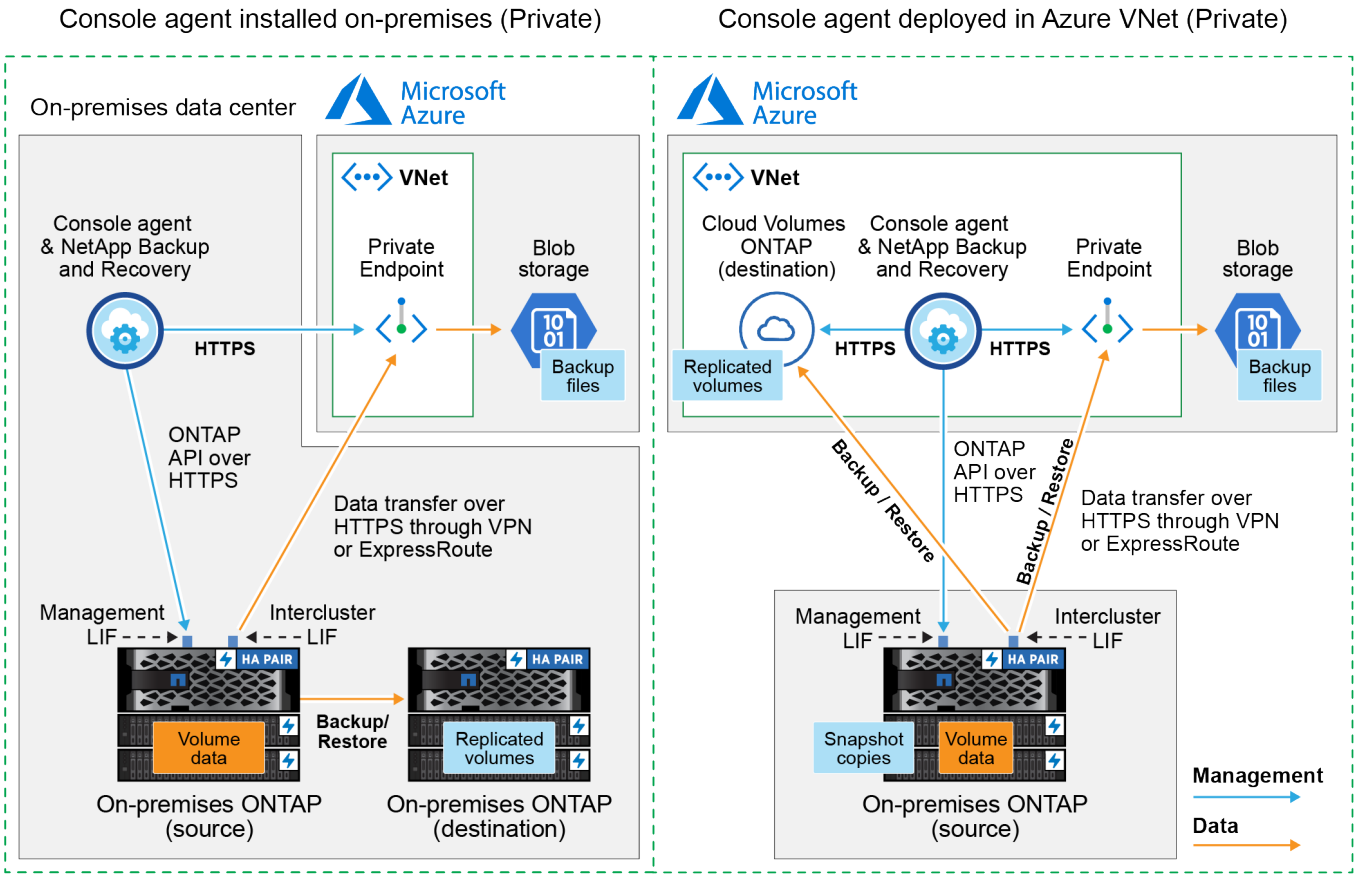
- **Conexão pública** - Conecte diretamente o sistema ONTAP ao armazenamento de Blobs do Azure usando um ponto de extremidade público do Azure.
- **Conexão privada** - Use uma VPN ou ExpressRoute e direcione o tráfego por meio de um VNet Private Endpoint que usa um endereço IP privado.

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

O diagrama a seguir mostra o método **conexão pública** e as conexões que você precisa preparar entre os componentes. Você pode usar um agente do Console instalado em suas instalações ou um agente do Console implantado na VNet do Azure.



O diagrama a seguir mostra o método de **conexão privada** e as conexões que você precisa preparar entre os componentes. Você pode usar um agente do Console instalado em suas instalações ou um agente do Console implantado na VNet do Azure.



Prepare seu agente de console

O agente do Console é o software principal para a funcionalidade do NetApp Console. Um agente do Console é necessário para fazer backup e restaurar seus dados ONTAP .

Criar ou alternar agentes do Console

Se você já tiver um agente do Console implantado na sua VNet do Azure ou em suas instalações, está tudo pronto.

Caso contrário, você precisará criar um agente de console em um desses locais para fazer backup de dados do ONTAP no armazenamento de Blobs do Azure. Você não pode usar um agente do Console implantado em outro provedor de nuvem.

- "Saiba mais sobre os agentes do Console"
- "Instalar um agente de console no Azure"
- "Instale um agente de console em suas instalações"
- "Instalar um agente de console em uma região do Azure Government"

  O NetApp Backup and Recovery tem suporte nas regiões do Azure Government quando o agente do Console é implantado na nuvem, não quando ele é instalado em suas instalações. Além disso, você deve implantar o agente do Console do Azure Marketplace. Não é possível implantar o agente do Console em uma região governamental a partir do site do Console SaaS.

Preparar a rede para o agente do Console

Certifique-se de que o agente do Console tenha as conexões de rede necessárias.

Passos

1. Certifique-se de que a rede onde o agente do Console está instalado habilite as seguintes conexões:
   - Uma conexão HTTPS pela porta 443 para o NetApp Backup and Recovery e para o armazenamento de objetos Blob("veja a lista de pontos de extremidade")
   - Uma conexão HTTPS pela porta 443 para seu LIF de gerenciamento de cluster ONTAP
   - Para que a funcionalidade de pesquisa e restauração do NetApp Backup and Recovery funcione, a porta 1433 deve estar aberta para comunicação entre o agente do Console e os serviços do Azure Synapse SQL.
   - Regras adicionais de grupo de segurança de entrada são necessárias para implantações do Azure e do Azure Government. Ver "Regras para o agente do Console no Azure" para mais detalhes.
2. Habilite um VNet Private Endpoint para armazenamento do Azure. Isso é necessário se você tiver uma conexão ExpressRoute ou VPN do seu cluster ONTAP para a VNet e quiser que a comunicação entre o agente do Console e o armazenamento de Blobs permaneça na sua rede privada virtual (uma conexão **privada**).

Verifique ou adicione permissões ao agente do Console

Para usar a funcionalidade de pesquisa e restauração do NetApp Backup and Recovery, você precisa ter permissões específicas na função do agente do Console para que ele possa acessar a conta do Azure Synapse Workspace e do Data Lake Storage. Veja as permissões abaixo e siga as etapas se precisar modificar a política.

Antes de começar

Você deve registrar o Provedor de Recursos do Azure Synapse Analytics (chamado "Microsoft.Synapse") com sua Assinatura. "Veja como registrar este provedor de recursos para sua assinatura" . Você deve ser o **Proprietário** ou **Colaborador** da Assinatura para registrar o provedor de recursos.

Passos

1. Identifique a função atribuída à máquina virtual do agente do Console:
   a. No portal do Azure, abra o serviço Máquinas virtuais.
   b. Selecione a máquina virtual do agente do Console.
   c. Em **Configurações**, selecione **Identidade**.
   d. Selecione **Atribuições de função do Azure**.
   e. Anote a função personalizada atribuída à máquina virtual do agente do Console.
2. Atualizar a função personalizada:
   a. No portal do Azure, abra sua assinatura do Azure.
   b. Selecione **Controle de acesso (IAM) > Funções**.
   c. Selecione as reticências (**…**) para a função personalizada e selecione **Editar**.
   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 para a política"

e. Selecione **Revisar + atualizar** e depois selecione **Atualizar**.

Verificar requisitos de licença

Você precisará verificar os requisitos de licença do Azure e do Console:

- Antes de ativar o NetApp Backup and Recovery para seu cluster, você precisará assinar uma oferta do Console Marketplace de pagamento conforme o uso (PAYGO) do Azure ou comprar e ativar uma licença BYOL do NetApp Backup and Recovery da NetApp. Essas licenças são para sua conta e podem ser usadas em vários sistemas.
  - Para o licenciamento PAYGO do NetApp Backup and Recovery, você precisará de uma assinatura do "Oferta do NetApp Console do Azure Marketplace" . O faturamento do NetApp Backup and Recovery é feito por meio desta assinatura.
  - Para o licenciamento BYOL do NetApp Backup and Recovery, você precisará do número de série da NetApp que lhe permitirá usar o serviço durante a duração e a capacidade da licença. "Aprenda a 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

Você pode criar backups de sistemas locais para o Azure Blob em todas as regiões, incluindo regiões do Azure Government. Você especifica a região onde os backups serão armazenados ao configurar o serviço.

Prepare seus clusters ONTAP

Você precisará preparar seu sistema ONTAP local de origem e quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP .

Preparar seus clusters ONTAP envolve as seguintes etapas:

- Descubra seus sistemas ONTAP no NetApp Console
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos
- Verifique os requisitos de rede ONTAP para replicar volumes

Descubra seus sistemas ONTAP no NetApp Console

Tanto o sistema ONTAP local de origem quanto quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP devem estar disponíveis na página **Sistemas** do NetApp Console.

Você precisará saber o endereço IP de gerenciamento do cluster e a senha da conta de usuário administrador para adicionar o cluster. "Aprenda como descobrir um cluster" .

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP sejam atendidos:

- Mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior é recomendado.
- Uma licença do SnapMirror (incluída como parte do Pacote Premium ou Pacote de Proteção de Dados).

  Observação: O "Hybrid Cloud Bundle" não é necessário ao usar o NetApp Backup and Recovery.

  Aprenda como "gerencie suas licenças de cluster" .

- A hora e o fuso horário estão definidos corretamente. Aprenda como "configure o tempo do seu cluster" .
- Se você for replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar os dados.

  "Ver versões ONTAP compatíveis para relacionamentos SnapMirror" .

Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos

Você deve configurar os seguintes requisitos no sistema que se conecta ao armazenamento de objetos.

- Para uma arquitetura de backup em fan-out, configure as seguintes configurações no sistema *primário*.
- Para uma arquitetura de backup em cascata, configure as seguintes configurações no sistema *secundário*.

Os seguintes requisitos de rede de cluster ONTAP são necessários:

- O cluster ONTAP inicia uma conexão HTTPS pela porta 443 do LIF intercluster para o armazenamento de Blobs do Azure para operações de backup e restauração.

  ONTAP lê e grava dados de e para armazenamento de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

- O ONTAP requer uma conexão de entrada do agente do Console para o LIF de gerenciamento do cluster. O agente do Console pode residir em uma VNet do Azure.
- Um LIF intercluster é necessário em cada nó ONTAP que hospeda os volumes dos quais você deseja fazer backup. O LIF deve ser associado ao *IPspace* que o ONTAP deve usar para se conectar ao armazenamento de objetos. "Saiba mais sobre IPspaces" .

  Ao configurar o NetApp Backup and Recovery, você será solicitado a informar o IPspace a ser usado. Você deve escolher o IPspace ao qual cada LIF está associado. Pode ser o IPspace "padrão" ou um IPspace personalizado que você criou.

- Os LIFs dos nós e interclusters conseguem acessar o armazenamento de objetos.
- Os servidores DNS foram configurados para a VM de armazenamento onde os volumes estão localizados. Veja como "configurar serviços DNS para o SVM" .
- Se você estiver usando 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 do NetApp Backup and Recovery do ONTAP para o armazenamento de objetos pela porta 443 e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS pela porta 53 (TCP/UDP).

Verifique os requisitos de rede ONTAP para replicar volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o NetApp Backup and Recovery, certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede ONTAP local

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

Como você pode replicar para o Cloud Volumes ONTAP ou para 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 do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: especificamente, regras para ICMP e portas 11104 e 11105. Essas regras estão incluídas no grupo de segurança predefinido.

Prepare o Azure Blob como seu destino de backup

1. Você pode usar suas próprias chaves personalizadas para criptografia de dados no assistente de ativação em vez de usar as chaves de criptografia padrão gerenciadas pela Microsoft. Neste caso, você precisará ter a Assinatura do Azure, o nome do Key Vault e a Chave. "Aprenda a usar suas próprias chaves" .

   Observe que o Backup e a recuperação oferecem suporte a *políticas de acesso do Azure* como modelo de permissão. O modelo de permissão *Controle de acesso baseado em função do Azure* (Azure RBAC) não é suportado no momento.

2. Se você quiser ter uma conexão mais segura pela internet pública do seu data center local para a VNet, há uma opção para configurar um Azure Private Endpoint no assistente de ativação. Nesse caso, você precisará saber a VNet e a Sub-rede para essa conexão. "Consulte os detalhes sobre o uso de um endpoint privado" .

Crie sua conta de armazenamento de Blobs do Azure

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 em seus volumes ONTAP

Ative backups a qualquer momento diretamente do seu sistema local.

Um assistente guia você pelas seguintes etapas principais:

- Selecione os volumes dos quais deseja fazer backup
- Defina a estratégia de backup
- Revise suas seleções

Você também podeMostrar os comandos da API na etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para sistemas futuros.

Inicie o assistente

Passos

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

   - Na página **Sistemas** do Console, selecione o sistema 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 na página **Sistemas** do Console, você poderá arrastar o cluster ONTAP para o armazenamento de objetos do Blob do Azure.

- Selecione **Volumes** na barra Backup e recuperação. Na aba Volumes, selecione **Ações*** ícone e selecione *Ativar backup** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos habilitado).

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

2. Continue com as seguintes opções:
   - Se você já tem um agente do Console, está tudo pronto. Basta selecionar **Avançar**.
   - Se você ainda não tiver um agente do Console, a opção **Adicionar um agente do Console** será exibida. Consulte Prepare seu agente de console .

Selecione os volumes dos quais deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem um ou mais dos seguintes: política de instantâneo, política de replicação, política de backup em objeto.

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

- Você pode ativar um backup somente em um único volume FlexGroup por vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock . Todos os volumes devem ter o SnapLock Enterprise habilitado ou o SnapLock desabilitado.

Passos

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

1. Na página Selecionar volumes, selecione o volume ou volumes que você 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 podem ser selecionados apenas um de cada vez). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e depois marque a caixa na linha de título.
   - Para fazer backup de volumes individuais, marque a caixa de cada volume.
2. Selecione **Avançar**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Se você deseja uma ou todas as opções de backup: instantâneos locais, replicação e backup para armazenamento de objetos
- Arquitetura
- Política de Snapshot 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 substituídas.

- 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 backup no armazenamento de objetos, instantâneos locais deverão ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP .
   - **Backup**: Faz backup de volumes no armazenamento de objetos.
2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascata**: As informações fluem do armazenamento primário para o secundário e do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do primário para o secundário *e* do primário para o armazenamento de objetos.

     Para obter detalhes sobre essas arquiteturas, consulte"Planeje sua jornada de proteção" .
3. **Instantâneo local**: escolha uma política de instantâneo existente ou crie uma nova.

   > Para criar uma política personalizada antes de ativar o instantâneo, consulte"Criar uma política" .

   Para criar uma política, selecione **Criar nova política** e faça o seguinte:
   - Digite o nome da política.
   - Selecione até cinco programações, normalmente com frequências diferentes.
   - Selecione **Criar**.
4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o sistema de destino e o SVM. Opcionalmente, selecione o(s) agregado(s) de destino e o prefixo ou sufixo que serão adicionados 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, consulte"Criar uma política" .

     Para criar uma política, selecione **Criar nova política** e faça o seguinte:
     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Selecione **Criar**.

5. **Fazer backup no objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Provedor**: 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 contêiner Blob ou selecione o tipo de grupo de recursos e o grupo.

     Se você quiser proteger seus arquivos de backup contra modificações ou exclusão, certifique-se de que a conta de armazenamento foi criada com armazenamento imutável habilitado usando um período de retenção de 30 dias.

     Se você quiser colocar arquivos de backup mais antigos no Armazenamento de Arquivos do Azure para otimizar ainda mais os custos, certifique-se de que a conta de armazenamento tenha 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 você usará as chaves de criptografia padrão do Azure ou escolherá suas próprias chaves gerenciadas pelo cliente na sua conta do Azure para gerenciar a criptografia 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 existente da Microsoft, as informações de criptografia já estão disponíveis, então você não precisa inseri-las agora.

   - **Rede**: Escolha o espaço IP e se você usará um ponto de extremidade privado. O Private Endpoint está desabilitado por padrão.
     i. O IPspace no cluster ONTAP onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet.
     ii. Opcionalmente, escolha se você usará um ponto de extremidade privado do Azure que você configurou anteriormente. "Saiba mais sobre como usar um ponto de extremidade privado do Azure" .
   - **Política de backup**: Selecione uma política de backup para armazenamento de objetos existente ou crie uma nova.

     Para criar uma política personalizada antes de ativar o backup, consulte"Criar uma política" .

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

     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Para políticas de backup para objeto, defina as configurações de DataLock e Resiliência de Ransomware. Para obter detalhes sobre DataLock e Ransomware Resilience, consulte"Configurações de política de backup para objeto" .

        - Selecione **Criar**.
    - **Exportar cópias de snapshot existentes para armazenamento de objetos como cópias de backup**: Se houver cópias de snapshot locais para volumes neste sistema que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este sistema (por exemplo, diário, semanal, etc.), este 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 **Avançar**.

Revise suas seleções

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

Passos

1. Na página Revisão, revise suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos da política de instantâneo com os rótulos da política de replicação e backup**. Isso cria instantâneos com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O NetApp Backup and Recovery começa 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 armazenamento primário. Transferências subsequentes contêm cópias diferenciais dos dados do sistema de armazenamento primário contidos em cópias de Snapshot.

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

Uma conta de armazenamento de Blobs 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.

Você também pode monitorar o status dos trabalhos de backup e restauração usando o"Página de monitoramento de tarefas" .

Mostrar os comandos da API

Talvez você queira exibir e, opcionalmente, copiar os comandos de API usados no assistente Ativar backup e recuperação. Talvez você queira fazer isso para automatizar a ativação de backup em sistemas futuros.

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**.

Faça backup de dados ONTAP locais no Google Cloud Storage com o NetApp Backup and Recovery

Conclua algumas etapas no NetApp Backup and Recovery para começar a fazer backup de dados de volume dos seus sistemas ONTAP primários locais para um sistema de armazenamento secundário e para o Google Cloud Storage.

Os "sistemas ONTAP locais" incluem sistemas FAS, AFF e ONTAP Select .

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

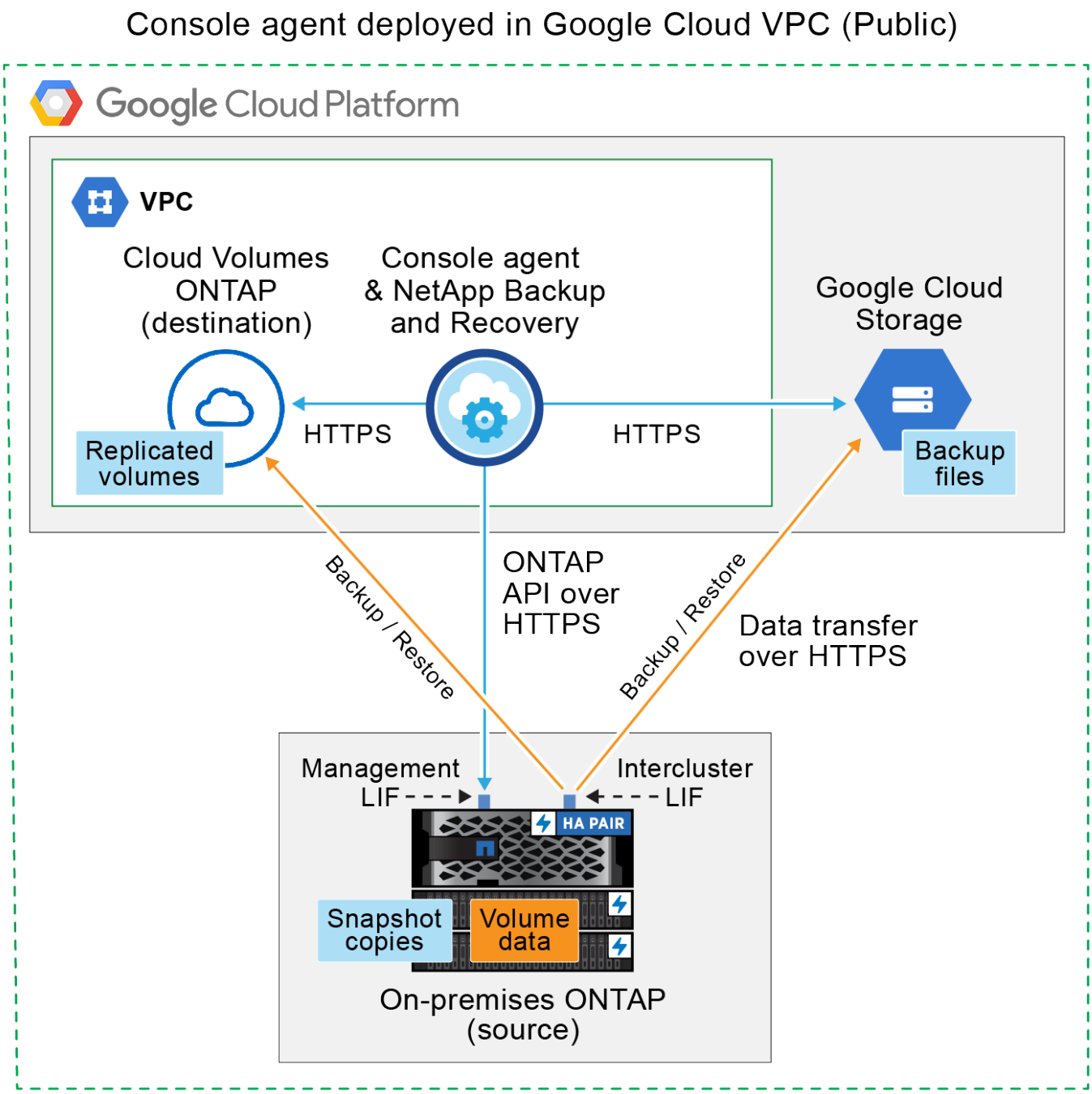
Identifique o método de conexão

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o Google Cloud Storage.

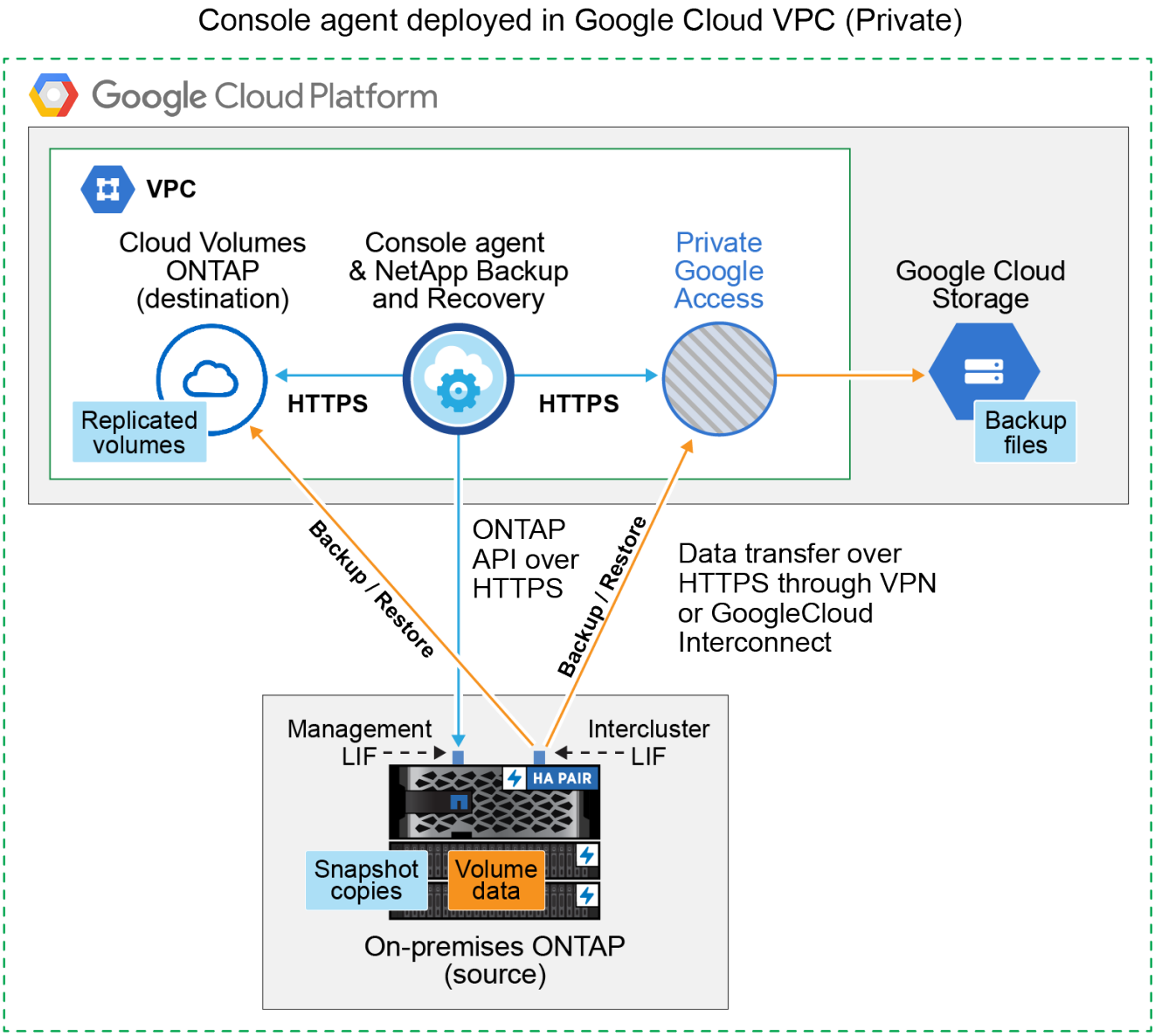
- **Conexão pública** - Conecte diretamente o sistema ONTAP ao Google Cloud Storage usando um ponto de extremidade público do Google.
- **Conexão privada** - Use uma VPN ou o Google Cloud Interconnect e direcione o tráfego por meio de uma interface de acesso privado do Google que usa um endereço IP privado.

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

O diagrama a seguir mostra o método **conexão pública** e as conexões que você precisa preparar entre os componentes. O agente do Console deve ser implantado na VPC do Google Cloud Platform.



O diagrama a seguir mostra o método de **conexão privada** e as conexões que você precisa preparar entre os componentes. O agente do Console deve ser implantado na VPC do Google Cloud Platform.



Prepare seu agente de console

O agente do Console é o software principal para a funcionalidade do Console. Um agente do Console é necessário para fazer backup e restaurar seus dados ONTAP .

Criar ou alternar agentes do Console

Se você já tiver um agente de console implantado na sua VPC do Google Cloud Platform, está tudo pronto.

Caso contrário, você precisará criar um agente do Console nesse local para fazer backup dos dados do ONTAP no Google Cloud Storage. Você não pode usar um agente do Console implantado em outro provedor de nuvem ou no local.

- "Saiba mais sobre os agentes do Console"
- "Instalar um agente de console no GCP"

Preparar a rede para o agente do Console

Certifique-se de que o agente do Console tenha as conexões de rede necessárias.

Passos

1. Certifique-se de que a rede onde o agente do Console está instalado habilite as seguintes conexões:
   - Uma conexão HTTPS pela porta 443 para o NetApp Backup and Recovery e para o seu armazenamento no Google Cloud("veja a lista de pontos de extremidade")
   - Uma conexão HTTPS pela porta 443 para seu LIF de gerenciamento de cluster ONTAP
2. Habilite o Private Google Access (ou Private Service Connect) na sub-rede onde você planeja implantar o agente do Console. "Acesso privado ao Google" ou "Conexão de serviço privado" são necessários se você tiver uma conexão direta do seu cluster ONTAP com a VPC e quiser que a comunicação entre o agente do Console e o Google Cloud Storage permaneça na sua rede privada virtual (uma conexão **privada**).

   Siga as instruções do Google para configurar essas opções de acesso privado. Certifique-se de que seus 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 agente do Console

Para usar a funcionalidade "Pesquisar e restaurar" do NetApp Backup and Recovery, você precisa ter permissões específicas na função do agente do Console para que ele possa acessar o serviço Google Cloud BigQuery. Revise as permissões abaixo e siga as etapas se precisar modificar a política.

Passos

1. No "Console do Google Cloud" , vá para a página **Funções**.
2. Usando a lista suspensa na parte superior da página, selecione o projeto ou a organização que contém a função que você 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.

Verificar requisitos de licença

- Antes de ativar o NetApp Backup and Recovery para seu cluster, você precisará assinar uma oferta do Console Marketplace de pagamento conforme o uso (PAYGO) do Google ou comprar e ativar uma licença BYOL do NetApp Backup and Recovery da NetApp. Essas licenças são para sua conta e podem ser usadas em vários sistemas.
  - Para o licenciamento PAYGO do NetApp Backup and Recovery, você precisará de uma assinatura do "Oferta do NetApp Console do Google Marketplace" . O faturamento do NetApp Backup and Recovery é feito por meio desta assinatura.
  - Para o licenciamento BYOL do NetApp Backup and Recovery, você precisará do número de série da NetApp que lhe permitirá usar o serviço durante a duração e a capacidade da licença. "Aprenda a 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

Você pode criar backups de sistemas locais para o Google Cloud Storage em todas as regiões. Você especifica a região onde os backups serão armazenados ao configurar o serviço.

Prepare seus clusters ONTAP

Você precisará preparar seu sistema ONTAP local de origem e quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP .

Preparar seus clusters ONTAP envolve as seguintes etapas:

- Descubra seus sistemas ONTAP no NetApp Console
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos
- Verifique os requisitos de rede ONTAP para replicar volumes

Descubra seus sistemas ONTAP no NetApp Console

Tanto o sistema ONTAP local de origem quanto quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP devem estar disponíveis na página **Sistemas** do NetApp Console.

Você precisará saber o endereço IP de gerenciamento do cluster e a senha da conta de usuário administrador para adicionar o cluster. "Aprenda como descobrir um cluster" .

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP sejam atendidos:

- Mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior é recomendado.
- Uma licença do SnapMirror (incluída como parte do Pacote Premium ou Pacote de Proteção de Dados).

  Observação: O "Hybrid Cloud Bundle" não é necessário ao usar o NetApp Backup and Recovery.

  Aprenda como "gerencie suas licenças de cluster" .
- A hora e o fuso horário estão definidos corretamente. Aprenda como "configure o tempo do seu cluster" .

- Se você for replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar os dados.

  "Ver versões ONTAP compatíveis para relacionamentos SnapMirror" .

Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos

Você deve configurar os seguintes requisitos no sistema que se conecta ao armazenamento de objetos.

- Para uma arquitetura de backup em fan-out, configure as seguintes configurações no sistema *primário*.
- Para uma arquitetura de backup em cascata, configure as seguintes configurações no sistema *secundário*.

Os seguintes requisitos de rede de cluster ONTAP são necessários:

- O cluster ONTAP inicia uma conexão HTTPS pela porta 443 do LIF intercluster para o Google Cloud Storage para operações de backup e restauração.

  ONTAP lê e grava dados de e para armazenamento de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.

- O ONTAP requer uma conexão de entrada do agente do Console para o LIF de gerenciamento do cluster. O agente do Console pode residir em uma VPC do Google Cloud Platform.
- Um LIF intercluster é necessário em cada nó ONTAP que hospeda os volumes dos quais você deseja fazer backup. O LIF deve ser associado ao *IPspace* que o ONTAP deve usar para se conectar ao armazenamento de objetos. "Saiba mais sobre IPspaces" .

  Ao configurar o NetApp Backup and Recovery, você será solicitado a informar o IPspace a ser usado. Você deve escolher o IPspace ao qual cada LIF está associado. Pode ser o IPspace "padrão" ou um IPspace personalizado que você criou.

- Os LIFs intercluster dos nós conseguem acessar o armazenamento de objetos.
- Os servidores DNS foram configurados para a VM de armazenamento onde os volumes estão localizados. Veja como "configurar serviços DNS para o SVM" .

  Se você estiver usando o Private Google Access ou o Private Service Connect, certifique-se de que seus servidores DNS foram configurados para apontar `storage.googleapis.com` para o endereço IP interno (privado) correto.

- Observe que se você estiver usando 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 do NetApp Backup and Recovery do ONTAP para o armazenamento de objetos pela porta 443 e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS pela porta 53 (TCP/UDP).

Verifique os requisitos de rede ONTAP para replicar volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o NetApp Backup and Recovery, certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede ONTAP local

- Se o cluster estiver em suas instalações, você deverá ter uma conexão da sua rede corporativa com sua rede virtual no provedor de nuvem. Normalmente, essa é uma conexão VPN.

- Os clusters ONTAP devem atender a requisitos adicionais de sub-rede, porta, firewall e cluster.

  Como você pode replicar para o Cloud Volumes ONTAP ou para 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 do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: especificamente, regras para ICMP e portas 11104 e 11105. Essas regras estão incluídas no grupo de segurança predefinido.

Prepare o Google Cloud Storage como seu destino de backup

Preparar o Google Cloud Storage como seu destino de backup envolve as seguintes etapas:

- Configurar permissões.
- (Opcional) Crie seus próprios buckets. (O serviço criará buckets para você, se desejar.)
- (Opcional) Configurar chaves gerenciadas pelo cliente para criptografia de dados

Configurar permissões

Você precisa fornecer chaves de acesso de armazenamento para uma conta de serviço que tenha permissões específicas usando uma função personalizada. Uma conta de serviço permite que o NetApp Backup and Recovery autentique e acesse 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 "Console do Google Cloud" , vá para a página **Funções**.
2. "Criar 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 de contas de serviço" .
4. Selecione seu projeto de nuvem.
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 a esta conta de serviço acesso 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 você ainda não tiver feito isso, selecione **Habilitar acesso de 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 você acabou de criar e clique em **Criar chave**.

      Você precisará inserir as chaves no NetApp Backup and Recovery mais tarde, ao configurar o serviço de backup.

Crie seus próprios baldes

Por padrão, o serviço cria buckets para você. Ou, se 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 criptografar dados em vez de usar as chaves de criptografia padrão gerenciadas pelo Google. Chaves entre regiões e entre projetos são suportadas, então você pode escolher um projeto para um bucket que seja diferente do projeto da chave CMEK.

Se você planeja 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 agente do Console:

```
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 no seu projeto. Veja o "Documentação do Google Cloud: Habilitando APIs" para mais detalhes.

Considerações sobre CMEK:

- Tanto chaves HSM (com suporte de hardware) quanto chaves geradas por software são suportadas.
- Chaves do Cloud KMS recém-criadas ou importadas são suportadas.
- Somente chaves regionais são suportadas, chaves globais não são suportadas.
- Atualmente, apenas a finalidade "Criptografar/descriptografar simetricamente" é suportada.
- O agente de serviço associado à conta de armazenamento recebe a função IAM "Criptografador/Descriptografador CryptoKey (roles/cloudkms.cryptoKeyEncrypterDecrypter)" do NetApp Backup and Recovery.

Ative backups em seus volumes ONTAP

Ative backups a qualquer momento diretamente do seu sistema local.

Um assistente guia você pelas seguintes etapas principais:

- Selecione os volumes dos quais deseja fazer backup
- Defina a estratégia de backup
- Revise suas seleções

Você também pode Mostrar os comandos da API na etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para sistemas futuros.

Inicie o assistente

Passos

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

   - Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar > Volumes de backup** ao lado de Backup e recuperação no painel direito.

     Se o destino do Google Cloud Storage para seus backups existir como na página **Sistemas** do Console, você poderá arrastar o cluster ONTAP para o armazenamento de objetos do Google Cloud.

   - Selecione **Volumes** na barra Backup e recuperação. Na aba Volumes, selecione **Ações*** ••• **ícone e selecione *Ativar backup** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos habilitado).

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

2. Continue com as seguintes opções:

   - Se você já tem um agente do Console, está tudo pronto. Basta selecionar **Avançar**.
   - Se você ainda não tiver um agente do Console, a opção **Adicionar um agente do Console** será exibida. Consulte Prepare seu agente de console .

Selecione os volumes dos quais deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem um ou mais dos seguintes: política de instantâneo, política de replicação, política de backup em objeto.

Você pode optar por proteger volumes FlexVol ou FlexGroup ; no entanto, não é possível selecionar uma mistura desses volumes ao ativar o backup de um sistema. Veja como"ativar backup para volumes adicionais

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

- Você pode ativar um backup somente em um único volume FlexGroup por vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock . Todos os volumes devem ter o SnapLock Enterprise habilitado ou o SnapLock desabilitado.

Passos

Se os volumes escolhidos já tiverem políticas de snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que você 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 podem ser selecionados apenas um de cada vez). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e depois marque a caixa na linha de título.
   - Para fazer backup de volumes individuais, marque a caixa de cada volume.
2. Selecione **Avançar**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Se você deseja uma ou todas as opções de backup: instantâneos locais, replicação e backup para armazenamento 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 substituídas.

- 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:
   - **Snapshots locais**: se você estiver executando replicação ou backup no armazenamento de objetos, Snapshots locais deverão ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP .
   - **Backup**: Faz backup de volumes no armazenamento de objetos.
2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascata**: 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 primário para o armazenamento de objetos.

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

3. **Instantâneo local**: escolha uma política de instantâneo existente ou crie uma nova.

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

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

   - Digite o nome da política.
   - Selecione até cinco programações, normalmente com frequências diferentes.
   - Selecione **Criar**.

4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o sistema de destino e o SVM. Opcionalmente, selecione o(s) agregado(s) de destino e o prefixo ou sufixo que serão adicionados ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma nova.

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

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

     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Selecione **Criar**.

5. **Fazer backup no objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Provedor**: 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 tenha criado.

     Se você quiser colocar arquivos de backup mais antigos no armazenamento do Google Cloud Archive para otimizar ainda mais os custos, certifique-se de que o bucket tenha a regra de ciclo de vida apropriada.

     Insira a chave de acesso e a chave secreta do Google Cloud.

   - **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 escolherá suas próprias chaves gerenciadas pelo cliente na sua conta do Google Cloud para gerenciar a criptografia dos seus dados.

     Se você escolheu uma conta de armazenamento existente do Google Cloud, as informações de criptografia já estão disponíveis, então você não precisa inseri-las agora.

     Se você optar por usar suas próprias chaves gerenciadas pelo cliente, insira o conjunto de chaves e o nome da chave. "Saiba mais sobre chaves de criptografia gerenciadas pelo cliente" .

- **Rede**: Escolha o IPspace.

  O IPspace no cluster ONTAP onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet.

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

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

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

  - Digite o nome da política.
  - Selecione até cinco programações, normalmente com frequências diferentes.
  - Selecione **Criar**.

- **Exportar cópias de snapshot existentes para armazenamento de objetos como cópias de backup**: Se houver cópias de snapshot locais para volumes neste sistema que correspondam ao rótulo de agendamento de backup que você acabou de selecionar para este sistema (por exemplo, diário, semanal, etc.), este 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 **Avançar**.

Revise suas seleções

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

Passos

1. Na página Revisão, revise suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos da política de instantâneo com os rótulos da política de replicação e backup**. Isso cria instantâneos com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O NetApp Backup and Recovery começa 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 armazenamento primário. Transferências subsequentes contêm cópias diferenciais dos dados do sistema de armazenamento primário contidos em cópias de Snapshot.

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

Um bucket 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.

Você também pode monitorar o status dos trabalhos de backup e restauração usando o"Página de monitoramento de tarefas" .

Mostrar os comandos da API

Talvez você queira exibir e, opcionalmente, copiar os comandos de API usados no assistente Ativar backup e recuperação. Talvez você queira fazer isso para automatizar a ativação de backup em sistemas futuros.

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**.

Faça backup de dados ONTAP locais no ONTAP S3 com o NetApp Backup and Recovery

Conclua algumas etapas no NetApp Backup and Recovery para começar a fazer backup de dados de volume dos seus principais sistemas ONTAP locais. Você pode enviar backups para um sistema de armazenamento ONTAP secundário (um volume replicado) ou para um bucket em um sistema ONTAP configurado como um servidor S3 (um arquivo de backup), ou ambos.

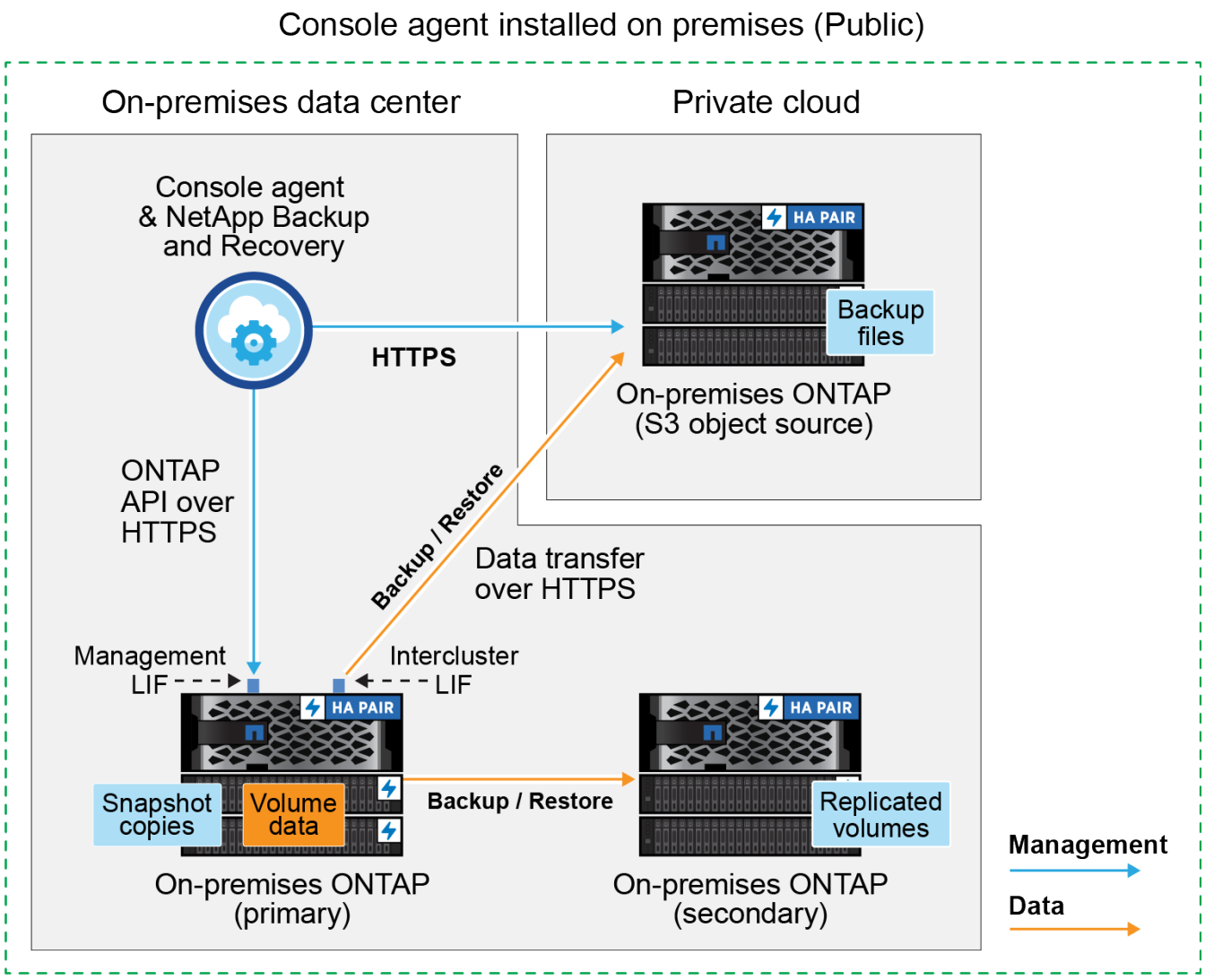
O sistema ONTAP local principal pode ser um sistema FAS, AFF ou ONTAP Select . O sistema ONTAP secundário pode ser um sistema ONTAP local ou Cloud Volumes ONTAP . O armazenamento de objetos pode estar em um sistema ONTAP local ou em um sistema Cloud Volumes ONTAP no qual você habilitou um servidor de armazenamento de objetos do Simple Storage Service (S3).

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Identifique o método de conexão

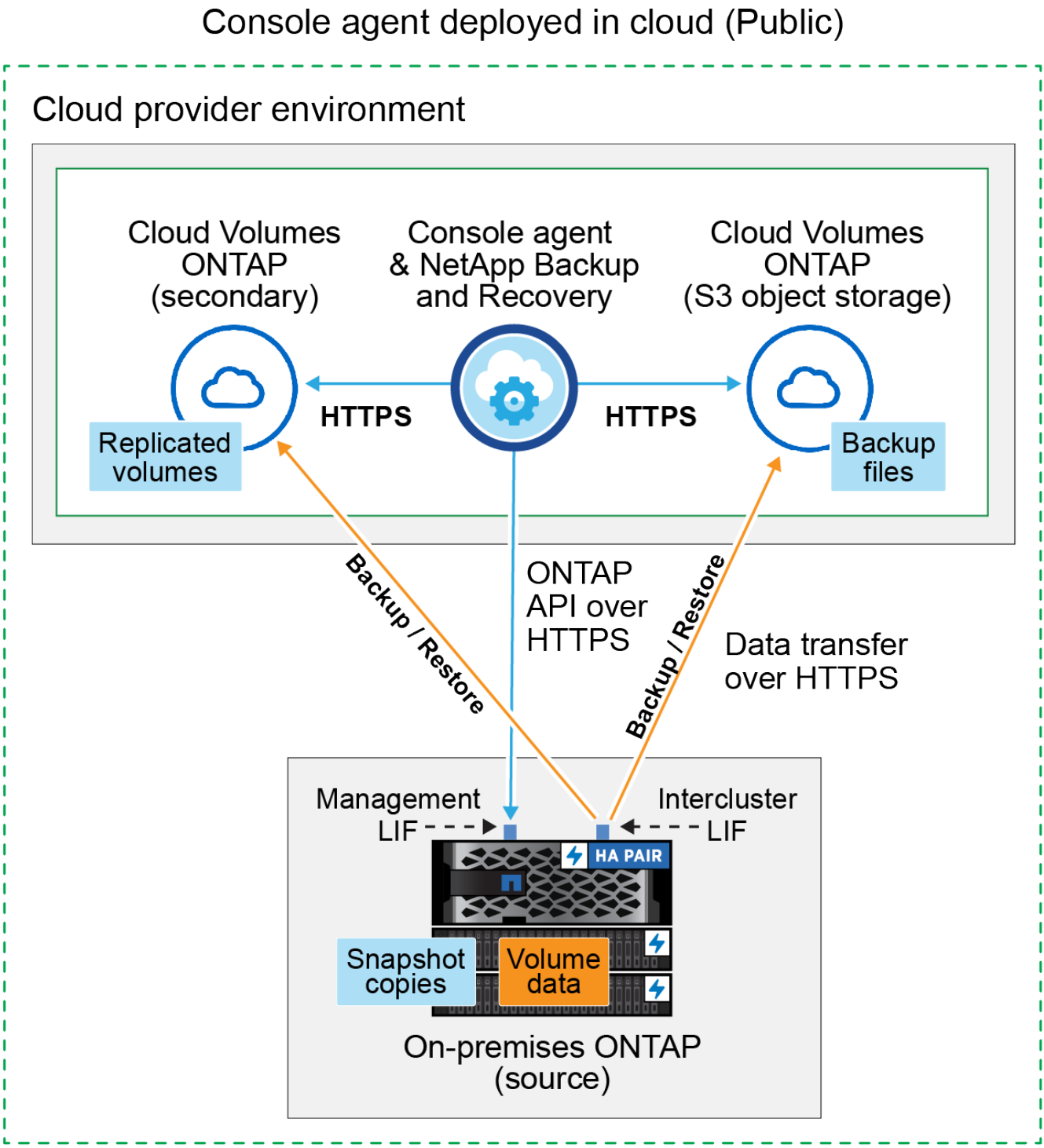
Há muitas configurações nas quais você pode criar backups para um bucket S3 em um sistema ONTAP . Dois cenários são mostrados abaixo.

A imagem a seguir mostra cada componente ao fazer backup de um sistema ONTAP local primário para um sistema ONTAP 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 agente do Console e o sistema ONTAP local principal são instalados em um local local sem acesso à Internet (uma implantação no modo "privado"), 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 local primário 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 do provedor de nuvem para replicar volumes.



Neste cenário, o agente do Console deve ser implantado no mesmo ambiente do provedor de nuvem em que os sistemas Cloud Volumes ONTAP são implantados.

Prepare seu agente de console

O agente do Console é o software principal para a funcionalidade do Console. Um agente do Console é necessário para fazer backup e restaurar seus dados ONTAP .

Criar ou alternar agentes do Console

Ao fazer backup de dados no ONTAP S3, um agente do Console deve estar disponível em suas instalações ou na nuvem. Você precisará instalar um novo agente do Console ou certificar-se de que o agente do Console selecionado atualmente resida em um desses locais. O agente do Console local pode ser instalado em um site com ou sem acesso à Internet.

- "Saiba mais sobre os agentes do Console"
- "Instale o agente do Console no seu ambiente de nuvem"
- "Instalando o agente do Console em um host Linux com acesso à Internet"
- "Instalando o agente do Console em um host Linux sem acesso à Internet"
- "Alternando entre agentes do Console"

Preparar os requisitos de rede do agente do console

Certifique-se de que a rede onde o agente do Console está instalado habilite as seguintes conexões:

- Uma conexão HTTPS pela porta 443 para o servidor ONTAP S3
- Uma conexão HTTPS pela porta 443 para seu LIF de gerenciamento de cluster ONTAP de origem
- Uma conexão de saída de internet pela porta 443 para o NetApp Backup and Recovery (não necessária quando o agente do Console está instalado em um site "escuro")

Considerações sobre o modo privado (site escuro)

A funcionalidade de backup e recuperação do NetApp está integrada ao agente do Console. Quando instalado no modo privado, você precisará atualizar o software do agente do Console periodicamente para ter acesso a novos recursos. Verifique o"Novidades do NetApp Backup and Recovery" para ver os novos recursos em cada versão do NetApp Backup and Recovery. Quando você quiser usar os novos recursos, siga as etapas para "atualizar o software do agente do Console" .

Quando você usa o NetApp Backup and Recovery em um ambiente SaaS padrão, os dados de configuração do NetApp Backup and Recovery são armazenados em backup na nuvem. Quando você usa o NetApp Backup and Recovery em um site sem acesso à Internet, os dados de configuração do NetApp Backup and Recovery são copiados para o bucket ONTAP S3 onde seus backups estão sendo armazenados.

Verificar requisitos de licença

Antes de ativar o NetApp Backup and Recovery para seu cluster, você precisará comprar e ativar uma licença BYOL do NetApp Backup and Recovery da NetApp. A licença é para backup e restauração no armazenamento de objetos - nenhuma licença é necessária para criar cópias de Snapshot ou volumes replicados. Esta licença é para a conta e pode ser usada em vários sistemas.

Você precisará do número de série da NetApp que lhe permitirá usar o serviço durante a duração e a capacidade da licença. "Aprenda a gerenciar suas licenças BYOL" .

O licenciamento PAYGO não é suportado ao fazer backup de arquivos no ONTAP S3.

Prepare seus clusters ONTAP

Você precisará preparar seu sistema ONTAP local de origem e quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP .

Preparar seus clusters ONTAP envolve as seguintes etapas:

- Descubra seus sistemas ONTAP no NetApp Console
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos
- Verifique os requisitos de rede ONTAP para replicar volumes

Descubra seus sistemas ONTAP no NetApp Console

Tanto o sistema ONTAP local de origem quanto quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP devem estar disponíveis na página **Sistemas** do NetApp Console.

Você precisará saber o endereço IP de gerenciamento do cluster e a senha da conta de usuário administrador para adicionar o cluster. "Aprenda como descobrir um cluster" .

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP sejam atendidos:

- Mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior é recomendado.
- Uma licença do SnapMirror (incluída como parte do Pacote Premium ou Pacote de Proteção de Dados).

  Observação: O "Hybrid Cloud Bundle" não é necessário ao usar o NetApp Backup and Recovery.

  Aprenda como "gerencie suas licenças de cluster" .
- A hora e o fuso horário estão definidos corretamente. Aprenda como "configure o tempo do seu cluster" .
- Se você for replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar os dados.

  "Ver versões ONTAP compatíveis para relacionamentos SnapMirror" .

Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos

Você deve garantir que os seguintes requisitos sejam atendidos no sistema que se conecta ao armazenamento de objetos.

- Ao usar uma arquitetura de backup fan-out, as configurações devem ser definidas no sistema de armazenamento *primário*.
- Ao usar uma arquitetura de backup em cascata, as configurações devem ser definidas no sistema de armazenamento *secundário*.

  "Saiba mais sobre os tipos de arquitetura de backup" .

Os seguintes requisitos de rede de cluster ONTAP são necessários:

- O cluster ONTAP inicia uma conexão HTTPS por meio de uma porta especificada pelo usuário do LIF intercluster para o servidor ONTAP S3 para operações de backup e restauração. A porta é configurável durante a configuração do backup.

  ONTAP lê e grava dados de e para armazenamento de objetos. O armazenamento de objetos nunca

inicia, ele apenas responde.

- O ONTAP requer uma conexão de entrada do agente do Console para o LIF de gerenciamento do cluster.
- Um LIF intercluster é necessário em cada nó ONTAP que hospeda os volumes dos quais você deseja fazer backup. O LIF deve ser associado ao *IPspace* que o ONTAP deve usar para se conectar ao armazenamento de objetos. "Saiba mais sobre IPspaces" .

  Ao configurar o NetApp Backup and Recovery, você será solicitado a informar o IPspace a ser usado. Você deve escolher o IPspace ao qual cada LIF está associado. Pode ser o IPspace "padrão" ou um IPspace personalizado que você criou.

- Os LIFs intercluster dos nós podem acessar o armazenamento de objetos (não é necessário quando o agente do Console está instalado em um site "escuro").
- Os servidores DNS foram configurados para a VM de armazenamento onde os volumes estão localizados. Veja como "configurar serviços DNS para o SVM" .
- Se você estiver usando 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 do NetApp Backup and Recovery do ONTAP para o armazenamento de objetos pela porta especificada (normalmente a porta 443) e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS pela porta 53 (TCP/UDP).

Verifique os requisitos de rede ONTAP para replicar volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o NetApp Backup and Recovery, certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede ONTAP local

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

  Como você pode replicar para o Cloud Volumes ONTAP ou para 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 do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: especificamente, regras para ICMP e portas 11104 e 11105. Essas regras estão incluídas no grupo de segurança predefinido.

Prepare o ONTAP S3 como seu destino de backup

Você deve habilitar um servidor de armazenamento de objetos do Simple Storage Service (S3) no cluster ONTAP que você planeja usar para backups de armazenamento de objetos. Veja o "Documentação do ONTAP S3" para mais detalhes.

Observação: você pode adicionar este cluster à página **Sistemas** do Console, mas ele não é identificado como um servidor de armazenamento de objetos S3, e você não pode arrastar e soltar um sistema de origem neste sistema S3 para iniciar a ativação do backup.

Este sistema ONTAP deve atender aos seguintes requisitos.

Versões ONTAP suportadas

ONTAP 9.8 e posteriores são necessários para sistemas ONTAP locais. ONTAP 9.9.1 e posteriores são necessários para sistemas Cloud Volumes ONTAP .

Credenciais S3

Você deve ter criado um usuário S3 para controlar o acesso ao seu armazenamento ONTAP S3. "Veja a documentação do ONTAP S3 para mais detalhes" .

Ao configurar o backup no 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 NetApp Backup and Recovery autentique e acesse os buckets do ONTAP S3 usados para armazenar backups. As chaves são necessárias para que o ONTAP S3 saiba quem está fazendo a solicitação.

Essas chaves de acesso devem ser associadas a um usuário que tenha as seguintes permissões:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Ative backups em seus volumes ONTAP

Ative backups a qualquer momento diretamente do seu sistema local.

Um assistente guia você pelas seguintes etapas principais:

- Selecione os volumes dos quais deseja fazer backup
- Definir a estratégia e as políticas de backup
- Revise suas seleções

Você também pode Mostrar os comandos da API na etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para sistemas futuros.

Inicie o assistente

Passos

1. Acesse o assistente Ativar backup e recuperação usando uma das seguintes maneiras:
   - Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar > Volumes de backup** ao lado de Backup e recuperação no painel direito.
   - Selecione **Volumes** na barra Backup e recuperação. Na guia Volumes, selecione a opção **Ações (...)** e selecione **Ativar backup** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos habilitado).

   A página Introdução do assistente mostra as opções de proteção, incluindo instantâneos locais, replicações e backups. Se você escolheu a segunda opção nesta etapa, a página Definir estratégia de backup aparecerá com um volume selecionado.

2. Continue com as seguintes opções:
    - Se você já tem um agente do Console, está tudo pronto. Basta selecionar **Avançar**.
    - Se você não tiver um agente do Console, a opção **Adicionar um agente do Console** será exibida. Consulte Prepare seu agente de console .

Selecione os volumes dos quais deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que possui um ou mais dos seguintes: política de instantâneo, política de replicação, política de backup para objeto.

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

- Você pode ativar um backup somente em um único volume FlexGroup por vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock . Todos os volumes devem ter o SnapLock Enterprise habilitado ou o SnapLock desabilitado.

Passos

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

1. Na página Selecionar volumes, selecione o volume ou volumes que você 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 podem ser selecionados apenas um de cada vez). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e depois marque a caixa na linha de título.
    - Para fazer backup de volumes individuais, marque a caixa de cada volume.
2. Selecione **Avançar**.

Defina a estratégia de backup

Definir a estratégia de backup envolve configurar as seguintes opções:

- Opções de proteção: se você deseja implementar uma ou todas as opções de backup: instantâneos locais, replicação e backup para armazenamento de objetos
- Arquitetura: se você deseja usar uma arquitetura de backup em cascata ou em fan-out
- 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:
    - **Local Snapshots**: Cria cópias de Snapshots 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:
   - **Cascata**: os dados de backup fluem do sistema primário para o secundário e, depois, do secundário para o armazenamento de objetos.
   - **Distribuição**: Os dados de backup fluem do sistema primário para o secundário *e* do primário para o armazenamento de objetos.

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

3. **Instantâneo local**: escolha uma política de instantâneo existente ou crie uma nova.

   Se você quiser criar uma política personalizada antes de ativar o Snapshot, você pode usar o System Manager ou o ONTAP CLI `snapmirror policy create` comando. Consulte .

   Para criar uma política personalizada usando este serviço, consulte"Criar uma política" .

   Para criar uma política, selecione **Criar nova política** e faça o seguinte:
   - Digite o nome da política.
   - Selecione até cinco programações, normalmente com frequências diferentes.
   - Selecione **Criar**.

4. **Replicação**: Se você selecionou **Replicação**, defina as seguintes opções:
   - **Destino de replicação**: Selecione o sistema de destino e o 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:
     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Selecione **Criar**.

5. **Fazer backup no objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Provedor**: 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 são para o usuário que você criou para dar ao cluster ONTAP acesso ao bucket S3.
   - **Rede**: Escolha o espaço IP no cluster ONTAP de origem onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet (não necessário quando o agente do Console está instalado em um site "escuro").

     Selecionar o IPspace correto garante que o NetApp Backup and Recovery possa configurar uma conexão do ONTAP para seu armazenamento de objetos ONTAP S3.

- **Política de backup**: Selecione uma política de backup existente ou crie uma nova.

  Você pode criar uma política com o System Manager ou o ONTAP CLI. Para criar uma política personalizada usando o ONTAP CLI `snapmirror policy create` comando, consulte .

  Para criar uma política personalizada usando este serviço, consulte"Criar uma política" .

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

  - Digite o nome da política.
  - Selecione até cinco programações, normalmente com frequências diferentes.
  - Para políticas de backup para objeto, defina as configurações de DataLock e Resiliência de Ransomware. Para obter detalhes sobre DataLock e Ransomware Resilience, consulte"Configurações de política de backup para objeto" .
  - Selecione **Criar**.

- **Exportar cópias de snapshot existentes para armazenamento de objetos como arquivos de backup**: Se houver cópias de snapshot locais para volumes neste sistema que correspondam ao rótulo de agendamento de backup que você acabou de selecionar (por exemplo, diário, semanal, etc.), este 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 **Avançar**.

Revise suas seleções

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

Passos

1. Na página Revisão, revise suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos da política de instantâneo com os rótulos da política de replicação e backup**. Isso cria instantâneos 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 NetApp Backup and Recovery começa 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. Transferências subsequentes contêm cópias diferenciais dos dados de armazenamento primário contidos em cópias de instantâneo.

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 pela 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.

Você também pode monitorar o status dos trabalhos de backup e restauração usando o"Página de monitoramento de tarefas" .

Mostrar os comandos da API

Talvez você queira exibir e, opcionalmente, copiar os comandos de API usados no assistente Ativar backup e recuperação. Talvez você queira fazer isso para automatizar a ativação de backup em sistemas futuros.

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**.

Faça backup de dados ONTAP locais no StorageGRID com o NetApp Backup and Recovery

Conclua algumas etapas no NetApp Backup and Recovery para começar a fazer backup de dados de volume dos seus sistemas ONTAP primários locais para um sistema de armazenamento secundário e para o armazenamento de objetos nos seus sistemas NetApp StorageGRID .

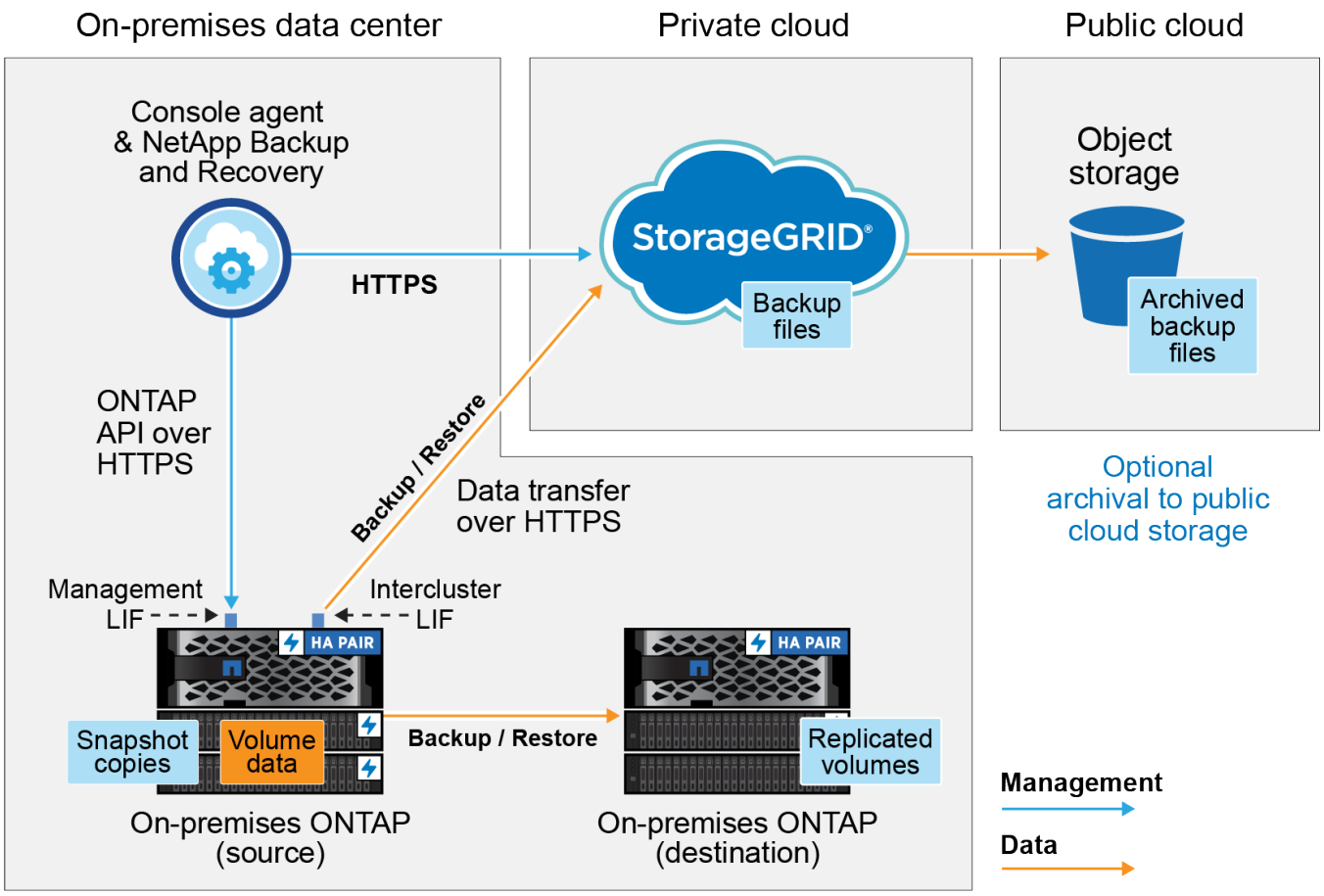
Os "sistemas ONTAP locais" incluem sistemas FAS, AFF e ONTAP Select .

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Identifique o método de conexão

A imagem a seguir mostra cada componente ao fazer backup de um sistema ONTAP local no 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 agente do Console e o sistema ONTAP local são instalados em um local local sem acesso à Internet (um "dark site"), 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 seu agente de console

O agente do Console é o software principal para a funcionalidade do Console. Um agente do Console é necessário para fazer backup e restaurar seus dados ONTAP .

Criar ou alternar agentes do Console

Ao fazer backup de dados no StorageGRID, um agente do Console deve estar disponível em suas instalações. Você precisará instalar um novo agente do Console ou certificar-se de que o agente do Console selecionado atualmente resida no local. O agente do Console pode ser instalado em um site com ou sem acesso à Internet.

- "Saiba mais sobre os agentes do Console"
- "Instalando o agente do Console em um host Linux com acesso à Internet"
- "Instalando o agente do Console em um host Linux sem acesso à Internet"
- "Alternando entre agentes do Console"

Preparar os requisitos de rede do agente do console

Certifique-se de que a rede onde o agente do Console está instalado habilite as seguintes conexões:

- Uma conexão HTTPS pela porta 443 para o nó do gateway StorageGRID
- Uma conexão HTTPS pela porta 443 para seu LIF de gerenciamento de cluster ONTAP
- Uma conexão de saída de internet pela porta 443 para o NetApp Backup and Recovery (não necessária quando o agente do Console está instalado em um site "escuro")

Considerações sobre o modo privado (site escuro)

- A funcionalidade de backup e recuperação do NetApp está integrada ao agente do Console. Quando instalado no modo privado, você precisará atualizar o software do agente do Console periodicamente para ter acesso a novos recursos. Verifique o"Novidades do NetApp Backup and Recovery" para ver os novos recursos em cada versão do NetApp Backup and Recovery. Quando você quiser usar os novos recursos, siga as etapas para "atualizar o software do agente do Console" .

  A nova versão do NetApp Backup and Recovery, que inclui a capacidade de agendar e criar cópias de snapshot e volumes replicados, além de criar backups para armazenamento de objetos, exige que você esteja usando a versão 3.9.31 ou superior do agente do Console. Portanto, é recomendável que você obtenha esta versão mais recente para gerenciar todos os seus backups.

- Quando você usa o NetApp Backup and Recovery em um ambiente SaaS, os dados de configuração do NetApp Backup and Recovery são armazenados em backup na nuvem. Quando você usa o NetApp Backup and Recovery em um site sem acesso à Internet, os dados de configuração do NetApp Backup and Recovery são copiados para o bucket StorageGRID onde seus backups estão sendo armazenados.

Verificar requisitos de licença

Antes de ativar o NetApp Backup and Recovery para seu cluster, você precisará comprar e ativar uma licença BYOL do NetApp Backup and Recovery da NetApp. Esta licença é para a conta e pode ser usada em vários sistemas.

Você precisará do número de série da NetApp que lhe permitirá usar o serviço durante a duração e a capacidade da licença. "Aprenda a gerenciar suas licenças BYOL" .

O licenciamento PAYGO não é suportado ao fazer backup de arquivos no StorageGRID.

Prepare seus clusters ONTAP

Você precisará preparar seu sistema ONTAP local de origem e quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP .

Preparar seus clusters ONTAP envolve as seguintes etapas:

- Descubra seus sistemas ONTAP no NetApp Console
- Verifique os requisitos do sistema ONTAP
- Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos
- Verifique os requisitos de rede ONTAP para replicar volumes

Descubra seus sistemas ONTAP no NetApp Console

Tanto o sistema ONTAP local de origem quanto quaisquer sistemas ONTAP locais secundários ou Cloud Volumes ONTAP devem estar disponíveis na página **Sistemas** do NetApp Console.

Você precisará saber o endereço IP de gerenciamento do cluster e a senha da conta de usuário administrador para adicionar o cluster. "Aprenda como descobrir um cluster" .

Verifique os requisitos do sistema ONTAP

Certifique-se de que os seguintes requisitos do ONTAP sejam atendidos:

- Mínimo de ONTAP 9.8; ONTAP 9.8P13 e posterior é recomendado.
- Uma licença do SnapMirror (incluída como parte do Pacote Premium ou Pacote de Proteção de Dados).

  Observação: O "Hybrid Cloud Bundle" não é necessário ao usar o NetApp Backup and Recovery.

  Aprenda como "gerencie suas licenças de cluster" .
- A hora e o fuso horário estão definidos corretamente. Aprenda como "configure o tempo do seu cluster" .
- Se você for replicar dados, verifique se os sistemas de origem e destino estão executando versões compatíveis do ONTAP antes de replicar os dados.

  "Ver versões ONTAP compatíveis para relacionamentos SnapMirror" .

Verifique os requisitos de rede ONTAP para fazer backup de dados no armazenamento de objetos

Você deve configurar os seguintes requisitos no sistema que se conecta ao armazenamento de objetos.

- Ao usar uma arquitetura de backup fan-out, as seguintes configurações devem ser definidas no sistema de armazenamento *primário*.
- Ao usar uma arquitetura de backup em cascata, as seguintes configurações devem ser definidas no sistema de armazenamento *secundário*.

Os seguintes requisitos de rede de cluster ONTAP são necessários:

- O cluster ONTAP inicia uma conexão HTTPS por meio de uma porta especificada pelo usuário do LIF intercluster para o nó do gateway StorageGRID para operações de backup e restauração. A porta é configurável durante a configuração do backup.

  ONTAP lê e grava dados de e para armazenamento de objetos. O armazenamento de objetos nunca inicia, ele apenas responde.
- O ONTAP requer uma conexão de entrada do agente do Console para o LIF de gerenciamento do cluster. O agente do Console deve residir em suas instalações.
- Um LIF intercluster é necessário em cada nó ONTAP que hospeda os volumes dos quais você deseja fazer backup. O LIF deve ser associado ao *IPspace* que o ONTAP deve usar para se conectar ao armazenamento de objetos. "Saiba mais sobre IPspaces" .

  Ao configurar o NetApp Backup and Recovery, você será solicitado a informar o IPspace a ser usado. Você deve escolher o IPspace ao qual cada LIF está associado. Pode ser o IPspace "padrão" ou um IPspace personalizado que você criou.

- Os LIFs intercluster dos nós podem acessar o armazenamento de objetos (não é necessário quando o agente do Console está instalado em um site "escuro").
- Os servidores DNS foram configurados para a VM de armazenamento onde os volumes estão localizados. Veja como "configurar serviços DNS para o SVM" .
- Se você estiver usando 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 do NetApp Backup and Recovery do ONTAP para o armazenamento de objetos pela porta especificada (normalmente a porta 443) e tráfego de resolução de nomes da VM de armazenamento para o servidor DNS pela porta 53 (TCP/UDP).

Verifique os requisitos de rede ONTAP para replicar volumes

Se você planeja criar volumes replicados em um sistema ONTAP secundário usando o NetApp Backup and Recovery, certifique-se de que os sistemas de origem e destino atendam aos seguintes requisitos de rede.

Requisitos de rede ONTAP local

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

  Como você pode replicar para o Cloud Volumes ONTAP ou para 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 do Cloud Volumes ONTAP

- O grupo de segurança da instância deve incluir as regras de entrada e saída necessárias: especificamente, regras para ICMP e portas 11104 e 11105. Essas regras estão incluídas no grupo de segurança predefinido.

Prepare o StorageGRID como seu destino de backup

O StorageGRID deve atender aos seguintes requisitos. Veja o "Documentação do StorageGRID" para mais informações.

Para obter detalhes sobre os requisitos de resiliência do DataLock e do Ransomware para StorageGRID, consulte"Opções de política de backup para objeto" .

Versões do StorageGRID suportadas

O StorageGRID 10.3 e versões posteriores são suportados.

Para usar o DataLock & Ransomware Resilience para seus backups, seus sistemas StorageGRID devem estar executando a versão 11.6.0.3 ou superior.

Para colocar backups mais antigos em camadas no armazenamento de arquivo em nuvem, seus sistemas StorageGRID devem estar executando a versão 11.3 ou superior. Além disso, seus sistemas StorageGRID devem ser descobertos na página **Sistemas** do Console.

Para usar o armazenamento de arquivo, é necessário acesso IP ao nó de administração.

O acesso IP do gateway é sempre necessário.

Credenciais S3

Você deve ter criado uma conta de locatário do S3 para controlar o acesso ao seu armazenamento StorageGRID . "Veja a documentação do StorageGRID para mais detalhes" .

Ao configurar 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 do locatário permite que o NetApp Backup and Recovery autentique e acesse os buckets do StorageGRID usados para armazenar backups. As chaves são necessárias para que o StorageGRID saiba quem está fazendo a solicitação.

Essas chaves de acesso devem ser 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 do objeto StorageGRID manualmente no bucket do armazenamento de objetos.

Prepare-se para arquivar arquivos de backup mais antigos no armazenamento em nuvem pública

Colocar arquivos de backup mais antigos em níveis de armazenamento de arquivamento economiza dinheiro ao usar uma classe de armazenamento mais barata para backups que você pode não precisar. O StorageGRID é uma solução local (nuvem privada) que não fornece armazenamento de arquivo, mas você pode mover arquivos de backup mais antigos para armazenamento de arquivo em nuvem pública. Quando usado dessa forma, os dados que são colocados em camadas no armazenamento em nuvem ou restaurados do armazenamento em nuvem vão entre o StorageGRID e o armazenamento em nuvem - o Console não está envolvido nessa transferência de dados.

O suporte atual permite arquivar backups no armazenamento AWS *S3 Glacier*/*S3 Glacier Deep Archive* ou *Azure Archive*.

- Requisitos ONTAP *
- Seu cluster deve estar usando o ONTAP 9.12.1 ou superior.
- Requisitos do StorageGRID *
- Seu StorageGRID deve estar usando 11.4 ou superior.
- Seu StorageGRID deve ser "descoberto e disponível no Console" .

Requisitos do Amazon S3

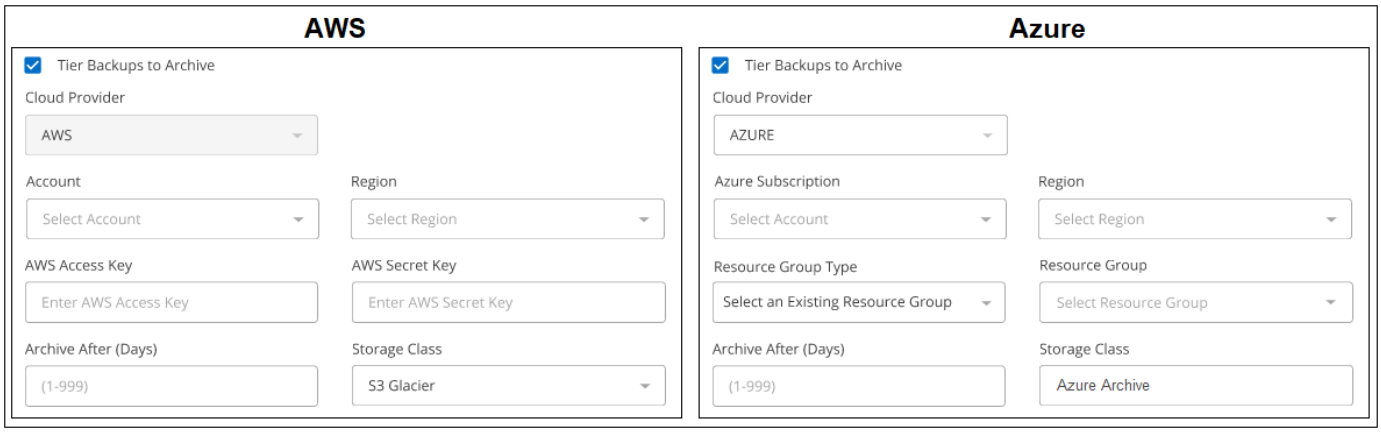
- Você precisará criar uma conta Amazon S3 para o espaço de armazenamento onde seus backups arquivados estarão localizados.
- Você pode optar por fazer backups em camadas no armazenamento AWS S3 Glacier ou S3 Glacier Deep Archive. "Saiba mais sobre as camadas de arquivamento da AWS" .

- 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 S3 ao StorageGRID:
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Requisitos do Azure Blob

- 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 contêiner de Blobs 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 seu cluster, você inserirá as credenciais do seu provedor de nuvem e selecionará a classe de armazenamento que deseja usar. O NetApp Backup and Recovery cria o bucket de nuvem quando você ativa o backup para o cluster. As informações necessárias para armazenamento de arquivo na AWS e no Azure são mostradas abaixo.



As configurações de política de arquivamento selecionadas gerarão uma política de gerenciamento do ciclo de vida das informações (ILM) no StorageGRID e adicionarão as configurações como "regras".

- Se houver uma política de ILM ativa, novas regras serão adicionadas à política de ILM para mover os dados para a camada de arquivamento.
- Se houver uma política de ILM existente no estado "proposta", a criação e ativação de uma nova política de ILM não será possível. "Saiba mais sobre as políticas e regras do StorageGRID ILM" .

Ative backups em seus volumes ONTAP

Ative backups a qualquer momento diretamente do seu sistema local.

Um assistente guia você pelas seguintes etapas principais:

- Selecione os volumes dos quais deseja fazer backup
- Defina a estratégia de backup
- Revise suas seleções

Você também podeMostrar os comandos da API na etapa de revisão, para que você possa copiar o código para automatizar a ativação de backup para sistemas futuros.

Inicie o assistente

Passos

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

   - Na página **Sistemas** do Console, selecione o sistema e selecione **Ativar > Volumes de backup** ao lado de Backup e recuperação no painel direito.

     Se o destino dos seus backups existir como um sistema na página **Sistemas** do Console, você poderá arrastar o cluster ONTAP para o armazenamento de objetos.

   - Selecione **Volumes** na barra Backup e recuperação. Na guia Volumes, selecione a opção **Ações (…)** e selecione **Ativar backup** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos habilitado).

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

2. Continue com as seguintes opções:

   - Se você já tem um agente do Console, está tudo pronto. Basta selecionar **Avançar**.
   - Se você ainda não tiver um agente do Console, a opção **Adicionar um agente do Console** será exibida. Consulte Prepare seu agente de console .

Selecione os volumes dos quais deseja fazer backup

Escolha os volumes que você deseja proteger. Um volume protegido é aquele que tem um ou mais dos seguintes: política de instantâneo, política de replicação, política de backup em objeto.

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

- Você pode ativar um backup somente em um único volume FlexGroup por vez.
- Os volumes selecionados devem ter a mesma configuração SnapLock . Todos os volumes devem ter o SnapLock Enterprise habilitado ou o SnapLock desabilitado.

Passos

Se os volumes escolhidos já tiverem políticas de snapshot ou replicação aplicadas, as políticas selecionadas posteriormente substituirão essas políticas existentes.

1. Na página Selecionar volumes, selecione o volume ou volumes que você 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 podem ser selecionados apenas um de cada vez). Para fazer backup de todos os volumes FlexVol existentes, marque primeiro um volume e depois marque a caixa na linha de título.
- Para fazer backup de volumes individuais, marque a caixa de cada volume.

2. Selecione **Avançar**.

Defina a estratégia de backup

Definir a estratégia de backup envolve definir as seguintes opções:

- Se você deseja uma ou todas as opções de backup: instantâneos locais, replicação e backup para armazenamento 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 substituídas.

- 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 backup no armazenamento de objetos, instantâneos locais deverão ser criados.
   - **Replicação**: Cria volumes replicados em outro sistema de armazenamento ONTAP .
   - **Backup**: Faz backup de volumes no armazenamento de objetos.
2. **Arquitetura**: Se você escolher replicação e backup, escolha um dos seguintes fluxos de informações:
   - **Cascata**: As informações fluem do primário para o secundário e, depois, do secundário para o armazenamento de objetos.
   - **Fan out**: As informações fluem do primário para o secundário *e* do primário para o armazenamento de objetos.

     Para obter detalhes sobre essas arquiteturas, consulte"Planeje sua jornada de proteção" .
3. **Instantâneo local**: escolha uma política de instantâneo existente ou crie uma nova.

   > Para criar uma política personalizada, consulte"Criar uma política" .

   Para criar uma política, selecione **Criar nova política** e faça o seguinte:
   - Digite o nome da política.
   - Selecione até cinco programações, normalmente com frequências diferentes.
   - Selecione **Criar**.

4. **Replicação**: Defina as seguintes opções:
   - **Destino de replicação**: Selecione o sistema de destino e o SVM. Opcionalmente, selecione o(s) agregado(s) de destino e o prefixo ou sufixo que serão adicionados ao nome do volume replicado.
   - **Política de replicação**: Escolha uma política de replicação existente ou crie uma.

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

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

     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Selecione **Criar**.
5. **Fazer backup no objeto**: Se você selecionou **Backup**, defina as seguintes opções:
   - **Provedor**: Selecione * StorageGRID*.
   - **Configurações do provedor**: insira os detalhes do FQDN do nó do gateway do provedor, porta, chave de acesso e chave secreta.

     A chave de acesso e a chave secreta são para o usuário do IAM que você criou para dar ao cluster ONTAP acesso ao bucket.
   - **Rede**: Escolha o espaço IP no cluster ONTAP onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet (não necessário quando o agente do Console está instalado em um site "escuro").

     Selecionar o IPspace correto garante que o NetApp Backup and Recovery possa configurar uma conexão do ONTAP para seu armazenamento de objetos StorageGRID .
   - **Política de backup**: Selecione uma política de backup para armazenamento de objetos existente ou crie uma.

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

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

     - Digite o nome da política.
     - Selecione até cinco programações, normalmente com frequências diferentes.
     - Para políticas de backup para objeto, defina as configurações de DataLock e Resiliência de Ransomware. Para obter detalhes sobre DataLock e Ransomware Resilience, consulte"Configurações de política de backup para objeto" .

       Se o seu cluster estiver usando o ONTAP 9.11.1 ou superior, você pode optar por proteger seus backups contra exclusão e ataques de ransomware configurando o *DataLock e o Ransomware Resilience*. O *DataLock* protege seus arquivos de backup contra modificações ou exclusão, e o *Ransomware Resilience* verifica seus arquivos de backup para procurar evidências de um ataque de ransomware em seus arquivos de backup.

     - Selecione **Criar**.

     Se o seu cluster estiver usando o ONTAP 9.12.1 ou superior e o seu sistema StorageGRID estiver usando a versão 11.4 ou superior, você poderá optar por colocar backups mais antigos em camadas

de arquivamento em nuvem pública após um determinado número de dias. O suporte atual é para níveis de armazenamento AWS S3 Glacier/S3 Glacier Deep Archive ou Azure Archive. Veja como configurar seus sistemas para essa funcionalidade .

- **Backup em camadas para nuvem pública**: Selecione o provedor de nuvem para o qual você deseja fazer backups em camadas e insira os detalhes do provedor.

  Selecione ou crie um novo cluster StorageGRID . Para obter detalhes sobre como criar um cluster StorageGRID para que o Console possa descobri-lo, consulte "Documentação do StorageGRID" .

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

6. Selecione **Avançar**.

Revise suas seleções

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

Passos

1. Na página Revisão, revise suas seleções.
2. Opcionalmente, marque a caixa para **Sincronizar automaticamente os rótulos da política de instantâneo com os rótulos da política de replicação e backup**. Isso cria instantâneos com um rótulo que corresponde aos rótulos nas políticas de replicação e backup.
3. Selecione **Ativar Backup**.

Resultado

O NetApp Backup and Recovery começa 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. Transferências subsequentes contêm cópias diferenciais dos dados de armazenamento primário contidos em cópias de 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 pela 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.

Você também pode monitorar o status dos trabalhos de backup e restauração usando o"Página de monitoramento de tarefas" .

Mostrar os comandos da API

Talvez você queira exibir e, opcionalmente, copiar os comandos de API usados no assistente Ativar backup e recuperação. Talvez você queira fazer isso para automatizar a ativação de backup em sistemas futuros.

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**.

Migrar volumes usando o SnapMirror para o Cloud Resync no NetApp Backup and Recovery

O recurso SnapMirror to Cloud Resync no NetApp Backup and Recovery simplifica a proteção de dados e a continuidade durante migrações de volume em ambientes NetApp . Quando um volume é migrado usando o SnapMirror Logical Replication (LRSE), de uma implantação NetApp local para outra, ou para uma solução baseada em nuvem, como o Cloud Volumes ONTAP ou o Cloud Volumes Service, o SnapMirror para o Cloud Resync garante que os backups em nuvem existentes permaneçam intactos e operacionais.

Esse recurso elimina a necessidade de uma operação de redefinição de linha de base demorada e que exige muitos recursos, permitindo que as operações de backup continuem após a migração. Esse recurso é valioso em cenários de migração de carga de trabalho, oferecendo suporte a FlexVols e FlexGroups, e está disponível a partir da versão 9.16.1 do ONTAP .

Este recurso está disponível a partir da versão 4.0.3 do NetApp Backup and Recovery, lançada em maio de 2025.

Ao manter a continuidade do backup em todos os ambientes, o SnapMirror to Cloud Resync aumenta a eficiência operacional e reduz a complexidade do gerenciamento de dados híbridos e multinuvem.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Antes de começar

Certifique-se de que estes pré-requisitos foram atendidos:

- O cluster ONTAP de destino deve estar executando o ONTAP versão 9.16.1 ou posterior.
- O antigo cluster ONTAP de origem deve ser protegido usando o NetApp Backup and Recovery.
- O recurso SnapMirror to Cloud Resync está disponível a partir do NetApp Backup and Recovery versão 4.0.3, lançado em maio de 2025.
- O backup mais recente no armazenamento de objetos deve ser o instantâneo comum na origem antiga, na nova origem e no armazenamento de objetos. O snapshot comum não pode ser mais antigo que o snapshot mais recente cujo backup foi feito no armazenamento de objetos.
- As políticas de snapshot e SnapMirror , que eram usadas no ONTAP mais antigo, devem ser criadas no novo cluster ONTAP antes de iniciar a operação de ressincronização. Se alguma política for usada no processo de ressincronização, essa política também deverá ser criada. A operação Resync não cria as políticas.
- Certifique-se de que a política do SnapMirror aplicada ao relacionamento do SnapMirror do volume de migração inclua o mesmo rótulo usado pelo relacionamento da nuvem. Para evitar problemas, use a política que controla um espelho exato do volume e de todos os instantâneos.

O SnapMirror para Cloud Resync após migrações usando os métodos SVM-Migrate, SVM-DR ou Head Swap não é suportado no momento.

Como funciona o NetApp Backup and Recovery SnapMirror para a ressincronização na nuvem

Se você concluir uma atualização técnica ou migrar volumes de um cluster ONTAP para outro, é importante que seus backups continuem funcionando sem interrupção. O NetApp Backup and Recovery SnapMirror to Cloud Resync ajuda com isso, garantindo que seus backups na nuvem permaneçam consistentes mesmo após uma migração de volume.

Aqui está um exemplo:

Imagine que você tem um volume local chamado Vol1a. Este volume tem três instantâneos: S1, S2 e S3. Esses instantâneos são como pontos de restauração. O Vol1 já está sendo copiado para um ponto de extremidade de armazenamento de objetos na nuvem usando o SnapMirror to Cloud (SM-C). Entretanto, somente S1 e S2 foram copiados para armazenamento de objetos até agora.

Agora, você deseja migrar o Vol1 para outro cluster ONTAP . Para fazer isso, crie um relacionamento SnapMirror Logical Replication (LRSE) com um novo volume de nuvem chamado Vol1b. Isso transfere todos os três instantâneos — S1, S2 e S3 — de Vol1a para Vol1b.

Após a conclusão da migração, você terá a seguinte configuração:

- O relacionamento SM-C original (Vol1a → Armazenamento de objetos) é excluído.
- A relação LRSE (Vol1a → Vol1b) também é excluída.
- Vol1b agora é seu volume ativo.

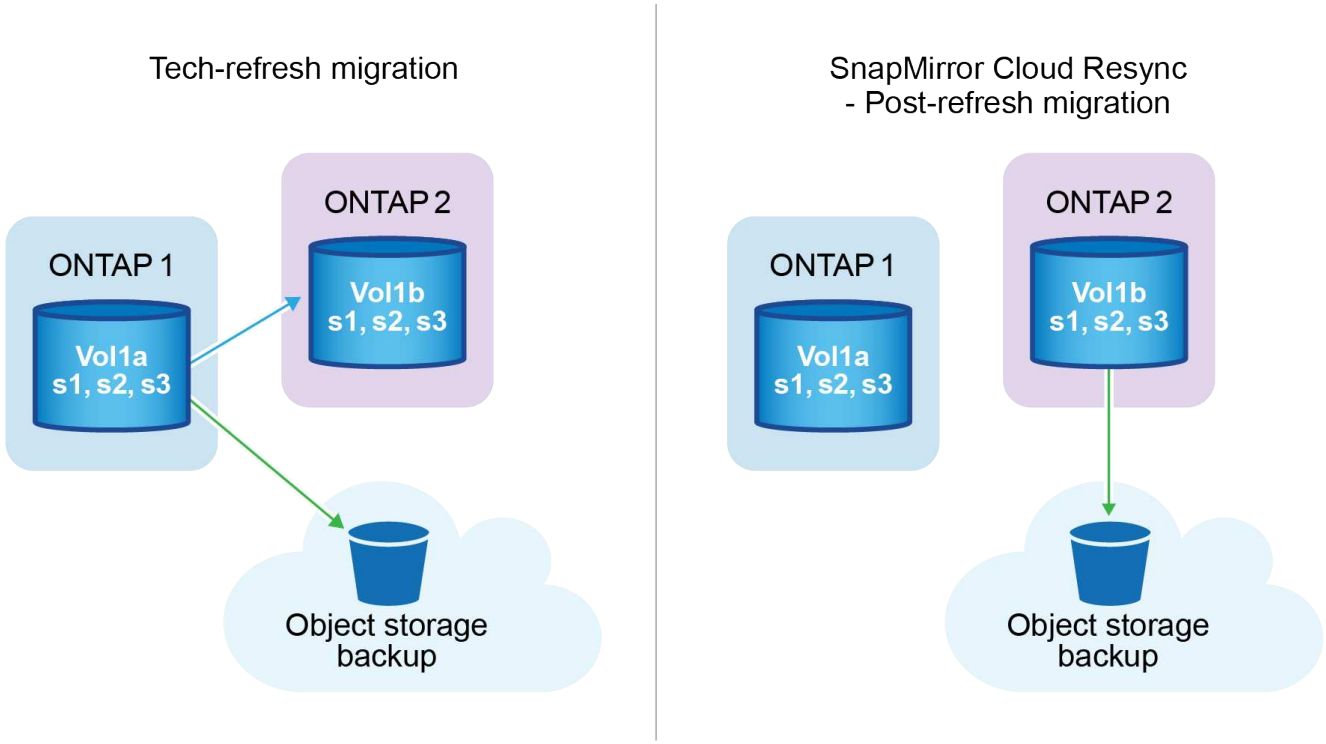
Neste ponto, você deseja continuar fazendo backup do Vol1b no mesmo ponto de extremidade da nuvem. Mas em vez de iniciar um backup completo do zero (o que levaria tempo e recursos), você usa o SnapMirror para Cloud Resync.

Veja como funciona a ressincronização:

- O sistema verifica se há um snapshot comum entre o Vol1a e o Object store. Neste caso, ambos têm S2.
- Devido a esse instantâneo compartilhado, o sistema precisa transferir apenas as alterações incrementais entre S2 e S3.

Isso significa que apenas os novos dados adicionados depois que S2 são enviados ao armazenamento de objetos, não o volume inteiro.

Esse processo evita o reenvio de dados que já foram copiados, economiza largura de banda e garante que sua cadeia de backup continue sem problemas após a migração.



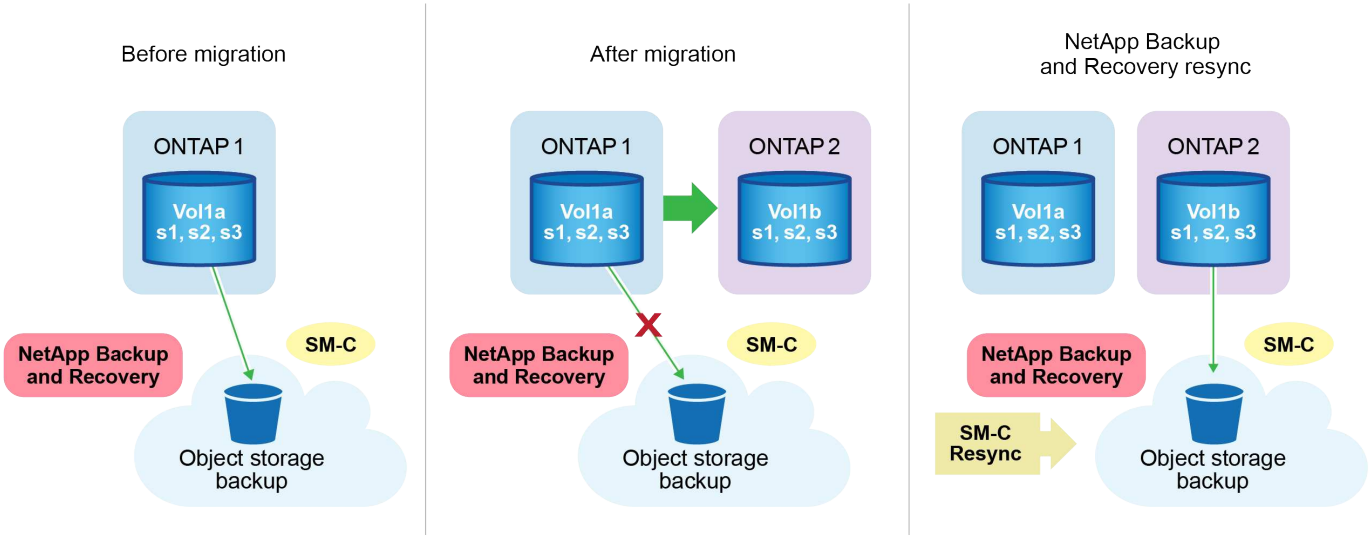
Notas de procedimento

- Migrações e atualizações tecnológicas não são realizadas usando o NetApp Backup and Recovery. Elas devem ser realizadas por uma equipe de serviços profissionais ou por um administrador de armazenamento qualificado.
- Uma equipe de migração da NetApp é responsável por criar o relacionamento SnapMirror entre os clusters ONTAP de origem e destino para facilitar a migração de volume.
- Garanta que a migração durante uma atualização tecnológica seja baseada na migração baseada no SnapMirror.

Como migrar volumes usando o SnapMirror para o Cloud Resync

A migração de volumes usando o SnapMirror para o Cloud Resync envolve as seguintes etapas principais, cada uma descrita com mais detalhes abaixo:

- **Siga uma lista de verificação pré-migração**: Antes de iniciar a migração, uma equipe da NetApp Tech Refresh garante que os seguintes pré-requisitos sejam atendidos para evitar perda de dados e garantir um processo de migração tranquilo.
- **Siga uma lista de verificação pós-migração**: Após a migração, uma equipe da NetApp Tech Refresh garante que as seguintes etapas sejam concluídas para estabelecer a proteção e se preparar para a ressincronização.
- **Executar uma ressincronização do SnapMirror para a nuvem**: após a migração, uma equipe do NetApp Tech Refresh executa uma operação de ressincronização do SnapMirror para a nuvem para retomar os backups na nuvem dos volumes recém-migrados.



Siga uma lista de verificação pré-migração

Antes de iniciar a migração, uma equipe da NetApp Tech Refresh garante que os seguintes pré-requisitos sejam atendidos para evitar perda de dados e garantir um processo de migração tranquilo.

1. Certifique-se de que todos os volumes que serão migrados estejam protegidos usando o NetApp Backup and Recovery.
2. Registre UUIDs de instância de volume. Anote os UUIDs de instância de todos os volumes antes de iniciar a migração. Esses identificadores são cruciais para operações de mapeamento e ressincronização posteriores.
3. Faça um instantâneo final de cada volume para preservar o estado mais recente, antes de excluir qualquer relacionamento do SnapMirror .
4. Documentar políticas do SnapMirror . Registre a política do SnapMirror atualmente anexada ao relacionamento de cada volume. Isso será necessário mais tarde durante o processo de ressincronização do SnapMirror para a Nuvem.
5. Exclua os relacionamentos do SnapMirror Cloud com o armazenamento de objetos.
6. Crie um relacionamento SnapMirror padrão com o novo cluster ONTAP para migrar o volume para o novo cluster ONTAP de destino.

Siga uma lista de verificação pós-migração

Após a migração, uma equipe de atualização técnica da NetApp garante que as seguintes etapas sejam concluídas para estabelecer a proteção e se preparar para a ressincronização.

1. Registre novos UUIDs de instância de volume de todos os volumes migrados no cluster ONTAP de destino.
2. Confirme se todas as políticas necessárias do SnapMirror que estavam disponíveis no antigo cluster ONTAP estão configuradas corretamente no novo cluster ONTAP .
3. Adicione o novo cluster ONTAP como um sistema na página **Sistemas** do Console.

> O UUID da instância do volume deve ser usado, não o ID do volume. O UUID da instância do volume é um identificador exclusivo que permanece consistente em todas as migrações, enquanto o ID do volume pode mudar após a migração.

Execute uma ressincronização do SnapMirror para a nuvem

Após a migração, uma equipe do NetApp Tech Refresh executa uma operação de ressincronização do SnapMirror para a nuvem para retomar os backups na nuvem dos volumes recém-migrados.

1. Adicione o novo cluster ONTAP como um sistema na página **Sistemas** do Console.
2. Consulte a página Volumes de backup e recuperação do NetApp para garantir que os detalhes do sistema de origem antigo estejam disponíveis.
3. Na página Volumes de backup e recuperação da NetApp , selecione **Configurações de backup**.
   - Na página Configurações de backup, selecione **Exibir tudo**.
   - No menu Ações… à direita da *nova* fonte, selecione **Ressincronizar backup**.
4. Na página do sistema Resync, faça o seguinte:
   a. **Novo sistema de origem**: Entre no novo cluster ONTAP para onde os volumes foram migrados.
   b. **Armazenamento de objetos de destino existente**: selecione o armazenamento de objetos de destino que contém os backups do sistema de origem antigo.
5. Selecione **Baixar modelo CSV** para baixar a planilha Excel Detalhes da ressincronização. Use esta planilha para inserir os detalhes dos volumes a serem migrados. No arquivo CSV, insira os seguintes detalhes:
   - O UUID da instância do volume antigo do cluster de origem
   - O novo UUID da instância de volume do cluster de destino
   - A política do SnapMirror a ser aplicada ao novo relacionamento.
6. Selecione **Upload** em **Upload Volume Mapping Details** para carregar a planilha CSV concluída na interface de usuário do NetApp Backup and Recovery.

   O UUID da instância do volume deve ser usado, não o ID do volume. O UUID da instância do volume é um identificador exclusivo que permanece consistente em todas as migrações, enquanto o ID do volume pode mudar após a migração.

7. Insira as informações de configuração do provedor e da rede necessárias para a operação de ressincronização.
8. Selecione **Enviar** para iniciar o processo de validação.

   O NetApp Backup and Recovery valida se cada volume selecionado para ressincronização é o snapshot mais recente e tem pelo menos um snapshot comum. Isso garante que os volumes estejam prontos para a operação de ressincronização do SnapMirror para a Nuvem.

9. Revise os resultados da validação, incluindo os novos nomes dos volumes de origem e o status de ressincronização de cada volume.
10. Verifique a elegibilidade do volume. O sistema verifica se os volumes são elegíveis para ressincronização. Se um volume não for elegível, significa que não é o snapshot mais recente ou que nenhum snapshot comum foi encontrado.

    Para garantir que os volumes permaneçam qualificados para a operação SnapMirror to Cloud Resync, faça um snapshot final de cada volume antes de excluir qualquer relacionamento do SnapMirror durante a fase de pré-migração. Isso preserva o estado mais recente dos dados.

11. Selecione **Ressincronizar** para iniciar a operação de ressincronização. O sistema usa o snapshot mais recente e comum para transferir apenas as alterações incrementais, garantindo a continuidade do backup.
12. Monitore o processo de ressincronização na página Monitor de tarefas.

Restaurar dados de configuração do NetApp Backup and Recovery em um site escuro

Ao usar o NetApp Backup and Recovery em um site sem acesso à Internet, conhecido como *modo privado*, os dados de configuração do NetApp Backup and Recovery são copiados para o bucket StorageGRID ou ONTAP S3 onde seus backups estão sendo armazenados. Se você tiver um problema com o sistema host do agente do Console, poderá implantar um novo agente do Console e restaurar os dados críticos do NetApp Backup and Recovery.

Este procedimento se aplica somente aos dados de volume ONTAP .

Quando você usa o NetApp Backup and Recovery em um ambiente SaaS onde o agente do Console é implantado no seu provedor de nuvem ou no seu próprio sistema host que tem acesso à Internet, todos os dados importantes de configuração do NetApp Backup and Recovery são armazenados em backup e protegidos na nuvem. Se você tiver um problema com o agente do Console, basta criar um novo agente do Console e adicionar seus sistemas e os detalhes do backup serão restaurados automaticamente.

Existem dois tipos de dados que são copiados:

- Banco de dados de backup e recuperação da NetApp - contém uma listagem de todos os volumes, arquivos de backup, políticas de backup e informações de configuração.
- Arquivos de catálogo indexados - contêm índices detalhados usados para a funcionalidade de pesquisa e restauração, tornando suas pesquisas muito rápidas e eficientes ao procurar dados de volume que você deseja restaurar.

É feito backup desses dados uma vez por dia à meia-noite, e no máximo 7 cópias de cada arquivo são retidas. Se o agente do Console estiver gerenciando vários sistemas ONTAP locais, os arquivos de backup e recuperação do NetApp estarão localizados no bucket do sistema que foi ativado primeiro.

Nenhum dado de volume é incluído no banco de dados do NetApp Backup and Recovery ou nos arquivos do Catálogo Indexado.

Restaurar dados de backup e recuperação do NetApp para um novo agente do Console

Se o seu agente do Console local tiver uma falha catastrófica, você precisará instalar um novo agente do Console e restaurar os dados do NetApp Backup and Recovery para o novo agente do Console.

Você precisará executar as seguintes tarefas para retornar seu sistema NetApp Backup and Recovery a um estado de funcionamento:

- Instalar um novo agente do Console
- Restaurar o banco de dados de backup e recuperação do NetApp
- Restaurar os arquivos do catálogo indexado
- Redescubra todos os seus sistemas ONTAP locais e sistemas StorageGRID na interface de usuário do NetApp Console

Depois de verificar se seu sistema está funcionando novamente, recomendamos que você crie novos arquivos de backup.

O que você vai precisar

Você precisará acessar os backups de banco de dados e índice mais recentes do bucket StorageGRID ou ONTAP S3 onde seus arquivos de backup estão sendo armazenados:

- Arquivo de banco de dados MySQL do NetApp Backup and Recovery

  Este arquivo está localizado no seguinte local no bucket `netapp-backup-<GUID>/mysql_backup/` , e é chamado `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Arquivo zip de backup do catálogo indexado

  Este arquivo está localizado no seguinte local no bucket `netapp-backup-<GUID>/catalog_backup/` , e é chamado `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Instalar um novo agente de console em um novo host Linux local

Ao instalar um novo agente do Console, certifique-se de baixar a mesma versão do software que você instalou no agente do Console original. Alterações periódicas na estrutura do banco de dados do NetApp Backup and Recovery podem tornar as versões mais recentes do software incompatíveis com os backups originais do banco de dados. Você pode "atualize o software do agente do Console para a versão mais atual após restaurar o banco de dados de backup" .

1. "Instale o agente do Console em um novo host Linux local"
2. Efetue login no Console usando as credenciais de usuário administrador que você acabou de criar.

Restaurar o banco de dados de backup e recuperação do NetApp

1. Copie o backup do MySQL do local de backup para o novo host do agente do Console. Usaremos o nome de arquivo de exemplo "CBS_DB_Backup_23_05_2023.sql" abaixo.
2. Copie o backup para o contêiner Docker do MySQL usando um dos seguintes comandos, dependendo se você estiver usando um contêiner 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. Entre no shell do contêiner MySQL usando um dos seguintes comandos, dependendo se você estiver usando um contêiner Docker ou Podman:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. No shell do contêiner, implante o "env".
5. Você precisará da senha do banco de dados MySQL, então copie o valor da chave "MYSQL_ROOT_PASSWORD".
6. Restaure o banco de dados MySQL do NetApp Backup and Recovery usando o seguinte comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verifique se o NetApp Backup and Recovery MySQL DB foi restaurado corretamente usando os seguintes comandos SQL:

```
mysql -u root -p cloud_backup
```

Digite a senha.

```
mysql> show tables;
mysql> select * from volume;
```

Verifique se os volumes exibidos são os mesmos que existiam no seu ambiente original.

Restaurar os arquivos do 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 agente do Console 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 garantir que a pasta "catalogdb1" foi criada com as subpastas "changes" e "snapshots" abaixo.

Descubra seus clusters ONTAP e sistemas StorageGRID

1. "Descubra todos os sistemas ONTAP on-prem"que estavam disponíveis no seu ambiente anterior. Isso inclui o sistema ONTAP que você usou como servidor S3.
2. "Descubra seus sistemas StorageGRID" .

Configurar os detalhes do ambiente StorageGRID

Adicione os detalhes do sistema StorageGRID associado aos seus sistemas ONTAP conforme eles foram configurados na configuração original do agente do Console usando o "APIs do console NetApp" .

As informações a seguir se aplicam a instalações em modo privado a partir do NetApp Console 3.9.xx. Para versões mais antigas, use o seguinte procedimento: "DarkSite Cloud Backup: backup e restauração de

MySQL e catálogo indexado" .

Você precisará executar essas etapas para cada sistema 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 '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":"pa
ssword"}
> '
```

   Embora o endereço IP, o nome de usuário e as senhas sejam valores personalizados, o nome da conta não é. O nome da conta é sempre "account-DARKSITE1". Além disso, o nome de usuário deve usar um nome no formato de e-mail.

   Esta API retornará uma resposta como a seguinte. Você pode recuperar o token de autorização conforme 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 sistema e o X-Agent-Id usando a API tenancy/external/resource.

```
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 em "resourceIdentifier" denota o *WorkingEnvironment Id* e o valor em "agentId" denota *x-agent-id*.

3. Atualize o banco de dados do NetApp Backup and Recovery com os detalhes do sistema StorageGRID associado aos sistemas. 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 NetApp

1. Selecione cada sistema ONTAP e clique em **Exibir backups** ao lado do serviço de backup e recuperação no painel direito.

   Você poderá ver todos os backups que foram criados para seus volumes.

2. No Painel de restauração, na seção Pesquisar e restaurar, clique em **Configurações de indexação**.

   Certifique-se de que os sistemas que tinham a Catalogação Indexada habilitada anteriormente permaneçam habilitados.

3. Na página Pesquisar e restaurar, execute algumas pesquisas de catálogo para confirmar se a restauração do catálogo indexado foi concluída com sucesso.

Gerencie backups para seus sistemas ONTAP com o NetApp Backup and Recovery

Com o NetApp Backup and Recovery, gerencie backups para seus sistemas Cloud Volumes ONTAP e ONTAP locais alterando o agendamento de backup, habilitando/desabilitando backups de volume, pausando backups, excluindo backups, forçando a exclusão de backups e muito mais. Isso inclui todos os tipos de backups, incluindo cópias de instantâneos, volumes replicados e arquivos de backup em armazenamento de objetos. Você também pode cancelar o registro do NetApp Backup and Recovery.

> Não gerencie ou altere arquivos de backup diretamente em seus sistemas de armazenamento ou no ambiente do seu provedor de nuvem. Isso pode corromper os arquivos e resultar em uma configuração não suportada.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Visualize o status de backup dos volumes em seus sistemas

Você pode visualizar uma lista de todos os volumes que estão sendo copiados no momento no Painel de Backup de Volumes. Isso inclui todos os tipos de backups, incluindo cópias de instantâneos, volumes replicados e arquivos de backup em armazenamento de objetos. Você também pode visualizar os volumes nesses sistemas que não estão sendo copiados no momento.

Passos

1. No menu Console, selecione **Proteção > Backup e recuperação**.
2. Selecione o menu **Volumes** para visualizar a lista de volumes de backup para seus sistemas Cloud Volumes ONTAP e ONTAP locais.
3. Se estiver procurando por volumes específicos em determinados sistemas, você pode refinar a lista por sistema e volume. Você também pode usar o filtro de pesquisa ou classificar as colunas com base no estilo do volume (FlexVol ou FlexGroup), tipo de volume e muito mais.

   Para mostrar colunas adicionais (agregados, estilo de segurança (Windows ou UNIX), política de snapshot, política de replicação e política de backup), selecione o sinal de mais.

4. Revise o status das opções de proteção na coluna "Proteção existente". Os 3 ícones representam "Cópias de instantâneos locais", "Volumes replicados" e "Backups no armazenamento de objetos".

   Cada ícone fica azul quando o tipo de backup está 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.

Ativar backup em volumes adicionais em um sistema

Se você ativou o backup apenas em alguns volumes de um sistema quando habilitou o NetApp Backup and Recovery pela primeira vez, poderá ativar backups em volumes adicionais posteriormente.

Passos

1. Na aba **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 de instantâneos locais, volumes replicados e arquivos de backup. Veja os detalhes das opções de backup dos volumes iniciais que você ativou neste sistema. Em seguida, selecione **Avançar**.
3. Revise as configurações de backup para este volume e selecione **Ativar backup**.

Alterar as configurações de backup atribuídas aos volumes existentes

Você pode alterar as políticas de backup atribuídas aos seus volumes existentes que têm políticas atribuídas. Você pode alterar as políticas para suas cópias de instantâneos locais, volumes replicados e arquivos de backup. Qualquer nova política de snapshot, replicação ou backup que você deseja aplicar aos volumes já deve existir.

Editar configurações de backup em um único volume

Passos

1. Na aba **Volumes**, identifique o volume no qual 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 de instantâneos locais, volumes replicados e arquivos de backup e selecione **Avançar**.

   Se você habilitou *DataLock e Ransomware Resilience* para backups em nuvem na política de backup inicial ao ativar o NetApp Backup and Recovery para este cluster, você verá apenas outras políticas que foram configuradas com DataLock. E se você não habilitou o *DataLock e a Resiliência contra Ransomware* ao ativar o NetApp Backup and Recovery, você verá apenas outras políticas de backup em nuvem que não têm o DataLock configurado.

3. Revise as configurações de backup para este volume e selecione **Ativar backup**.

Editar configurações de backup em vários volumes

Se quiser usar as mesmas configurações de backup em vários volumes, você pode ativar ou editar as configurações de backup em vários volumes ao mesmo tempo. Você pode selecionar volumes que não têm configurações de backup, apenas configurações de instantâneo, apenas configurações de backup em nuvem e assim por diante, 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 características comuns:

- mesmo sistema
- mesmo estilo (volume FlexVol ou FlexGroup)
- mesmo tipo (volume de leitura e gravação ou proteção de dados)

Quando mais de cinco volumes são habilitados para backup, o NetApp Backup and Recovery inicializa apenas cinco volumes por vez. Quando eles são concluídos, ele cria o próximo lote de cinco subtarefas para iniciar o próximo conjunto e continua até que todos os volumes sejam inicializados.

Passos

1. Na guia **Volumes**, filtre pelo sistema no qual os volumes residem.
2. Selecione todos os volumes nos quais você 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 backup…	Selecione este botão…
Gerenciar configurações de backup de instantâneo	**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. Esta opção também permite que você altere a arquitetura de backup.	**Gerenciar backup e recuperação**

4. Na página de backup exibida, faça alterações nas políticas de backup existentes para cópias de instantâneos locais, volumes replicados ou arquivos de backup e selecione **Salvar**.

   Se você habilitou *DataLock e Ransomware Resilience* para backups em nuvem na política de backup inicial ao ativar o NetApp Backup and Recovery para este cluster, você verá apenas outras políticas que foram configuradas com DataLock. E se você não habilitou o *DataLock e a Resiliência contra Ransomware* ao ativar o NetApp Backup and Recovery, você verá apenas outras políticas de backup em nuvem que não têm o DataLock configurado.

Crie um backup de volume manual 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 foram feitas em um volume e você não quiser esperar pelo próximo backup agendado para proteger esses dados. Você também pode usar essa funcionalidade para criar um backup para um volume que não está sendo feito backup no momento e você deseja capturar seu estado atual.

Você pode criar uma cópia instantânea ad-hoc ou backup para um objeto de um volume. Não é possível criar um volume replicado ad hoc.

O nome do backup inclui o registro de data e hora para que você possa identificar seu backup sob demanda de outros backups agendados.

Se você habilitou *DataLock e Ransomware Resilience* ao ativar o NetApp Backup and Recovery para este cluster, o backup sob demanda também será configurado com DataLock e o período de retenção será de 30 dias. As verificações de ransomware não são suportadas para backups ad-hoc. "Saiba mais sobre a proteção DataLock e Ransomware" .

Quando você cria um backup ad-hoc, um instantâneo é criado no volume de origem. Como esse snapshot não faz parte de uma programação normal de snapshot, ele não será desativado. Talvez você queira excluir manualmente este instantâneo do volume de origem quando o backup estiver concluído. Isso permitirá que os blocos relacionados a este instantâneo sejam liberados. O nome do Snapshot começará com `cbs-snapshot-adhoc-` . "Veja como excluir um Snapshot usando o ONTAP CLI" .

O backup de volume sob demanda não é suportado em volumes de proteção de dados.

Passos

1. Na aba **Volumes**, selecione••• para o volume e selecione **Backup** > **Criar backup ad-hoc**.

A coluna Status do backup desse volume exibe "Em andamento" até que o backup seja criado.

Veja a lista de backups para cada volume

Você pode visualizar a lista de todos os arquivos de backup existentes para cada volume. Esta página exibe detalhes sobre o volume de origem, o local de destino e detalhes do backup, como o último backup feito, a política de backup atual, o tamanho do arquivo de backup e muito mais.

Passos

1. Na aba **Volumes**, selecione••• para o volume de origem e selecione **Exibir detalhes do volume**.

   Os detalhes do volume e a lista de cópias de instantâneos são exibidos.

2. Selecione **Instantâneo**, **Replicação** ou **Backup** para ver a lista de todos os arquivos de backup para cada tipo de backup.

Execute uma verificação de ransomware em um backup de volume no armazenamento de objetos

O NetApp Backup and Recovery verifica seus arquivos de backup em busca de evidências de um ataque de ransomware quando um backup em um arquivo de objeto é criado e quando os dados de um arquivo de backup estão sendo restaurados. Você também pode executar uma verificação sob demanda a qualquer momento para verificar a usabilidade de um arquivo de backup específico no armazenamento de objetos. Isso pode ser útil se você teve um problema de ransomware em um volume específico e deseja verificar se os backups desse volume não foram afetados.

Este recurso estará disponível somente se o backup de volume tiver sido criado em um sistema com ONTAP 9.11.1 ou superior e se você tiver habilitado *DataLock e Ransomware Resilience* na política de backup para objeto.

Passos

1. Na aba **Volumes**, selecione••• para o volume de origem e selecione **Exibir detalhes do volume**.

   Os detalhes do volume são exibidos.

2. Selecione **Backup** para ver a lista de arquivos de backup no armazenamento de objetos.
3. Selecione••• para o arquivo de backup de volume que você deseja verificar em busca de ransomware e clique em **Verificar em busca de ransomware**.

   A coluna Resiliência do Ransomware mostra que a verificação está Em andamento.

Gerenciar o relacionamento de replicação com o volume de origem

Depois de configurar a replicação de dados entre dois sistemas, você pode gerenciar o relacionamento de replicação de dados.

Passos

1. Na aba **Volumes**, selecione ••• para o volume de origem e selecione a opção **Replicação**. Você pode ver todas as opções disponíveis.
2. Selecione a ação de replicação que você deseja executar.

   A tabela a seguir descreve as ações disponíveis:

Ação	Descrição
Exibir replicação	Mostra detalhes sobre o relacionamento de volume: informações de transferência, informações da última transferência, detalhes sobre o volume e informações sobre a política de proteção atribuída ao relacionamento.
Atualizar replicação	Inicia uma transferência incremental para atualizar o volume de destino a ser sincronizado com o volume de origem.
Pausar replicação	Pause a transferência incremental de cópias do Snapshot para atualizar o volume de destino. Você pode Retomar mais tarde se quiser reiniciar as atualizações incrementais.
Interromper a replicação	Quebra o relacionamento entre os volumes de origem e destino e ativa o volume de destino para acesso a dados, tornando-o leitura e gravação. Esta opção normalmente é usada quando o volume de origem não pode fornecer dados devido a eventos como corrupção de dados, exclusão acidental ou estado offline.https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["Aprenda 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 desabilita a capacidade de restaurar um volume. Nenhum backup existente será excluído. Isso não exclui o relacionamento 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 o momento em que o volume de origem foi desabilitado não são preservados.
Excluir relacionamento	Exclui o relacionamento 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 a dados, o que significa que não o torna leitura e gravação. Esta ação também exclui o relacionamento de pares do cluster e o relacionamento de pares da VM de armazenamento (SVM), se não houver outros relacionamentos de proteção de dados entre os sistemas.

Resultado

Depois de selecionar uma ação, o Console atualiza o relacionamento.

Editar uma política de backup para nuvem existente

Você pode alterar os atributos de uma política de backup que está sendo aplicada atualmente aos volumes em um sistema. Alterar a política de backup afeta todos os volumes existentes que estão usando a política.

- Se você habilitou *DataLock e Resiliência contra Ransomware* na política inicial ao ativar o NetApp Backup and Recovery para este cluster, todas as políticas que você editar deverão ser configuradas com a mesma configuração de DataLock (Governança ou Conformidade). E se você não habilitou o *DataLock e o Ransomware Resilience* ao ativar o NetApp Backup and Recovery, não será possível habilitar 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 NetApp Backup and Recovery, essa camada será a única camada de arquivamento disponível ao editar políticas de backup. E se você não selecionou nenhuma camada de arquivamento em sua primeira política de backup, o *S3 Glacier* será sua única opção de arquivamento ao editar uma política.

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, selecione••• para o sistema no qual você deseja alterar as configurações de política e selecione **Gerenciar políticas**.
3. Na página *Gerenciar políticas*, selecione **Editar** para a política de backup que você deseja alterar nesse sistema.
4. Na página *Editar política*, selecione a seta para baixo para expandir a seção *Rótulos e retenção* para alterar o agendamento e/ou a retenção de backup e selecione **Salvar**.

   Se o seu cluster estiver executando o ONTAP 9.10.1 ou superior, você também terá a opção de habilitar ou desabilitar o armazenamento em camadas de backups para arquivamento após um determinado número de dias.

"Saiba mais sobre o uso do armazenamento de arquivamento da AWS" .

"Saiba mais sobre como usar o armazenamento de arquivamento do Azure" .

"Saiba mais sobre como usar o armazenamento de arquivo do Google" . (Requer ONTAP 9.12.1.)

+ Observe que todos os arquivos de backup que foram hierarquizados para armazenamento de arquivamento serão deixados nessa camada se você parar de hierarquizar backups para arquivamento - eles não serão movidos automaticamente de volta para a camada padrão. Somente novos backups de volume residirão na camada padrão.

Adicionar uma nova política de backup para a nuvem

Quando você habilita o NetApp Backup and Recovery para um sistema, todos os volumes selecionados inicialmente são copiados usando a política de backup padrão que você definiu. Se você quiser atribuir políticas de backup diferentes a determinados volumes que têm objetivos de ponto de recuperação (RPO) diferentes, você pode criar políticas adicionais para esse cluster e atribuí-las a outros volumes.

Se você quiser aplicar uma nova política de backup a determinados volumes em um sistema, primeiro precisará adicionar a política de backup ao sistema. Então você podeaplicar a política aos volumes desse sistema .

- Se você habilitou *DataLock e Resiliência contra Ransomware* na política inicial ao ativar o NetApp Backup and Recovery para este cluster, quaisquer políticas adicionais que você criar deverão ser configuradas com a mesma configuração de DataLock (Governança ou Conformidade). E se você não habilitou o *DataLock e o Ransomware Resilience* ao ativar o NetApp Backup and Recovery, não poderá 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 NetApp Backup and Recovery, essa camada será a única camada de arquivamento disponível para futuras políticas de backup para esse cluster. E se você não selecionou nenhuma camada de arquivamento em sua primeira política de backup, o *S3 Glacier* será sua única opção de arquivamento para políticas futuras.

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, selecione ••• para o sistema onde você deseja adicionar a nova política e selecione **Gerenciar políticas**.
3. Na página *Gerenciar políticas*, selecione **Adicionar nova política**.
4. Na página *Adicionar nova política*, selecione a seta para baixo para expandir a seção *Rótulos e retenção* para definir o agendamento e a retenção de backup e selecione **Salvar**.

   Se o seu cluster estiver executando o ONTAP 9.10.1 ou superior, você também terá a opção de habilitar ou desabilitar o armazenamento em camadas de backups para arquivamento após um determinado número de dias.

"Saiba mais sobre o uso do armazenamento de arquivamento da AWS" .

"Saiba mais sobre como usar o armazenamento de arquivamento do Azure" .

"Saiba mais sobre como usar o armazenamento de arquivo do Google" . (Requer ONTAP 9.12.1.)

Excluir backups

O NetApp Backup and Recovery permite que você exclua um único arquivo de backup, exclua todos os backups de um volume ou exclua todos os backups de todos os volumes em um sistema. Talvez você queira excluir todos os backups se não precisar mais deles ou se tiver excluído o volume de origem e quiser remover todos os backups.

Você não pode excluir arquivos de backup que você bloqueou usando a proteção DataLock e Ransomware. A opção "Excluir" não estará disponível na interface do usuário se você selecionar um ou mais arquivos de backup bloqueados.

Se você planeja excluir um sistema ou cluster que tenha backups, você deve excluir os backups **antes** de excluir o sistema. O NetApp Backup and Recovery não exclui backups automaticamente quando você exclui um sistema e não há suporte atual na interface do usuário para excluir os backups após o sistema ter sido excluído. Você continuará sendo cobrado pelos custos de armazenamento de objetos para quaisquer backups restantes.

Excluir todos os arquivos de backup de um sistema

A exclusão de todos os backups no armazenamento de objetos de um sistema não desabilita backups futuros de volumes neste sistema. Se você quiser parar de criar backups de todos os volumes em um sistema, você

pode desativar os backupsconforme descrito aqui .

Observe que esta ação não afeta cópias de Snapshot ou volumes replicados - esses tipos de arquivos de backup não são excluídos.

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Selecione••• para o sistema onde você deseja excluir todos os backups e selecione **Excluir todos os backups**.
3. Na caixa de diálogo de confirmação, insira o nome do sistema.
4. Selecione **Configurações avançadas**.
5. **Forçar exclusão de backups**: indique se você deseja ou não forçar a exclusão de todos os backups.

   Em alguns casos extremos, você pode querer que o NetApp Backup and Recovery não tenha mais acesso aos backups. Isso pode acontecer, por exemplo, se o serviço não tiver mais acesso ao bucket de backup ou se os backups forem protegidos pelo DataLock, mas você não os quiser mais. Anteriormente, não era possível excluí-los sozinho e era necessário ligar para o Suporte da NetApp . Com esta versão, você pode usar a opção para forçar a exclusão de backups (em níveis de volume e ambiente de trabalho).

   Use esta opção com cuidado e somente em casos de extrema necessidade de limpeza. O NetApp Backup and Recovery não terá mais acesso a esses backups, mesmo que eles não sejam excluídos do armazenamento de objetos. Você precisará ir ao seu provedor de nuvem e excluir manualmente os backups.

6. Selecione **Excluir**.

Excluir todos os arquivos de backup de um volume

Excluir todos os backups de um volume também desabilita backups futuros para esse volume.

Passos

1. Na aba **Volumes**, clique em••• para o volume de origem e selecione **Detalhes e lista de backup**.

   A lista de todos os arquivos de backup é exibida.

2. Selecione **Ações** > **Excluir todos os backups**.
3. Digite o nome do volume.
4. Selecione **Configurações avançadas**.
5. **Forçar exclusão de backups**: indique se você deseja ou não forçar a exclusão de todos os backups.

   Em alguns casos extremos, você pode querer que o NetApp Backup and Recovery não tenha mais acesso aos backups. Isso pode acontecer, por exemplo, se o serviço não tiver mais acesso ao bucket de backup ou se os backups estiverem protegidos pelo DataLock, mas você não os quiser mais. Anteriormente, não era possível excluí-los sozinho e era necessário ligar para o Suporte da NetApp . Com esta versão, você pode usar a opção para forçar a exclusão de backups (em níveis de volume e ambiente de trabalho).

   Use esta opção com cuidado e somente em casos de extrema necessidade de limpeza. O NetApp Backup and Recovery não terá mais acesso a esses backups, mesmo que eles não sejam excluídos do armazenamento de objetos. Você precisará ir ao seu provedor de nuvem e excluir manualmente os backups.

6. Selecione **Excluir**.

Excluir um único arquivo de backup de 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 de instantâneo de volume ou de um backup no armazenamento de objetos.

Não é possível excluir volumes replicados (volumes de proteção de dados).

Passos

1. Na aba **Volumes**, selecione••• para o volume de origem e selecione **Exibir detalhes do volume**.

   Os detalhes do volume são exibidos e você pode selecionar **Instantâneo**, **Replicação** ou **Backup** para ver a lista de todos os arquivos de backup do volume. Por padrão, as cópias de instantâneos disponíveis são exibidas.

2. Selecione **Instantâneo** ou **Backup** para ver o tipo de arquivo de backup que você deseja excluir.
3. Selecione••• para o arquivo de backup de volume que você deseja excluir e selecione **Excluir**.
4. Na caixa de diálogo de confirmação, selecione **Excluir**.

Excluir relacionamentos de backup de volume

Excluir o 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 lhe dá a capacidade de restaurar o volume do arquivo de backup no futuro, se necessário, enquanto libera espaço do seu sistema de armazenamento de origem.

Você não precisa necessariamente excluir o volume de origem. Você pode excluir o relacionamento de backup de um volume e manter o volume de origem. Nesse caso, você pode "Ativar" o backup no volume posteriormente. A cópia de backup de base original continua a ser usada neste caso - uma nova cópia de backup 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.

Este recurso estará disponível somente se o seu sistema estiver executando o ONTAP 9.12.1 ou superior.

Não é possível excluir o volume de origem da interface do usuário do NetApp Backup and Recovery. No entanto, você pode abrir a página Detalhes do Volume na página **Sistemas** do Console e "apague o volume de lá" .

> Não é possível excluir arquivos de backup de volume individuais depois que o relacionamento tiver sido excluído. No entanto, você pode excluir todos os backups do volume.

Passos

1. Na aba **Volumes**, selecione••• para o volume de origem e selecione **Backup** > **Excluir relacionamento**.

Desativar o NetApp Backup and Recovery para um sistema

Desativar o NetApp Backup and Recovery para um sistema desabilita os backups de cada volume no sistema e também desabilita a capacidade de restaurar um volume. Nenhum backup existente será excluído. Isso não cancela o registro do serviço de backup deste sistema; 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 armazenamento de

objetos referentes à capacidade que seus backups usam, a menos que vocêexcluir os backups .

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, selecione••• para o sistema onde você deseja desabilitar backups e selecione **Desativar Backup**.
3. Na caixa de diálogo de confirmação, selecione **Desativar**.

> Um botão **Ativar backup** aparece para esse sistema enquanto o backup está desativado. Você pode selecionar este botão quando quiser reativar a funcionalidade de backup para esse sistema.

Cancelar o registro do NetApp Backup and Recovery para um sistema

Você pode cancelar o registro do NetApp Backup and Recovery para um sistema se não quiser mais usar a funcionalidade de backup e quiser parar de ser cobrado por backups nesse sistema. Normalmente, esse recurso é usado quando você planeja excluir um sistema e deseja cancelar o serviço de backup.

Você também pode usar esse recurso se quiser alterar o armazenamento de objetos de destino onde seus backups de cluster estão sendo armazenados. Depois de cancelar o registro do NetApp Backup and Recovery para o sistema, você poderá habilitar o NetApp Backup and Recovery para esse cluster usando as novas informações do provedor de nuvem.

Antes de cancelar o registro do NetApp Backup and Recovery, você deve executar as seguintes etapas, nesta ordem:

- Desativar o NetApp Backup and Recovery para o sistema
- Excluir todos os backups desse sistema

A opção de cancelar o registro não estará disponível até que essas duas ações sejam concluídas.

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, selecione••• para o sistema em que você deseja cancelar o registro do serviço de backup e selecione **Cancelar registro**.
3. Na caixa de diálogo de confirmação, selecione **Cancelar registro**.

Restaure dados ONTAP de arquivos de backup com o NetApp Backup and Recovery

Os backups dos dados do seu volume ONTAP estão disponíveis nos locais onde você os criou: cópias de instantâneo, volumes replicados e backups armazenados no armazenamento de objetos. Você pode restaurar dados de um ponto específico no tempo a partir de qualquer um desses locais de backup. Com o NetApp Backup and Recovery, restaure um volume ONTAP inteiro a partir de um arquivo de backup ou, se precisar restaurar apenas alguns arquivos, restaure uma pasta ou arquivos individuais.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

- Você pode restaurar um **volume** (como um novo volume) para o sistema original, para um sistema diferente que esteja usando a mesma conta de nuvem ou para um sistema ONTAP local.
- Você pode restaurar uma **pasta** para um volume no sistema original, para um volume em um sistema diferente que esteja usando a mesma conta de nuvem ou para um volume em um sistema ONTAP local.
- Você pode restaurar **arquivos** para um volume no sistema original, para um volume em um sistema diferente que esteja usando a mesma conta de nuvem ou para um volume em um sistema ONTAP local.

Uma licença válida do NetApp Backup and Recovery é necessária para restaurar dados de arquivos de backup para um sistema de produção.

Para resumir, estes são os fluxos válidos que você pode usar para restaurar dados de volume em um sistema ONTAP :

- Arquivo de backup → volume restaurado
- Volume replicado → volume restaurado
- Cópia instantânea → volume restaurado

Se a operação de restauração não for concluída, não tente o processo de restauração novamente até que o Job Monitor mostre que a operação de restauração falhou. Se você tentar o processo de restauração novamente antes que o Job Monitor mostre que a operação de restauração falhou, a operação de restauração falhará novamente. Quando o status do Job Monitor for "Falha", você poderá tentar o processo de restauração novamente.

Para limitações relacionadas à restauração de dados ONTAP , consulte"Limitações de backup e restauração para volumes ONTAP" .

O Painel de Restauração

Use o Painel de Restauração para executar operações de restauração de volumes, pastas e arquivos. Você acessa o Painel de Restauração clicando em **Backup e recuperação** no menu Console e, em seguida, clicando na guia **Restaurar**. Você também pode clicar > **Visualizar Painel de Restauração** no serviço de Backup e recuperação no painel Serviços.

O NetApp Backup and Recovery já deve estar ativado para pelo menos um sistema e os arquivos de backup iniciais devem existir.

O Painel de Restauração oferece duas maneiras diferentes de restaurar dados de arquivos de backup: **Navegar e Restaurar** e **Pesquisar e Restaurar**.

Comparando Navegar e Restaurar e Pesquisar e Restaurar

Em termos gerais, *Navegar e Restaurar* normalmente é melhor quando você precisa restaurar um volume, pasta ou arquivo específico da última semana ou mês — e você sabe o nome e o local do arquivo, além da data em que ele esteve em boas condições pela última vez. *Pesquisar e Restaurar* normalmente é melhor quando você precisa restaurar um volume, pasta ou arquivo, mas não se lembra do nome exato, do volume em que ele reside ou da data em que esteve em boas condições pela última vez.

Esta tabela fornece uma comparação de recursos dos dois métodos.

Navegar e restaurar	Pesquisar e restaurar
Navegue por uma estrutura de estilo de pasta para encontrar o volume, a pasta ou o arquivo dentro de um único arquivo de backup.	Pesquise um volume, pasta ou arquivo em **todos os arquivos de backup** por nome parcial ou completo do volume, nome parcial ou completo da pasta/arquivo, intervalo de tamanho e filtros de pesquisa adicionais.
Não realiza a recuperação de arquivos se o arquivo foi excluído ou renomeado e o usuário não sabe o nome original do arquivo	Manipula diretórios recém-criados/excluídos/renomeados e arquivos recém-criados/excluídos/renomeados
Não são necessários recursos adicionais do provedor de nuvem	Ao restaurar da nuvem, recursos adicionais de bucket e provedor de nuvem pública são necessários por conta.
Não são necessários custos adicionais com provedores de nuvem	Ao restaurar da nuvem, custos adicionais são necessários ao verificar seus backups e volumes em busca de 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 seus arquivos de backup residem.

Tipo de backup	Navegar e restaurar			Pesquisar e restaurar		
	Restaurar volume	**Restaurar arquivos**	**Restaurar pasta**	**Restaurar volume**	**Restaurar arquivos**	**Restaurar pasta**
Cópia instantânea	Sim	Não	Não	Sim	Sim	Sim
Volume replicado	Sim	Não	Não	Sim	Sim	Sim
Arquivo de backup	Sim	Sim	Sim	Sim	Sim	Sim

Antes de usar qualquer método de restauração, certifique-se de ter configurado seu ambiente para os requisitos de recursos exclusivos. Esses requisitos são descritos nas seções abaixo.

Veja os requisitos e as etapas de restauração para o tipo de operação de restauração que você deseja usar:

- Restaurar volumes usando Navegar e Restaurar
- Restaurar pastas e arquivos usando Navegar e Restaurar
- Restaurar volumes, pastas e arquivos usando Pesquisar e Restaurar

Restaurar dados ONTAP usando Navegar e Restaurar

Antes de começar a restaurar um volume, pasta ou arquivo, você deve saber o nome do volume do qual deseja restaurar, o nome do sistema e do SVM onde o volume reside e a data aproximada do arquivo de backup do qual deseja restaurar. Você pode restaurar dados do ONTAP de uma cópia do Snapshot, de um

volume replicado ou de backups armazenados no armazenamento de objetos.

Observação: Se o arquivo de backup contendo os dados que você deseja restaurar estiver no armazenamento em nuvem de arquivamento (a partir do ONTAP 9.10.1), a operação de restauração levará mais tempo 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 arquivo, 9.12.1 para Google Archive e StorageGRID e 9.13.1 para restauração de pasta.

"Saiba mais sobre a restauração do armazenamento de arquivo da AWS" .

"Saiba mais sobre a restauração do armazenamento de arquivamento do Azure" .

"Saiba mais sobre como restaurar do armazenamento de arquivo do Google" .

A alta prioridade não é suportada ao restaurar dados do armazenamento de arquivamento do Azure para sistemas StorageGRID .

Navegar e restaurar sistemas suportados e provedores de armazenamento de objetos

Você pode restaurar dados do ONTAP de um arquivo de backup que reside em um sistema secundário (um volume replicado) ou em um armazenamento de objetos (um arquivo de backup) para os seguintes sistemas. Cópias de instantâneos residem no sistema de origem e podem ser restauradas somente no mesmo sistema.

Observação: você pode restaurar um volume de qualquer tipo de arquivo de backup, mas pode restaurar uma pasta ou arquivos individuais somente de um arquivo de backup no armazenamento de objetos neste momento.

Do Object Store (Backup)	Da Primária (Instantâneo)	Do Sistema Secundário (Replicação)	Para o sistema de destino ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Cloud Volumes ONTAP no sistema ONTAP local da AWS endif::aws[] ifdef::azure[]	Blob do Azure
Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure endif::azure[] ifdef::gcp[]	Armazenamento em nuvem do Google	Cloud Volumes ONTAP no sistema Google On-premises ONTAP
Cloud Volumes ONTAP no sistema ONTAP local do Google endif::gcp[]	NetApp StorageGRID	Sistema ONTAP local	Sistema ONTAP local Cloud Volumes ONTAP
Para o sistema ONTAP local	ONTAP S3	Sistema ONTAP local	Sistema ONTAP local Cloud Volumes ONTAP

Para Navegar e Restaurar, o agente do Console pode ser instalado nos seguintes locais:

- Para o Amazon S3, o agente do Console pode ser implantado na AWS ou em suas instalações
- Para o Azure Blob, o agente do Console pode ser implantado no Azure ou em suas instalações
- Para o Google Cloud Storage, o agente do Console deve ser implantado na sua VPC do Google Cloud Platform
- Para StorageGRID, o agente do Console deve ser implantado em suas instalações; com ou sem acesso à

Internet

- Para o ONTAP S3, o agente do Console 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 locais" incluem sistemas FAS, AFF e ONTAP Select .

Se a versão do ONTAP no seu sistema for inferior a 9.13.1, você não poderá restaurar pastas ou arquivos se o arquivo de backup tiver sido configurado com DataLock & Ransomware. Nesse caso, você pode restaurar o volume inteiro a partir do arquivo de backup e depois acessar os arquivos necessários.

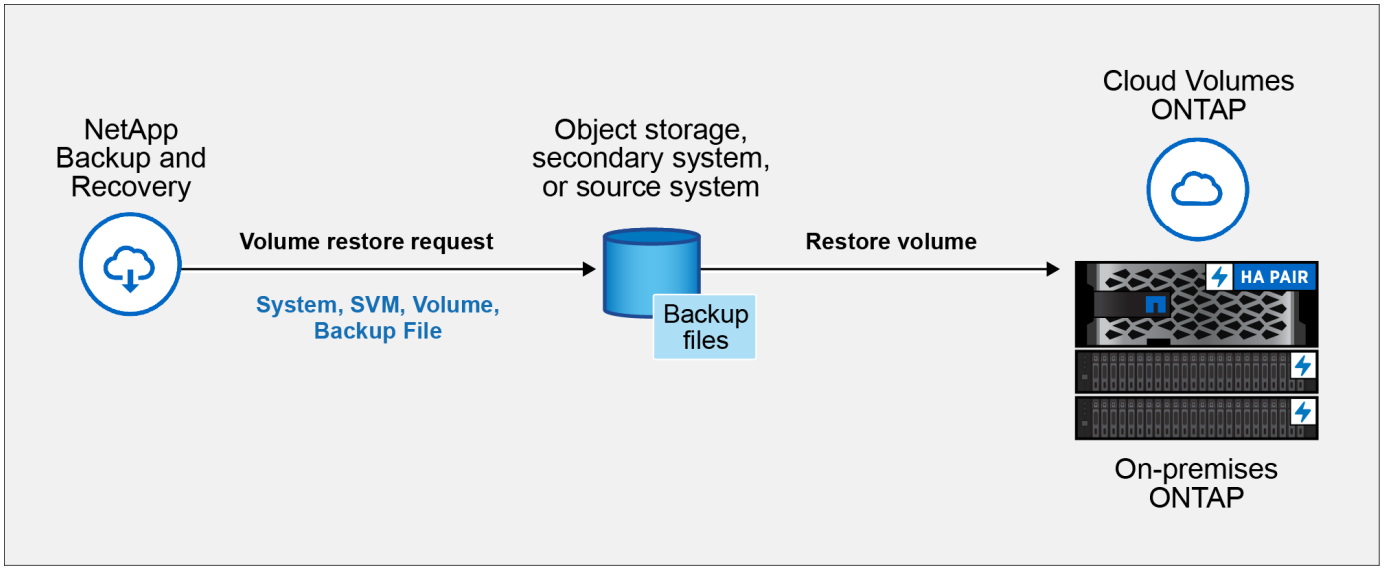
Restaurar volumes usando Navegar e Restaurar

Quando você restaura um volume de um arquivo de backup, o NetApp Backup and Recovery cria um *novo* volume usando os dados do backup. Ao usar um backup do armazenamento de objetos, você pode restaurar os dados para um volume no sistema original, para um sistema diferente localizado na mesma conta de nuvem que o sistema de origem ou para um sistema ONTAP 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 o arquivo de backup inteiro. A restauração rápida não é recomendada para aplicativos sensíveis ao desempenho ou à latência e não é compatível com backups em armazenamento arquivado.

A restauração rápida é suportada para volumes FlexGroup somente se o sistema de origem do qual o backup em nuvem foi criado estiver executando o ONTAP 9.12.1 ou superior. E ele é compatível com volumes SnapLock somente se o sistema de origem estiver executando o ONTAP 9.11.0 ou superior.

Ao restaurar de um volume replicado, você pode restaurar o volume para o sistema original ou para um sistema Cloud Volumes ONTAP ou ONTAP local.



Como você pode ver, você precisará saber o nome do sistema de origem, a VM de armazenamento, o nome do volume e a data do arquivo de backup para executar uma restauração de volume.

Passos

1. No menu Console, selecione **Proteção > Backup e recuperação**.
2. Selecione a aba **Restaurar** e o Painel de Restauração será exibido.
3. Na seção *Navegar e restaurar*, selecione **Restaurar volume**.
4. Na página *Selecionar origem*, navegue até o arquivo de backup do volume que você deseja restaurar. Selecione o **sistema**, o **Volume** e o arquivo de **Backup** que tem o registro de data/hora do qual você deseja restaurar.

   A coluna **Local** mostra se o arquivo de backup (Snapshot) é **Local** (uma cópia do 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. Selecione **Avançar**.

   Observe que se você selecionar um arquivo de backup no armazenamento de objetos e a Resiliência contra Ransomware estiver ativa para esse backup (se você habilitou o DataLock e a Resiliência contra Ransomware na política de backup), você será solicitado a executar uma verificação de ransomware adicional no arquivo de backup antes de restaurar os dados. Recomendamos que você verifique se há ransomware no arquivo de backup. (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 **sistema** onde você 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 do cluster com o armazenamento de objetos, serão solicitadas informações adicionais:
   - Ao restaurar do Amazon S3, selecione o IPspace no cluster ONTAP onde o volume de destino residirá, insira a chave de acesso e a chave secreta do usuário que você criou para dar ao cluster ONTAP acesso ao bucket S3 e, opcionalmente, escolha um endpoint VPC privado para transferência segura de dados.
     - Ao restaurar do Azure Blob, selecione o IPspace no cluster 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 segura de dados selecionando a VNet e a Sub-rede.
     - Ao restaurar do Google Cloud Storage, selecione o Google Cloud Project e a Access Key e a Secret Key para acessar o armazenamento de objetos, a região onde os backups são armazenados e o IPspace no cluster ONTAP onde o volume de destino residirá.
     - Ao restaurar do StorageGRID, insira 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 IPspace no cluster ONTAP onde o volume de destino residirá.
     - Ao restaurar do ONTAP S3, insira 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 a Chave Secreta necessárias para acessar o armazenamento de objetos e o espaço IP no cluster ONTAP onde o volume de destino residirá.
       a. Digite o nome que você 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 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 armazenamento de arquivamento (disponível a partir do ONTAP 9.10.1), você pode selecionar a Prioridade de restauração.

"Saiba mais sobre a restauração do armazenamento de arquivo da AWS" .

"Saiba mais sobre a restauração do armazenamento de arquivamento do Azure" .

"Saiba mais sobre como restaurar do armazenamento de arquivo do Google" . Os arquivos de backup no nível de armazenamento do Google Archive são restaurados quase imediatamente e não exigem Prioridade de Restauração.

1. Selecione **Avançar** para escolher se deseja fazer uma restauração normal ou um processo de restauração rápida:
   - **Restauração normal**: use a restauração normal em volumes que exigem alto desempenho. Os volumes não estarão disponíveis até que o processo de restauração seja concluído.
   - **Restauração rápida**: Os volumes e dados restaurados estarão disponíveis imediatamente. Não use isso em volumes que exigem alto desempenho porque, durante o processo de restauração rápida, o acesso aos dados pode ser mais lento que o normal.
2. Selecione **Restaurar** e você retornará ao Painel de Restauração para poder revisar o progresso da operação de restauração.

Resultado

O NetApp Backup and Recovery cria um novo volume com base no backup selecionado.

Observe que restaurar um volume de um arquivo de backup que reside no armazenamento de arquivamento pode levar muitos minutos ou horas, dependendo da camada de arquivamento e da prioridade de restauração. Você pode selecionar a aba **Monitoramento de Tarefas** para ver o progresso da restauração.

Restaurar pastas e arquivos usando Navegar e Restaurar

Se precisar restaurar apenas alguns arquivos de um backup de volume ONTAP , você pode optar por restaurar uma pasta ou arquivos individuais em vez de restaurar o volume inteiro. Você pode restaurar pastas e arquivos para um volume existente no sistema original ou para um sistema diferente que esteja usando a mesma conta de nuvem. Você também pode restaurar pastas e arquivos para um volume em um sistema ONTAP local.

No momento, você pode restaurar uma pasta ou arquivos individuais somente de um arquivo de backup no armazenamento de objetos. Atualmente, não há suporte para restauração de arquivos e pastas a partir de uma cópia de instantâneo local ou de um arquivo de backup que reside em um sistema secundário (um volume replicado).

Se você selecionar vários arquivos, todos eles serão restaurados no mesmo volume de destino escolhido. Portanto, se você quiser restaurar arquivos em volumes diferentes, precisará executar o processo de restauração várias vezes.

Ao usar o ONTAP 9.13.0 ou superior, você pode restaurar uma pasta junto com todos os arquivos e subpastas dentro dela. Ao usar uma versão do ONTAP anterior à 9.13.0, somente os arquivos dessa pasta são

restaurados - nenhuma subpasta ou arquivo em subpastas é restaurado.

- Se o arquivo de backup tiver sido configurado com proteção DataLock e Ransomware, a restauração em nível de pasta será suportada somente se a versão do ONTAP for 9.13.1 ou superior. Se estiver usando uma versão anterior do ONTAP, você poderá restaurar o volume inteiro a partir do arquivo de backup e então 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 usando uma versão anterior do ONTAP, você pode restaurar a pasta a partir de um arquivo de backup mais recente que não foi arquivado ou pode restaurar o volume inteiro a partir do backup arquivado e então acessar a pasta e os arquivos necessários.
- Com o ONTAP 9.15.1, você pode restaurar pastas do FlexGroup usando a opção "Navegar e restaurar". Este recurso está em modo de visualização de tecnologia.

  Você pode testá-lo usando um sinalizador especial descrito no "Blog de lançamento do NetApp Backup and Recovery de julho de 2024" .

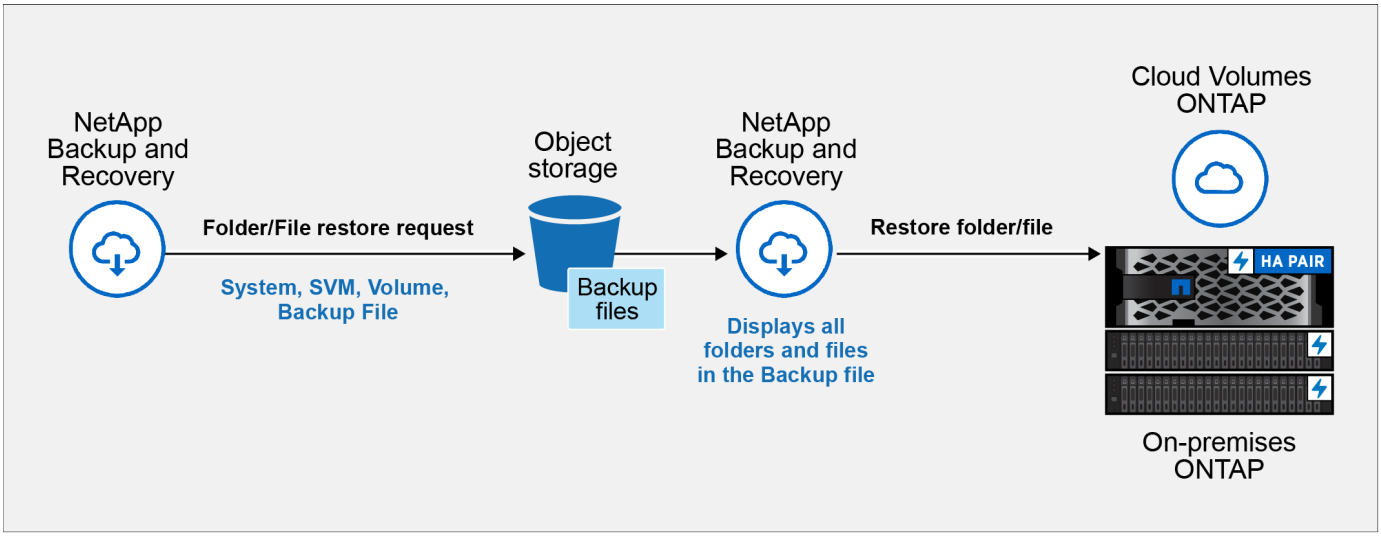
Pré-requisitos

- A versão do ONTAP deve ser 9.6 ou superior para executar operações de restauração de *arquivos*.
- A versão do ONTAP deve ser 9.11.1 ou superior para executar operações de restauração de *pasta*. A versão 9.13.1 do ONTAP é necessária se os dados estiverem em armazenamento de arquivo ou se o arquivo de backup estiver usando proteção DataLock e Ransomware.
- A versão do ONTAP deve ser 9.15.1 p2 ou superior para restaurar diretórios FlexGroup usando a opção Procurar e restaurar.

Processo de restauração de pastas e arquivos

O processo é assim:

1. Quando quiser restaurar uma pasta, ou um ou mais arquivos, de um backup de volume, clique na aba **Restaurar** e clique em **Restaurar Arquivos ou Pasta** em *Navegar e Restaurar*.
2. Selecione o sistema de origem, o volume e o arquivo de backup nos quais a pasta ou o(s) arquivo(s) residem.
3. O NetApp Backup and Recovery exibe as pastas e os arquivos existentes no arquivo de backup selecionado.
4. Selecione a pasta ou arquivo(s) que você deseja restaurar desse backup.
5. Selecione o local de destino onde você deseja que a pasta ou o(s) arquivo(s) sejam restaurados (o sistema, o volume e a pasta) e clique em **Restaurar**.
6. O(s) arquivo(s) são restaurados.



Como você pode ver, você precisa saber o nome do sistema, o nome do volume, a data do arquivo de backup e o nome da pasta/arquivo para executar uma restauração de pasta ou arquivo.

Restaurar pastas e arquivos

Siga estas etapas para restaurar pastas ou arquivos para um volume a partir de um backup de volume ONTAP . Você deve saber o nome do volume e a data do arquivo de backup que deseja usar para restaurar a pasta ou o(s) arquivo(s). Esta funcionalidade usa a Navegação ao Vivo para que você possa visualizar a lista de diretórios e arquivos dentro de cada arquivo de backup.

Passos

1. No menu Console, selecione **Proteção > Backup e recuperação**.
2. Selecione a aba **Restaurar** e o Painel de Restauração será exibido.
3. Na seção *Navegar e restaurar*, selecione **Restaurar arquivos ou pastas**.
4. Na página *Selecionar origem*, navegue até o arquivo de backup do volume que contém a pasta ou os arquivos que você deseja restaurar. Selecione o **sistema**, o **Volume** e o **Backup** que tem o registro de data/hora dos arquivos dos quais você deseja restaurar.
5. Selecione **Avançar** e a lista de pastas e arquivos do backup de volume será exibida.

   Se estiver restaurando pastas ou arquivos de um arquivo de backup que reside em uma camada de armazenamento de arquivamento, você pode selecionar a Prioridade de restauração.

   "Saiba mais sobre a restauração do armazenamento de arquivo da AWS" . "Saiba mais sobre a restauração do armazenamento de arquivamento do Azure" . "Saiba mais sobre como restaurar do armazenamento de arquivo do Google" . Os arquivos de backup no nível de armazenamento do Google Archive são restaurados quase imediatamente e não exigem Prioridade de Restauração.

   E se a Resiliência contra Ransomware estiver ativa para o arquivo de backup (se você habilitou o DataLock e a Resiliência 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 se há ransomware no arquivo de backup. (Você incorrerá em custos extras de saída do seu provedor de nuvem para acessar o conteúdo do arquivo de backup.)

6. Na página *Selecionar itens*, selecione a pasta ou arquivo(s) que deseja restaurar e selecione **Continuar**. Para ajudar você a encontrar o item:
   - Você pode selecionar o nome da pasta ou do arquivo se o vir.

- Você pode selecionar o ícone de pesquisa e digitar o nome da pasta ou arquivo para navegar diretamente até o item.
- Você pode navegar pelos níveis inferiores nas pastas usando a seta para baixo no final da linha para encontrar arquivos específicos.

  Conforme você seleciona os arquivos, eles são adicionados ao lado esquerdo da página para que você possa ver os arquivos que já escolheu. Você pode remover um arquivo desta lista, se necessário, selecionando o **x** ao lado do nome do arquivo.

7. Na página *Selecionar destino*, selecione o **sistema** onde você deseja restaurar os itens.

   Se você selecionar um cluster local e ainda não tiver configurado a conexão do cluster com o armazenamento de objetos, serão solicitadas informações adicionais:

   - Ao restaurar do Amazon S3, insira o IPspace no cluster ONTAP onde o volume de destino reside e a Chave de acesso e a Chave secreta da AWS necessárias para acessar o armazenamento de objetos. Você também pode selecionar uma Configuração de Link Privado para a conexão com o cluster.
     - Ao restaurar do Azure Blob, insira o IPspace no cluster ONTAP onde o volume de destino reside. Você também pode selecionar uma Configuração de Endpoint Privado para a conexão com o cluster.
     - Ao restaurar do Google Cloud Storage, insira o IPspace no cluster ONTAP onde os volumes de destino residem, além da chave de acesso e da chave secreta necessárias para acessar o armazenamento de objetos.
     - Ao restaurar do StorageGRID, insira o FQDN do servidor StorageGRID e a porta que o ONTAP deve usar para comunicação HTTPS com o StorageGRID, insira a Chave de Acesso e a Chave Secreta necessárias para acessar o armazenamento de objetos e o IPspace no cluster ONTAP onde o volume de destino reside.

       a. Em seguida, selecione o **Volume** e a **Pasta** onde você deseja restaurar a pasta ou o(s) arquivo(s).

          Você tem algumas opções de local para restaurar pastas e arquivos.

     - Quando você tiver escolhido **Selecionar 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 as subpastas e, em seguida, selecionar uma pasta.
     - Se você tiver selecionado o mesmo sistema de destino e volume onde a pasta/arquivo de origem estava localizado, você pode selecionar **Manter caminho da pasta de origem** para restaurar a pasta, ou arquivo(s), para a mesma pasta onde eles estavam na estrutura de origem. Todas as mesmas pastas e subpastas já devem existir; 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. Selecione **Restaurar** e você retornará ao Painel de Restauração para poder revisar o progresso da operação de restauração. Você também pode clicar na aba **Monitoramento de Tarefas** para ver o progresso da restauração.

Restaurar dados ONTAP usando Pesquisar e Restaurar

Você pode restaurar um volume, pasta ou arquivos de um arquivo de backup do ONTAP usando Pesquisar e Restaurar. A Pesquisa e Restauração permite que você pesquise um volume, pasta ou arquivo específico em todos os backups e, em seguida, execute uma restauração. Você não precisa saber o nome exato do sistema,

o nome do volume ou o nome do arquivo: a pesquisa examina todos os arquivos de backup do volume.

A operação de pesquisa examina todas as cópias de instantâneos locais que existem para seus volumes ONTAP , todos os volumes replicados em sistemas de armazenamento secundário e todos os arquivos de backup que existem no armazenamento de objetos. Como restaurar dados de uma cópia local do Snapshot ou de um volume replicado pode ser mais rápido e menos custoso do que restaurar de um arquivo de backup no armazenamento de objetos, talvez você queira restaurar dados desses outros locais.

Quando você restaura um *volume completo* de um arquivo de backup, o NetApp Backup and Recovery cria um *novo* volume usando os dados do backup. Você pode restaurar os dados como um volume no sistema original, em um sistema diferente localizado na mesma conta de nuvem que o sistema de origem ou em um sistema ONTAP local.

Você pode restaurar *pastas ou arquivos* para o local do volume original, para um volume diferente no mesmo sistema, para um sistema diferente que esteja usando a mesma conta de nuvem ou para um volume em um sistema ONTAP local.

Ao usar o ONTAP 9.13.0 ou superior, você pode restaurar uma pasta junto com todos os arquivos e subpastas dentro dela. Ao usar uma versão do ONTAP anterior à 9.13.0, somente os arquivos dessa pasta são restaurados - nenhuma subpasta ou arquivo em subpastas é restaurado.

Se o arquivo de backup do volume que você deseja restaurar estiver no armazenamento de arquivamento (disponível a partir do ONTAP 9.10.1), a operação de restauração levará mais tempo 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 arquivo, 9.12.1 para Google Archive e StorageGRID e 9.13.1 para restauração de pasta.

"Saiba mais sobre a restauração do armazenamento de arquivo da AWS" .

"Saiba mais sobre a restauração do armazenamento de arquivamento do Azure" .

"Saiba mais sobre como restaurar do armazenamento de arquivo do Google" .

- Se o arquivo de backup no armazenamento de objetos tiver sido configurado com proteção DataLock e Ransomware, a restauração em nível de pasta será suportada somente se a versão do ONTAP for 9.13.1 ou superior. Se estiver usando uma versão anterior do ONTAP, você poderá restaurar o volume inteiro a partir do arquivo de backup e então 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 usando uma versão anterior do ONTAP, você pode restaurar a pasta a partir de um arquivo de backup mais recente que não foi arquivado ou pode restaurar o volume inteiro a partir do backup arquivado e então acessar a pasta e os arquivos necessários.
- A prioridade de restauração "Alta" não é suportada ao restaurar dados do armazenamento de arquivamento do Azure para sistemas StorageGRID .
- Atualmente, a restauração de pastas não é suportada em volumes no armazenamento de objetos ONTAP S3.

Antes de começar, você deve ter uma ideia do nome ou local do volume ou arquivo que deseja restaurar.

Sistemas suportados de pesquisa e restauração e provedores de armazenamento de objetos

Você pode restaurar dados do ONTAP de um arquivo de backup que reside em um sistema secundário (um volume replicado) ou em um armazenamento de objetos (um arquivo de backup) para os seguintes sistemas. Cópias de instantâneos residem no sistema de origem e podem ser restauradas somente no mesmo sistema.

Observação: você pode restaurar volumes e arquivos de qualquer tipo de arquivo de backup, mas, no momento, você só pode restaurar uma pasta de arquivos de backup no armazenamento de objetos.

Localização do arquivo de backup		Sistema de destino
Armazenamento de Objetos (Backup)	**Sistema Secundário (Replicação)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Cloud Volumes ONTAP no sistema ONTAP local da AWS endif::aws[] ifdef::azure[]
Blob do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure endif::azure[] ifdef::gcp[]
Armazenamento em nuvem do Google	Cloud Volumes ONTAP no sistema Google On-premises ONTAP	Cloud Volumes ONTAP no sistema ONTAP local do Google endif::gcp[]
NetApp StorageGRID	Sistema ONTAP local Cloud Volumes ONTAP	Sistema ONTAP local
ONTAP S3	Sistema ONTAP local Cloud Volumes ONTAP	Sistema ONTAP local

Para Pesquisar e Restaurar, o agente do Console pode ser instalado nos seguintes locais:

- Para o Amazon S3, o agente do Console pode ser implantado na AWS ou em suas instalações
- Para o Azure Blob, o agente do Console pode ser implantado no Azure ou em suas instalações
- Para o Google Cloud Storage, o agente do Console deve ser implantado na sua VPC do Google Cloud Platform
- Para StorageGRID, o agente do Console deve ser implantado em suas instalações; com ou sem acesso à Internet
- Para o ONTAP S3, o agente do Console 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 locais" incluem sistemas FAS, AFF e ONTAP Select .

Pré-requisitos

- Requisitos do cluster:
  - A versão do ONTAP deve ser 9.8 ou superior.
  - A VM de armazenamento (SVM) na qual o volume reside deve ter um LIF de dados configurado.
  - O NFS deve estar habilitado no volume (tanto os volumes NFS quanto os SMB/CIFS são suportados).
  - O servidor SnapDiff RPC deve ser ativado no SVM. O Console faz isso automaticamente quando você habilita a indexação no sistema. (SnapDiff é a tecnologia que identifica rapidamente as diferenças de arquivo e diretório entre cópias do Snapshot.)

- Requisitos da AWS:
  - Permissões específicas do Amazon Athena, AWS Glue e AWS S3 devem ser adicionadas à função de usuário que fornece permissões ao Console. "Certifique-se de que todas as permissões estejam configuradas corretamente" .

    Observe que, se você já estava usando o NetApp Backup and Recovery com um agente do Console configurado anteriormente, será necessário adicionar as permissões Athena e Glue à função de usuário do Console agora. Eles são necessários para Pesquisar e Restaurar.

- Requisitos do Azure:
  - Você deve registrar o Provedor de Recursos do Azure Synapse Analytics (chamado "Microsoft.Synapse") com sua Assinatura. "Veja como registrar este provedor de recursos para sua assinatura" . Você deve ser o **Proprietário** ou **Colaborador** da Assinatura para registrar o provedor de recursos.
  - Permissões específicas do Azure Synapse Workspace e da conta de armazenamento do Data Lake devem ser adicionadas à função de usuário que fornece permissões ao Console. "Certifique-se de que todas as permissões estejam configuradas corretamente" .

    Observe que, se você já estava usando o NetApp Backup and Recovery com um agente do Console configurado anteriormente, será necessário adicionar as permissões da conta do Azure Synapse Workspace e do Data Lake Storage à função de usuário do Console agora. Eles são necessários para Pesquisar e Restaurar.

  - O agente do Console deve ser configurado **sem** um servidor proxy para comunicação HTTP com a Internet. Se você tiver configurado um servidor proxy HTTP para seu agente do Console, não poderá usar a funcionalidade Pesquisar e Restaurar.
- Requisitos do Google Cloud:
  - Permissões específicas do Google BigQuery devem ser adicionadas à função de usuário que fornece permissões ao NetApp Console. "Certifique-se de que todas as permissões estejam configuradas corretamente" .

    Se você já estava usando o NetApp Backup and Recovery com um agente do Console configurado anteriormente, será necessário adicionar as permissões do BigQuery à função de usuário do Console agora. Eles são necessários para Pesquisar e Restaurar.

- Requisitos do StorageGRID e do ONTAP S3:

  Dependendo da sua configuração, há duas maneiras de implementar a Pesquisa e Restauração:

  - Se não houver credenciais de provedor de nuvem em sua conta, as informações do Catálogo Indexado serão armazenadas no agente do Console.

    Para obter informações sobre o Catálogo Indexado v2, consulte a seção abaixo sobre como habilitar o Catálogo Indexado.

  - Se você estiver usando um agente do Console em um site privado (escuro), as informações do Catálogo Indexado serão armazenadas no agente do Console (requer o agente do Console versão 3.9.25 ou superior).
  - Se você tem "Credenciais AWS" ou "Credenciais do Azure" na conta, o Catálogo Indexado é armazenado no provedor de nuvem, assim como acontece com um agente do Console implantado na nuvem. (Se você tiver ambas as credenciais, a AWS será selecionada por padrão.)

Mesmo que você esteja usando um agente do Console local, os requisitos do provedor de nuvem devem ser atendidos para permissões do agente do Console e recursos do provedor de nuvem. Veja os requisitos da AWS e do Azure acima ao usar esta implementação.

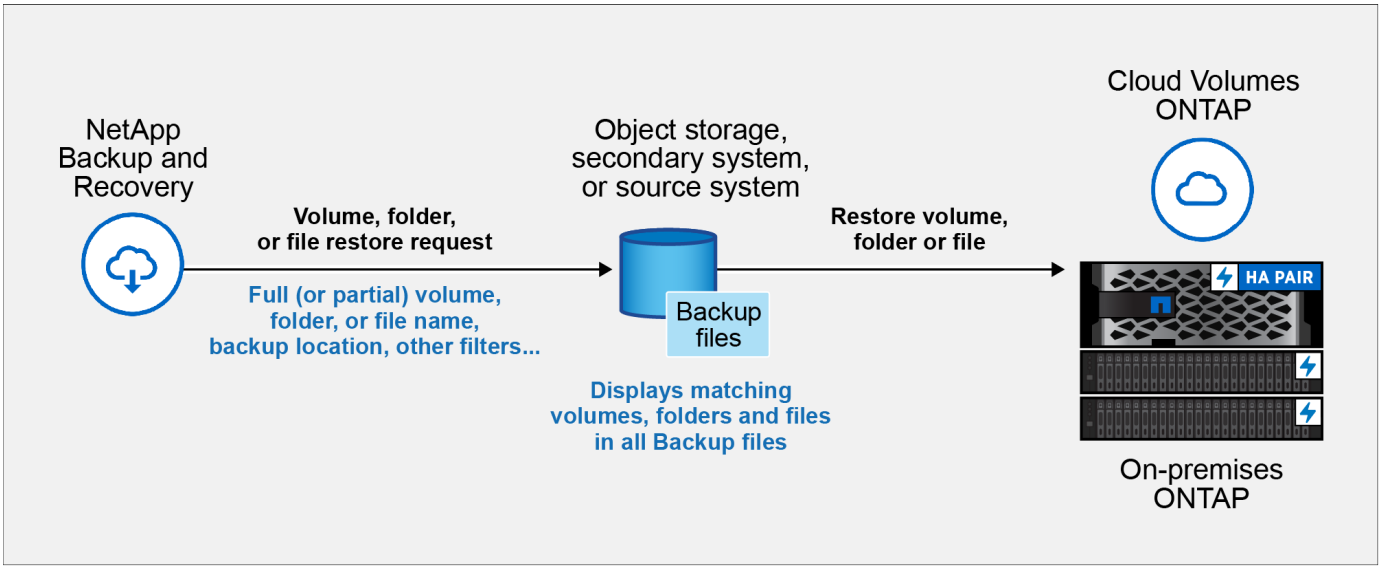
Processo de busca e restauração

O processo é assim:

1. Antes de poder usar a Pesquisa e Restauração, você precisa habilitar a "Indexação" em cada sistema de origem do qual deseja restaurar dados de volume. Isso permite que o Catálogo Indexado rastreie os arquivos de backup de cada volume.
2. Quando quiser restaurar um volume ou arquivos de um backup de volume, em *Pesquisar e restaurar*, selecione **Pesquisar e restaurar**.
3. Insira os critérios de pesquisa para um volume, pasta ou arquivo por nome parcial ou completo do volume, nome parcial ou completo do arquivo, local do backup, intervalo de tamanho, intervalo de data de criação, outros filtros de pesquisa e selecione **Pesquisar**.

   A página Resultados da pesquisa exibe todos os locais que têm um arquivo ou volume que corresponde aos seus critérios de pesquisa.

4. Selecione **Exibir todos os backups** para o local que deseja usar para restaurar o volume ou arquivo e, em seguida, selecione **Restaurar** no arquivo de backup que deseja usar.
5. Selecione o local onde você deseja que o volume, a pasta ou o(s) arquivo(s) sejam restaurados e selecione **Restaurar**.
6. O volume, pasta ou arquivo(s) são restaurados.



Como você pode ver, você só precisa saber um nome parcial e o NetApp Backup and Recovery pesquisará todos os arquivos de backup que correspondem à sua pesquisa.

Habilitar o Catálogo Indexado para cada sistema

Antes de poder usar a Pesquisa e Restauração, você precisa habilitar a "Indexação" em cada sistema de origem do qual planeja restaurar volumes ou arquivos. Isso permite que o Catálogo Indexado rastreie cada volume e cada arquivo de backup, tornando suas pesquisas muito rápidas e eficientes.

O Catálogo Indexado é um banco de dados que armazena metadados sobre todos os volumes e arquivos de backup no seu sistema. Ele é usado pela funcionalidade Pesquisar e Restaurar para encontrar rapidamente os arquivos de backup que contêm os dados que você deseja restaurar.

Recursos do Catálogo Indexado v2

O Catálogo Indexado v2, lançado em fevereiro de 2025 e atualizado em junho de 2025, inclui recursos que o tornam mais eficiente e fácil de usar. Esta versão tem uma melhoria significativa de desempenho e é habilitada por padrão para todos os novos clientes.

Revise as seguintes considerações sobre a v2:

- O Catálogo Indexado v2 está disponível em modo de visualização.
- Se você já é cliente e deseja usar o Catálogo v2, precisa reindexar completamente seu ambiente.
- O Catálogo v2 indexa apenas os instantâneos que têm um rótulo de instantâneo.
- O NetApp Backup and Recovery não indexa snapshots com rótulos SnapMirror "por hora". Se você quiser indexar snapshots com o rótulo SnapMirror "por hora", será necessário habilitá-lo manualmente enquanto a versão 2 estiver no modo de visualização.
- O NetApp Backup and Recovery indexará volumes e snapshots associados a sistemas protegidos pelo NetApp Backup and Recovery somente com o Catálogo v2. Outros sistemas descobertos na plataforma Console não serão indexados.
- A indexação de dados com o Catalog v2 ocorre em ambientes locais e em ambientes Amazon Web Services, Microsoft Azure e Google Cloud Platform (GCP).

O Catálogo Indexado v2 suporta o seguinte:

- Eficiência de pesquisa global em menos de 3 minutos
- Até 5 bilhões de arquivos
- Até 5000 volumes por cluster
- Até 100 mil instantâneos por volume
- O tempo máximo para indexação de linha de base é inferior a 7 dias. O tempo real variará dependendo do seu ambiente.

Habilitando o Catálogo Indexado para um sistema

O serviço não provisiona um bucket separado quando você usa o Catálogo Indexado v2. Em vez disso, para backups armazenados no AWS, Azure, Google Cloud Platform, StorageGRID ou ONTAP S3, o serviço provisiona espaço no agente do Console ou no ambiente do provedor de nuvem.

Se você habilitou o Catálogo Indexado antes do lançamento da v2, o seguinte ocorre com os sistemas:

- Para backups armazenados na AWS, ele provisiona um novo bucket S3 e o "Serviço de consulta interativa Amazon Athena" e "Serviço de integração de dados sem servidor AWS Glue" .
- Para backups armazenados no Azure, ele provisiona um espaço de trabalho do Azure Synapse e um sistema de arquivos do Data Lake como o contêiner que armazenará os dados do espaço de trabalho.
- Para backups armazenados no Google Cloud, ele provisiona um novo bucket e o "Serviços do Google Cloud BigQuery" são provisionados em nível de conta/projeto.
- Para backups armazenados no StorageGRID ou ONTAP S3, ele provisiona espaço no agente do Console ou no ambiente do provedor de nuvem.

Se a indexação já estiver habilitada para seu sistema, vá para a próxima seção para restaurar seus dados.

Etapas para habilitar a indexação de um sistema:

1. Faça um dos seguintes:
   - Se nenhum sistema tiver sido indexado, no Painel de Restauração, em *Pesquisar e Restaurar*, selecione **Ativar Indexação para Sistemas**.
   - Se pelo menos um sistema já tiver sido indexado, no Painel de Restauração, em *Pesquisar e Restaurar*, selecione **Configurações de Indexação**.
2. Selecione **Ativar indexação** para o sistema.

Resultado

Depois que todos os serviços forem provisionados e o Catálogo Indexado for ativado, o sistema será mostrado como "Ativo".

Dependendo do tamanho dos volumes no sistema e do número de arquivos de backup em todos os três locais de backup, o processo de indexação inicial pode levar até uma hora. Depois disso, ele é atualizado de forma transparente a cada hora, com alterações incrementais para se manter atualizado.

Restaurar volumes, pastas e arquivos usando Pesquisar e Restaurar

Depois de você terindexação habilitada para seu sistema , você pode restaurar volumes, pastas e arquivos usando Pesquisar e Restaurar. Isso permite que você use uma ampla gama de filtros para encontrar o arquivo ou volume exato que deseja restaurar de todos os arquivos de backup.

Passos

1. No menu Console, selecione **Proteção > Backup e recuperação**.
2. Selecione a aba **Restaurar** e o Painel de Restauração será exibido.
3. Na seção *Pesquisar e restaurar*, selecione **Pesquisar e restaurar**.
4. Na seção *Pesquisar e restaurar*, selecione **Pesquisar e restaurar**.
5. Na página Pesquisar e Restaurar:
   a. Na *Barra de pesquisa*, insira um nome de volume completo ou parcial, nome de 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 sistema 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 em cópias de instantâneo disponíveis ou arquivos de backup no armazenamento de objetos.
6. Selecione **Pesquisar** e a área Resultados da pesquisa exibirá todos os recursos que têm um arquivo, pasta ou volume que corresponde à sua pesquisa.
7. Localize o recurso que contém os dados que você deseja restaurar e selecione **Exibir todos os backups** para exibir todos os arquivos de backup que contêm o volume, pasta ou arquivo correspondente.
8. Localize o arquivo de backup que você deseja usar para restaurar os dados e selecione **Restaurar**.

   Observe que os resultados identificam cópias de instantâneos de volumes locais e volumes replicados remotos que contêm o arquivo em sua pesquisa. Você pode escolher restaurar a partir do arquivo de backup na nuvem, da cópia do Snapshot ou do volume replicado.

9. Selecione o local de destino onde você deseja que o volume, a pasta ou o(s) arquivo(s) sejam restaurados e selecione **Restaurar**.

- Para volumes, você pode selecionar o sistema de destino original ou um sistema alternativo. Ao restaurar um volume FlexGroup , você precisará escolher vários agregados.
- Para pastas, você pode restaurar para o local original ou selecionar um local alternativo; incluindo o sistema, o volume e a pasta.
- Para arquivos, você pode restaurar para o local original ou selecionar um local alternativo; incluindo o sistema, o volume e a pasta. Ao selecionar o local original, você pode optar por substituir o(s) arquivo(s) de origem ou criar novo(s) arquivo(s).

  Se você selecionar um sistema ONTAP local e ainda não tiver configurado a conexão do cluster com o armazenamento de objetos, serão solicitadas informações adicionais:

  - Ao restaurar do Amazon S3, selecione o IPspace no cluster ONTAP onde o volume de destino residirá, insira a chave de acesso e a chave secreta do usuário que você criou para dar ao cluster ONTAP acesso ao bucket S3 e, opcionalmente, escolha um endpoint VPC privado para transferência segura de dados. "Veja detalhes sobre esses requisitos" .
    - Ao restaurar do Azure Blob, selecione o IPspace no cluster ONTAP onde o volume de destino residirá e, opcionalmente, escolha um ponto de extremidade privado para transferência segura de dados selecionando a VNet e a Sub-rede. "Veja detalhes sobre esses requisitos" .
    - Ao restaurar do Google Cloud Storage, selecione o IPspace no cluster ONTAP onde o volume de destino residirá, além da Chave de acesso e da Chave secreta para acessar o armazenamento de objetos. "Veja detalhes sobre esses requisitos" .
    - Ao restaurar do StorageGRID, insira o FQDN do servidor StorageGRID e a porta que o ONTAP deve usar para comunicação HTTPS com o StorageGRID, insira a Chave de Acesso e a Chave Secreta necessárias para acessar o armazenamento de objetos e o IPspace no cluster ONTAP onde o volume de destino reside. "Veja detalhes sobre esses requisitos" .
    - Ao restaurar do ONTAP S3, insira 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 a Chave Secreta necessárias para acessar o armazenamento de objetos e o espaço IP 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 retorna ao Painel de Restauração para poder revisar o progresso da operação de restauração. Você também pode selecionar a aba **Monitoramento de Tarefas** para ver o progresso da restauração. Ver "Página do monitor de tarefas" .

Proteja as cargas de trabalho do Microsoft SQL Server

Visão geral da proteção de cargas de trabalho do Microsoft SQL com o NetApp Backup and Recovery

Proteja os dados dos seus aplicativos Microsoft SQL Server de sistemas ONTAP locais para Amazon Web Services, Microsoft Azure ou StorageGRID usando o NetApp Backup and Recovery. Os backups são gerados automaticamente e armazenados em um repositório de objetos na sua conta de nuvem pública ou privada com base nas políticas que você cria. Você pode implementar uma estratégia 3-2-1, na qual você tem 3 cópias dos seus dados de origem em 2 sistemas de armazenamento diferentes, além de 1 cópia na nuvem.

Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados fornecem proteção multicamadas contra ameaças de segurança cibernética internas e externas.
- Vários tipos de mídia garantem a viabilidade de failover no caso de falha física ou lógica de um tipo de mídia.
- A cópia no local facilita restaurações rápidas, com cópias externas disponíveis caso a cópia no local seja comprometida.

O NetApp Backup and Recovery utiliza a tecnologia de replicação de dados NetApp SnapMirror para garantir que todos os backups sejam totalmente sincronizados, criando cópias instantâneas e transferindo-as para os locais de backup.

Você pode atingir as seguintes metas de proteção:

- "Configurar itens adicionais se importar do SnapCenter"
- "Descubra cargas de trabalho do Microsoft SQL Server e, opcionalmente, importe recursos do SnapCenter"
- "Faça backup de cargas de trabalho com snapshots locais no armazenamento primário ONTAP local"
- "Replique cargas de trabalho para armazenamento secundário ONTAP"
- "Fazer backup de cargas de trabalho em um local de armazenamento de objetos"
- "Faça backup das cargas de trabalho agora"
- "Restaurar cargas de trabalho"
- "Clonar cargas de trabalho"
- "Gerenciar inventário de cargas de trabalho"
- "Gerenciar instantâneos"

Para fazer backup de cargas de trabalho, normalmente você cria políticas que controlam as operações de backup e restauração. Ver "Criar políticas" para maiores informações.

Destinos de backup suportados

O NetApp Backup and Recovery permite que você faça backup de instâncias e bancos de dados do Microsoft SQL Server dos seguintes sistemas de origem para os seguintes sistemas secundários e armazenamento de objetos em provedores de nuvem pública e privada. Cópias de instantâneos residem no sistema de origem.

Sistema de origem	Sistema secundário (Replicação)	Armazenamento de Objetos de Destino (Backup)
Cloud Volumes ONTAP na AWS	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Amazon S3 ONTAP S3
Cloud Volumes ONTAP no Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Azure Blob ONTAP S3
Sistema ONTAP local	Sistema Cloud Volumes ONTAP ONTAP	Amazon S3 Azure Blob NetApp StorageGRID ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	NA ifdef::gcp[] fim se::gcp[] ifdef::gcp[] fim se::gcp[]

Destinos de restauração suportados

Você pode restaurar instâncias e bancos de dados do Microsoft SQL Server de um backup que reside no

armazenamento primário ou em um sistema secundário (um volume replicado) ou no armazenamento de objetos (um arquivo de backup) para os seguintes sistemas. Cópias de instantâneos residem no sistema de origem e podem ser restauradas somente no mesmo sistema.

Do local do arquivo de backup		Para o sistema de destino
Armazenamento de Objetos (Backup)	**Sistema Secundário (Replicação)**	
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Volumes de nuvem no sistema ONTAP local da AWS ONTAP S3
Blob do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure ONTAP S3 ifdef::gcp[] endif::gcp[]
StorageGRID	Sistema Cloud Volumes ONTAP ONTAP	Sistema ONTAP local ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	N / D

Referências a "sistemas ONTAP locais" incluem sistemas FAS e AFF .

Pré-requisitos para importação do serviço Plug-in para o NetApp Backup and Recovery

Se você for importar recursos do serviço SnapCenter Plug-in para Microsoft SQL Server para o NetApp Backup and Recovery, precisará configurar mais alguns itens.

Crie sistemas no NetApp Console primeiro

Se você for importar recursos do SnapCenter, adicione todo o armazenamento de cluster do SnapCenter local à página **Sistemas** do Console antes de importar do SnapCenter. Isso garante que os recursos do host possam ser descobertos e importados corretamente.

Garantir os requisitos do host para instalar o plug-in SnapCenter

Para importar recursos do SnapCenter Plug-in para Microsoft SQL Server, certifique-se de que os requisitos do host para instalar o SnapCenter Plug-in para Microsoft SQL Server sejam atendidos.

Verifique especificamente os requisitos do SnapCenter em"Pré-requisitos do NetApp Backup and Recovery" .

Desabilitar restrições remotas do Controle de Conta de Usuário

Antes de importar recursos do SnapCenter, desabilite as restrições remotas do Controle de Conta de Usuário (UAC) no host do SnapCenter no Windows. Desative o UAC se você usar uma conta administrativa local para se conectar remotamente ao host do SnapCenter Server ou ao host do SQL.

Considerações de segurança

Considere as seguintes questões antes de desabilitar as restrições remotas do UAC:

- Riscos de segurança: desabilitar a filtragem de tokens pode expor seu sistema a vulnerabilidades de segurança, especialmente se contas administrativas locais forem comprometidas por agentes mal-intencionados.

- Use com cautela:
  - Modifique esta configuração somente se ela for essencial para suas tarefas administrativas.
  - Certifique-se de que senhas fortes e outras medidas de segurança estejam em vigor para proteger contas administrativas.

Soluções alternativas

- Se for necessário acesso administrativo remoto, considere usar contas de domínio com privilégios apropriados.
- Use ferramentas seguras de gerenciamento remoto que sigam as melhores práticas de segurança para minimizar riscos.

Etapas para desabilitar as restrições remotas do Controle de Conta de Usuário

1. Modifique o `LocalAccountTokenFilterPolicy` chave de registro no host SnapCenter Windows.

   Faça isso usando um dos seguintes métodos, com instruções a seguir:

   - Método 1: Editor do Registro
   - Método 2: script do PowerShell

Método 1: Desabilite o Controle de Conta de Usuário usando o Editor do Registro

Este é um dos métodos que você pode usar para desabilitar o Controle de Conta de Usuário.

Passos

1. Abra o Editor do Registro no host SnapCenter Windows fazendo o seguinte:
   a. Imprensa `Windows+R` para abrir a caixa de diálogo Executar.
   b. Tipo `regedit` e pressione `Enter` .
2. Navegue até a Chave de Política:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
   ```

3. Crie ou modifique o `DWORD` valor:
   a. Localizar: `LocalAccountTokenFilterPolicy`
   b. Se não existir, crie um novo `DWORD` (32 bits) Valor nomeado `LocalAccountTokenFilterPolicy` .
4. Os seguintes valores são suportados. Para este cenário, defina o valor como `1` :
   - `0`(Padrão): As restrições remotas do UAC estão habilitadas. Contas locais têm tokens filtrados ao acessar remotamente.
   - `1`: As restrições remotas do UAC estão desabilitadas. Contas locais ignoram a filtragem de tokens e têm privilégios administrativos completos ao acessar remotamente.
5. Clique em **OK**.
6. Feche o Editor do Registro.
7. Reinicie o host do SnapCenter no Windows.

Exemplo de modificação de registro

Este exemplo define LocalAccountTokenFilterPolicy como "1", desabilitando restrições remotas do UAC.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

Método 2: Desabilitar o Controle de Conta de Usuário usando um script do PowerShell

Este é outro método que você pode usar para desabilitar o Controle de Conta de Usuário.

Executar comandos do PowerShell com privilégios elevados pode afetar as configurações do sistema. Certifique-se de entender os comandos e suas implicações antes de executá-los.

Passos

1. Abra uma janela do PowerShell com privilégios administrativos no host SnapCenter Windows:
   a. Clique no menu **Iniciar**.
   b. Pesquise por **PowerShell 7** ou **Windows Powershell**.
   c. Clique com o botão direito do mouse nessa opção e selecione **Executar como administrador**.
2. Certifique-se de que o PowerShell esteja instalado no seu sistema. Após a instalação, ele deverá aparecer no menu **Iniciar**.

   O PowerShell está incluído por padrão no Windows 7 e versões posteriores.

3. Para desabilitar as restrições remotas do UAC, defina LocalAccountTokenFilterPolicy como "1" executando o seguinte comando:

   ```
   Set-ItemProperty -Path
   "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
   "LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
   ```

4. Verifique se o valor atual está definido como "1" em `LocalAccountTokenFilterPolicy` executando:

   ```
   Get-ItemProperty -Path
   "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
   "LocalAccountTokenFilterPolicy"
   ```

   - Se o valor for 1, as restrições remotas do UAC serão desabilitadas.
   - Se o valor for 0, as restrições remotas do UAC serão habilitadas.
5. Para aplicar as alterações, reinicie o computador.

Exemplo de comandos do PowerShell 7 para desabilitar restrições remotas do UAC:

Este exemplo com o valor definido como "1" indica que as restrições remotas do UAC estão desabilitadas.

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

Descubra cargas de trabalho do Microsoft SQL Server e, opcionalmente, importe do SnapCenter no NetApp Backup and Recovery

O NetApp Backup and Recovery precisa primeiro descobrir as cargas de trabalho do Microsoft SQL Server para que você possa usar o serviço. Opcionalmente, você pode importar dados e políticas de backup do SnapCenter se já tiver o SnapCenter instalado.

Função necessária do NetApp Console Superadministrador de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Descubra cargas de trabalho do Microsoft SQL Server e, opcionalmente, importe recursos do SnapCenter

Durante a descoberta, o NetApp Backup and Recovery analisa instâncias e bancos de dados do Microsoft SQL Server em sistemas dentro da sua organização.

O NetApp Backup and Recovery avalia aplicativos do Microsoft SQL Server. O serviço avalia o nível de proteção existente, incluindo as políticas atuais de proteção de backup, cópias de instantâneos e opções de backup e recuperação.

A descoberta ocorre das seguintes maneiras:

- Se você já tiver o SnapCenter, importe os recursos do SnapCenter para o NetApp Backup and Recovery usando a interface do usuário do NetApp Backup and Recovery.

  Se você já tem o SnapCenter, primeiro verifique se atendeu aos pré-requisitos antes de importar do SnapCenter. Por exemplo, você deve adicionar sistemas de armazenamento em cluster SnapCenter locais ao NetApp Console antes de importar do SnapCenter. Ver "Pré-requisitos para importar recursos do SnapCenter" .

- Se você ainda não tiver o SnapCenter, ainda poderá descobrir cargas de trabalho adicionando um vCenter manualmente e executando a descoberta.

Se o SnapCenter já estiver instalado, importe os recursos do SnapCenter para o NetApp Backup and Recovery

Se você já tiver o SnapCenter instalado, importe os recursos do SnapCenter para o NetApp Backup and Recovery seguindo estas etapas. O NetApp Console descobre recursos, hosts, credenciais e agendamentos do SnapCenter; você não precisa recriar todas essas informações.

Você pode fazer isso das seguintes maneiras:

- Durante a descoberta, selecione uma opção para importar recursos do SnapCenter.
- Após a descoberta, na página Inventário, selecione uma opção para importar recursos do SnapCenter .
- Após a descoberta, no menu Configurações, selecione uma opção para importar recursos do SnapCenter . Para obter detalhes, consulte "Configurar o NetApp Backup and Recovery" .

Este é um processo de duas partes:

- Importar recursos do aplicativo e do host do SnapCenter Server
- Gerenciar recursos selecionados do host SnapCenter

Importar recursos do aplicativo e do host do SnapCenter Server

Esta primeira etapa importa recursos de host do SnapCenter e exibe esses recursos na página Inventário de backup e recuperação do NetApp . Nesse ponto, os recursos ainda não são gerenciados pelo NetApp Backup and Recovery.

Depois de importar os recursos do host do SnapCenter , o NetApp Backup and Recovery não assume o gerenciamento de proteção automaticamente. Para fazer isso, você deve selecionar explicitamente gerenciar os recursos importados no NetApp Backup and Recovery. Isso garante que você esteja pronto para ter esses recursos armazenados em backup pelo NetApp Backup and Recovery.

Passos

1. Na navegação à esquerda do NetApp Console, selecione **Proteção** > **Backup e recuperação**.
2. Selecione **Inventário**.
3. Selecione **Descobrir recursos**.
4. Na página Descobrir recursos de carga de trabalho do NetApp Backup and Recovery, selecione **Importar do SnapCenter**.
5. Insira * Credenciais do aplicativo SnapCenter *:
   a. * FQDN ou endereço IP do SnapCenter *: insira o FQDN ou endereço IP do próprio aplicativo SnapCenter .
   b. **Porta**: insira o número da porta para o SnapCenter Server.
   c. **Nome de usuário** e **Senha**: Digite o nome de usuário e a senha do SnapCenter Server.
   d. **Agente de console**: Selecione o agente de console para o SnapCenter.
6. Insira * Credenciais do host do servidor SnapCenter *:
   a. **Credenciais existentes**: Se você selecionar esta opção, poderá usar as credenciais existentes que você já adicionou. Escolha o nome das credenciais.
   b. **Adicionar novas credenciais**: Se você não tiver credenciais de host do SnapCenter existentes, poderá adicionar novas credenciais. Digite o nome das credenciais, o modo de autenticação, o nome de usuário e a senha.

7. Selecione **Importar** para validar suas entradas e registrar o SnapCenter Server.

   Se o SnapCenter Server já estiver registrado, você poderá atualizar os detalhes de registro existentes.

Resultado

A página Inventário mostra os recursos importados do SnapCenter que incluem hosts, instâncias e bancos de dados do MS SQL.

Para ver os detalhes dos recursos importados do SnapCenter , selecione a opção **Exibir detalhes** no menu Ações.

Gerenciar recursos do host SnapCenter

Depois de importar os recursos do SnapCenter , gerencie esses recursos de host no NetApp Backup and Recovery. Depois de selecionar o gerenciamento desses recursos, o NetApp Backup and Recovery poderá fazer backup e recuperar os recursos que você importou do SnapCenter. Você não gerencia mais esses recursos no SnapCenter Server.

Passos

1. Depois de importar os recursos do SnapCenter , no menu Backup e Recuperação, selecione **Inventário**.
2. Na página Inventário, selecione o host SnapCenter importado que você deseja que o NetApp Backup and Recovery gerencie a partir de agora.
3. Selecione o ícone Ações ••• > **Ver detalhes** para exibir os detalhes da carga de trabalho.
4. Na página Inventário > carga de trabalho, selecione o ícone Ações ••• > **Gerenciar** para exibir a página Gerenciar host.
5. Selecione **Gerenciar**.
6. Na página Gerenciar host, selecione se deseja usar um vCenter existente ou adicionar um novo vCenter.
7. Selecione **Gerenciar**.

   A página Inventário mostra os recursos do SnapCenter recém-gerenciados.

Opcionalmente, você pode criar um relatório dos recursos gerenciados selecionando a opção **Gerar relatórios** no menu Ações.

Importar recursos do SnapCenter após a descoberta na página Inventário

Se você já descobriu recursos, pode importar recursos do SnapCenter da página Inventário.

Passos

1. Na navegação à esquerda do Console, selecione **Proteção** > **Backup e Recuperação**.
2. Selecione **Inventário**.
3. Na página Inventário, selecione *Importar recursos do SnapCenter *.
4. Siga as etapas na seção *Importar recursos do SnapCenter * acima para importar recursos do SnapCenter .

Se você não tiver o SnapCenter instalado, adicione um vCenter e descubra recursos

Se você ainda não tiver o SnapCenter instalado, poderá adicionar informações do vCenter e fazer com que o backup e a recuperação do NetApp descubram cargas de trabalho. Em cada agente do Console, selecione os sistemas onde você deseja descobrir cargas de trabalho.

Isso é opcional se você tiver um ambiente VMware.

Passos

1. Na navegação à esquerda do Console, selecione **Proteção** > **Backup e Recuperação**.

   Se esta for a primeira vez que você faz login neste serviço, você já tem um sistema no Console, mas não descobriu nenhum recurso, a página inicial "Bem-vindo ao novo NetApp Backup and Recovery" aparece e mostra uma opção para **Descobrir recursos**.

2. Selecione **Descobrir recursos**.
3. Insira as seguintes informações:
   a. **Tipo de carga de trabalho**: Para esta versão, somente o Microsoft SQL Server está disponível.
   b. **Configurações do vCenter**: Selecione um vCenter existente ou adicione um novo. Para adicionar um novo vCenter, insira o FQDN ou endereço IP do vCenter, nome de usuário, senha, porta e protocolo.

      Se você estiver inserindo informações do vCenter, insira informações para as configurações do vCenter e o registro do Host. Se você adicionou ou inseriu informações do vCenter aqui, também precisará adicionar informações do plugin em Configurações avançadas.

   c. **Registro de host**: Selecione **Adicionar credenciais** e insira informações sobre os hosts que contêm as cargas de trabalho que você deseja descobrir.

      Se você estiver adicionando um servidor autônomo e não um servidor vCenter, insira apenas as informações do host.

4. Selecione **Descobrir**.

   Este processo pode levar alguns minutos.

5. Continue com Configurações avançadas.

Defina as opções de configurações avançadas durante a descoberta e instale o plugin

Com as Configurações avançadas, você pode instalar manualmente o agente do plugin em todos os servidores que estão sendo registrados. Isso permite que você importe todas as cargas de trabalho do SnapCenter para o NetApp Backup and Recovery para que você possa gerenciar backups e restaurações lá. O NetApp Backup and Recovery mostra as etapas necessárias para instalar o plugin.

Passos

1. Na página Descobrir recursos, continue até Configurações avançadas clicando na seta para baixo à direita.
2. Na página Descobrir recursos de carga de trabalho, insira as seguintes informações.
   - **Digite o número da porta do plug-in**: Digite o número da porta que o plug-in usa.

- **Caminho de instalação**: Digite o caminho onde o plugin será instalado.

3. Se você quiser instalar o agente SnapCenter manualmente, marque as caixas das seguintes opções:
   - **Usar instalação manual**: Marque esta caixa para instalar o plugin manualmente.
   - **Adicionar todos os hosts no cluster**: marque esta caixa para adicionar todos os hosts no cluster ao NetApp Backup and Recovery durante a descoberta.
   - **Ignorar verificações de pré-instalação opcionais**: marque esta caixa para ignorar verificações de pré-instalação opcionais. Você pode querer fazer isso, por exemplo, se souber que considerações de memória ou espaço serão alteradas em um futuro próximo e quiser instalar o plugin agora.
4. Selecione **Descobrir**.

Continue para o Painel de Backup e Recuperação da NetApp

1. Para exibir o Painel de Backup e Recuperação do NetApp , no menu Backup e Recuperação, selecione **Painel**.
2. Revise a saúde da proteção de dados. O número de cargas de trabalho em risco ou protegidas aumenta com base nas cargas de trabalho recém-descobertas, protegidas e armazenadas em backup.

   "Saiba o que o Painel mostra para você" .

Faça backup de cargas de trabalho do Microsoft SQL Server com o NetApp Backup and Recovery

Faça backup de dados de aplicativos do Microsoft SQL Server de sistemas ONTAP locais para Amazon Web Services, Microsoft Azure e StorageGRID para garantir que seus dados estejam protegidos. Os backups são gerados automaticamente e armazenados em um armazenamento de objetos na sua conta de nuvem pública ou privada.

- Para fazer backup de cargas de trabalho em um cronograma, crie políticas que controlem as operações de backup e restauração. Ver"Criar políticas" para obter instruções.
- Configure o diretório de log para hosts descobertos antes de iniciar um backup.
- Faça backup das cargas de trabalho agora (crie um backup sob demanda agora).

Exibir status de proteção da carga de trabalho

Antes de iniciar um backup, visualize o status de proteção das suas cargas de trabalho.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, administrador de backup e recuperação, administrador de restauração de backup e recuperação, administrador de clone de backup e recuperação ou função de visualizador de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.

4. Revise os detalhes nas guias Hosts, Grupos de proteção, Grupos de disponibilidade, Instâncias e Bancos de dados.

Configurar o diretório de log para hosts descobertos

Antes de fazer backup de suas cargas de trabalho, defina o caminho para os logs de atividades dos hosts descobertos. Isso ajuda você a rastrear o status das operações.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, administrador de backup de backup e recuperação ou função de administrador de restauração de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione um host.
5. Selecione o ícone Ações ••• > **Configurar diretório de log**.
6. Forneça o caminho do host ou navegue por uma lista de hosts ou nós no host para localizar onde você deseja que o log do host seja armazenado.
7. Selecione aqueles nos quais você deseja armazenar os logs.

   Os campos exibidos diferem dependendo do modelo de implantação selecionado, por exemplo, instância de cluster de failover ou autônomo.

8. Selecione **Salvar**.

Crie um grupo de proteção

Você pode criar um grupo de proteção para gerenciar as operações de backup e restauração de um conjunto de cargas de trabalho. Um grupo de proteção é um agrupamento lógico de cargas de trabalho que você deseja proteger juntas.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione **Criar grupo de proteção**.
6. Forneça um nome para o grupo de proteção.
7. Selecione as instâncias ou bancos de dados que você deseja incluir no grupo de proteção.
8. Selecione **Avançar**.

9. Selecione a **Política de backup** que você deseja aplicar ao grupo de proteção.

   Se você quiser criar uma política, selecione **Criar nova política** e siga as instruções para criar uma política. Ver "Criar políticas" para maiores informações.

10. Selecione **Avançar**.
11. Revise a configuração.
12. Selecione **Criar** para criar o grupo de proteção.

Faça backup de cargas de trabalho agora com um backup sob demanda

Crie um backup sob demanda imediatamente. Talvez você queira executar um backup sob demanda se estiver prestes a fazer alterações no seu sistema e quiser garantir que tenha um backup antes de começar.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupo de Proteção**, **Instâncias** ou **Bancos de Dados**.
5. Selecione a instância ou banco de dados que você deseja fazer backup.
6. Selecione o ícone Ações ••• > **Faça backup agora**.
7. Selecione a política que você deseja aplicar ao backup.
8. Selecione o nível de agendamento.
9. Selecione **Fazer backup agora**.

Suspender o agendamento de backup

Suspender o agendamento impede que o backup seja executado temporariamente no horário agendado. Talvez você queira fazer isso se estiver realizando manutenção no sistema ou se estiver tendo problemas com o backup.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupo de Proteção**, **Instâncias** ou **Bancos de Dados**.
5. Selecione o grupo de proteção, instância ou banco de dados que você deseja suspender.
6. Selecione o ícone Ações ••• > **Suspender**.

Excluir um grupo de proteção

Você pode criar um grupo de proteção para gerenciar as operações de backup e restauração de um conjunto de cargas de trabalho. Um grupo de proteção é um agrupamento lógico de cargas de trabalho que você deseja proteger juntas.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione o ícone Ações ••• > **Excluir grupo de proteção**.

Remover proteção de uma carga de trabalho

Você pode remover a proteção de uma carga de trabalho se não quiser mais fazer backup dela ou se quiser parar de gerenciá-la no NetApp Backup and Recovery.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupo de Proteção**, **Instâncias** ou **Bancos de Dados**.
5. Selecione o grupo de proteção, instância ou banco de dados.
6. Selecione o ícone Ações ••• > **Remover proteção**.
7. Na caixa de diálogo Remover proteção, selecione se deseja manter os backups e metadados ou excluí-los.
8. Selecione **Remover** para confirmar a ação.

Restaure cargas de trabalho do Microsoft SQL Server com o NetApp Backup and Recovery

Restaure cargas de trabalho do Microsoft SQL Server de cópias de snapshot, de um backup de carga de trabalho replicado para armazenamento secundário ou de backups armazenados em armazenamento de objetos usando o NetApp Backup and Recovery. Você pode restaurar uma carga de trabalho para o sistema original, para um sistema diferente que esteja usando a mesma conta de nuvem ou para um sistema ONTAP local.

Restaurar a partir desses locais

Você pode restaurar cargas de trabalho de diferentes locais de partida:

- Restaurar de um local primário
- Restaurar de um recurso replicado
- Restaurar de um backup de armazenamento de objetos

Restaurar esses pontos

Você pode restaurar dados para o snapshot mais recente ou para estes pontos:

- Restaurar a partir de instantâneos
- Restaurar para um ponto específico no tempo. Isso é útil se você souber o nome e a localização do arquivo, além da data em que ele esteve em boas condições pela última vez.
- Restaurar para o backup mais recente

Considerações sobre restauração de armazenamento de objetos

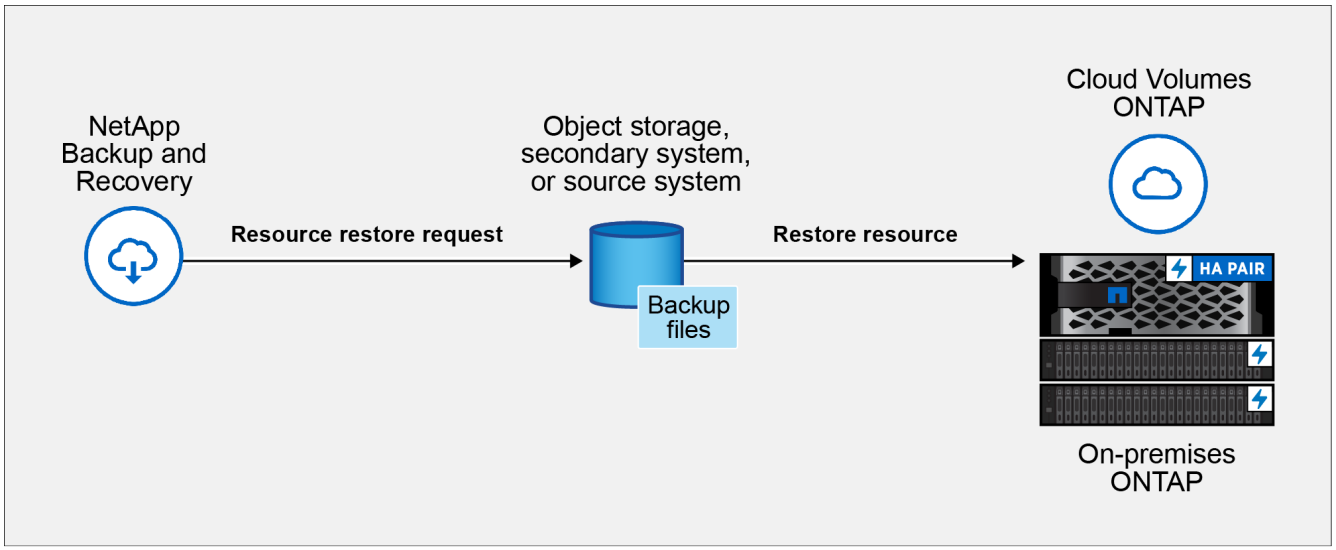
Se você selecionar um arquivo de backup no armazenamento de objetos e a Resiliência contra Ransomware estiver ativa para esse backup (se você habilitou o DataLock e a Resiliência contra Ransomware na política de backup), você será solicitado a executar uma verificação de integridade adicional no arquivo de backup antes de restaurar os dados. Recomendamos que você execute a verificação.

Você incorrerá em custos extras de saída do seu provedor de nuvem para acessar o conteúdo do arquivo de backup.

Como funciona a restauração de cargas de trabalho

Ao restaurar cargas de trabalho, ocorre o seguinte:

- Quando você restaura uma carga de trabalho de um arquivo de backup, o NetApp Backup and Recovery cria um *novo* recurso usando os dados do backup.
- Ao restaurar uma carga de trabalho replicada, você pode restaurar a carga de trabalho para o sistema original ou para um sistema ONTAP local.



- Ao restaurar um backup do armazenamento de objetos, você pode restaurar os dados para o sistema original ou para um sistema ONTAP local.

Métodos de restauração

Você pode restaurar cargas de trabalho usando um dos seguintes métodos. Normalmente, escolha um dos seguintes métodos com base nas suas necessidades de restauração:

- **Da página Restaurar**: Use isto quando precisar restaurar um recurso, mas não se lembra do nome exato ou do local em que ele reside, ou da data em que esteve em boas condições pela última vez. Você pode pesquisar o instantâneo usando filtros.
- **Da página Inventário**: Use isto quando precisar restaurar um recurso específico da última semana ou mês — e você souber o nome e a localização do recurso, além da data em que ele esteve em boas condições pela última vez. Navegue por uma lista de recursos para encontrar aquele que deseja restaurar.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Restaurar dados de carga de trabalho a partir da opção Restaurar

Restaure cargas de trabalho do banco de dados usando a opção Restaurar.

Passos

1. No menu NetApp Backup and Recovery, selecione **Restaurar**.
2. Selecione o banco de dados que você deseja restaurar. Utilize os filtros para pesquisar.
3. Selecione a opção de restauração:
    - Restaurar a partir de instantâneos
    - Restaurar para um ponto específico no tempo. Isso é útil se você souber o nome e a localização do arquivo, além da data em que ele esteve em boas condições pela última vez.
    - Restaurar para o backup mais recente

Restaurar cargas de trabalho de snapshots

1. Continuando na página Opções de restauração, selecione **Restaurar de instantâneos**.

   Uma lista de instantâneos é exibida.

2. Selecione o instantâneo que você deseja restaurar.
3. Selecione **Avançar**.

   Você verá as opções de destino em seguida.

4. Na página Detalhes do destino, insira as seguintes informações:
    - **Configurações de destino**: escolha se deseja restaurar os dados para o local original ou para um local alternativo. Para um local alternativo, selecione o nome do host e a instância, insira o nome do banco de dados e insira o caminho de destino onde deseja restaurar o instantâneo.
    - **Opções de pré-restauração**:
        - **Substituir o banco de dados com o mesmo nome durante a restauração**: Durante a restauração, o nome original do banco de dados é preservado.
        - **Manter configurações de replicação do banco de dados SQL**: mantém as configurações de replicação do banco de dados SQL após a operação de restauração.

        - **Criar backup do log de transações antes da restauração**: Cria um backup do log de transações antes da operação de restauração.*** Encerrar a restauração se o backup do log de transações antes da restauração falhar**: Interrompe a operação de restauração se o backup do log de transações falhar.
        - **Prescript**: Insira o caminho completo para um script que deve ser executado antes da operação de restauração, quaisquer argumentos que o script use e quanto tempo esperar para que o script seja concluído.
    - **Opções pós-restauração**:
        - **Operacional**, mas indisponível para restaurar logs de transações adicionais. Isso coloca o banco de dados online novamente depois que os backups do log de transações são aplicados.
        - **Não operacional**, mas disponível para restaurar logs de transações adicionais. Mantém o banco de dados em um estado não operacional após a operação de restauração enquanto restaura backups do log de transações. Esta opção é útil para restaurar logs de transações adicionais.
        - **Modo somente leitura** e disponível para restaurar logs de transações adicionais. Restaura o banco de dados em modo somente leitura e aplica backups de log de transações.
        - **Postscript**: Insira o caminho completo para um script que deve ser executado após a operação de restauração e quaisquer argumentos que o script aceite.
5. Selecione **Restaurar**.

Restaurar para um ponto específico no tempo

O NetApp Backup and Recovery usa logs e os snapshots mais recentes para criar uma restauração pontual dos seus dados.

1. Continuando na página Opções de restauração, selecione **Restaurar para um ponto específico no tempo**.
2. Selecione **Avançar**.
3. Na página Restaurar para um ponto específico no tempo, insira as seguintes informações:
    - **Data e hora para restauração de dados**: Insira a data e hora exatas dos dados que você deseja restaurar. Esta data e hora são do host do banco de dados Microsoft SQL Server.
4. Selecione **Pesquisar**.
5. Selecione o instantâneo que você deseja restaurar.
6. Selecione **Avançar**.
7. Na página Detalhes do destino, insira as seguintes informações:
    - **Configurações de destino**: escolha se deseja restaurar os dados para o local original ou para um local alternativo. Para um local alternativo, selecione o nome do host e a instância, insira o nome do banco de dados e insira o caminho de destino.
    - **Opções de pré-restauração**:
        - **Preservar nome original do banco de dados**: Durante a restauração, o nome original do banco de dados é preservado.
        - **Manter configurações de replicação do banco de dados SQL**: mantém as configurações de replicação do banco de dados SQL após a operação de restauração.
        - **Prescript**: Insira o caminho completo para um script que deve ser executado antes da operação de restauração, quaisquer argumentos que o script use e quanto tempo esperar para que o script seja concluído.

- **Opções pós-restauração**:
  - **Operacional**, mas indisponível para restaurar logs de transações adicionais. Isso coloca o banco de dados online novamente depois que os backups do log de transações são aplicados.
  - **Não operacional**, mas disponível para restaurar logs de transações adicionais. Mantém o banco de dados em um estado não operacional após a operação de restauração enquanto restaura backups do log de transações. Esta opção é útil para restaurar logs de transações adicionais.
  - **Modo somente leitura** e disponível para restaurar logs de transações adicionais. Restaura o banco de dados em modo somente leitura e aplica backups de log de transações.
  - **Postscript**: Insira o caminho completo para um script que deve ser executado após a operação de restauração e quaisquer argumentos que o script aceite.

8. Selecione **Restaurar**.

Restaurar para o backup mais recente

Esta opção usa os backups completos e de log mais recentes para restaurar seus dados ao último estado bom. O sistema verifica os logs do último instantâneo até o presente. O processo rastreia alterações e atividades para restaurar a versão mais recente e precisa dos seus dados.

1. Continuando na página Opções de restauração, selecione **Restaurar para o backup mais recente**.

   O NetApp Backup and Recovery mostra os snapshots disponíveis para a operação de restauração.

2. Na página Restaurar para o estado mais recente, selecione o local do instantâneo do armazenamento local, secundário ou de objeto.
3. Selecione **Avançar**.
4. Na página Detalhes do destino, insira as seguintes informações:
   - **Configurações de destino**: escolha se deseja restaurar os dados para o local original ou para um local alternativo. Para um local alternativo, selecione o nome do host e a instância, insira o nome do banco de dados e insira o caminho de destino.
   - **Opções de pré-restauração**:
     - **Substituir o banco de dados com o mesmo nome durante a restauração**: Durante a restauração, o nome original do banco de dados é preservado.
     - **Manter configurações de replicação do banco de dados SQL**: mantém as configurações de replicação do banco de dados SQL após a operação de restauração.
     - **Criar backup do log de transações antes da restauração**: Cria um backup do log de transações antes da operação de restauração.
     - **Encerrar a restauração se o backup do log de transações antes da restauração falhar**: Interrompe a operação de restauração se o backup do log de transações falhar.
     - **Prescript**: Insira o caminho completo para um script que deve ser executado antes da operação de restauração, quaisquer argumentos que o script use e quanto tempo esperar para que o script seja concluído.
   - **Opções pós-restauração**:
     - **Operacional**, mas indisponível para restaurar logs de transações adicionais. Isso coloca o banco de dados online novamente depois que os backups do log de transações são aplicados.
     - **Não operacional**, mas disponível para restaurar logs de transações adicionais. Mantém o banco de dados em um estado não operacional após a operação de restauração enquanto restaura backups do log de transações. Esta opção é útil para restaurar logs de transações adicionais.

- **Modo somente leitura** e disponível para restaurar logs de transações adicionais. Restaura o banco de dados em modo somente leitura e aplica backups de log de transações.
- **Postscript**: Insira o caminho completo para um script que deve ser executado após a operação de restauração e quaisquer argumentos que o script aceite.

5. Selecione **Restaurar**.

Restaurar dados de carga de trabalho da opção Inventário

Restaure cargas de trabalho do banco de dados na página Inventário. Usando a opção Inventário, você pode restaurar apenas bancos de dados, não instâncias.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Escolha o host onde o recurso que você deseja restaurar está localizado.
3. Selecione as **Ações*** ••• **ícone e selecione *Ver detalhes**.
4. Na página do Microsoft SQL Server, selecione a guia **Bancos de dados**.
5. Na guia Bancos de dados, selecione o banco de dados que mostra o status "Protegido", indicando que há um backup que você pode restaurar.
6. Selecione as **Ações*** ••• **ícone e selecione *Restaurar**.

   As mesmas três opções aparecem quando você restaura na página Restaurar:

   - Restaurar a partir de instantâneos
   - Restaurar para um ponto específico no tempo
   - Restaurar para o backup mais recente
7. Continue com os mesmos passos para a opção de restauração na página Restaurar

Clonar cargas de trabalho do Microsoft SQL Server com o NetApp Backup and Recovery

Clone dados de aplicativos do Microsoft SQL Server na mesma VM ou em uma VM diferente para fins de desenvolvimento, teste ou proteção usando o NetApp Backup and Recovery. Você pode criar clones a partir de snapshots instantâneos ou snapshots existentes de suas cargas de trabalho do Microsoft SQL Server.

Escolha entre os seguintes tipos de clones:

- **Snapshot e clone instantâneos**: Você pode criar um clone das suas cargas de trabalho do Microsoft SQL Server a partir de um snapshot instantâneo. Um snapshot instantâneo é uma cópia pontual dos dados de origem criada a partir de um backup. O clone é armazenado em um repositório de objetos na sua conta de nuvem pública ou privada. Você pode usar o clone para restaurar suas cargas de trabalho em caso de perda ou corrupção de dados.
- **Clonar de um snapshot existente**: Você pode escolher um snapshot existente em uma lista de snapshots disponíveis para a carga de trabalho. Esta opção é útil se você quiser criar um clone de um ponto específico no tempo. Clonar para armazenamento primário ou secundário.

Você pode atingir as seguintes metas de proteção:

- Criar um clone
- Atualizar um clone
- Dividir um clone
- Excluir um clone

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Criar um clone

Você pode criar um clone das suas cargas de trabalho do Microsoft SQL Server. Um clone é uma cópia dos dados de origem criada a partir de um backup. O clone é armazenado em um repositório de objetos na sua conta de nuvem pública ou privada. Você pode usar o clone para restaurar suas cargas de trabalho em caso de perda ou corrupção de dados.

Você pode criar um clone a partir de um snapshot existente ou de um snapshot instantâneo. Um snapshot instantâneo é uma cópia pontual dos dados de origem criada a partir de um backup. Você pode usar o clone para restaurar suas cargas de trabalho em caso de perda ou corrupção de dados.

Passos

1. No menu NetApp Backup and Recovery, selecione **Clonar**.
2. Selecione **Criar novo clone**.
3. Selecione o tipo de clone:
   - **Clonar e atualizar o banco de dados a partir do snapshot existente**: Escolha o snapshot para o clone e configure as opções para o clone. Isso é útil se você quiser escolher o instantâneo para o clone e configurar opções.
   - **Instantâneo e clone instantâneos**: Faça um instantâneo agora dos dados de origem e crie um clone a partir desse instantâneo. Esta opção é útil se você quiser criar um clone a partir dos dados mais recentes na carga de trabalho de origem.
4. Preencha a seção **Fonte do banco de dados**:
   - **Clone único ou clone em massa**: selecione se deseja criar um único clone ou vários clones. Se você selecionar **Clone em massa**, poderá criar vários clones de uma só vez usando um grupo de proteção que você já criou. Esta opção é útil se você quiser criar vários clones para diferentes cargas de trabalho.
   - **Host, instância e nome do banco de dados de origem**: Selecione o host, a instância e o nome do banco de dados de origem para o clone. O banco de dados de origem é o banco de dados a partir do qual o clone será criado.
5. Preencha a seção **Destino do banco de dados**:
   - **Host, instância e nome do banco de dados de destino**: Selecione o host, a instância e o nome do banco de dados de destino para o clone. O banco de dados de destino é o local onde o clone será criado.

     Opcionalmente, selecione **Sufixo** na lista suspensa de nomes de destino e anexe um sufixo ao nome do banco de dados clonado. Se você não especificar um sufixo, o nome do banco de dados clonado será o mesmo que o nome do banco de dados de origem.

   - **QoS (taxa de transferência máxima)**: Selecione a taxa de transferência máxima da qualidade de serviço (QoS) em MBps para o clone. O QoS define as características de desempenho do clone, como

a taxa de transferência máxima e IOPS.

6. Complete a seção **Montar**:
   - **Atribuir ponto de montagem automaticamente**: Selecione esta opção para atribuir automaticamente um ponto de montagem para o clone. O ponto de montagem é o local onde o clone será montado no armazenamento de objetos.
   - **Definir caminho do ponto de montagem**: Insira um ponto de montagem para o clone. O ponto de montagem é o local onde o clone será montado no armazenamento de objetos. Selecione a letra da unidade, insira o caminho do arquivo de dados e insira o caminho do arquivo de log.
7. Selecione **Avançar**.
8. Selecione o ponto de restauração:
   - **Snapshots existentes**: selecione um snapshot existente na lista de snapshots disponíveis para a carga de trabalho. Esta opção é útil se você quiser criar um clone de um ponto específico no tempo.
   - **Snapshot e clone instantâneos**: Selecione o snapshot mais recente na lista de snapshots disponíveis para a carga de trabalho. Esta opção é útil se você quiser criar um clone a partir dos dados mais recentes na carga de trabalho de origem.
9. Se você escolher criar **Instantâneo instantâneo e clone**, escolha o local de armazenamento do clone:
   - **Armazenamento local**: Selecione esta opção para criar o clone no armazenamento local do sistema ONTAP . O armazenamento local é o armazenamento que está diretamente conectado ao sistema ONTAP .
   - **Armazenamento secundário**: Selecione esta opção para criar o clone no armazenamento secundário do sistema ONTAP . O armazenamento secundário é o armazenamento usado para cargas de trabalho de backup e recuperação.
10. Selecione o local de destino para os dados e registros.
11. Selecione **Avançar**.
12. Preencha a seção **Opções avançadas**.
13. Se você escolheu **Instant snapshot and clone**, complete as seguintes opções:
    - **Cronograma de atualização e expiração do clone**: Se você escolher **Clone instantâneo**, insira a data em que deseja iniciar a atualização do clone. O cronograma de clone define quando o clone será criado.
      - **Excluir clone se o agendamento expirar**: Se você quiser excluir o clone na data de expiração do clone.
      - **Atualizar clone a cada**: Selecione com que frequência o clone deve ser atualizado. Você pode optar por atualizar o clone a cada hora, dia, semana, mês ou trimestre. Esta opção é útil se você quiser manter o clone atualizado com a carga de trabalho de origem.
    - **Prescritos e pós-escritos**: Opcionalmente, especifique scripts pré e pós-clone para serem executados antes e depois da criação do clone. Esses scripts podem ser usados para executar tarefas adicionais, como configurar o clone ou enviar notificações.
    - **Notificação**: Opcionalmente, especifique endereços de e-mail para receber notificações sobre o status da criação do clone junto com o relatório do trabalho. Você também pode especificar um URL de webhook para receber notificações sobre o status de criação do clone. Você pode especificar se deseja notificações de sucesso e falha ou apenas uma ou outra.
    - **Tags**: Selecione um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos e selecione **Aplicar**. Por exemplo, se você adicionar "RH" como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
14. Selecione **Criar**.

15. Quando o clone for criado, você poderá visualizá-lo na página **Inventário**.

Atualizar um clone

Você pode atualizar um clone de suas cargas de trabalho do Microsoft SQL Server. Atualizar um clone atualiza o clone com os dados mais recentes da carga de trabalho de origem. Isso é útil se você quiser manter o clone atualizado com a carga de trabalho de origem.

Você tem a opção de alterar o nome do banco de dados, usar o snapshot instantâneo mais recente ou atualizar a partir de um snapshot de produção existente.

Passos

1. No menu NetApp Backup and Recovery, selecione **Clonar**.
2. Selecione o clone que você deseja atualizar.
3. Selecione o ícone Ações ••• > **Atualizar clone**.
4. Preencha a seção **Configurações avançadas**:
   - **Escopo de recuperação**: escolha se deseja recuperar todos os backups de log ou os backups de log até um momento específico. Esta opção é útil se você quiser recuperar o clone para um ponto específico no tempo.
   - **Cronograma de atualização e expiração do clone**: Se você escolher **Clone instantâneo**, insira a data em que deseja iniciar a atualização do clone. O cronograma de clone define quando o clone será criado.
     - **Excluir clone se o agendamento expirar**: Se você quiser excluir o clone na data de expiração do clone.
     - **Atualizar clone a cada**: Selecione com que frequência o clone deve ser atualizado. Você pode optar por atualizar o clone a cada hora, dia, semana, mês ou trimestre. Esta opção é útil se você quiser manter o clone atualizado com a carga de trabalho de origem.
   - **Configurações do iGroup**: Selecione o igroup para o clone. O igroup é um agrupamento lógico de iniciadores que são usados para acessar o clone. Você pode selecionar um igroup existente ou criar um novo. Selecione o igroup do sistema de armazenamento ONTAP primário ou secundário.
   - **Prescritos e pós-escritos**: Opcionalmente, especifique scripts pré e pós-clone para serem executados antes e depois da criação do clone. Esses scripts podem ser usados para executar tarefas adicionais, como configurar o clone ou enviar notificações.
   - **Notificação**: Opcionalmente, especifique endereços de e-mail para receber notificações sobre o status da criação do clone junto com o relatório do trabalho. Você também pode especificar um URL de webhook para receber notificações sobre o status de criação do clone. Você pode especificar se deseja notificações de sucesso e falha ou apenas uma ou outra.
   - **Tags**: Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar "RH" como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
5. Na caixa de diálogo de confirmação de atualização, para continuar, selecione **Atualizar**.

Pular uma atualização de clone

Talvez você queira pular uma atualização de clone se não quiser atualizar o clone com os dados mais recentes da carga de trabalho de origem. Pular uma atualização de clone permite que você mantenha o clone como está sem atualizá-lo.

Passos

1. No menu NetApp Backup and Recovery, selecione **Clonar**.
2. Selecione o clone cuja atualização você deseja pular.
3. Selecione o ícone Ações ••• > **Ignorar atualização**.
4. Na caixa de diálogo de confirmação de Ignorar atualização, faça o seguinte:
   a. Para pular apenas a próxima programação de atualização, selecione **Ignorar apenas a próxima programação de atualização**.
   b. Para continuar, selecione **Ignorar**.

Dividir um clone

Você pode dividir um clone de suas cargas de trabalho do Microsoft SQL Server. Dividir um clone cria um novo backup a partir do clone. O novo backup pode ser usado para restaurar as cargas de trabalho.

Você pode escolher dividir um clone em clones independentes ou de longo prazo. Um assistente mostra a lista de agregados que fazem parte do SVM, seus tamanhos e onde o volume clonado reside. O NetApp Backup and Recovery também indica se há espaço suficiente para dividir o clone. Após o clone ser dividido, ele se torna um banco de dados independente para proteção.

O trabalho de clonagem não pode ser removido e pode ser reutilizado para outros clones.

Passos

1. No menu NetApp Backup and Recovery, selecione **Clonar**.
2. Selecione um clone.
3. Selecione o ícone Ações ••• > **Clone dividido**.
4. Revise os detalhes do clone dividido e selecione **Dividir**.
5. Quando o clone dividido for criado, você poderá visualizá-lo na página **Inventário**.

Excluir um clone

Você pode excluir um clone de suas cargas de trabalho do Microsoft SQL Server. Excluir um clone remove o clone do armazenamento de objetos e libera espaço de armazenamento.

Se o clone estiver protegido por uma política, o clone será excluído, incluindo o trabalho.

Passos

1. No menu NetApp Backup and Recovery, selecione **Clonar**.
2. Selecione um clone.
3. Selecione o ícone Ações ••• > **Excluir clone**.
4. Na caixa de diálogo de confirmação de exclusão do clone, revise os detalhes da exclusão.
   a. Para excluir os recursos clonados do SnapCenter , mesmo que os clones ou seu armazenamento não estejam acessíveis, selecione **Forçar exclusão**.
   b. Selecione **Excluir**.
5. Quando o clone é excluído, ele é removido da página **Inventário**.

Gerencie o inventário do Microsoft SQL Server com o NetApp Backup and Recovery

O NetApp Backup and Recovery permite que você gerencie informações do host de carga de trabalho, informações do banco de dados e informações de instâncias do Microsoft SQL Server. Você pode visualizar, editar e excluir configurações de proteção do seu inventário.

Você pode realizar as seguintes tarefas relacionadas ao gerenciamento do seu inventário:

- Gerenciar informações do host
  - Suspender horários
  - Editar ou excluir hosts
- Gerenciar informações de instâncias
  - Associar credenciais a um recurso
  - Faça backup agora iniciando um backup sob demanda
  - Editar configurações de proteção
- Gerenciar informações do banco de dados
  - Proteger bancos de dados
  - Restaurar bancos de dados
  - Editar configurações de proteção
  - Faça backup agora iniciando um backup sob demanda
- Configure o diretório de log (em Inventário > Hosts). Se você quiser fazer backup de logs para seus hosts de banco de dados no snapshot, primeiro configure os logs no NetApp Backup and Recovery. Para mais detalhes, consulte"Configurar as configurações de backup e recuperação do NetApp" .

Gerenciar informações do host

Você pode gerenciar as informações do host para garantir que os hosts certos estejam protegidos. Você pode visualizar, editar e excluir informações do host.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, administrador de backup de backup e recuperação, administrador de restauração de backup e recuperação ou função de administrador de clone de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

- Configurar diretório de log. Para mais detalhes, consulte"Configurar as configurações de backup e recuperação do NetApp" .
- Suspender horários
- Editar um host
- Excluir um host

Gerenciar hosts

Você pode gerenciar os hosts descobertos no seu sistema. Você pode gerenciá-los separadamente ou em grupo.

Você pode gerenciar apenas os hosts que mostram o status "Não gerenciado" na coluna Hosts. Se o status for "Gerenciado", significa que o host já está sendo gerenciado pelo NetApp Backup and Recovery.

Depois de gerenciar os hosts no NetApp Backup and Recovery, o SnapCenter não gerencia mais os recursos nesses hosts.

Função necessária do NetApp Console Visualizador de armazenamento ou superadministrador de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Hosts**.
5. Selecione um ou mais hosts. Se você selecionar vários hosts, uma opção Ações em massa será exibida, onde você poderá selecionar **Gerenciar (até 5 hosts)**.
6. Selecione o ícone Ações ••• > **Gerenciar**.
7. Revise as dependências do host:
   - Se o vCenter não for exibido, selecione o ícone de lápis para adicionar ou editar os detalhes do vCenter.
   - Se você adicionar um vCenter, também deverá registrá-lo selecionando **Registrar vCenter**.
8. Selecione **Validar configurações** para testar suas configurações.
9. Selecione **Gerenciar** para gerenciar o host.

Suspender horários

Você pode suspender agendamentos para interromper as operações de backup e restauração de um host. Talvez você queira fazer isso se precisar realizar atividades de manutenção no host.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione o host no qual você deseja suspender os agendamentos.
3. Selecione as **Ações*** ••• **ícone e selecione *Suspender agendamentos**.
4. Na caixa de diálogo de confirmação, selecione **Suspender**.

Editar um host

Você pode alterar as informações do servidor vCenter, as credenciais de registro do host e as opções de configurações avançadas.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione o host que você deseja editar.
3. Selecione as **Ações*** ••• **ícone e selecione *Editar host**.
4. Edite as informações do host.

5. Selecione **Concluído**.

Excluir um host

Você pode excluir as informações do host para interromper as cobranças de serviço.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione o host que você deseja excluir.
3. Selecione as **Ações*** ••• **ícone e selecione *Excluir host**.
4. Revise as informações de confirmação e selecione **Excluir**.

Gerenciar informações de instâncias

Você pode gerenciar informações de instâncias para garantir que os recursos tenham as credenciais apropriadas para proteção e pode fazer backup de recursos das seguintes maneiras:

- Proteger instâncias
- Credenciais de associado
- Desassociar credenciais
- Proteção de edição
- Faça backup agora

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Proteger instâncias de banco de dados

Você pode atribuir uma política a uma instância de banco de dados usando políticas que controlam os agendamentos e a retenção da proteção de recursos.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione a carga de trabalho que você deseja visualizar e selecione **Exibir**.
3. Selecione a aba **Instâncias**.
4. Selecione a instância.
5. Selecione as **Ações*** ••• **ícone e selecione *Proteger**.
6. Selecione uma política ou crie uma nova.

   Para obter detalhes sobre como criar uma política, consulte"Criar uma política" .

7. Forneça informações sobre os scripts que você deseja executar antes e depois do backup.
   - **Pré-script**: insira o nome do arquivo do script e o local para executá-lo automaticamente antes que a ação de proteção seja acionada. Isso é útil para executar tarefas ou configurações adicionais que precisam ser executadas antes do fluxo de trabalho de proteção.
   - **Pós-script**: Insira o nome do arquivo do script e o local para executá-lo automaticamente após a conclusão da ação de proteção. Isso é útil para executar tarefas ou configurações adicionais que

precisam ser executadas após o fluxo de trabalho de proteção.

8. Forneça informações sobre como você deseja que o snapshot seja verificado:
   - Local de armazenamento: selecione o local onde o instantâneo de verificação será armazenado.
   - Recurso de verificação: selecione se o recurso que você deseja verificar está no snapshot local e no armazenamento secundário ONTAP .
   - Cronograma de verificação: selecione a frequência: horária, diária, semanal, mensal ou anual.

Associar credenciais a um recurso

Você pode associar credenciais a um recurso para que a proteção possa ocorrer.

Para obter detalhes, consulte "Configurar as configurações de backup e recuperação do NetApp , incluindo credenciais" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione a carga de trabalho que você deseja visualizar e selecione **Exibir**.
3. Selecione a aba **Instâncias**.
4. Selecione a instância.
5. Selecione as **Ações*** ••• **ícone e selecione *Associar credenciais**.
6. Use credenciais existentes ou crie novas.

Editar configurações de proteção

Você pode alterar a política, criar uma nova política, definir um cronograma e definir configurações de retenção.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione a carga de trabalho que você deseja visualizar e selecione **Exibir**.
3. Selecione a aba **Instâncias**.
4. Selecione a instância.
5. Selecione as **Ações*** ••• **ícone e selecione *Editar proteção**.

   Para obter detalhes sobre como criar uma política, consulte"Criar uma política" .

Faça backup agora

Você pode fazer backup dos seus dados agora para garantir que eles sejam protegidos imediatamente.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione a carga de trabalho que você deseja visualizar e selecione **Exibir**.
3. Selecione a aba **Instâncias**.
4. Selecione a instância.
5. Selecione as **Ações*** ••• **ícone e selecione *Fazer backup agora**.

6. Escolha o tipo de backup e defina o agendamento.

   Para obter detalhes sobre como criar um backup ad hoc, consulte"Criar uma política" .

Gerenciar informações do banco de dados

Você pode gerenciar informações do banco de dados das seguintes maneiras:

- Proteger bancos de dados
- Restaurar bancos de dados
- Ver detalhes de proteção
- Editar configurações de proteção
- Faça backup agora

Proteger bancos de dados

Você pode alterar a política, criar uma nova política, definir um cronograma e definir configurações de retenção.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione a carga de trabalho que você deseja visualizar e selecione **Exibir**.
3. Selecione a aba **Bancos de dados**.
4. Selecione o banco de dados.
5. Selecione as **Ações*** ••• **ícone e selecione *Proteger**.

   Para obter detalhes sobre como criar uma política, consulte"Criar uma política" .

Restaurar bancos de dados

Você pode restaurar um banco de dados para garantir que seus dados estejam protegidos.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

1. Selecione a aba **Bancos de dados**.
2. Selecione o banco de dados.
3. Selecione as **Ações*** ••• **ícone e selecione *Restaurar**.

   Para obter informações sobre como restaurar cargas de trabalho, consulte"Restaurar cargas de trabalho" .

Editar configurações de proteção

Você pode alterar a política, criar uma nova política, definir um cronograma e definir configurações de retenção.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione a carga de trabalho que você deseja visualizar e selecione **Exibir**.
3. Selecione a aba **Bancos de dados**.
4. Selecione o banco de dados.
5. Selecione as **Ações*** ••• **ícone e selecione *Editar proteção**.

   Para obter detalhes sobre como criar uma política, consulte"Criar uma política" .

Faça backup agora

Você pode fazer backup de suas instâncias e bancos de dados do Microsoft SQL Server agora para garantir que seus dados sejam protegidos imediatamente.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione a carga de trabalho que você deseja visualizar e selecione **Exibir**.
3. Selecione a aba **Instâncias** ou **Bancos de dados**.
4. Selecione a instância ou banco de dados.
5. Selecione as **Ações*** ••• **ícone e selecione *Fazer backup agora**.

Gerencie snapshots do Microsoft SQL Server com o NetApp Backup and Recovery

Você pode gerenciar snapshots do Microsoft SQL Server excluindo-os do NetApp Backup and Recovery.

Excluir um instantâneo

Você pode excluir somente snapshots locais.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No NetApp Backup and Recovery, selecione **Inventário**.

2. Selecione a carga de trabalho e selecione **Exibir**.
3. Selecione a aba **Bancos de dados**.
4. Selecione o banco de dados do qual você deseja excluir um snapshot.
5. No menu Ações, selecione **Exibir detalhes de proteção**.
6. Selecione o instantâneo local que você deseja excluir.

   O ícone de instantâneo local na coluna **Localização** dessa linha deve aparecer em azul.

7. Selecione as **Ações*** ícone e selecione *Excluir instantâneo local**.
8. Na caixa de diálogo de confirmação, selecione **Remover**.

Crie relatórios para cargas de trabalho do Microsoft SQL Server no NetApp Backup and Recovery

No NetApp Backup and Recovery, crie relatórios para cargas de trabalho do Microsoft SQL Server para visualizar o status dos seus backups, incluindo o número de backups, o número de backups bem-sucedidos e o número de backups com falha. Você também pode visualizar os detalhes de cada backup, incluindo o tipo de backup, o sistema de armazenamento usado para o backup e a hora do backup.

Criar um relatório

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, administrador de backup e recuperação, administrador de restauração de backup e recuperação, administrador de clone de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

1. No menu NetApp Backup and Recovery, selecione a opção **Relatórios**.
2. Selecione **Criar relatório**.
3. Insira os detalhes do escopo do relatório:
   - **Nome do relatório**: insira um nome exclusivo para o relatório.
   - **Tipo de relatório**: Escolha se deseja um relatório por conta ou por carga de trabalho (Microsoft SQL Server).
   - **Selecionar host**: Se você selecionou por carga de trabalho, selecione o host para o qual deseja gerar o relatório.
   - **Selecionar conteúdo**: Escolha se deseja que o relatório inclua um resumo de todos os backups ou detalhes de cada backup. (Se você escolheu "Por conta")
4. Insira o intervalo do relatório: escolha se deseja que o relatório inclua dados do último dia, dos últimos 7 dias, dos últimos 30 dias, do último trimestre ou do último ano.
5. Insira os detalhes de entrega do relatório: Se desejar que o relatório seja entregue por e-mail, marque **Enviar relatório por e-mail**. Insira os endereços de e-mail para onde você deseja que o relatório seja enviado.

   Configure notificações por e-mail na página Configurações. Para obter detalhes sobre como configurar notificações por e-mail, consulte"Configurar definições" .

Proteja as cargas de trabalho do VMware (visualização sem o plug-in SnapCenter para VMware)

Visão geral da proteção de cargas de trabalho do VMware com o NetApp Backup and Recovery

Proteja suas VMs e armazenamentos de dados VMware com o NetApp Backup and Recovery. O NetApp Backup and Recovery oferece operações de backup e restauração rápidas, com economia de espaço, consistentes em caso de falhas e consistentes com VMs. Você pode fazer backup de cargas de trabalho do VMware no Amazon Web Services S3 ou StorageGRID e restaurar cargas de trabalho do VMware em um host VMware local.

Esta versão do NetApp Backup and Recovery oferece suporte apenas ao VMware vCenter e não descobre vVols ou VMs em vVols.

Use o NetApp Backup and Recovery para implementar uma estratégia 3-2-1, na qual você tem 3 cópias dos seus dados de origem em 2 sistemas de armazenamento diferentes, além de 1 cópia na nuvem. Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados fornecem proteção multicamadas contra ameaças de segurança cibernética internas e externas.
- Vários tipos de mídia garantem a viabilidade de failover no caso de falha física ou lógica de um tipo de mídia.
- A cópia no local facilita restaurações rápidas, com cópias externas disponíveis caso a cópia no local seja comprometida.

NOTA Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery, consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Você pode usar o NetApp Backup and Recovery para executar as seguintes tarefas relacionadas às cargas de trabalho do VMware:

- "Descubra as cargas de trabalho da VMware"
- "Crie e gerencie grupos de proteção para cargas de trabalho do VMware"
- "Fazer backup de cargas de trabalho do VMware"
- "Restaurar cargas de trabalho do VMware"

Descubra cargas de trabalho VMware com NetApp Backup and Recovery

O serviço NetApp Backup and Recovery precisa primeiro descobrir datastores e VMs VMware em execução em sistemas ONTAP para que você possa usar o serviço. Opcionalmente, você pode importar dados e políticas de backup do SnapCenter Plug-in for VMware vSphere se já o tiver instalado.

Função de console necessária Superadministrador de backup e recuperação. Aprenda sobre"Funções e

privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Descubra cargas de trabalho do VMware e, opcionalmente, importe recursos do SnapCenter

Durante a descoberta, o NetApp Backup and Recovery analisa as cargas de trabalho do VMware na sua organização e avalia e importa políticas de proteção existentes, cópias de instantâneos e opções de backup e restauração.

Você pode importar datastores e VMs VMware NFS e VMFS do SnapCenter Plug-in for VMware vSphere para o inventário do NetApp Backup and Recovery.

> Esta versão do NetApp Backup and Recovery oferece suporte apenas ao VMware vCenter e não descobre vVols ou VMs em vVols.

Durante o processo de importação, o NetApp Backup and Recovery executa as seguintes tarefas:

- Permite acesso SSH seguro ao servidor vCenter.
- Ativa o modo de manutenção em todos os Grupos de Recursos no servidor vCenter.
- Prepara os metadados do vCenter e os marca como não gerenciados no NetApp Console.
- Configura o acesso ao banco de dados.
- Descobre o VMware vCenter, datastores e VMs.
- Importa políticas de proteção existentes, cópias de instantâneos e opções de backup e restauração do SnapCenter Plug-in for VMware vSphere.
- Exibe os recursos descobertos na página Inventário de backup e recuperação da NetApp .

A descoberta ocorre das seguintes maneiras:

- Se você já tiver o SnapCenter Plug-in for VMware vSphere, importe os recursos do SnapCenter para o NetApp Backup and Recovery usando a interface do usuário do NetApp Backup and Recovery.

  > Se você já tiver o SnapCenter Plug-in, certifique-se de atender aos pré-requisitos antes de importar do SnapCenter. Por exemplo, você deve criar sistemas no NetApp Console para todo o armazenamento de cluster SnapCenter local antes de importar do SnapCenter. Ver "Pré-requisitos para importar recursos do SnapCenter" .

- Se você ainda não tiver o plug-in SnapCenter , ainda poderá descobrir cargas de trabalho em seus sistemas adicionando um vCenter manualmente e executando a descoberta.

Se o plug-in SnapCenter ainda não estiver instalado, adicione um vCenter e descubra recursos

Se você ainda não tiver o SnapCenter Plug-in para VMware instalado, adicione informações do vCenter e faça com que o NetApp Backup and Recovery descubra cargas de trabalho. Em cada agente do Console, selecione os sistemas onde você deseja descobrir cargas de trabalho.

Passos

1. Na navegação à esquerda do NetApp Console, selecione **Proteção** > **Backup e recuperação**.

   Se esta for a primeira vez que você faz login neste serviço, você já tem um sistema no Console, mas não descobriu nenhum recurso, a página inicial "Bem-vindo ao novo NetApp Backup and Recovery" aparece e mostra uma opção para **Descobrir recursos**.

2. Selecione **Descobrir recursos**.
3. Insira as seguintes informações:
   a. **Tipo de carga de trabalho**: Selecione **VMware**.
   b. **Configurações do vCenter**: Adicione um novo vCenter. Para adicionar um novo vCenter, insira o FQDN ou endereço IP do vCenter, nome de usuário, senha, porta e protocolo.

      Se você estiver inserindo informações do vCenter, insira informações para as configurações do vCenter e o registro do Host. Se você adicionou ou inseriu informações do vCenter aqui, também precisará adicionar informações do plugin em Configurações avançadas.

   c. **Registro de host**: Não necessário para VMware.
4. Selecione **Descobrir**.

   Este processo pode levar alguns minutos.

5. Continue com Configurações avançadas.

Se o SnapCenter Plug-in já estiver instalado, importe os recursos do SnapCenter Plug-in para VMware no NetApp Backup and Recovery

Se você já tiver o SnapCenter Plug-in para VMware instalado, importe os recursos do SnapCenter Plug-in para o NetApp Backup and Recovery seguindo estas etapas. O Console descobre hosts ESXi, datastores e VMs em vCenters e agenda a partir do Plug-in; você não precisa recriar todas essas informações.

Você pode fazer isso das seguintes maneiras:

- Durante a descoberta, selecione uma opção para importar recursos do plug-in SnapCenter .
- Após a descoberta, na página Inventário, selecione uma opção para importar recursos do plug-in SnapCenter .
- Após a descoberta, no menu Configurações, selecione uma opção para importar recursos do plug-in SnapCenter . Para obter detalhes, consulte "Configurar o NetApp Backup and Recovery" . Isso não é suportado pelo VMware.

Este é um processo de duas partes descrito nesta seção:

1. Importe os metadados do vCenter do plug-in SnapCenter . Os recursos importados do vCenter ainda não são gerenciados pelo NetApp Backup and Recovery.
2. Inicie o gerenciamento de vCenters, VMs e datastores selecionados no NetApp Backup and Recovery. Depois de iniciar o gerenciamento, o NetApp Backup and Recovery rotula o vCenter como "Gerenciado" na página Inventário e consegue fazer backup e recuperar os recursos que você importou. Depois de iniciar o gerenciamento no NetApp Backup and Recovery, você não gerencia mais esses recursos no SnapCenter Plug-in.

Importar metadados do vCenter do plug-in SnapCenter

Esta primeira etapa importa os metadados do vCenter do plug-in SnapCenter . Nesse ponto, os recursos ainda não são gerenciados pelo NetApp Backup and Recovery.

Depois de importar metadados do vCenter do plug-in SnapCenter , o NetApp Backup and Recovery não assume o gerenciamento de proteção automaticamente. Para fazer isso, você deve selecionar explicitamente gerenciar os recursos importados no NetApp Backup and Recovery. Isso garante que você esteja pronto para ter esses recursos armazenados em backup pelo NetApp Backup and Recovery.

Passos

1. Na navegação à esquerda do Console, selecione **Proteção** > **Backup e Recuperação**.
2. Selecione **Inventário**.
3. Na página Descobrir recursos de carga de trabalho do NetApp Backup and Recovery, selecione **Importar do SnapCenter**.
4. No campo Importar de, selecione * SnapCenter Plug-in para VMware*.
5. Insira as **credenciais do VMware vCenter**:
   a. **IP/nome do host do vCenter**: insira o FQDN ou endereço IP do vCenter que você deseja importar para o NetApp Backup and Recovery.
   b. **Número da porta do vCenter**: insira o número da porta do vCenter.
   c. **Nome de usuário e *Senha** do vCenter: insira o nome de usuário e a senha do vCenter.
   d. **Conector**: Selecione o agente do Console para o vCenter.
6. Insira * Credenciais do host do plug-in SnapCenter *:
   a. **Credenciais existentes**: Se você selecionar esta opção, poderá usar as credenciais existentes que você já adicionou. Escolha o nome das credenciais.
   b. **Adicionar novas credenciais**: Se você não tiver credenciais de host do SnapCenter Plug-in existentes, poderá adicionar novas credenciais. Digite o nome das credenciais, o modo de autenticação, o nome de usuário e a senha.
7. Selecione **Importar** para validar suas entradas e registrar o plug-in SnapCenter .

Se o plug-in SnapCenter já estiver registrado, você poderá atualizar os detalhes de registro existentes.

Resultado

A página Inventário mostra o vCenter como não gerenciado no NetApp Backup and Recovery até que você selecione explicitamente gerenciá-lo.

Gerenciar recursos importados do plug-in SnapCenter

Depois de importar os metadados do vCenter do SnapCenter Plug-in para VMware, gerencie os recursos no NetApp Backup and Recovery. Depois de selecionar o gerenciamento desses recursos, o NetApp Backup and Recovery poderá fazer backup e recuperar os recursos que você importou. Depois de iniciar o gerenciamento no NetApp Backup and Recovery, você não gerencia mais esses recursos no SnapCenter Plug-in.

Depois de selecionar o gerenciamento dos recursos, os recursos, as VMs e as políticas são importados do SnapCenter Plug-in para VMware. Os grupos de recursos, políticas e snapshots são migrados do plug-in e passam a ser gerenciados no NetApp Backup and Recovery.

Passos

1. Depois de importar os recursos do VMware do SnapCenter Plug-in, no menu Backup e Recuperação, selecione **Inventário**.

2. Na página Inventário, selecione o vCenter importado que você deseja que o NetApp Backup and Recovery gerencie a partir de agora.
3. Selecione o ícone Ações ••• > **Ver detalhes** para exibir os detalhes da carga de trabalho.
4. Na página Inventário > carga de trabalho, selecione o ícone Ações ••• > **Gerenciar** para exibir a página Gerenciar vCenter.
5. Marque a caixa "Deseja continuar com a migração?" e selecione **Migrar**.

Resultado

A página Inventário mostra os recursos do vCenter recém-gerenciados.

Crie e gerencie grupos de proteção para cargas de trabalho VMware com o NetApp Backup and Recovery

Crie grupos de proteção para gerenciar as operações de backup e restauração de um conjunto de cargas de trabalho. Um grupo de proteção é um agrupamento lógico de recursos, como VMs e armazenamentos de dados, que você deseja proteger juntos.

Você pode executar as seguintes tarefas relacionadas a grupos de proteção:

- Crie um grupo de proteção.
- Ver detalhes da proteção.
- Crie um grupo de proteção agora. Ver "Faça backup das cargas de trabalho do VMware agora" .
- Suspenda e retome o agendamento de backup de um grupo de proteção.
- Excluir um grupo de proteção.

Crie um grupo de proteção

Agrupe as cargas de trabalho que você deseja proteger em um grupo de proteção. Você pode criar um grupo de proteção para um conjunto de cargas de trabalho que deseja fazer backup e restaurar juntas.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione **Criar grupo de proteção**.
6. Forneça um nome para o grupo de proteção.
7. Selecione as VMs ou bancos de dados que você deseja incluir no grupo de proteção.
8. Selecione **Avançar**.
9. Selecione a **Política de backup** que você deseja aplicar ao grupo de proteção.

   Se você quiser criar uma política, selecione **Criar nova política** e siga as instruções para criar uma

política. Ver "Criar políticas" para maiores informações.

10. Selecione **Avançar**.
11. Revise a configuração.
12. Selecione **Criar** para criar o grupo de proteção.

Suspender o agendamento de backup de um grupo de proteção

Suspender um grupo de proteção pausa os backups agendados para o grupo de proteção. Talvez você queira suspender um grupo de proteção se quiser interromper temporariamente os backups das cargas de trabalho nesse grupo.

O status da proteção muda para "Em manutenção" quando você suspende um grupo de proteção. Você pode retomar o agendamento de backup a qualquer momento.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione o ícone Ações ••• > **Suspender grupo de proteção**.
6. Revise a mensagem de confirmação e selecione **Suspender**.

Retomar o cronograma de backup de um grupo de proteção

Retomar um grupo de proteção suspenso reinicia os backups agendados para o grupo de proteção.

O status da proteção muda de "Em manutenção" quando você suspende um grupo de proteção para "Protegido" quando você o retoma. Você pode retomar o agendamento de backup a qualquer momento.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione o ícone Ações ••• > **Grupo de proteção de currículos**.
6. Revise a mensagem de confirmação e selecione **Continuar**.

Resultado

O sistema valida os agendamentos e altera o status da proteção para "Protegido" se os agendamentos forem válidos. Se os agendamentos não forem válidos, o sistema exibirá uma mensagem de erro e não retomará o grupo de proteção.

Excluir um grupo de proteção

A exclusão de um grupo de proteção o remove, juntamente com todos os agendamentos de backup associados. Talvez você queira excluir um grupo de proteção se ele não for mais necessário.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione o grupo de proteção que você deseja excluir.
6. Selecione o ícone Ações ••• > **Excluir**.
7. Revise a mensagem de confirmação sobre a exclusão dos backups associados e confirme a exclusão.

Faça backup de cargas de trabalho do VMware com o NetApp Backup and Recovery

Faça backup de VMs e datastores VMware de sistemas ONTAP locais para Amazon Web Services, Azure NetApp Files ou StorageGRID para garantir que seus dados estejam protegidos. Os backups são gerados automaticamente e armazenados em um armazenamento de objetos na sua conta de nuvem pública ou privada.

- Para fazer backup de cargas de trabalho em um cronograma, crie políticas que controlem as operações de backup e restauração. Ver"Criar políticas" para obter instruções.
- Crie grupos de proteção para gerenciar as operações de backup e restauração de um conjunto de recursos. Ver "Crie e gerencie grupos de proteção para cargas de trabalho VMware com o NetApp Backup and Recovery" para maiores informações.
- Faça backup das cargas de trabalho agora (crie um backup sob demanda agora).

Faça backup de cargas de trabalho agora com um backup sob demanda

Crie um backup sob demanda imediatamente. Talvez você queira executar um backup sob demanda se estiver prestes a fazer alterações no seu sistema e quiser garantir que tenha um backup antes de começar.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu Backup e Recuperação, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**, **Datastores** ou **Máquinas virtuais**.
5. Selecione o grupo de proteção, os armazenamentos de dados ou as máquinas virtuais dos quais você deseja fazer backup.
6. Selecione o ícone Ações ••• > **Faça backup agora**.

   A política aplicada ao backup é a mesma política atribuída ao grupo de proteção, ao armazenamento de dados ou à máquina virtual.

7. Selecione o nível de agendamento.
8. Selecione **Fazer backup agora**.

Restaure cargas de trabalho do VMware com o NetApp Backup and Recovery

Restaure cargas de trabalho do VMware de cópias de snapshot, de um backup de carga de trabalho replicado para armazenamento secundário ou de backups armazenados em armazenamento de objetos usando o NetApp Backup and Recovery.

Restaurar a partir desses locais

Você pode restaurar cargas de trabalho de diferentes locais de partida:

- Restaurar de um local primário (instantâneo local)
- Restaurar de um recurso replicado no armazenamento secundário
- Restaurar de um backup de armazenamento de objetos

Restaurar esses pontos

Você pode restaurar dados para estes pontos:

- Restaurar para o local original

Considerações sobre restauração de armazenamento de objetos

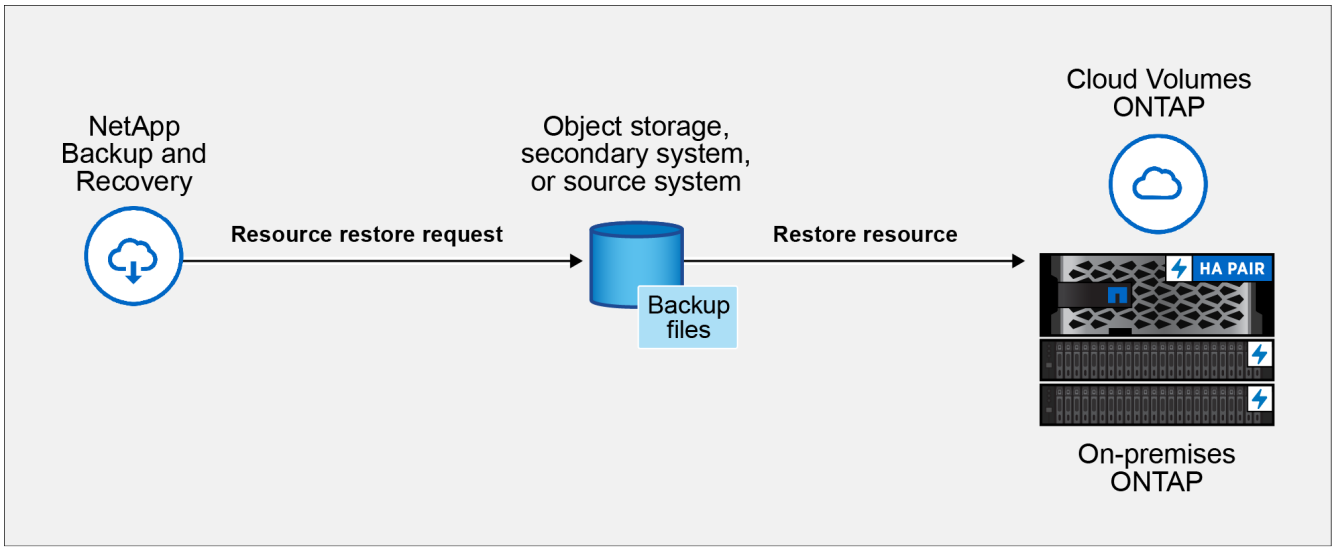
Se você selecionar um arquivo de backup no armazenamento de objetos e a proteção contra ransomware estiver ativa para esse backup (se você habilitou o DataLock e o Ransomware Resilience na política de backup), você será solicitado a executar uma verificação de integridade adicional no arquivo de backup antes de restaurar os dados. Recomendamos que você execute a verificação.

Você incorrerá em custos extras de saída do seu provedor de nuvem para acessar o conteúdo do arquivo de backup.

Como funciona a restauração de cargas de trabalho

Ao restaurar cargas de trabalho, ocorre o seguinte:

- Quando você restaura uma carga de trabalho de um arquivo de backup local, o NetApp Backup and Recovery cria um *novo* recurso usando os dados do backup.
- Ao restaurar uma carga de trabalho replicada, você pode restaurar a carga de trabalho para o sistema original ou para um sistema ONTAP local.



- Ao restaurar um backup do armazenamento de objetos, você pode restaurar os dados para o sistema original ou para um sistema ONTAP local.

Na página Restaurar (também conhecida como Pesquisar e Restaurar), você pode restaurar um recurso, mesmo que não se lembre do nome exato, do local em que ele reside ou da data em que esteve em boas condições pela última vez. Você pode pesquisar o instantâneo usando filtros.

Restaurar dados de carga de trabalho a partir da opção Restaurar (Pesquisar e Restaurar)

Restaure cargas de trabalho do VMware usando a opção Restaurar. Você pode procurar o instantâneo pelo nome ou usando filtros.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, função de administrador de restauração de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Restaurar**.
2. Na lista suspensa à direita do campo de pesquisa de nome, selecione **Máquinas virtuais**.
3. Insira o nome do recurso que você deseja restaurar ou filtre pelo vCenter, datacenter ou armazenamento de dados onde o recurso que você deseja restaurar está localizado.

   Aparece uma lista de instantâneos que correspondem aos seus critérios de pesquisa.

4. Selecione o instantâneo que você deseja restaurar.

   Uma lista de opções de local de restauração é exibida.

5. Selecione o local de restauração onde você deseja restaurar o instantâneo:
   - Local: restaura o instantâneo para o local original.
   - Armazenamento secundário: restaura o instantâneo em um local de armazenamento secundário.

     Se você escolher o armazenamento secundário, insira as informações de origem e destino, bem como os locais de origem e secundário dos logs.

   - Armazenamento de objetos: restaura o instantâneo em um local de armazenamento de objetos.

     Se você escolher o armazenamento de objetos, verifique se deseja verificar o instantâneo novamente antes de restaurá-lo.

6. Selecione **Concluído** ou **Avançar** para continuar para a página Restaurar configurações de destino.

   Em seguida, você pode escolher as configurações de destino e as opções de pré e pós-restauração.

Seleção de destino

1. Escolha as configurações de destino e as opções de pré e pós-restauração.

Restaurar para o local original

Na página Detalhes do destino da restauração, insira as seguintes informações:

1. **Ativar restauração rápida**: selecione esta opção para executar uma operação de restauração rápida. Os volumes e dados restaurados estarão disponíveis imediatamente. Não use isso em volumes que exigem alto desempenho porque, durante o processo de restauração rápida, o acesso aos dados pode ser mais lento que o normal.
2. **Opções de pré-restauração**: insira o caminho completo para um script que deve ser executado antes da operação de restauração e quaisquer argumentos que o script aceite.
3. **Opções pós-restauração**:
   - **Reiniciar VM**: selecione esta opção para reiniciar a VM após a conclusão da operação de restauração e após a aplicação do script pós-restauração.
   - **Postscript**: Insira o caminho completo para um script que deve ser executado após a operação de restauração e quaisquer argumentos que o script aceite.
4. Seção **Notificação**:
   - **Ativar notificações por e-mail**: selecione esta opção para receber notificações por e-mail sobre a operação de restauração e indique que tipo de notificação você deseja receber.
5. Selecione **Restaurar**.

Restaurar para local alternativo

Não disponível para visualização do VMware.

1. Selecione **Restaurar**.

Proteja as cargas de trabalho do VMware (com o plug-in SnapCenter para VMware)

Visão geral sobre proteção de cargas de trabalho de máquinas virtuais no NetApp Backup and Recovery

Proteja as cargas de trabalho das suas máquinas virtuais com o NetApp Backup and Recovery. O NetApp Backup and Recovery oferece operações de backup e restauração rápidas, com economia de espaço, consistentes em caso de falhas e consistentes com VMs, repositórios de dados e VMDKs.

Você pode fazer backup de datastores no Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform e StorageGRID e restaurar máquinas virtuais de volta para o host SnapCenter Plug-in for VMware vSphere local.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Para obter instruções sobre como proteger cargas de trabalho de máquinas virtuais, consulte os seguintes tópicos:

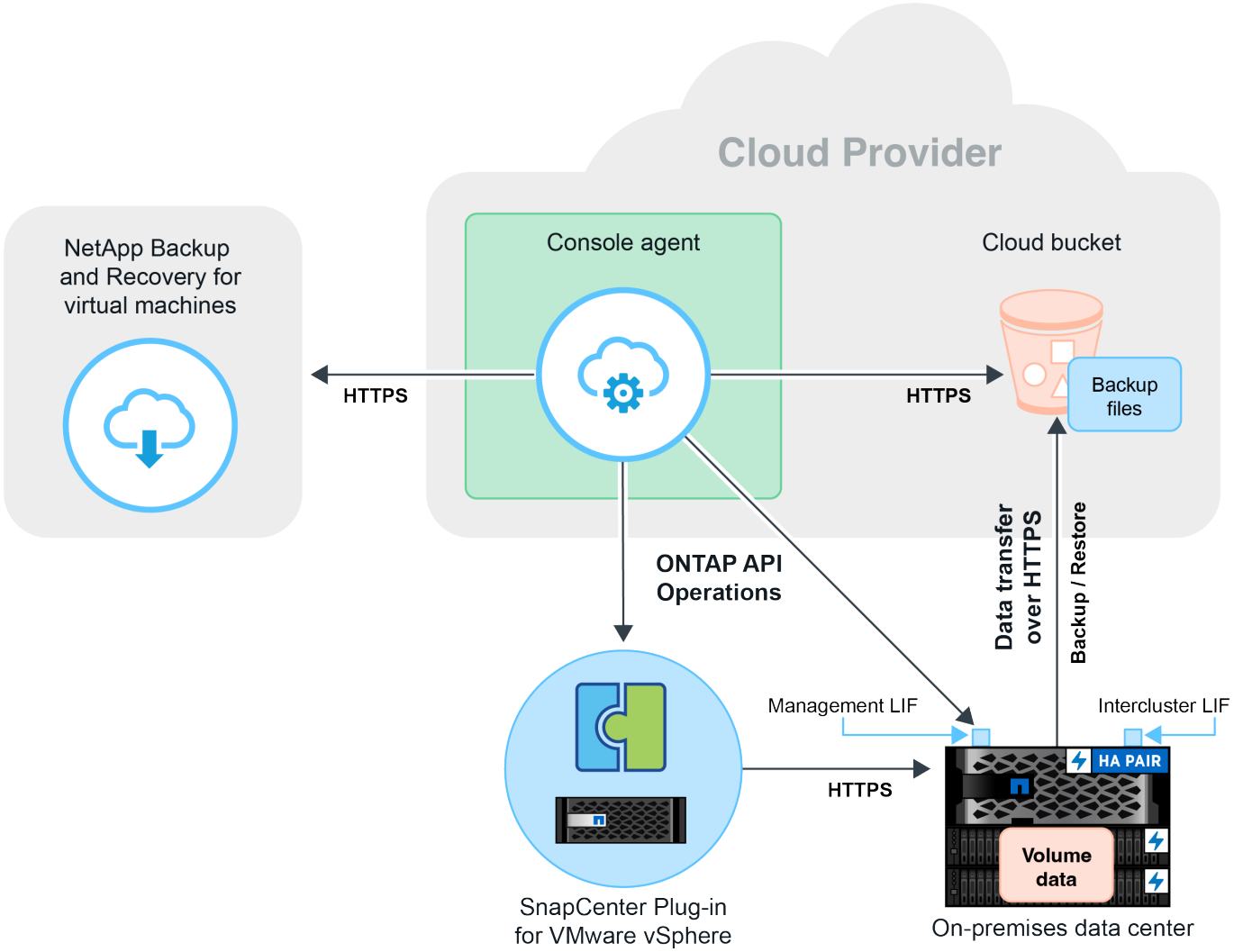
- "Crie uma política para cargas de trabalho do VMware"
- "Fazer backup de datastores VMware no Amazon Web Services"
- "Fazer backup de datastores VMware no Microsoft Azure"
- "Faça backup dos datastores do VMware no Google Cloud Platform"
- "Fazer backup de datastores VMware no StorageGRID"
- "Restaurar cargas de trabalho do VMware"
- "Gerenciar proteção para cargas de trabalho VMware"

Pré-requisitos para cargas de trabalho de máquinas virtuais no NetApp Backup and Recovery

Antes de começar a proteger suas cargas de trabalho de máquinas virtuais com o NetApp Backup and Recovery, certifique-se de atender aos seguintes pré-requisitos:

- SnapCenter Plug-in for VMware vSphere 4.6P1 ou posterior
  - Você deve usar o SnapCenter Plug-in for VMware vSphere 4.7P1 ou posterior para fazer backup de datastores do armazenamento secundário local.
- ONTAP 9.8 ou posterior
- Console NetApp
- Os armazenamentos de dados NFS e VMFS são suportados. Os vVols não são suportados.
- Para suporte ao VMFS, o SnapCenter Plug-in for VMware vSphere deve estar em execução na versão 4.9 ou posterior. Certifique-se de fazer um backup do armazenamento de dados VMFS se o SnapCenter Plug-in for VMware vSphere foi atualizado de uma versão anterior para a versão 4.9.
- Pelo menos um backup deve ter sido feito no SnapCenter Plug-in for VMware vSphere 4.6P1.
- Pelo menos uma política diária, semanal ou mensal no SnapCenter Plug-in for VMware vSphere sem rótulo ou com o mesmo rótulo da política de Máquinas Virtuais no Console.
- Para uma política predefinida, a camada de agendamento deve ser a mesma para o armazenamento de dados no SnapCenter Plug-in for VMware vSphere e na nuvem.
- Certifique-se de que não haja volumes FlexGroup no armazenamento de dados, pois o backup e a restauração de volumes FlexGroup não são suportados.
- Desabilite "**_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 na nuvem e, consequentemente, 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 da máquina virtual, como VMDK, VMX, VMSD e assim por diante.
- Certifique-se de que o armazenamento de dados de destino não tenha arquivos de máquina virtual obsoletos no formato restore_xxx_xxxxxx_filename de falhas de operação de restauração anteriores. Você deve excluir os arquivos obsoletos antes de iniciar uma operação de restauração.
- Para implantar um conector com proxy configurado, certifique-se de que todas as chamadas de saída do conector sejam roteadas pelo servidor proxy.
- Se um volume que faz backup de um armazenamento de dados já estiver protegido na guia Volumes (NetApp Backup and Recovery → Volumes), o mesmo armazenamento de dados não poderá ser protegido novamente na guia Máquinas virtuais (NetApp Backup and Recovery → Máquinas virtuais).

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



Registre o SnapCenter Plug-in for VMware vSphere para usar com o NetApp Backup and Recovery

Você deve registrar o SnapCenter Plug-in for VMware vSphere no NetApp Backup and Recovery para que os datastores e máquinas virtuais sejam exibidos. Somente um usuário com acesso administrativo pode registrar o SnapCenter Plug-in for VMware vSphere .

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Passos

1. Na interface do usuário do NetApp Console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais**.
2. No menu suspenso **Configurações**, selecione * SnapCenter Plug-in for VMware vSphere*.
3. Selecione **Registrar SnapCenter Plug-in for VMware vSphere**.

4. Especifique os seguintes detalhes:
    a. No campo SnapCenter Plug-in for VMware vSphere , especifique o FQDN ou endereço IP do host SnapCenter Plug-in for VMware vSphere .
    b. No campo Porta, especifique o número da porta na qual o host do SnapCenter Plug-in for VMware vSphere está sendo executado.

        Você deve garantir que a comunicação esteja aberta entre o host local do SnapCenter Plug-in for VMware vSphere , que está sendo executado na porta padrão 8144, e a instância do agente do Console, que pode estar sendo executada 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. Selecione **Registrar**.

Depois que você terminar

Selecione **Backup e recuperação** > **Máquinas virtuais** para visualizar todos os armazenamentos de dados e máquinas virtuais que estão protegidos usando o SnapCenter Plug-in for VMware vSphere .

Crie uma política para fazer backup de datastores no NetApp Backup and Recovery

Você pode criar uma política ou usar uma das seguintes políticas predefinidas disponíveis no NetApp Backup and Recovery.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

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 arquivo, 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 ao arquivo para cada provedor de nuvem.

Sobre esta tarefa

As seguintes políticas predefinidas estão disponíveis no NetApp Console:

Nome da Política	Rótulo	Valor de retenção
LTR diário de 1 ano (retenção de longo prazo)	Diário	366
5 anos de LTR diário	Diário	1830
LTR semanal de 7 anos	Semanalmente	370

Nome da Política	Rótulo	Valor de retenção
LTR mensal de 10 anos	Mensal	120

Passos

1. Na página Máquinas virtuais, na lista suspensa Configurações, selecione **Políticas**.
2. Selecione **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 retidos.
5. Selecione Primário ou Secundário como fonte de armazenamento de backup.
6. (Opcional) Se você quiser mover backups do armazenamento de objetos para o armazenamento de arquivamento após um determinado número de dias para otimização de custos, marque a caixa de seleção **Backups em camadas para arquivamento** e insira o número de dias após os quais o backup deve ser arquivado.
7. Selecione **Criar**.

Você não pode editar ou excluir uma política que esteja associada a um armazenamento de dados.

Faça backup de datastores no Amazon Web Services no NetApp Backup and Recovery

Você pode fazer backup e arquivar um ou mais armazenamentos de dados com o NetApp Backup and Recovery para Amazon Web Services para melhorar a eficiência do armazenamento e a transição para a nuvem.

Se o armazenamento de dados estiver associado a uma política de arquivamento, você terá a opção de selecionar a camada de arquivamento. Os níveis de arquivamento suportados são Glacier e Glacier Deep.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Antes de começar

Certifique-se de ter cumprido todos os"requisitos de proteção de máquina virtual" antes de fazer backup dos armazenamentos de dados na nuvem.

Passos

1. Na interface do usuário do console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais**.
2. Selecione ••• correspondente ao armazenamento de dados que você deseja fazer backup e clique em **Ativar backup**.
3. Na página Atribuir política, selecione a política e selecione **Avançar**.
4. Adicione o sistema.

   Configure o LIF de gerenciamento de cluster que você deseja que o Console descubra. Depois de

adicionar o sistema para um dos datastores, ele pode ser reutilizado para todos os outros datastores que residem no mesmo cluster ONTAP .

a. Selecione **Adicionar sistema** correspondente ao SVM.
b. No assistente Adicionar sistema:
    i. Especifique o endereço IP do LIF de gerenciamento do cluster.
    ii. Especifique as credenciais do usuário do cluster ONTAP .
c. Selecione **Adicionar sistema**.

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 você deseja criar os backups.
    e. Especifique os endereços IP do LIF de gerenciamento de cluster que foram adicionados como sistemas.
    f. Selecione a camada de arquivamento.

    É recomendável definir a camada de arquivamento porque essa é uma atividade única e não pode ser configurá-la posteriormente.

6. Revise os detalhes e selecione **Ativar backup**.

Faça backup de datastores no Microsoft Azure com o NetApp Backup and Recovery

Você pode fazer backup de um ou mais armazenamentos de dados no Microsoft Azure integrando o SnapCenter Plug-in for VMware vSphere com o NetApp Backup and Recovery. Isso ajudará os administradores de VM a fazer backup e arquivar dados de forma fácil e rápida para eficiência de armazenamento e acelerar a transição para a nuvem.

Se o armazenamento de dados estiver associado a uma política de arquivamento, você terá a opção de selecionar a camada de arquivamento. A camada de arquivamento com suporte é o Azure Archive Blob Storage.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Antes de começar

Certifique-se de ter cumprido todos os"requisitos de proteção de máquina virtual" antes de fazer backup dos armazenamentos de dados na nuvem.

Passos

1. Na interface do usuário do NetApp Console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais**.

2. Selecione ••• correspondente ao armazenamento de dados que você deseja fazer backup e selecione **Ativar backup**.
3. Na página Atribuir política, selecione a política e selecione **Avançar**.
4. Adicione o sistema.

   Configure o LIF de gerenciamento de cluster que você deseja que o Console descubra. Depois de adicionar o sistema para um dos datastores, ele pode ser reutilizado para todos os outros datastores que residem no mesmo cluster ONTAP .

   a. Selecione **Adicionar sistema** correspondente ao SVM.
   b. No assistente Adicionar sistema:
      i. Especifique o endereço IP do LIF de gerenciamento do cluster.
      ii. Especifique as credenciais do usuário do cluster ONTAP .
   c. Selecione **Adicionar sistema**.
5. Selecione **Microsoft Azure** para configurá-lo como o provedor de nuvem.
   a. Especifique o ID da assinatura do Azure.
   b. Selecione a região onde você 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 sistemas.
   e. Selecione a camada de arquivamento.

      É recomendável definir a camada de arquivamento porque esta é uma atividade única e você não poderá configurá-la posteriormente.
6. Revise os detalhes e selecione **Ativar backup**.

Faça backup de armazenamentos de dados no Google Cloud Platform com o NetApp Backup and Recovery

Você pode fazer backup de um ou mais armazenamentos de dados no Google Cloud Platform integrando o SnapCenter Plug-in for VMware vSphere com o NetApp Backup and Recovery. Isso ajudará os administradores de VM a fazer backup e arquivar dados de forma fácil e rápida para eficiência de armazenamento e acelerar a transição para a nuvem.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Antes de começar

Certifique-se de ter cumprido todos os"requisitos de proteção de máquina virtual" antes de fazer backup dos armazenamentos de dados na nuvem.

Passos

1. Na interface do usuário do NetApp Console, selecione **Proteção** > **Backup e recuperação** > **Máquinas**

virtuais.

2. Selecione ••• correspondente ao armazenamento de dados que você deseja fazer backup e selecione **Ativar backup**.
3. Na página Atribuir política, selecione a política e selecione **Avançar**.
4. Adicione o sistema.

   Configure o LIF de gerenciamento de cluster que você deseja que o Console descubra. Depois de adicionar o sistema para um dos datastores, ele pode ser reutilizado para todos os outros datastores que residem no mesmo cluster ONTAP .

   a. Selecione **Adicionar sistema** correspondente ao SVM.
   b. No assistente Adicionar sistema:
      i. Especifique o endereço IP do LIF de gerenciamento do cluster.
      ii. Especifique as credenciais do usuário do cluster ONTAP .
   c. Selecione **Adicionar sistema**.
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 você deseja criar os backups.
   e. Especifique o espaço IP.
6. Revise os detalhes e selecione **Ativar backup**.

Faça backup de datastores no StorageGRID com o NetApp Backup and Recovery

Você pode fazer backup de um ou mais armazenamentos de dados no StorageGRID integrando o SnapCenter Plug-in for VMware vSphere com o NetApp Backup and Recovery. Isso ajudará os administradores de VM a fazer backup e arquivar dados de forma fácil e rápida para eficiência de armazenamento e acelerar a transição para a nuvem.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Antes de começar

Certifique-se de ter cumprido todos os"requisitos de proteção de máquina virtual" antes de fazer backup dos armazenamentos de dados na nuvem.

Passos

1. Na interface do usuário do NetApp Console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais**.
2. Selecione ••• correspondente ao armazenamento de dados que você deseja fazer backup e clique em **Ativar backup**.

3. Na página Atribuir política, selecione a política e selecione **Avançar**.
4. Adicione o sistema.

   Configure o LIF de gerenciamento de cluster que você deseja que o Console descubra. Depois de adicionar o sistema para um dos datastores, ele pode ser reutilizado para todos os outros datastores que residem no mesmo cluster ONTAP .

   a. Selecione **Adicionar sistema** correspondente ao SVM.
   b. No assistente Adicionar sistema:
      i. Especifique o endereço IP do LIF de gerenciamento do cluster.
      ii. Especifique as credenciais do usuário do cluster ONTAP .
   c. Selecione **Adicionar sistema**.
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 selecione **Ativar backup**.

Gerencie a proteção de datastores e VMs no NetApp Backup and Recovery

Você pode visualizar políticas, armazenamentos de dados e máquinas virtuais antes de fazer backup e restaurar dados com o NetApp Backup and Recovery. Dependendo da alteração no banco de dados, nas políticas ou nos grupos de recursos, você pode visualizar as atualizações na interface do usuário do NetApp Console.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Ver políticas

Você pode visualizar todas as políticas padrão predefinidas. Para cada uma dessas políticas, quando você visualiza os detalhes, todas as políticas e máquinas virtuais associadas são listadas.

1. Na interface do usuário do console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais**.
2. No menu suspenso **Configurações**, selecione **Políticas**.
3. Selecione **Exibir detalhes** correspondente à apólice cujos detalhes você deseja visualizar.

As políticas e máquinas virtuais associadas são listadas.

Exibir armazenamentos de dados e máquinas virtuais

Os datastores e máquinas virtuais protegidos usando o SnapCenter Plug-in for VMware vSphere são exibidos.

Passos

1. Na interface do usuário do console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais** > **Configurações** > * SnapCenter Plug-in for VMware vSphere*.
2. Selecione o SnapCenter Plug-in for VMware vSphere cujos datastores e máquinas virtuais você deseja

ver.

Desproteger armazenamentos de dados

Você pode desproteger um armazenamento de dados que já estava protegido anteriormente. Você pode desproteger um armazenamento de dados quando quiser excluir os backups na nuvem ou não quiser mais fazer backup na nuvem. O armazenamento de dados pode ser protegido novamente após a desproteção ser bem-sucedida.

Passos

1. Na interface do usuário do console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais**.
2. Selecione o ícone Ações ••• correspondente ao armazenamento de dados que você deseja desproteger e selecione **Desproteger**.

Editar o SnapCenter Plug-in for VMware vSphere

Você pode editar os detalhes do SnapCenter Plug-in for VMware vSphere no Console.

Passos

1. Na interface do usuário do console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais** > **Configurações** > * SnapCenter Plug-in for VMware vSphere*.
2. Selecione o ícone Ações ••• e selecione **Editar**.
3. Modifique os detalhes conforme necessário.
4. Selecione **Salvar**.

Atualizar recursos e backups

Se quiser visualizar os últimos armazenamentos de dados e backups que foram adicionados ao aplicativo, atualize os recursos e backups. Isso iniciará a descoberta dos recursos e backups e os detalhes mais recentes serão exibidos.

1. Selecione **Backup e Recuperação** > **Máquinas Virtuais**.
2. No menu suspenso **Configurações**, selecione * SnapCenter Plug-in for VMware vSphere*.
3. Selecione o ícone Ações ••• correspondente ao SnapCenter Plug-in for VMware vSphere e selecione **Atualizar recursos e backups**.

Atualizar política ou grupo de recursos

Se houver uma alteração na política ou no grupo de recursos, você deverá atualizar o relacionamento de proteção.

1. Selecione **Backup e Recuperação** > **Máquinas Virtuais**.
2. Selecione o ícone Ações ••• correspondente ao armazenamento de dados e selecione **Atualizar proteção**.

Cancelar registro do SnapCenter Plug-in for VMware vSphere

Todos os armazenamentos de dados e máquinas virtuais associados ao SnapCenter Plug-in for VMware vSphere ficarão desprotegidos.

1. Selecione **Backup e Recuperação** > **Máquinas Virtuais**.

2. No menu suspenso **Configurações**, selecione * SnapCenter Plug-in for VMware vSphere*.
3. Selecione o ícone Ações ••• correspondente ao SnapCenter Plug-in for VMware vSphere e selecione **Cancelar registro**.

Monitorar empregos

Os trabalhos são criados para todas as operações de backup e recuperação do NetApp . Você pode monitorar todos os trabalhos e todas as subtarefas que são executadas como parte de cada tarefa.

1. Selecione **Backup e recuperação** > **Monitoramento de tarefas**.

   Quando você inicia uma operação, uma janela aparece informando que o trabalho foi iniciado. Você pode selecionar o link para monitorar o trabalho.

2. Selecione a tarefa principal para visualizar as subtarefas e o status de cada uma delas.

Restaure dados de máquinas virtuais com o NetApp Backup and Recovery

Você pode restaurar dados de máquinas virtuais da nuvem para o vCenter local com o NetApp Backup and Recovery. Você pode restaurar a máquina virtual exatamente no mesmo local de onde o backup foi feito ou em um local alternativo. Se o backup da máquina virtual foi feito usando a política de arquivamento, você pode definir a prioridade de restauração de arquivamento.

Não é possível restaurar máquinas virtuais que abrangem vários repositórios de dados.

NOTA Para alternar entre cargas de trabalho de backup e recuperação do NetApp , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

Antes de começar

- Certifique-se de ter cumprido todos os"requisitos de proteção de máquina virtual" antes de fazer backup dos armazenamentos de dados na nuvem.
- Se você estiver restaurando para um local alternativo:
  - Certifique-se de que os vCenters de origem e destino estejam no modo vinculado.
  - Certifique-se de que os detalhes do cluster de origem e destino sejam adicionados na página **Sistemas** do NetApp Console e no modo vinculado dos vCenters no SnapCenter Plug-in for VMware vSphere .
  - Certifique-se de que o sistema seja adicionado correspondente ao local alternativo na página **Sistemas** do Console.

Passos

1. Na interface do usuário do console, selecione **Proteção** > **Backup e recuperação** > **Máquinas virtuais** > * SnapCenter Plug-in for VMware vSphere* e selecione o host do SnapCenter Plug-in for VMware vSphere .

Se a máquina virtual de origem for movida para outro local (vMotion) e se o usuário acionar uma restauração dessa máquina virtual no Console, a máquina virtual será restaurada para o local de origem de onde o backup foi feito.

1. Você pode restaurar a máquina virtual para o local original ou para um local alternativo a partir do armazenamento de dados ou de máquinas virtuais:

Se você quiser restaurar a máquina virtual…	Faça isso…
para o local original do armazenamento de dados	1. Selecione o ícone Ações ••• correspondente ao armazenamento de dados que você deseja restaurar e clique em **Exibir detalhes**. 2. Selecione **Restaurar** correspondente ao backup que você deseja restaurar. 3. Selecione a máquina virtual que você deseja restaurar do backup e selecione **Avançar**. 4. Certifique-se de que **Original** esteja selecionado e selecione **Continuar**. 5. Se a máquina virtual estiver protegida usando uma política em que as configurações de arquivamento são definidas, selecione **Prioridade de restauração de arquivamento** e selecione **Avançar**. As prioridades de restauração de arquivamento suportadas para Amazon Web Services são alta, padrão e baixa, e as prioridades de restauração de arquivamento suportadas para Microsoft Azure são alta e padrão. 6. Revise os detalhes e selecione **Restaurar**.

Se você quiser restaurar a máquina virtual…	Faça isso…
para um local alternativo do armazenamento de dados	1. Selecione o ícone Ações ••• correspondente ao armazenamento de dados que você deseja restaurar e selecione **Exibir detalhes**. 2. Selecione **Restaurar** correspondente ao backup que você deseja restaurar. 3. Selecione a máquina virtual que você deseja restaurar do backup e selecione **Avançar**. 4. Selecione **Alternativo**. 5. Selecione o vCenter Server, o host ESXi, o armazenamento de dados e a rede alternativos. 6. Forneça um nome para a VM após a restauração e selecione **Continuar**. 7. Se a máquina virtual estiver protegida usando uma política em que as configurações de arquivamento são definidas, selecione **Prioridade de restauração de arquivamento** e selecione **Avançar**. As prioridades de restauração de arquivamento suportadas para Amazon Web Services são alta, padrão e baixa, e as prioridades de restauração de arquivamento suportadas para Microsoft Azure são alta e padrão. 8. Revise os detalhes e selecione **Restaurar**.
para o local original das máquinas virtuais	1. Selecione o ícone Ações ••• correspondente à máquina virtual que você deseja restaurar e selecione **Restaurar**. 2. Selecione o backup por meio do qual você deseja restaurar a máquina virtual. 3. Certifique-se de que **Original** esteja selecionado e selecione **Continuar**. 4. Se a máquina virtual estiver protegida usando uma política em que as configurações de arquivamento são definidas, selecione **Prioridade de restauração de arquivamento** e selecione **Avançar**. As prioridades de restauração de arquivamento suportadas para Amazon Web Services são alta, padrão e baixa, e as prioridades de restauração de arquivamento suportadas para Microsoft Azure são alta e padrão. 5. Revise os detalhes e selecione **Restaurar**.

Se você quiser restaurar a máquina virtual…	Faça isso…
para um local alternativo de máquinas virtuais	1. Selecione o ícone Ações ••• correspondente à máquina virtual que você deseja restaurar e selecione **Restaurar**. 2. Selecione o backup por meio do qual você deseja restaurar a máquina virtual. 3. Selecione **Alternativo**. 4. Selecione o vCenter Server, o host ESXi, o armazenamento de dados e a rede alternativos. 5. Forneça um nome para a VM após a restauração e selecione **Continuar**. 6. Se a máquina virtual estiver protegida usando uma política em que as configurações de arquivamento são definidas, selecione **Prioridade de restauração de arquivamento** e selecione **Avançar**. As prioridades de restauração de arquivamento suportadas para Amazon Web Services são alta, padrão e baixa, e as prioridades de restauração de arquivamento suportadas para Microsoft Azure são alta e padrão. 7. Revise os detalhes e selecione **Restaurar**.

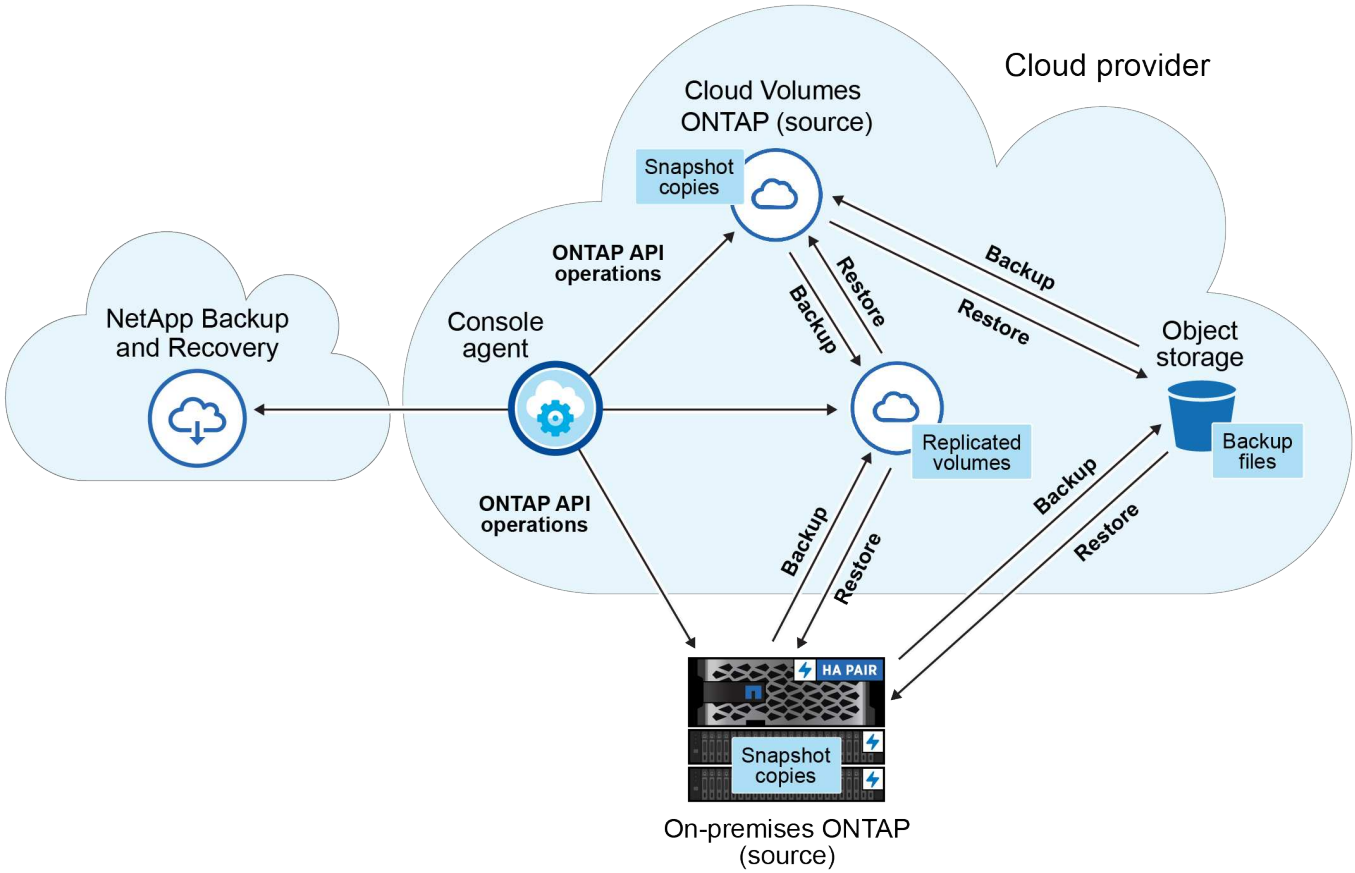
Se a operação de restauração não for concluída, não tente o processo de restauração novamente até que o Job Monitor mostre que a operação de restauração falhou. Se você tentar o processo de restauração novamente antes que o Job Monitor mostre que a operação de restauração falhou, a operação de restauração falhará novamente. Quando o status do Job Monitor for "Falha", você poderá tentar o processo de restauração novamente.

Proteja cargas de trabalho do KVM (visualização)

Visão geral das cargas de trabalho de proteção do KVM

Proteja suas VMs KVM e pools de armazenamento com o NetApp Backup and Recovery. O NetApp Backup and Recovery oferece operações de backup e restauração rápidas, com economia de espaço, consistentes em caso de falhas e consistentes com VMs.

Você pode fazer backup de cargas de trabalho do KVM no Amazon Web Services S3, Azure NetApp Files ou StorageGRID e restaurar cargas de trabalho do KVM de volta para um host KVM local.



Use o NetApp Backup and Recovery para implementar uma estratégia de proteção 3-2-1, na qual você tem 3 cópias dos seus dados de origem em 2 sistemas de armazenamento diferentes, além de 1 cópia na nuvem. Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados fornecem proteção multicamadas contra ameaças de segurança cibernética internas e externas.
- Vários tipos de mídia garantem a viabilidade de failover no caso de falha física ou lógica de um tipo de mídia.
- A cópia no local facilita restaurações rápidas, com cópias externas disponíveis caso a cópia no local seja comprometida.

Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery, consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Você pode usar o NetApp Backup and Recovery para executar as seguintes tarefas relacionadas às cargas de trabalho do KVM:

- "Descubra cargas de trabalho KVM"
- "Crie e gerencie grupos de proteção para cargas de trabalho KVM"
- "Fazer backup de cargas de trabalho do KVM"
- "Restaurar cargas de trabalho do KVM"

Descubra cargas de trabalho KVM no NetApp Backup and Recovery

O NetApp Backup and Recovery precisa primeiro descobrir hosts KVM e máquinas virtuais para que você possa protegê-los.

Função de console necessária Superadministrador de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Adicionar um host KVM e descobrir recursos

Adicione informações do host KVM e deixe o NetApp Backup and Recovery descobrir cargas de trabalho. Em cada agente do Console, selecione os sistemas onde você deseja descobrir cargas de trabalho.

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. No bloco KVM, selecione **Descobrir e gerenciar**.

   Se esta for a primeira vez que você faz login neste serviço, você já tem um sistema no Console, mas não descobriu nenhum recurso, a página inicial "Bem-vindo ao novo NetApp Backup and Recovery" aparece e mostra uma opção para **Descobrir recursos**.

3. Selecione **Descobrir recursos**.
4. Insira as seguintes informações:
   a. **Tipo de carga de trabalho**: Selecione **KVM**.
   b. Se você ainda não armazenou credenciais para este host KVM, selecione **Adicionar credenciais**.
      i. Selecione o agente do Console a ser usado com este host.
      ii. Digite um nome para esta credencial.
      iii. Escolha se deseja usar credenciais root ou credenciais não root.
      iv. Digite o nome de usuário e a senha da conta.
      v. Selecione **Concluído**.
   c. **Registro de host**: Adicione um novo host KVM. Insira o FQDN ou endereço IP do host, credenciais, agente do console e número da porta.
5. Selecione **Descobrir**.

   Este processo pode levar alguns minutos.

Resultado

A carga de trabalho do KVM é exibida na lista de cargas de trabalho na página Inventário.

Continue para o Painel de Backup e Recuperação da NetApp

1. Para exibir o Painel de Backup e Recuperação do NetApp , no menu superior, selecione **Painel**.
2. Revise a saúde da proteção de dados. O número de cargas de trabalho em risco ou protegidas aumenta com base nas cargas de trabalho recém-descobertas, protegidas e armazenadas em backup.

Crie e gerencie grupos de proteção para cargas de trabalho KVM com o NetApp Backup and Recovery

Crie grupos de proteção para gerenciar as operações de backup de um conjunto de recursos do KVM. Um grupo de proteção é um agrupamento lógico de recursos, como VMs e pools de armazenamento, que você deseja proteger juntos. Você precisa criar um grupo de proteção para fazer backup de máquinas virtuais KVM ou pools de armazenamento.

Você pode executar as seguintes tarefas relacionadas a grupos de proteção:

- Crie um grupo de proteção.
- Ver detalhes da proteção.
- Crie um grupo de proteção agora. Ver "Faça backup de cargas de trabalho do KVM agora" .
- Excluir um grupo de proteção.

Crie um grupo de proteção

Agrupe VMs e pools de armazenamento que você deseja proteger em um grupo de proteção.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione **Criar grupo de proteção**.
6. Forneça um nome para o grupo de proteção.
7. Selecione as VMs ou pools de armazenamento que você deseja incluir no grupo de proteção.
8. Selecione **Avançar**.
9. Selecione a **Política de backup** que você deseja aplicar ao grupo de proteção.

   Para obter mais informações sobre como criar uma política de backup, consulte"Criar e gerenciar políticas" .
10. Selecione **Avançar**.
11. Revise a configuração.
12. Selecione **Criar** para criar o grupo de proteção.

Excluir um grupo de proteção

A exclusão de um grupo de proteção o remove, juntamente com todos os agendamentos de backup associados. Talvez você queira excluir um grupo de proteção se ele não for mais necessário.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione o grupo de proteção que você deseja excluir.
6. Selecione o ícone Ações ••• > **Excluir**.
7. Revise a mensagem de confirmação sobre a exclusão dos backups associados e confirme a exclusão.

Faça backup de cargas de trabalho do KVM com o NetApp Backup and Recovery

Faça backup de grupos de proteção KVM de sistemas ONTAP locais para Amazon Web Services, Azure NetApp Files ou StorageGRID para garantir que seus dados estejam protegidos. Ao fazer backup de um grupo de proteção, o NetApp Console faz backup das VMs e dos pools de armazenamento contidos no grupo de proteção. Os backups são gerados automaticamente e armazenados em um armazenamento de objetos na sua conta de nuvem pública ou privada.

Para fazer backup de grupos de proteção em um cronograma, crie políticas que controlem as operações de backup e restauração. Ver"Criar políticas" para obter instruções.

- Crie grupos de proteção para gerenciar as operações de backup e restauração de um conjunto de recursos. Ver "Crie e gerencie grupos de proteção para cargas de trabalho KVM com o NetApp Backup and Recovery" para maiores informações.

Faça backup de grupos de proteção agora com um backup sob demanda

Você pode executar um backup sob demanda imediatamente. Isso é útil se você estiver prestes a fazer alterações no seu sistema e quiser garantir que tenha um backup antes de começar.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. No bloco KVM, selecione **Descobrir e gerenciar**.
3. Selecione **Inventário**.
4. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
5. Selecione o ícone Ações ••• > **Ver detalhes**.
6. Selecione a aba **Grupos de proteção**, **Datastores** ou **Máquinas virtuais**.
7. Selecione o grupo de proteção que você deseja fazer backup.
8. Selecione o ícone Ações ••• > **Faça backup agora**.

A política aplicada ao backup é a mesma política atribuída ao grupo de proteção.

9. Selecione o nível de agendamento.
10. Selecione **Fazer backup**.

Restaurar máquinas virtuais KVM com o NetApp Backup and Recovery

Restaure máquinas virtuais KVM de cópias de snapshot, de um backup de grupo de proteção replicado para armazenamento secundário ou de backups armazenados em armazenamento de objetos usando o NetApp Backup and Recovery.

Restaurar a partir desses locais

Você pode restaurar máquinas virtuais de diferentes locais de inicialização:

- Restaurar de um local primário (instantâneo local)
- Restaurar de um recurso replicado no armazenamento secundário
- Restaurar de um backup de armazenamento de objetos

Restaurar esses pontos

Você pode restaurar dados para o local original; restaurar para um local alternativo não está disponível nesta versão de visualização.

- Restaurar para o local original

Considerações sobre restauração de armazenamento de objetos

Se você selecionar um arquivo de backup no armazenamento de objetos e a proteção contra ransomware estiver ativa para esse backup (se você habilitou o DataLock e o Ransomware Resilience na política de backup), você será solicitado a executar uma verificação de integridade adicional no arquivo de backup antes de restaurar os dados. Recomendamos que você execute a verificação.

Você incorrerá em custos extras de saída do seu provedor de nuvem para acessar o conteúdo do arquivo de backup.

Como funciona a restauração de máquinas virtuais

Ao restaurar máquinas virtuais, ocorre o seguinte:

- Quando você restaura uma carga de trabalho de um arquivo de backup local, o NetApp Backup and Recovery cria um *novo* recurso usando os dados do backup.
- Ao restaurar a partir de uma VM replicada, você pode restaurá-la para o sistema original ou para um sistema ONTAP local.
- Ao restaurar um backup do armazenamento de objetos, você pode restaurar os dados para o sistema original ou para um sistema ONTAP local.

Na página Restaurar (também conhecida como Pesquisar e Restaurar), você pode restaurar uma VM, mesmo que não se lembre do nome exato, do local em que ela reside ou da data em que esteve em boas condições pela última vez. Você pode pesquisar o instantâneo usando filtros.

Restaurar VMs a partir da opção Restaurar (Pesquisar e Restaurar)

Restaure máquinas virtuais KVM usando a opção Restaurar. Você pode procurar o instantâneo pelo nome ou usando filtros.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de restauração de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. No menu NetApp Backup and Recovery, selecione **Restaurar**.
3. Na lista suspensa à direita do campo de pesquisa de nome, selecione **KVM**.
4. Insira o nome da VM que você deseja restaurar ou filtre pelo host da VM ou pool de armazenamento onde o recurso que você deseja restaurar está localizado.

   Aparece uma lista de instantâneos que correspondem aos seus critérios de pesquisa.

5. Selecione o botão **Restaurar** para o instantâneo que você deseja restaurar.

   Uma lista de possíveis pontos de restauração é exibida.

6. Selecione o ponto de restauração que você deseja usar.
7. Selecione um local de origem para o instantâneo.
8. Selecione **Concluído** ou **Avançar** para continuar para a página Restaurar configurações de destino.

   Em seguida, você pode escolher as configurações de destino e as opções de pré e pós-restauração.

Seleção de destino

1. Escolha as configurações de destino e as opções de pré e pós-restauração.

Restaurar para o local original

1. **Ativar restauração rápida**: selecione esta opção para executar uma operação de restauração rápida. Os volumes e dados restaurados estarão disponíveis imediatamente. Não use isso em volumes que exigem alto desempenho porque, durante o processo de restauração rápida, o acesso aos dados pode ser mais lento que o normal.
2. **Opções de pré-restauração**: insira o caminho completo para um script que deve ser executado antes da operação de restauração e quaisquer argumentos que o script aceite.
3. **Opções pós-restauração**:
   - **Reiniciar VM**: selecione esta opção para reiniciar a VM após a conclusão da operação de restauração e após a aplicação do script pós-restauração.
   - **Postscript**: Insira o caminho completo para um script que deve ser executado após a operação de restauração e quaisquer argumentos que o script aceite.
4. Seção **Notificação**:
   - **Ativar notificações por e-mail**: selecione esta opção para receber notificações por e-mail sobre a operação de restauração e indique que tipo de notificação você deseja receber.
5. Selecione **Restaurar**.

Restaurar para local alternativo

Não disponível para visualização do KVM.

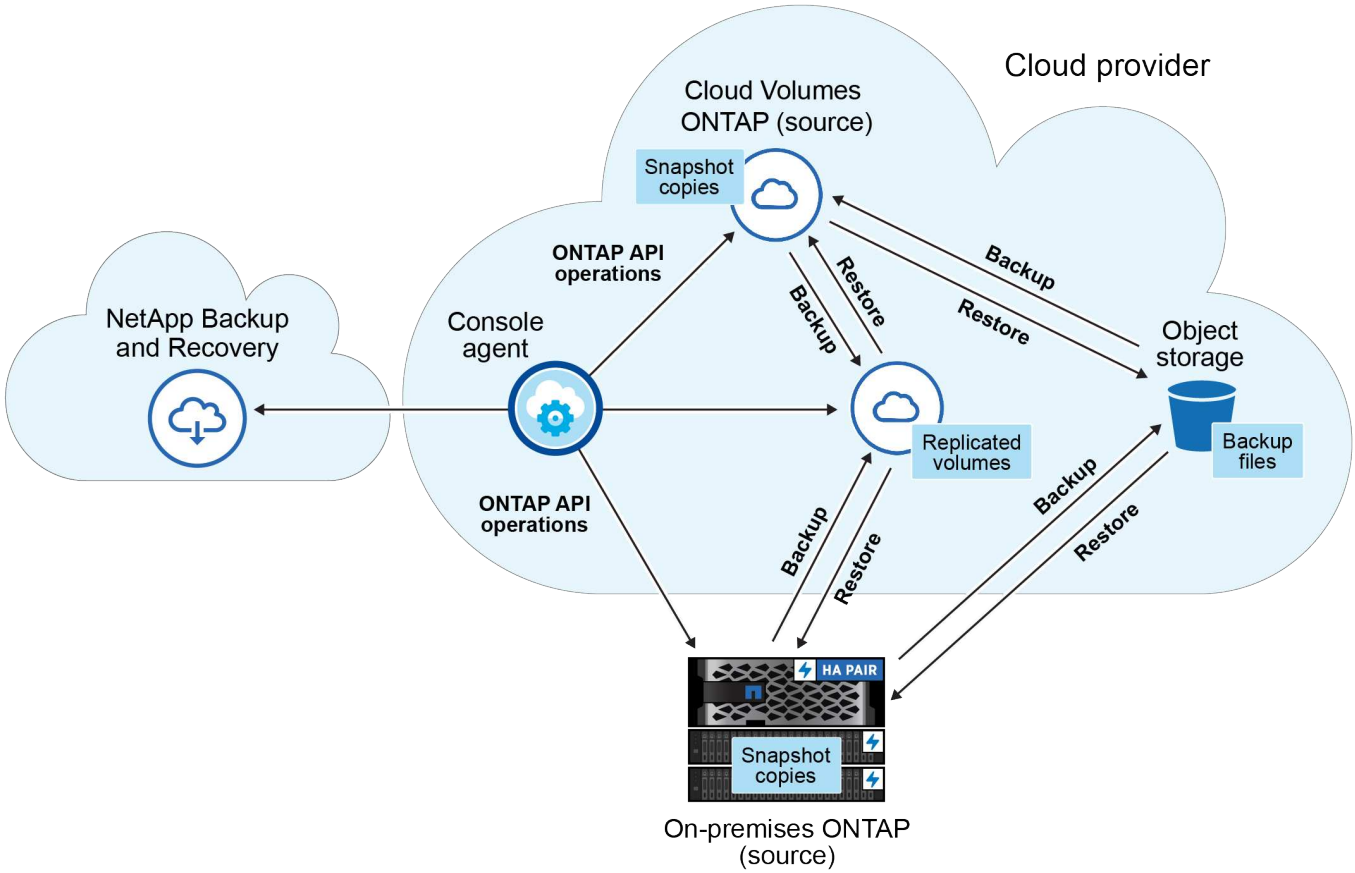
1. Selecione **Restaurar**.

Proteja as cargas de trabalho do Hyper-V (visualização)

Visão geral das cargas de trabalho de proteção do Hyper-V

Proteja suas VMs Hyper-V com o NetApp Backup and Recovery. O NetApp Backup and Recovery oferece operações de backup e restauração rápidas, com economia de espaço, consistentes em caso de falhas e consistentes com VMs para instâncias de cluster autônomas e FCI.

Você pode fazer backup de cargas de trabalho do Hyper-V no Amazon Web Services S3 ou StorageGRID e restaurar cargas de trabalho do Hyper-V em um host Hyper-V local.



Use o NetApp Backup and Recovery para implementar uma estratégia de proteção 3-2-1, na qual você tem 3 cópias dos seus dados de origem em 2 sistemas de armazenamento diferentes, além de 1 cópia na nuvem. Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados fornecem proteção multicamadas contra ameaças de segurança cibernética internas e externas.
- Vários tipos de mídia garantem a viabilidade de failover no caso de falha física ou lógica de um tipo de mídia.
- A cópia no local facilita restaurações rápidas, com cópias externas disponíveis caso a cópia no local seja comprometida.

Quando você adiciona hosts Hyper-V e descobre recursos, o NetApp Backup and Recovery instala o plug-in NetApp Hyper-V e o plug-in NetApp SnapCenter Windows FileSystem no host Hyper-V para ajudar a gerenciar e proteger máquinas virtuais.

Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery, consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Você pode usar o NetApp Backup and Recovery para executar as seguintes tarefas relacionadas às cargas de trabalho do Hyper-V:

- "Descubra as cargas de trabalho do Hyper-V"
- "Crie e gerencie grupos de proteção para cargas de trabalho do Hyper-V"
- "Fazer backup de cargas de trabalho do Hyper-V"
- "Restaurar cargas de trabalho do Hyper-V"

Descubra as cargas de trabalho do Hyper-V no NetApp Backup and Recovery

O NetApp Backup and Recovery precisa primeiro descobrir as máquinas virtuais Hyper-V para que você possa protegê-las.

Função de console necessária Superadministrador de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Adicionar um host Hyper-V e descobrir recursos

Adicione informações do host Hyper-V e deixe o NetApp Backup and Recovery descobrir máquinas virtuais. Em cada agente do Console, selecione os sistemas onde você deseja descobrir os recursos.

Quando você adiciona hosts Hyper-V e descobre recursos, o NetApp Backup and Recovery instala o plug-in NetApp Hyper-V e o plug-in NetApp SnapCenter Windows FileSystem no host Hyper-V para ajudar a gerenciar e proteger máquinas virtuais.

Passos

1. No menu do NetApp Console, selecione **Proteção** > **Backup e recuperação**.

   Se esta for a primeira vez que você faz login no NetApp Backup and Recovery, você já tem um sistema no Console, mas não descobriu nenhum recurso. A página inicial "Bem-vindo ao novo NetApp Backup and Recovery" aparece e mostra uma opção para **Descobrir recursos**.

2. Selecione **Descobrir recursos**.
3. Insira as seguintes informações:
   a. **Tipo de carga de trabalho**: Selecione **Hyper-V**.
   b. Se você ainda não armazenou credenciais para este host Hyper-V, selecione **Adicionar credenciais**.
      i. Selecione o agente do Console a ser usado com este host.
      ii. Digite um nome para esta credencial.
      iii. Digite o nome de usuário e a senha da conta.
      iv. Selecione **Concluído**.
   c. **Registro de host**: Adicione um novo host Hyper-V. Insira o FQDN ou endereço IP do host, credenciais, agente do console e número da porta.
4. Selecione **Descobrir**.

   Este processo pode levar alguns minutos.

Resultado

Depois que o NetApp Backup and Recovery descobre recursos, a carga de trabalho do Hyper-V é exibida na lista de cargas de trabalho na página Inventário.

Continue para o Painel de Backup e Recuperação da NetApp

1. Para exibir o Painel de Backup e Recuperação do NetApp , no menu do Console do NetApp , selecione **Painel**.

2. Revise a saúde da proteção de dados. O número de cargas de trabalho em risco ou protegidas aumenta com base nas cargas de trabalho recém-descobertas, protegidas e armazenadas em backup.

Crie e gerencie grupos de proteção para cargas de trabalho do Hyper-V com o NetApp Backup and Recovery

Crie grupos de proteção para gerenciar as operações de backup de um conjunto de máquinas virtuais. Um grupo de proteção é um agrupamento lógico de recursos, como VMs, que você deseja proteger juntos.

Você pode executar as seguintes tarefas relacionadas a grupos de proteção:

- Crie um grupo de proteção.
- Ver detalhes da proteção.
- Crie um grupo de proteção agora. Ver "Faça backup das cargas de trabalho do Hyper-V agora" .
- Excluir um grupo de proteção.

Crie um grupo de proteção

Agrupe as cargas de trabalho que você deseja proteger em um grupo de proteção. Você pode criar um grupo de proteção para um conjunto de cargas de trabalho que deseja fazer backup e restaurar juntas.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione **Criar grupo de proteção**.
6. Forneça um nome para o grupo de proteção.
7. Selecione as VMs que você deseja incluir no grupo de proteção.
8. Selecione **Avançar**.
9. Selecione a **Política de backup** que você deseja aplicar ao grupo de proteção.
10. Selecione **Avançar**.
11. Revise a configuração.
12. Selecione **Criar** para criar o grupo de proteção.

Excluir um grupo de proteção

A exclusão de um grupo de proteção o remove, juntamente com todos os agendamentos de backup associados. Talvez você queira excluir um grupo de proteção se ele não for mais necessário.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione o grupo de proteção que você deseja excluir.
6. Selecione o ícone Ações ••• > **Excluir**.
7. Revise a mensagem de confirmação sobre a exclusão dos backups associados e confirme a exclusão.

Faça backup de cargas de trabalho do Hyper-V com o NetApp Backup and Recovery

Faça backup de VMs Hyper-V de sistemas ONTAP locais para Amazon Web Services, Azure NetApp Files ou StorageGRID para garantir que seus dados estejam protegidos. Os backups são gerados automaticamente e armazenados em um armazenamento de objetos na sua conta de nuvem pública ou privada.

- Para fazer backup de cargas de trabalho em um cronograma, crie políticas que controlem as operações de backup e restauração. Ver"Criar políticas" para obter instruções.
- Crie grupos de proteção para gerenciar as operações de backup e restauração de um conjunto de recursos. Ver "Crie e gerencie grupos de proteção para cargas de trabalho do Hyper-V com o NetApp Backup and Recovery" para maiores informações.
- Faça backup das cargas de trabalho agora (crie um backup sob demanda agora).

Faça backup de cargas de trabalho agora com um backup sob demanda

Você pode executar um backup sob demanda imediatamente. Isso é útil se você estiver prestes a fazer alterações no seu sistema e quiser garantir que tenha um backup antes de começar.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**, **Datastores** ou **Máquinas virtuais**.
5. Selecione o grupo de proteção ou as máquinas virtuais das quais você deseja fazer backup.
6. Selecione o ícone Ações ••• > **Faça backup agora**.

   A política aplicada ao backup é a mesma política atribuída ao grupo de proteção ou à máquina virtual.

7. Selecione o nível de agendamento.
8. Selecione **Fazer backup**.

Restaure cargas de trabalho do Hyper-V com o NetApp Backup and Recovery

Restaure cargas de trabalho do Hyper-V de cópias de snapshot, de um backup de carga de trabalho replicado para armazenamento secundário ou de backups armazenados em armazenamento de objetos usando o NetApp Backup and Recovery.

Restaurar a partir desses locais

Você pode restaurar cargas de trabalho de diferentes locais de partida:

- Restaurar de um local primário (instantâneo local)
- Restaurar de um recurso replicado no armazenamento secundário
- Restaurar de um backup de armazenamento de objetos

Restaurar esses pontos

Você pode restaurar dados para o local original; restaurar para um local alternativo não está disponível nesta versão de visualização privada.

Considerações sobre restauração de armazenamento de objetos

Se você selecionar um arquivo de backup no armazenamento de objetos e a proteção contra ransomware estiver ativa para esse backup (se você habilitou o DataLock e o Ransomware Resilience na política de backup), você será solicitado a executar uma verificação de integridade adicional no arquivo de backup antes de restaurar os dados. Recomendamos que você execute a verificação.

Você incorrerá em custos extras de saída do seu provedor de nuvem para acessar o conteúdo do arquivo de backup.

Como funciona a restauração de cargas de trabalho

Ao restaurar cargas de trabalho, ocorre o seguinte:

- Quando você restaura uma carga de trabalho de um arquivo de backup local, o NetApp Backup and Recovery cria um *novo* recurso usando os dados do backup.
- Ao restaurar uma carga de trabalho replicada, você pode restaurar a carga de trabalho para o sistema original ou para um sistema ONTAP local.

Na página Restaurar (também conhecida como Pesquisar e Restaurar)*, você pode restaurar um recurso, mesmo que não se lembre do nome exato, do local em que ele reside ou da data em que esteve em boas condições pela última vez. Você pode pesquisar o instantâneo usando filtros.

Restaurar dados de carga de trabalho a partir da opção Restaurar (Pesquisar e Restaurar)

Restaure cargas de trabalho do Hyper-V usando a opção Restaurar. Você pode procurar o instantâneo pelo nome ou usando filtros.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de restauração de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Restaurar**.
2. Na lista suspensa à direita do campo de pesquisa de nome, selecione **Hyper-V**.

3. Insira o nome do recurso que você deseja restaurar ou filtre pelo nome da VM, host da VM ou pool de armazenamento onde o recurso que você deseja restaurar está localizado.

   Aparece uma lista de instantâneos que correspondem aos seus critérios de pesquisa.

4. Selecione o botão **Restaurar** para o instantâneo que você deseja restaurar.

   Uma lista de possíveis pontos de restauração é exibida.

5. Selecione o ponto de restauração que você deseja usar.
6. Selecione um local de origem para o instantâneo.
7. Selecione **Concluído** ou **Avançar** para continuar para a página Restaurar configurações de destino.

   Em seguida, você pode escolher as configurações de destino e as opções de pré e pós-restauração.

Seleção de destino

1. Escolha as configurações de destino e as opções de pré e pós-restauração.

Restaurar para o local original

1. **Ativar restauração rápida**: selecione esta opção para executar uma operação de restauração rápida. Os volumes e dados restaurados estarão disponíveis imediatamente. Não use isso em volumes que exigem alto desempenho porque, durante o processo de restauração rápida, o acesso aos dados pode ser mais lento que o normal.
2. **Opções de pré-restauração**: insira o caminho completo para um script que deve ser executado antes da operação de restauração e quaisquer argumentos que o script aceite.
3. **Opções pós-restauração**:
   - **Reiniciar VM**: selecione esta opção para reiniciar a VM após a conclusão da operação de restauração e após a aplicação do script pós-restauração.
   - **Postscript**: Insira o caminho completo para um script que deve ser executado após a operação de restauração e quaisquer argumentos que o script aceite.
4. Seção **Notificação**:
   - **Ativar notificações por e-mail**: selecione esta opção para receber notificações por e-mail sobre a operação de restauração e indique que tipo de notificação você deseja receber.
5. Selecione **Restaurar**.

Restaurar para local alternativo

Não disponível para visualização privada do Hyper-V.

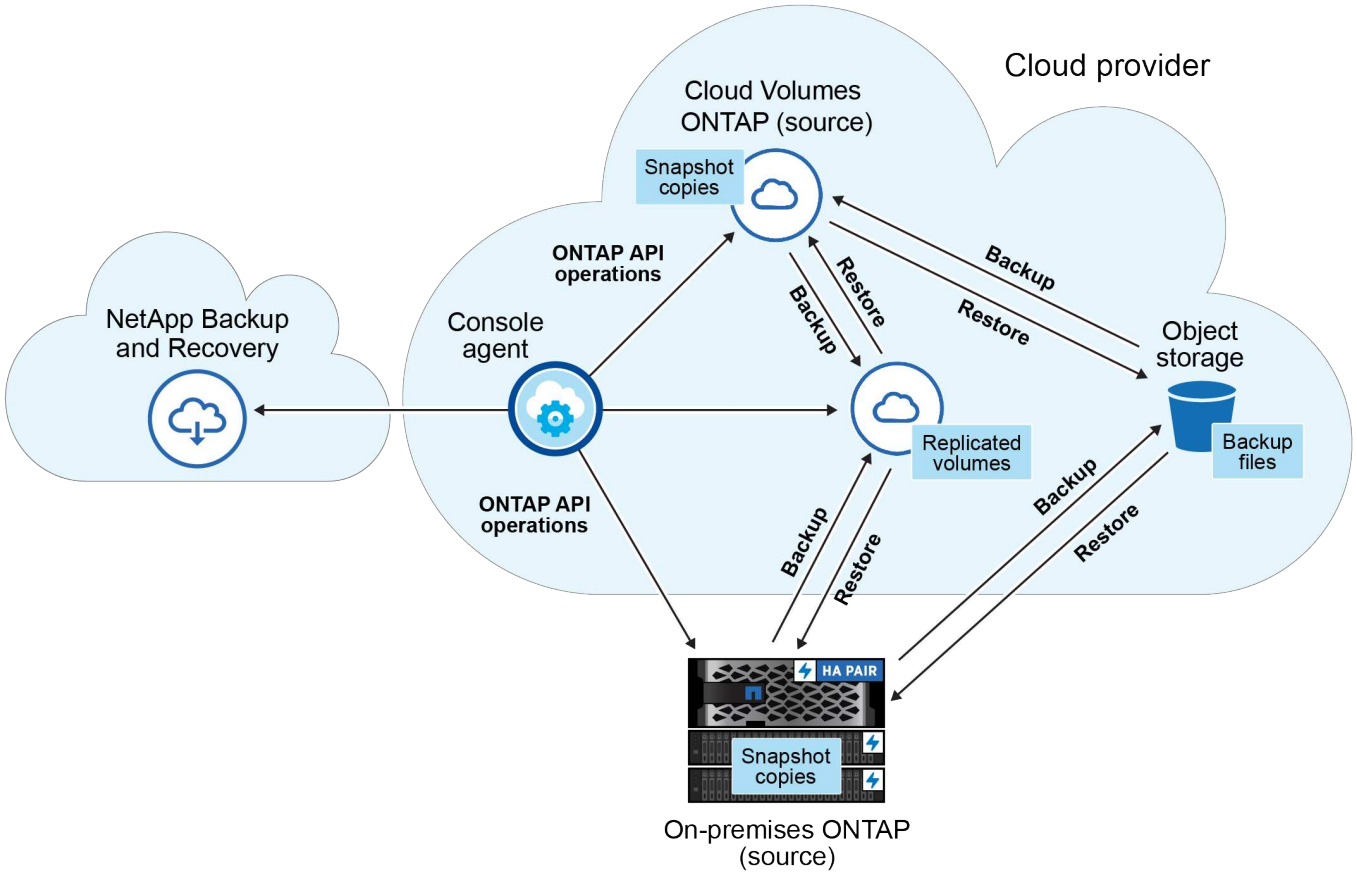
1. Selecione **Restaurar**.

Proteja as cargas de trabalho do Oracle (visualização)

Visão geral da proteção de cargas de trabalho do Oracle Database

Proteja seus bancos de dados e logs Oracle com o NetApp Backup and Recovery. O

NetApp Backup and Recovery oferece operações de backup e restauração rápidas, com economia de espaço, consistentes em caso de falhas e consistentes em banco de dados. Você pode fazer backup de cargas de trabalho do Oracle no Amazon Web Services S3, NetApp StorageGRID, Microsoft Azure Blob Storage ou ONTAP S3 e restaurá-las em um host Oracle local.



Use o NetApp Backup and Recovery para implementar uma estratégia de proteção 3-2-1, na qual você tem 3 cópias dos seus dados de origem em 2 sistemas de armazenamento diferentes, além de 1 cópia na nuvem. Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados fornecem proteção multicamadas contra ameaças de segurança cibernética internas e externas.
- Vários tipos de mídia garantem a viabilidade de failover no caso de falha física ou lógica de um tipo de mídia.
- A cópia no local facilita restaurações rápidas, com cópias externas disponíveis caso a cópia no local seja comprometida.

Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery, consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Você pode usar o NetApp Backup and Recovery para executar as seguintes tarefas relacionadas às cargas de trabalho do Oracle:

- "Descubra as cargas de trabalho da Oracle"
- "Crie e gerencie grupos de proteção para cargas de trabalho Oracle"

- "Fazer backup de cargas de trabalho Oracle"
- "Restaurar cargas de trabalho Oracle"

Descubra as cargas de trabalho do Oracle no NetApp Backup and Recovery

O NetApp Backup and Recovery precisa primeiro descobrir seus bancos de dados Oracle para que você possa protegê-los.

Função de console necessária Superadministrador de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Adicionar um host Oracle e descobrir recursos

Adicione informações do host Oracle e deixe o NetApp Backup and Recovery descobrir cargas de trabalho. Em cada agente do Console, selecione os sistemas onde você deseja descobrir cargas de trabalho.

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. No bloco Oracle, selecione **Descobrir e gerenciar**.

   Se esta for a primeira vez que você faz login neste serviço, você já tem um sistema no Console, mas não descobriu nenhum recurso, a página inicial "Bem-vindo ao novo NetApp Backup and Recovery" aparece e mostra uma opção para **Descobrir recursos**.

3. Selecione **Descobrir recursos**.
4. Insira as seguintes informações:
   a. **Tipo de carga de trabalho**: Selecione **Oracle**.
   b. Se você ainda não armazenou credenciais para este host Oracle, selecione **Adicionar credenciais**.
      i. Selecione o agente do Console a ser usado com este host.
      ii. Digite um nome para esta credencial.
      iii. Digite o nome de usuário e a senha da conta.
      iv. Selecione **Concluído**.
   c. **Registro de host**: Adicione um novo host Oracle. Insira o FQDN ou endereço IP do host, credenciais, agente do console e número da porta.
5. Selecione **Descobrir**.

   Este processo pode levar alguns minutos.

Resultado

A carga de trabalho do Oracle é exibida na lista de cargas de trabalho na página Inventário.

Continue para o Painel de Backup e Recuperação da NetApp

1. Para exibir o Painel de Backup e Recuperação do NetApp , no menu superior, selecione **Painel**.
2. Revise a saúde da proteção de dados. O número de cargas de trabalho em risco ou protegidas aumenta com base nas cargas de trabalho recém-descobertas, protegidas e armazenadas em backup.

Crie e gerencie grupos de proteção para cargas de trabalho Oracle com o NetApp Backup and Recovery

Crie grupos de proteção para gerenciar as operações de backup de um conjunto de recursos do Oracle Database. Um grupo de proteção é um agrupamento lógico de recursos, como bancos de dados, que você deseja proteger juntos. Você precisa criar um grupo de proteção para fazer backup de bancos de dados Oracle.

Você pode executar as seguintes tarefas relacionadas a grupos de proteção:

- Crie um grupo de proteção.
- Ver detalhes da proteção.
- Crie um grupo de proteção agora. Ver "Faça backup das cargas de trabalho do Oracle agora" .
- Excluir um grupo de proteção.

Crie um grupo de proteção

Agrupe VMs e pools de armazenamento que você deseja proteger em um grupo de proteção.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione **Criar grupo de proteção**.
6. Forneça um nome para o grupo de proteção.
7. Selecione as VMs ou pools de armazenamento que você deseja incluir no grupo de proteção.
8. Selecione **Avançar**.
9. Selecione a **Política de backup** que você deseja aplicar ao grupo de proteção.

   Se você quiser criar uma política, selecione **Criar nova política** e siga as instruções para criar uma política. Ver "Criar políticas" para maiores informações.

10. Selecione **Avançar**.
11. Revise a configuração.
12. Selecione **Criar** para criar o grupo de proteção.

Excluir um grupo de proteção

A exclusão de um grupo de proteção o remove, juntamente com todos os agendamentos de backup associados. Talvez você queira excluir um grupo de proteção se ele não for mais necessário.

Passos

1. No menu NetApp Backup and Recovery, selecione **Inventário**.
2. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
3. Selecione o ícone Ações ••• > **Ver detalhes**.
4. Selecione a aba **Grupos de proteção**.
5. Selecione o grupo de proteção que você deseja excluir.
6. Selecione o ícone Ações ••• > **Remover proteção**.
7. Revise a mensagem de confirmação sobre a exclusão dos backups associados e confirme a exclusão.

Faça backup de cargas de trabalho Oracle com o NetApp Backup and Recovery

Faça backup de grupos de proteção ou bancos de dados do Oracle Database de sistemas ONTAP locais para Amazon Web Services S3, NetApp StorageGRID, Microsoft Azure Blob Storage ou ONTAP S3 para garantir que seus dados estejam protegidos. Ao fazer backup de um grupo de proteção, o NetApp Console faz backup dos bancos de dados e dos dados de log contidos no grupo de proteção.

Para fazer backup de grupos de proteção ou bancos de dados individuais em um cronograma, crie políticas que controlem as operações de backup e restauração. Ver"Criar políticas" para obter instruções.

- Crie grupos de proteção para gerenciar as operações de backup e restauração de um conjunto de recursos. Ver "Crie e gerencie grupos de proteção para cargas de trabalho Oracle com o NetApp Backup and Recovery" para maiores informações.
- Faça backup de um grupo de proteção agora (crie um backup sob demanda agora).
- Faça backup de um banco de dados agora.

Faça backup de grupos de proteção agora com um backup sob demanda

Você pode executar um backup sob demanda imediatamente. Isso é útil se você estiver prestes a fazer alterações no seu sistema e quiser garantir que tenha um backup antes de começar.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. No bloco Oracle, selecione **Descobrir e gerenciar**.
3. Selecione **Inventário**.
4. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
5. Selecione o ícone Ações ••• > **Ver detalhes**.
6. Selecione a aba **Grupos de proteção**, **Datastores** ou **Máquinas virtuais**.
7. Selecione o grupo de proteção que você deseja fazer backup.
8. Selecione o ícone Ações ••• > **Faça backup agora**.

A política aplicada ao backup é a mesma política atribuída ao grupo de proteção.

9. Selecione o nível de agendamento.
10. Selecione **Fazer backup**.

Faça backup de um banco de dados agora com um backup sob demanda

Você pode executar um backup sob demanda de um único banco de dados.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de backup de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. No bloco Oracle, selecione **Descobrir e gerenciar**.
3. Selecione **Inventário**.
4. Selecione uma carga de trabalho para visualizar os detalhes da proteção.
5. Selecione o ícone Ações ••• > **Ver detalhes**.
6. Selecione a aba **Bancos de dados**.
7. Selecione o banco de dados que você deseja fazer backup.
8. Selecione o ícone Ações ••• > **Faça backup agora**.
9. Selecione o nível de agendamento.
10. Selecione **Fazer backup**.

Restaure bancos de dados Oracle com o NetApp Backup and Recovery

Restaure bancos de dados Oracle de cópias de snapshot, de um backup replicado para armazenamento secundário ou de backups armazenados em armazenamento de objetos usando o NetApp Backup and Recovery.

Restaurar a partir desses locais

Você pode restaurar bancos de dados de diferentes locais de partida:

- Restaurar de um local primário (instantâneo local)
- Restaurar de um recurso replicado no armazenamento secundário
- Restaurar de um backup de armazenamento de objetos

Restaurar esses pontos

Você pode restaurar dados para o local original; restaurar para um local alternativo não está disponível nesta versão de visualização privada.

- Restaurar para o local original

Como funciona a restauração de bancos de dados Oracle

Ao restaurar bancos de dados Oracle, ocorre o seguinte:

- Quando você restaura um banco de dados de um snapshot local, o NetApp Backup and Recovery cria um *novo* recurso usando os dados do backup.
- Ao restaurar a partir do armazenamento replicado, você pode restaurá-lo para o local original.
- Ao restaurar um backup do armazenamento de objetos, você pode restaurar os dados para o armazenamento de origem ou para um sistema ONTAP local e recuperar o banco de dados de lá.

Na página Restaurar (também conhecida como Pesquisar e Restaurar), você pode restaurar um banco de dados, mesmo que não se lembre do nome exato, do local em que ele reside ou da data em que esteve em boas condições pela última vez. Você pode pesquisar no banco de dados usando filtros.

Restaurar um banco de dados Oracle

Dependendo de suas necessidades, restaure um banco de dados Oracle para um ponto específico no tempo, para um número de alteração do sistema (SCN) específico ou para o último estado bom. Você também pode simplesmente restaurar o banco de dados a partir de instantâneos e pular o processo de recuperação automatizado. Talvez você queira pular o processo de recuperação automatizado se quiser executar a recuperação manualmente. Você pode pesquisar o banco de dados usando seu nome ou com filtros específicos.

Função de console necessária Superadministrador de backup e recuperação ou função de administrador de restauração de backup e recuperação. "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. No menu NetApp Backup and Recovery, selecione **Restaurar**.
3. Na lista suspensa à direita do campo de pesquisa de nome, selecione **Oracle**.
4. Digite o nome do banco de dados que você deseja restaurar ou filtre pelo host do banco de dados onde o banco de dados que você deseja restaurar está localizado.

   Aparece uma lista de instantâneos que correspondem aos seus critérios de pesquisa.

5. Selecione o botão **Restaurar** para o banco de dados que você deseja restaurar.
6. Escolha uma opção de restauração:

Restaurar para um ponto específico no tempo

a. Selecione **Restaurar para um ponto específico no tempo**.
b. Selecione **Avançar**.
c. Escolha uma data no menu suspenso e selecione **Pesquisar**.

   Uma lista de instantâneos correspondentes na data especificada é exibida.

Restaurar para um número de alteração do sistema (SCN) específico

a. Selecione **Restaurar para um número de alteração do sistema (SCN) específico**.
b. Selecione **Avançar**.
c. Digite o SCN a ser usado como ponto de restauração e selecione **Pesquisar**.

   Uma lista de instantâneos correspondentes para o SCN especificado é exibida.

Restaurar para o backup mais recente (último estado bom)

a. Selecione **Restaurar para o backup mais recente**.
b. Selecione **Avançar**.

   Os backups completos e de log mais recentes são exibidos.

Restaurar de instantâneos sem recuperação

a. Selecione **Restaurar de instantâneos sem recuperação**.
b. Selecione **Avançar**.

   Os instantâneos correspondentes são exibidos.

7. Selecione um local de origem para o instantâneo.
8. Selecione **Avançar** para continuar para a página Restaurar configurações de destino.

   Em seguida, você pode escolher as configurações de destino e as opções de pré e pós-restauração.

Seleção de destino

1. Escolha as configurações de destino e as opções de pré e pós-restauração.

Restaurar para o local original

1. **Configurações de destino**:
   - Escolha restaurar o banco de dados inteiro ou apenas os tablespaces do banco de dados.
   - **Arquivos de controle**: Opcionalmente, habilite esta opção para restaurar também os arquivos de controle do banco de dados.
2. **Opções de pré-restauração**:
   - Opcionalmente, habilite esta opção e insira o caminho completo para um script que deve ser executado antes da operação de restauração e quaisquer argumentos que o script aceite.
   - Escolha um valor de tempo limite para o script. Se o script não for executado dentro desse período, a restauração continuará de qualquer maneira.
3. **Opções pós-restauração**:
   - **Postscript**: Opcionalmente, habilite esta opção e insira o caminho completo para um script que deve ser executado após a operação de restauração e quaisquer argumentos que o script aceite.
   - **Abra o banco de dados ou o banco de dados contêiner no modo LEITURA-GRAVAÇÃO após a recuperação**: Após a conclusão da operação de restauração, o Backup e Recuperação habilitará o modo LEITURA-GRAVAÇÃO para o banco de dados.
4. Seção **Notificação**:
   - **Ativar notificações por e-mail**: selecione esta opção para receber notificações por e-mail sobre a operação de restauração e indique que tipo de notificação você deseja receber.
5. Selecione **Restaurar**.

Restaurar para local alternativo

Não disponível para visualização de cargas de trabalho Oracle.

Monte e desmonte pontos de recuperação do banco de dados Oracle com o NetApp Backup and Recovery

Talvez você queira montar um ponto de recuperação do Oracle Database se precisar acessar o banco de dados em um estado controlado para executar operações de recuperação.

Montar um ponto de restauração do banco de dados Oracle

Se você configurar a política de proteção para um banco de dados para reter logs de arquivamento, poderá montar os pontos de recuperação do banco de dados para visualizar o histórico de todas as alterações feitas no banco de dados.

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. Selecione o bloco Oracle.
3. No menu Backup e Recuperação, selecione **Inventário**.
4. Para a carga de trabalho do Oracle Database na lista, selecione **Exibir**.
5. Selecione o menu **Bancos de dados**.

6. Escolha um banco de dados da lista e selecione o ícone Ações ••• > **Ver detalhes da proteção**.

   Uma lista de pontos de recuperação para esse banco de dados é exibida.

7. Escolha um ponto de recuperação da lista e selecione o ícone Ações ••• > **Monte**.
8. Na caixa de diálogo que aparece, faça o seguinte:
   a. Escolha o host que deve montar o ponto de recuperação na lista.
   b. Selecione qual local o Backup and Recovery deve usar para montar o ponto de recuperação. Para a versão de pré-visualização, a montagem a partir do armazenamento de objetos não é suportada.

      O caminho de montagem que o Backup and Recovery deve usar é exibido.

9. Selecione **Montar**.

   O ponto de recuperação é montado no host Oracle.

Desmontar um ponto de restauração do banco de dados Oracle

Desmonte o ponto de recuperação quando não precisar mais visualizar as alterações feitas no banco de dados.

Passos

1. No menu do NetApp Console, selecione **Proteção > Backup e recuperação**.
2. Selecione o bloco Oracle.
3. No menu Backup e Recuperação, selecione **Inventário**.
4. Para a carga de trabalho do Oracle na lista, selecione **Exibir**.
5. Selecione o menu **Bancos de dados**.
6. Escolha um banco de dados da lista e selecione o ícone Ações ••• > **Ver detalhes da proteção**.

   Uma lista de pontos de recuperação para esse banco de dados é exibida.

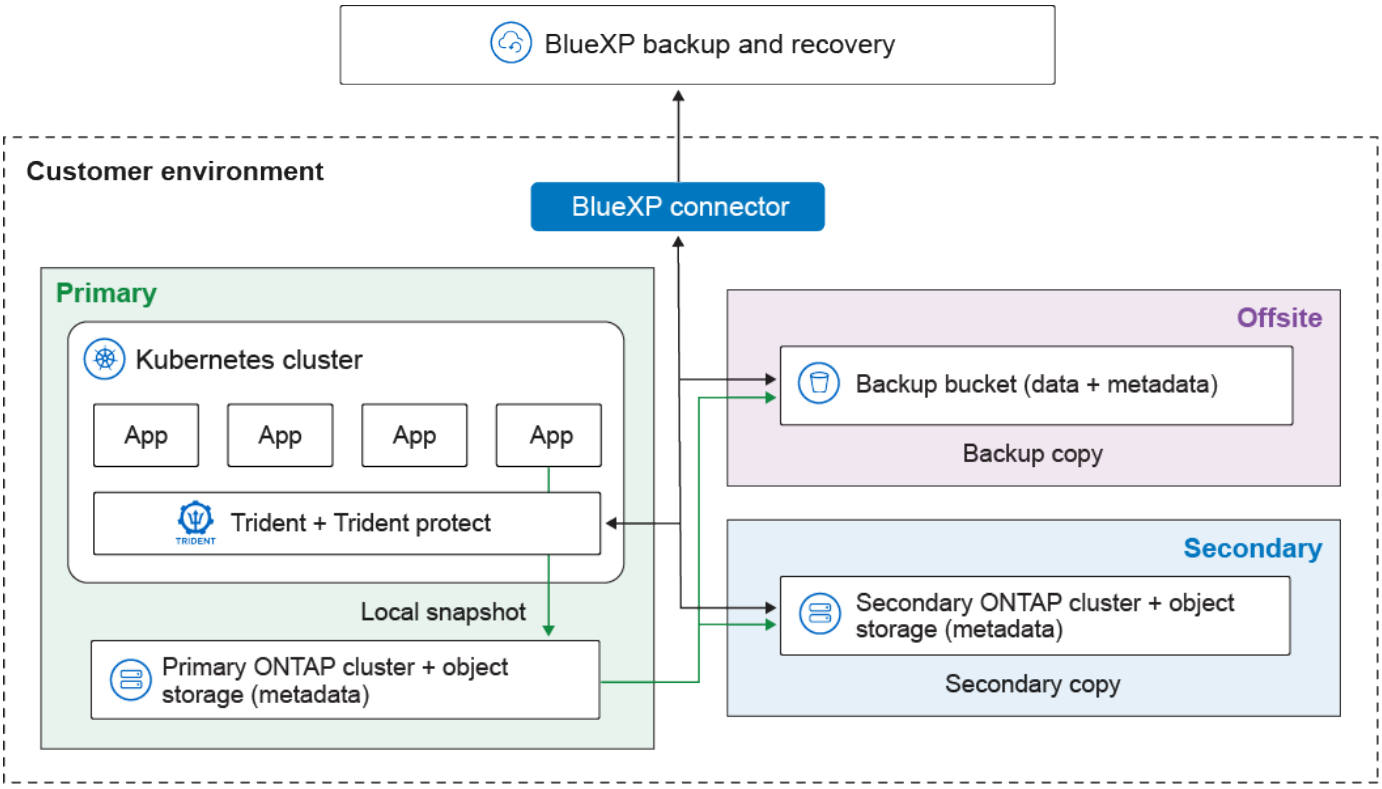
7. Escolha um ponto de recuperação da lista e selecione o ícone Ações ••• > **Desmontar**.
8. Confirme a ação selecionando **Desmontar**.

Proteja as cargas de trabalho do Kubernetes (visualização)

Visão geral do gerenciamento de cargas de trabalho do Kubernetes

Gerenciar cargas de trabalho do Kubernetes no NetApp Backup and Recovery permite que você descubra, gerencie e proteja seus clusters e aplicativos do Kubernetes em um só lugar. Você pode gerenciar recursos e aplicações hospedados em seus clusters do Kubernetes. Você também pode criar e associar políticas de proteção às suas cargas de trabalho do Kubernetes, tudo usando uma única interface.

O diagrama a seguir mostra os componentes e a arquitetura básica de backup e recuperação para cargas de trabalho do Kubernetes e como diferentes cópias dos seus dados podem ser armazenadas em diferentes locais:



O NetApp Backup and Recovery oferece os seguintes benefícios para o gerenciamento de cargas de trabalho do Kubernetes:

- Um único plano de controle para proteger aplicativos executados em vários clusters do Kubernetes. Esses aplicativos podem incluir contêineres ou máquinas virtuais em execução nos seus clusters do Kubernetes.
- Integração nativa com o NetApp SnapMirror, permitindo recursos de descarregamento de armazenamento para todos os fluxos de trabalho de backup e recuperação.
- Backups incrementais permanentes para aplicativos Kubernetes, o que se traduz em Objetivos de Ponto de Recuperação (RPOs) e Objetivos de Tempo de Recuperação (RTOs) mais baixos.

Esta documentação é fornecida como uma prévia da tecnologia. Durante a visualização, a funcionalidade do Kubernetes não é recomendada para cargas de trabalho de produção. Com esta oferta de visualização, a NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da disponibilidade geral.

Você pode realizar as seguintes tarefas relacionadas ao gerenciamento de cargas de trabalho do Kubernetes:

- "Descubra as cargas de trabalho do Kubernetes" .
- "Gerenciar clusters do Kubernetes" .
- "Adicionar e proteger aplicativos Kubernetes" .
- "Gerenciar aplicativos Kubernetes" .
- "Restaurar aplicativos Kubernetes" .

Descubra cargas de trabalho do Kubernetes no NetApp Backup and Recovery

O NetApp Backup and Recovery precisa primeiro descobrir as cargas de trabalho do Kubernetes para que você possa usar o serviço.

Função necessária do NetApp Console Superadministrador de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Descubra as cargas de trabalho do Kubernetes

No inventário de backup e recuperação, você pode descobrir cargas de trabalho do Kubernetes em execução no seu ambiente. A descoberta de uma carga de trabalho adiciona um cluster Kubernetes ao NetApp Backup and Recovery, permitindo que você adicione aplicativos ao cluster e proteja os recursos hospedados pelo cluster.

Passos

1. Faça um dos seguintes:
   - Se você estiver descobrindo cargas de trabalho do Kubernetes pela primeira vez, no NetApp Backup and Recovery, selecione **Descobrir e gerenciar** no tipo de carga de trabalho do Kubernetes.
   - Se você já descobriu cargas de trabalho do Kubernetes, no NetApp Backup and Recovery, selecione **Inventário** > **Cargas de trabalho** e, em seguida, selecione **Descobrir recursos**.
2. Selecione o tipo de carga de trabalho **Kubernetes**.
3. Insira um nome de cluster e escolha um conector para usar com o cluster.
4. Siga as instruções da linha de comando que aparecem:
   - Crie um namespace de proteção Trident
   - Crie um segredo do Kubernetes
   - Adicionar um repositório Helm
   - Instalar o Trident Protect e o conector Trident Protect

     Essas etapas garantem que o NetApp Backup and Recovery possa interagir com o cluster.
5. Após concluir as etapas, selecione **Descobrir**.

   O cluster é adicionado ao inventário.
6. Selecione **Exibir** na carga de trabalho do Kubernetes associada para ver a lista de aplicativos, clusters e namespaces para essa carga de trabalho.

Continue para o Painel de Backup e Recuperação da NetApp

Para exibir o Painel de Backup e Recuperação do NetApp , siga estas etapas.

1. No menu superior, selecione **Painel**.
2. Revise a saúde da proteção de dados. O número de cargas de trabalho em risco ou protegidas aumenta com base nas cargas de trabalho recém-descobertas, protegidas e armazenadas em backup.

   "Saiba o que o Painel mostra para você" .

Adicionar e proteger aplicativos Kubernetes

O NetApp Backup and Recovery permite que você descubra facilmente seus clusters Kubernetes, sem gerar e carregar arquivos kubeconfig. Você pode conectar clusters do Kubernetes e instalar o software necessário usando comandos simples copiados da

interface do usuário do NetApp Console.

Função necessária do NetApp Console

Administrador da organização ou administrador do SnapCenter . "Saiba mais sobre as funções de acesso do NetApp Backup and Recovery" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Adicionar e proteger um novo aplicativo Kubernetes

O primeiro passo para proteger aplicativos Kubernetes é criar um aplicativo no NetApp Backup and Recovery. Ao criar um aplicativo, você torna o Console ciente do aplicativo em execução no cluster do Kubernetes.

Antes de começar

Antes de poder adicionar e proteger um aplicativo Kubernetes, você precisa "descubra as cargas de trabalho do Kubernetes" .

Passos

1. No NetApp Backup and Recovery, selecione **Inventário**.
2. Escolha uma instância do Kubernetes e selecione **Exibir** para visualizar os recursos associados a essa instância.
3. Selecione a aba **Aplicativos**.
4. Selecione **Criar aplicativo**.
5. Digite um nome para o aplicativo.
6. Opcionalmente, escolha qualquer um dos seguintes campos para pesquisar os recursos que você deseja proteger:
   - Cluster associado
   - Espaços de nomes associados
   - Tipos de recursos
   - Seletores de rótulos
7. Opcionalmente, selecione **Recursos com Escopo de Cluster** para escolher quaisquer recursos com escopo no nível do cluster. Se você incluí-los, eles serão adicionados ao aplicativo quando você o criar.
8. Opcionalmente, selecione **Pesquisar** para encontrar os recursos com base nos seus critérios de pesquisa.

   O Console não armazena os parâmetros ou resultados da pesquisa; os parâmetros são usados para pesquisar no cluster Kubernetes selecionado recursos que podem ser incluídos no aplicativo.

9. O Console exibe uma lista de recursos que correspondem aos seus critérios de pesquisa.
10. Se a lista contiver os recursos que você deseja proteger, selecione **Avançar**.
11. Opcionalmente, na área **Política**, escolha uma política de proteção existente para proteger o aplicativo ou crie uma nova. Se você não selecionar uma política, o aplicativo será criado sem uma política de proteção. Você pode"adicionar uma política de proteção" mais tarde.
12. Na área **Prescrições e postscripts**, habilite e configure quaisquer ganchos de execução de prescrições ou postscripts que você deseja executar antes ou depois das operações de backup. Para habilitar prescrições ou pós-escritos, você deve ter criado pelo menos um"modelo de gancho de execução" .

13. Selecione **Criar**.

Resultado

O aplicativo é criado e aparece na lista de aplicativos na guia **Aplicativos** do inventário do Kubernetes. O NetApp Console permite a proteção do aplicativo com base em suas configurações, e você pode monitorar o progresso na área **Monitoramento** de backup e recuperação.

Proteja um aplicativo Kubernetes existente

Habilite uma política de proteção em um aplicativo Kubernetes que você já adicionou.

Passos

1. No NetApp Backup and Recovery, selecione **Inventário**.
2. Escolha uma instância do Kubernetes e selecione **Exibir** para visualizar os recursos associados a essa instância.
3. Selecione a aba **Aplicativos**.
4. Na lista de aplicativos, escolha um aplicativo que você deseja proteger e selecione o menu Ações associado.
5. Selecione **Proteger**.
6. Na área **Política**, escolha uma política de proteção existente para proteger o aplicativo ou crie uma nova política. Consulte"Criar uma política" para obter mais informações sobre a criação de políticas de proteção.
7. Na área **Prescrições e pós-scripts**, habilite e configure quaisquer ganchos de execução de prescrições ou pós-scripts que você deseja executar antes ou depois das operações de backup. Você pode configurar o tipo de gancho de execução, o modelo que ele usa, argumentos e seletores de rótulos.
8. Selecione **Concluído**.

Resultado

O Console ativa a proteção do aplicativo com base em suas configurações, e você pode monitorar o progresso na área **Monitoramento** de backup e recuperação. Assim que você habilita a proteção para um aplicativo, o Console cria um backup completo do aplicativo. Quaisquer backups incrementais futuros são criados com base no agendamento definido na política de proteção associada ao aplicativo.

Faça backup de um aplicativo Kubernetes agora

Crie manualmente um backup de um aplicativo Kubernetes para estabelecer uma linha de base para futuros backups e snapshots ou para garantir que os dados mais recentes estejam protegidos.

Passos

1. No NetApp Backup and Recovery, selecione **Inventário**.
2. Escolha uma instância do Kubernetes e selecione **Exibir** para visualizar os recursos associados a essa instância.
3. Selecione a aba **Aplicativos**.
4. Na lista de aplicativos, escolha um aplicativo que você deseja fazer backup e selecione o menu Ações associado.
5. Selecione **Fazer backup agora**.
6. Certifique-se de que o nome correto do aplicativo esteja selecionado.

7. Selecione **Fazer backup**.

Resultado

O Console cria um backup do aplicativo e exibe o progresso na área **Monitoramento** de Backup e Recuperação. O backup é criado com base na política de proteção associada ao aplicativo.

Restaurar aplicativos Kubernetes

O NetApp Backup and Recovery permite restaurar aplicativos que você protegeu com uma política de proteção. Para restaurar um aplicativo, ele precisa ter pelo menos um ponto de restauração disponível. Um ponto de restauração consiste no snapshot local ou no backup no repositório de objetos (ou ambos). Você pode restaurar um aplicativo usando o arquivo local, secundário ou do repositório de objetos.

Função necessária do NetApp Console

Administrador da organização ou administrador do SnapCenter . "Saiba mais sobre as funções de acesso do NetApp Backup and Recovery" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Passos

1. No NetApp Backup and Recovery, selecione **Inventário**.
2. Escolha uma instância do Kubernetes e selecione **Exibir** para visualizar os recursos associados a essa instância.
3. Selecione a aba **Aplicativos**.
4. Na lista de aplicativos, escolha um aplicativo que você deseja restaurar e selecione o menu Ações associado.
5. Selecione **Exibir e restaurar**.

   A lista de pontos de restauração é exibida.

6. Abra o menu Ações do ponto de restauração que você deseja usar e selecione **Restaurar**.

Configurações gerais

1. Escolha a origem da restauração (local ou armazenamento de objetos).
2. Escolha o cluster de destino na lista **Cluster**.
3. Escolha o namespace de destino da restauração.

   Você pode restaurar para o namespace original ou restaurar para um novo namespace.

4. Selecione **Avançar**.

Seleção de recursos

1. Escolha se deseja restaurar todos os recursos associados ao aplicativo ou usar um filtro para selecionar recursos específicos para restaurar:

Restaurar todos os recursos

1. Selecione **Restaurar todos os recursos**.
2. Selecione **Avançar**.

Restaurar recursos específicos

1. Selecione **Recursos seletivos**.
2. Escolha o comportamento do filtro de recursos. Se você escolher **Incluir**, os recursos selecionados serão restaurados. Se você escolher **Excluir**, os recursos selecionados não serão restaurados.
3. Selecione **Adicionar regras** para adicionar regras que definem filtros para selecionar recursos. Você precisa de pelo menos uma regra para filtrar recursos.

   Cada regra pode filtrar critérios como namespace do recurso, rótulos, grupo, versão e tipo.
4. Selecione **Salvar** para salvar cada regra.
5. Depois de adicionar todas as regras necessárias, selecione **Pesquisar** para ver os recursos disponíveis no arquivo de backup que correspondem aos seus critérios de filtro.

   Os recursos mostrados são os recursos que existem atualmente no cluster.
6. Quando estiver satisfeito com os resultados, selecione **Avançar**.

Configurações de destino

1. Escolha restaurar para a classe de armazenamento padrão ou para uma classe de armazenamento diferente.
2. Opcionalmente, se você optar por restaurar para uma classe de armazenamento diferente, selecione uma classe de armazenamento de destino para corresponder a cada classe de armazenamento de origem.
3. Selecione **Restaurar**.

Gerenciar clusters do Kubernetes

O NetApp Backup and Recovery permite que você descubra e gerencie seus clusters Kubernetes para que possa proteger os recursos hospedados pelos clusters.

Função necessária do NetApp Console

Administrador da organização ou administrador do SnapCenter . "Saiba mais sobre as funções de acesso do NetApp Backup and Recovery" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Para descobrir clusters do Kubernetes, consulte "Descubra as cargas de trabalho do Kubernetes" .

Editar informações do cluster Kubernetes

Você pode editar um cluster se precisar alterar seu nome.

Passos

1. No NetApp Backup and Recovery, selecione **Inventário** > **Clusters**.
2. Na lista de clusters, escolha um cluster que você deseja editar e selecione o menu Ações associado.
3. Selecione **Editar cluster**.
4. Faça as alterações necessárias no nome do cluster. O nome do cluster precisa corresponder ao nome que você usou com o comando Helm durante o processo de descoberta.
5. Selecione **Concluído**.

Remover um cluster do Kubernetes

Se você não precisar mais proteger os recursos hospedados por um cluster Kubernetes, poderá removê-lo do NetApp Backup and Recovery. A remoção de um cluster não exclui o cluster nem seus recursos; apenas remove o cluster do inventário do NetApp Console. Antes de remover um cluster, você precisa desabilitar a proteção e excluir os aplicativos associados do NetApp Backup and Recovery.

Passos

1. No NetApp Backup and Recovery, selecione **Inventário** > **Clusters**.
2. Na lista de clusters, escolha um cluster que você deseja editar e selecione o menu Ações associado.
3. Selecione **Remover cluster**.
4. Revise as informações na caixa de diálogo de confirmação e selecione **Remover**.

Gerenciar aplicativos Kubernetes

O NetApp Backup and Recovery permite que você desproteja e exclua seus aplicativos Kubernetes e recursos associados.

Função necessária do NetApp Console

Administrador da organização ou administrador do SnapCenter . "Saiba mais sobre as funções de acesso do NetApp Backup and Recovery" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Desproteger um aplicativo Kubernetes

Você pode desproteger um aplicativo se não quiser mais protegê-lo. Quando você desprotege um aplicativo, o NetApp Backup and Recovery para de protegê-lo, mas mantém todos os backups e instantâneos associados.

Passos

1. No NetApp Backup and Recovery, selecione **Inventário**.
2. Escolha uma instância do Kubernetes e selecione **Exibir** para visualizar os recursos associados a essa instância.
3. Selecione a aba **Aplicativos**.
4. Na lista de aplicativos, escolha um aplicativo que você deseja desproteger e selecione o menu Ações associado.
5. Selecione **Desproteger**.
6. Leia o aviso e, quando estiver pronto, selecione **Desproteger**.

Excluir um aplicativo Kubernetes

Você pode excluir um aplicativo se não precisar mais dele. Quando você exclui um aplicativo, o NetApp Backup and Recovery para de protegê-lo e exclui todos os backups e snapshots associados.

Passos

1. No NetApp Backup and Recovery, selecione **Inventário**.
2. Escolha uma instância do Kubernetes e selecione **Exibir** para visualizar os recursos associados a essa instância.
3. Selecione a aba **Aplicativos**.
4. Na lista de aplicativos, escolha um aplicativo que você deseja excluir e selecione o menu Ações associado.
5. Selecione **Excluir**.
6. Habilite **Excluir snapshots e backups** para remover todos os snapshots e backups do aplicativo.

   Você não poderá mais restaurar o aplicativo usando esses snapshots e backups.

7. Confirme a ação e selecione **Excluir**.

Gerenciar modelos de ganchos de execução de backup e recuperação do NetApp para cargas de trabalho do Kubernetes

Um gancho de execução é uma ação personalizada que você pode configurar para ser executada em conjunto com uma operação de proteção de dados de um aplicativo Kubernetes gerenciado. Por exemplo, se você tiver um aplicativo de banco de dados, poderá usar um gancho de execução para pausar todas as transações do banco de dados antes de um instantâneo e retomar as transações após a conclusão do instantâneo. Isso garante instantâneos consistentes com o aplicativo. Ao criar um modelo de gancho de execução, você pode especificar o tipo de gancho, o script a ser executado e quaisquer filtros que determinem a quais contêineres o gancho se aplica. Você pode então usar o modelo para associar ganchos de execução aos seus aplicativos.

Por padrão, o NetApp Backup and Recovery congela e descongela automaticamente os sistemas de arquivos de determinados aplicativos, como o KubeVirt, durante operações de proteção de dados. Opcionalmente, você pode desabilitar esse comportamento globalmente ou para aplicativos específicos usando instruções da documentação do Trident Protect:

- Para desabilitar esse comportamento para todos os aplicativos, consulte "Protegendo dados com VMs KubeVirt" .
- Para desabilitar esse comportamento para um aplicativo específico, consulte "Definir uma aplicação" .

Função necessária do NetApp Console

Administrador da organização ou administrador do SnapCenter . "Saiba mais sobre as funções de acesso do NetApp Backup and Recovery" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Tipos de ganchos de execução

O NetApp Backup and Recovery oferece suporte aos seguintes tipos de ganchos de execução, com base em quando eles podem ser executados:

- Pré-instantâneo
- Pós-instantâneo
- Pré-backup
- Pós-backup
- Pós-restauração

Ordem de execução

Quando uma operação de proteção de dados é executada, os eventos de gancho de execução ocorrem na seguinte ordem:

1. Todos os ganchos de execução de pré-operação personalizados aplicáveis são executados nos contêineres apropriados. Você pode criar e executar quantos ganchos de pré-operação personalizados precisar, mas a ordem de execução desses ganchos antes da operação não é garantida nem configurável.
2. Congelamentos do sistema de arquivos ocorrem, se aplicável.
3. A operação de proteção de dados é realizada.
4. Sistemas de arquivos congelados são descongelados, se aplicável.
5. Todos os ganchos de execução pós-operação personalizados aplicáveis são executados nos contêineres apropriados. Você pode criar e executar quantos ganchos pós-operação personalizados precisar, mas a ordem de execução desses ganchos após a operação não é garantida nem configurável.

Se você criar vários ganchos de execução do mesmo tipo (por exemplo, pré-instantâneo), a ordem de execução desses ganchos não será garantida. Entretanto, a ordem de execução de ganchos de diferentes tipos é garantida. Por exemplo, a seguir está a ordem de execução de uma configuração que possui todos os diferentes tipos de ganchos:

1. Ganchos pré-instantâneos executados
2. Ganchos pós-instantâneos executados
3. Ganchos de pré-backup executados
4. Ganchos pós-backup executados

> Você deve sempre testar seus scripts de gancho de execução antes de habilitá-los em um ambiente de produção. Você pode usar o comando 'kubectl exec' para testar os scripts convenientemente. Depois de habilitar os ganchos de execução em um ambiente de produção, teste os snapshots e backups resultantes para garantir que sejam consistentes. Você pode fazer isso clonando o aplicativo em um namespace temporário, restaurando o snapshot ou backup e, em seguida, testando o aplicativo.

> Se um gancho de execução pré-snapshot adicionar, alterar ou remover recursos do Kubernetes, essas alterações serão incluídas no snapshot ou backup e em qualquer operação de restauração subsequente.

Notas importantes sobre ganchos de execução personalizados

Considere o seguinte ao planejar ganchos de execução para seus aplicativos.

- Um gancho de execução deve usar um script para executar ações. Muitos ganchos de execução podem referenciar o mesmo script.
- Os ganchos de execução precisam ser escritos no formato de scripts de shell executáveis.
- O tamanho do script é limitado a 96 KB.
- As configurações do gancho de execução e quaisquer critérios correspondentes são usados para determinar quais ganchos são aplicáveis a uma operação de snapshot, backup ou restauração.

> Como os ganchos de execução geralmente reduzem ou desabilitam completamente a funcionalidade do aplicativo em que estão sendo executados, você deve sempre tentar minimizar o tempo que seus ganchos de execução personalizados levam para serem executados. Se você iniciar uma operação de backup ou snapshot com ganchos de execução associados, mas depois cancelá-la, os ganchos ainda poderão ser executados se a operação de backup ou snapshot já tiver começado. Isso significa que a lógica usada em um gancho de execução pós-backup não pode assumir que o backup foi concluído.

Filtros de gancho de execução

Ao adicionar ou editar um gancho de execução para um aplicativo, você pode adicionar filtros ao gancho de execução para gerenciar quais contêineres o gancho corresponderá. Os filtros são úteis para aplicativos que usam a mesma imagem de contêiner em todos os contêineres, mas podem usar cada imagem para uma finalidade diferente (como o Elasticsearch). Os filtros permitem que você crie cenários em que os ganchos de execução são executados em alguns contêineres idênticos, mas não necessariamente em todos. Se você criar vários filtros para um único gancho de execução, eles serão combinados com um operador lógico AND. Você pode ter até 10 filtros ativos por gancho de execução.

Cada filtro que você adiciona a um gancho de execução usa uma expressão regular para corresponder aos contêineres no seu cluster. Quando um gancho corresponde a um contêiner, o gancho executará seu script associado naquele contêiner. Expressões regulares para filtros usam a sintaxe Regular Expression 2 (RE2), que não oferece suporte à criação de um filtro que exclua contêineres da lista de correspondências. Para obter informações sobre a sintaxe que o NetApp Backup and Recovery oferece suporte para expressões regulares em filtros de gancho de execução, consulte "Suporte à sintaxe de Expressão Regular 2 (RE2)" .

> Se você adicionar um filtro de namespace a um gancho de execução executado após uma operação de restauração ou clonagem e a origem e o destino da restauração ou clonagem estiverem em namespaces diferentes, o filtro de namespace será aplicado somente ao namespace de destino.

Exemplos de ganchos de execução

Visite o "Projeto NetApp Verda GitHub" para baixar ganchos de execução reais para aplicativos populares, como Apache Cassandra e Elasticsearch. Você também pode ver exemplos e obter ideias para estruturar seus próprios ganchos de execução personalizados.

Crie um modelo de gancho de execução

Você pode criar um modelo de gancho de execução personalizado que pode ser usado para executar ações antes ou depois de uma operação de proteção de dados em um aplicativo.

Passos

1. No Console, vá para **Proteção** > **Backup e recuperação**.
2. Selecione a aba **Configurações**.
3. Expanda a seção **Modelo de gancho de execução**.
4. Selecione **Criar modelo de gancho de execução**.
5. Digite um nome para o gancho de execução.
6. Opcionalmente, escolha um tipo de gancho. Por exemplo, um gancho pós-restauração é executado após a conclusão da operação de restauração.
7. Na caixa de texto **Script**, insira o script de shell executável que você deseja executar como parte do modelo de gancho de execução. Opcionalmente, você pode selecionar **Carregar script** para carregar um arquivo de script.
8. Selecione **Criar**.

   O modelo é criado e aparece na lista de modelos na seção **Modelo de gancho de execução**.

Monitorar tarefas no NetApp Backup and Recovery

Com o NetApp Backup and Recovery, monitore o status de snapshots locais, replicações e trabalhos de backup em armazenamento de objetos que você iniciou, além de trabalhos de restauração que você iniciou. Você pode ver os trabalhos que foram concluídos, estão em andamento ou falharam para poder diagnosticar e corrigir problemas. Usando o NetApp Console Notification Center, você pode habilitar o envio de notificações por e-mail para que você possa ser informado sobre atividades importantes do sistema, mesmo quando não estiver conectado ao sistema. Usando a Linha do tempo do console, você pode ver detalhes de todas as ações iniciadas por meio da interface do usuário ou da API.

O NetApp Backup and Recovery retém as informações do trabalho por 15 dias, após os quais elas são apagadas e não ficam mais visíveis no Job Monitor.

Função necessária do NetApp Console Visualizador de armazenamento, superadministrador de backup e recuperação, administrador de backup e recuperação, administrador de restauração de backup e recuperação, administrador de clone de backup e recuperação ou função de visualizador de backup e recuperação. Aprenda sobre"Funções e privilégios de backup e recuperação" . "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços" .

Ver o status do trabalho no Job Monitor

Você pode visualizar uma lista de todas as operações de snapshot, replicação, backup para armazenamento de objetos e restauração e seus status atuais na guia **Monitoramento de tarefas**. Isso inclui operações do seu Cloud Volumes ONTAP, ONTAP local, aplicativos e máquinas virtuais. Cada operação, ou trabalho, tem um ID e um status exclusivos.

O status pode ser:

- Sucesso
- Em andamento

- Na fila
- Aviso
- Fracassado

Snapshots, replicações, backups para armazenamento de objetos e operações de restauração que você iniciou na interface do usuário e na API do NetApp Backup and Recovery estão disponíveis na guia Monitoramento de tarefas.

Se você atualizou seus sistemas ONTAP para 9.13.x e não vê operações de backup agendadas em andamento no Job Monitor, será necessário reiniciar o NetApp Backup and Recovery. "Aprenda a reiniciar o NetApp Backup and Recovery" .

Passos

1. No menu NetApp Backup and Recovery, selecione **Monitoramento**.
2. Para mostrar colunas adicionais (Sistema, SVM, Nome de usuário, Carga de trabalho, Nome da política, Rótulo de instantâneo), selecione o sinal de mais.

Pesquise e filtre a lista de empregos

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

Por padrão, a página Monitoramento de tarefas mostra tarefas de proteção e recuperação das últimas 24 horas. Você pode alterar o período usando o filtro Período de tempo.

Passos

1. No menu NetApp Backup and Recovery, selecione **Monitoramento**.
2. Para classificar os resultados de forma diferente, selecione cada título de coluna para classificar por Status, Hora de início, Nome do recurso e muito mais.
3. Se você estiver procurando por empregos específicos, selecione a área **Pesquisa e filtragem avançadas** para abrir o painel de pesquisa.

   Use este painel para inserir uma pesquisa de texto livre para qualquer recurso; por exemplo, "volume 1" ou "aplicativo 3". Você também pode filtrar a lista de trabalhos de acordo com os itens nos menus suspensos.

   A maioria dos filtros é autoexplicativa. O filtro "Carga de trabalho" permite que você visualize trabalhos nas seguintes categorias:

   - Volumes ONTAP (Cloud Volumes ONTAP e volumes ONTAP locais)
   - Servidor Microsoft SQL
   - Máquinas Virtuais
   - Kubernetes

   - Você pode pesquisar dados dentro de um "SVM" específico somente se tiver selecionado primeiro um Sistema.
   - Você pode pesquisar usando o filtro "Tipo de proteção" somente quando tiver selecionado o "Tipo" de "Proteção".

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

Ver detalhes do trabalho

Você pode visualizar detalhes correspondentes a um trabalho concluído específico. Você pode exportar detalhes de um trabalho específico em um formato JSON.

Você pode visualizar detalhes como tipo de trabalho (agendado ou sob demanda), tipo de backup do SnapMirror (inicial ou periódico), horários de início e término, duração, quantidade de dados transferidos do sistema para o armazenamento de objetos, taxa média de transferência, nome da política, bloqueio de retenção habilitado, verificação de ransomware realizada, detalhes da origem da proteção e detalhes do destino da proteção.

Os trabalhos de restauração mostram detalhes como provedor de destino de backup (Amazon Web Services, Microsoft Azure, Google Cloud, local), nome do bucket S3, nome do SVM, nome do volume de origem, volume de destino, rótulo do instantâneo, contagem de objetos recuperados, nomes de arquivos, tamanhos de arquivos, data da última modificação e caminho completo do arquivo.

Passos

1. No menu NetApp Backup and Recovery, selecione **Monitoramento**.
2. Selecione o nome do trabalho.
3. Selecione o menu Ações ••• e selecione **Ver detalhes**.
4. Expanda cada seção para ver detalhes.

Baixe os resultados do monitoramento de tarefas como um relatório

Você pode baixar o conteúdo da página principal do Job Monitoring como um relatório depois de refiná-lo. O NetApp Backup and Recovery gera e baixa um arquivo .CSV que você pode revisar e enviar para outros grupos, conforme necessário. O arquivo .CSV inclui até 10.000 linhas de dados.

Nas informações de Detalhes do monitoramento de trabalho, você pode baixar um arquivo JSON contendo detalhes de um único trabalho.

Passos

1. No menu NetApp Backup and Recovery, selecione **Monitoramento**.
2. Para baixar um arquivo CSV para todos os trabalhos, selecione o botão Download e localize o arquivo no seu diretório de download.
3. Para baixar um arquivo JSON para um único trabalho, selecione o menu Ações ••• para o trabalho, selecione **Baixar arquivo JSON** e localize o arquivo no seu diretório de download.

Revisar tarefas de retenção (ciclo de vida de backup)

O monitoramento dos fluxos de retenção (ou *ciclo de vida do backup*) ajuda você com a integridade da auditoria, a responsabilização e a segurança do backup. Para ajudar você a rastrear 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 rastreia todas as cópias de Snapshot que são excluídas ou estão na fila para serem excluídas. A partir do ONTAP 9.13, você pode ver todos os tipos de trabalho chamados "Retenção" na página Monitoramento de Trabalho.

O tipo de trabalho "Retenção" captura todos os trabalhos de exclusão de instantâneo iniciados em um volume protegido pelo NetApp Backup and Recovery.

Passos

1. No menu NetApp Backup and Recovery, selecione **Monitoramento**.
2. Selecione a área **Pesquisa e filtragem avançadas** para abrir o painel Pesquisa.
3. Selecione "Retenção" como o tipo de trabalho.

Revise os alertas de backup e restauração no Centro de Notificações do NetApp Console

O Centro de Notificações do NetApp Console rastreia o progresso dos trabalhos de backup e restauração que você iniciou 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 Console 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 conectado ao sistema. "Saiba mais sobre o Centro 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 por e-mail:

Tipo de operação	Evento	Nível de alerta	E-mail enviado
Ativação	Falha na ativação do backup e recuperação do sistema	Erro	Sim
Ativação	Falha na edição de backup e recuperação do sistema	Erro	Sim
Instantâneo local	Falha na tarefa de criação de snapshot ad hoc do NetApp Backup and Recovery	Erro	Sim
Replicação	Falha na tarefa de replicação ad hoc do NetApp Backup and Recovery	Erro	Sim
Replicação	Falha na tarefa de pausa de replicação do NetApp Backup and Recovery	Erro	Não
Replicação	Falha na tarefa de interrupção da replicação do NetApp Backup and Recovery	Erro	Não
Replicação	Falha na tarefa de ressincronização de replicação do NetApp Backup and Recovery	Erro	Não
Replicação	Falha na tarefa de interrupção da replicação do NetApp Backup and Recovery	Erro	Não
Replicação	Falha na tarefa de ressincronização reversa da replicação do NetApp Backup and Recovery	Erro	Sim
Replicação	Falha na exclusão da tarefa de replicação do NetApp Backup and Recovery	Erro	Sim

A partir do ONTAP 9.13.0, todos os alertas aparecem para o Cloud Volumes ONTAP e sistemas ONTAP locais. Para sistemas com Cloud Volumes ONTAP 9.13.0 e ONTAP local, somente o alerta relacionado a "Trabalho de restauração concluído, mas com avisos" é exibido.

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

Para receber alertas por e-mail do NetApp Backup and Recovery, você precisará selecionar os tipos de gravidade de notificação "Crítico", "Aviso" e "Erro" na página de configurações de Notificações.

"Aprenda a enviar e-mails de alerta para tarefas de backup e restauração" .

Passos

1. No menu Console, selecione ( ).
2. Revise as notificações.

Revisar a atividade da operação na Linha do Tempo do Console

Você pode visualizar detalhes das operações de backup e restauração para investigação posterior na Linha do tempo do console. A Linha do tempo do console fornece detalhes de cada evento, seja iniciado pelo usuário ou pelo sistema, e mostra ações iniciadas na interface do usuário ou por meio da API.

"Saiba mais sobre as diferenças entre a Linha do Tempo e a Central de Notificações" .

Reinicie o NetApp Backup and Recovery

Pode haver situações em que você precisará reiniciar o NetApp Backup and Recovery.

A funcionalidade de backup e recuperação do NetApp está integrada ao agente do Console.

Passos

1. Conecte-se ao sistema Linux no qual o agente do Console está sendo executado.

Localização do agente do console	Procedimento
Implantação em nuvem	Siga as instruções para "conectando-se à máquina virtual Linux do agente do console" dependendo do provedor de nuvem que você estiver usando.
Instalação manual	Efetue login no sistema Linux.

2. Digite o comando para reiniciar o serviço.

Localização do agente do console	Comando Docker	Comando Podman
Implantação em nuvem	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`

Localização do agente do console	Comando Docker	Comando Podman
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`

Automatize com APIs REST de backup e recuperação da NetApp

Os recursos de backup e recuperação do NetApp disponíveis por meio da interface de usuário da Web também estão disponíveis por meio da API RESTful.

Há dez categorias de endpoints definidas no NetApp Backup and Recovery:

- backup - gerencia 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 NetApp Console
- trabalho - gerencia entradas de detalhes do trabalho no banco de dados do NetApp Console
- licença - recupera a validade da licença dos sistemas do NetApp Console
- verificação de ransomware - inicia uma verificação de ransomware em um arquivo de backup específico
- restaurar - permite que você execute 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 (Navegar e Restaurar)
- storagegrid - recupera detalhes sobre um servidor StorageGRID e permite que você descubra um servidor StorageGRID
- sistema - gerencia as políticas de backup e configura o armazenamento de objetos de destino associado a um sistema

Referência de API

A documentação para cada API de backup e recuperação da NetApp está disponível em "Automação do NetApp Console para backup e recuperação do NetApp" .

Começando

Para começar a usar as APIs de backup e recuperação do NetApp , você precisará obter um token de usuário, sua ID de conta do NetApp Console e a ID do agente do Console.

Ao fazer chamadas de API, você adicionará o token do usuário no cabeçalho Authorization e o ID do agente do Console no cabeçalho x-agent-id. Você deve usar o ID da conta do NetApp Console nas APIs.

Se estiver usando uma conta de serviço, você deverá usar o token de acesso de serviço em vez de um token de usuário. O valor para "client_id" ("Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC") é um valor fixo e não pode ser alterado. Neste caso, siga as instruções aqui: "Crie um token de acesso ao serviço" .

Passos

1. Obtenha um token de usuário no site do NetApp NetApp Console.

   Certifique-se de gerar o token de atualização no seguinte xref:./ https://services.cloud.netapp.com/refresh-

token/. O token de atualização é uma sequência 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 do usuário do site do NetApp Console tem uma data de validade. A resposta da API inclui um campo "expires_in" que indica quando o token expira. Para atualizar o token, você precisará chamar esta API novamente.

2. Obtenha o ID da sua conta do NetApp Console.

```
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 o ID do agente do Console.
```

```
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 NetApp Backup and Recovery em um sistema com uma nova política que tem rótulos diários, horários e semanais definidos, arquivamento após dias definido como 180 dias, na região East-US-2 na nuvem do Azure. Observe que isso só habilita o backup no sistema, mas nenhum volume é copiado.

Solicitação de API

Você verá que usamos o ID da conta do NetApp Console `account-DpTFcxN3` , ID do agente do console `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients` , e 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
        }
    ]
}
```

Monitore até que o "status" seja "CONCLUÍDO".

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "COMPLETED",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

Referência

Políticas no SnapCenter comparadas com aquelas no NetApp Backup and Recovery

Há algumas diferenças entre as políticas usadas no SnapCenter e aquelas usadas no NetApp Backup and Recovery que podem afetar o que você vê após importar recursos e políticas do SnapCenter.

Níveis de programação

O SnapCenter usa os seguintes níveis de agendamento:

- **Por hora**: Várias horas e minutos com quaisquer horas (0-23) e quaisquer minutos (0-60).
- **Diariamente**: Inclui uma opção para repetir a cada tantos dias, por exemplo, a cada 3 dias.
- **Semanal**: de domingo a segunda-feira, com a opção de realizar um snapshot no primeiro dia da semana ou em vários dias da semana.
- **Mensal**: Meses de janeiro a dezembro, com opção de execução em dias específicos do mês, por exemplo, no dia 7 de cada mês e até mesmo em vários dias do mês.

O NetApp Backup and Recovery usa os seguintes níveis de agendamento, que são ligeiramente diferentes:

- **Por hora**: executa instantâneos somente em intervalos de 15 minutos, por exemplo, intervalos de 1 hora ou 15 minutos menores que 60.
- **Diariamente**: Horas do dia (0-23) com horário de início, por exemplo, às 10:00, com opção de execução a cada tantas horas.
- **Semanal**: Dia da semana (domingo a segunda-feira) com opção de apresentação em 1 dia ou em vários dias. Isso é o mesmo que o SnapCenter.
- **Mensal**: Datas do mês (0-30) com hora de início em várias datas do mês.
- **Anual**: Mensal. Isso corresponde ao mensal do SnapCenter.

Várias políticas no SnapCenter com o mesmo nível de agendamento

Você pode atribuir várias políticas com o mesmo nível de agendamento a um recurso no SnapCenter. No entanto, o NetApp Backup and Recovery não oferece suporte a várias políticas em um recurso que usa a mesma camada de agendamento.

Exemplo: Se você usar três políticas (para Dados, Log e Log de snapshots) no SnapCenter, após a migração do SnapCenter, o NetApp Backup and Recovery usará uma única política em vez de todas as três.

Agendas diárias importadas do SnapCenter

O NetApp Backup and Recovery ajusta os agendamentos do SnapCenter da seguinte forma:

- Se o agendamento do SnapCenter for definido como menor ou igual a 7 dias, o NetApp Backup and Recovery definirá o agendamento como semanal. Alguns instantâneos serão pulados durante a semana.

  Exemplo: Se você tiver uma política diária do SnapCenter com um intervalo de repetição de 3 dias a partir

de segunda-feira, o NetApp Backup and Recovery definirá o agendamento para semanalmente às segundas, quintas e domingos. Alguns dias serão pulados porque não são exatamente a cada 3 dias.

- Se o agendamento do SnapCenter for definido para mais de 7 dias, o NetApp Backup and Recovery definirá o agendamento como mensal. Alguns instantâneos serão ignorados durante o mês.

  Exemplo: Se você tiver uma política diária do SnapCenter com um intervalo de repetição de 10 dias a partir do dia 2 do mês, o NetApp Backup and Recovery (pós-migração) definirá o agendamento como mensal nos dias 2, 12 e 22 do mês. Alguns dias serão pulados no mês seguinte.

Cronogramas horários importados do SnapCenter

As políticas horárias do SnapCenter com intervalos de repetição maiores que uma hora são convertidas em uma política diária no NetApp Backup and Recovery.

Qualquer política horária com intervalos repetidos que não sejam um fator de 24 (por exemplo, 5, 7, etc.) pulará alguns instantâneos em um dia.

Exemplo: Se você tiver uma política horária do SnapCenter com um intervalo de repetição a cada 5 horas, começando à 1h, o NetApp Backup and Recovery (após a migração) definirá a programação como diária com intervalos de 5 horas à 1h, 6h, 11h, 16h e 21h. Algumas horas serão ignoradas, depois das 21:00 deve ser 2:00 da manhã para repetir a cada 5 horas, mas será sempre 1:00 da manhã.

Retenção de logs de políticas do SnapCenter

Se você tiver um recurso no SnapCenter com várias políticas, o NetApp Backup and Recovery usará a seguinte ordem de prioridade para atribuir o valor de retenção de log:

- Para "Backup completo com política de backup de log" mais políticas "somente log" no SnapCenter, o NetApp Backup and Recovery usa o valor de retenção da política somente log.
- Para as políticas "Backup completo somente com log" e "Completo e log" no SnapCenter, o NetApp Backup and Recovery usa o valor de retenção somente log.
- Para "Backup completo e log" mais "Backup completo" no SnapCenter, o NetApp Backup and Recovery usa o valor de retenção "Backup completo e log".
- Se você tiver apenas um backup completo no SnapCenter, o NetApp Backup and Recovery não habilitará o backup de log.

Retenção de backup de log

Com o SnapCenter, você pode ter vários valores de retenção em várias políticas anexadas a um recurso. No entanto, o NetApp Backup and Recovery oferece suporte apenas a um único valor de retenção para todas as políticas anexadas a um recurso.

Contagem de retenção de políticas do SnapCenter

Se você tiver um recurso com proteção secundária habilitada no SnapCenter com vários volumes de origem, vários volumes de destino e vários relacionamentos SnapMirror , o NetApp Backup and Recovery usará apenas a contagem de retenção da primeira política.

Exemplo: Se você tiver uma política do SnapCenter com uma contagem de retenção de 5 e outra política com uma contagem de retenção de 10, o NetApp Backup and Recovery usará a contagem de retenção de 5.

Rótulos SnapMirror de políticas SnapCenter

Os rótulos do SnapMirror para cada política no SnapCenter permanecem intactos após a migração, mesmo que o nível seja alterado.

Exemplo: Uma política horária do SnapCenter pode mudar para diária no NetApp Backup and Recovery. No entanto, os rótulos do SnapMirror permanecem os mesmos após a migração.

Funções de gerenciamento de identidade e acesso (IAM) do NetApp Backup and Recovery

O NetApp Backup and Recovery emprega o Identity and Access Management (IAM) para controlar o acesso que cada usuário tem a recursos e ações específicos.

Para saber mais sobre as funções do IAM específicas do NetApp Backup and Recovery, consulte "Funções de backup e recuperação do NetApp no NetApp Console" .

Restaurar dados de configuração do NetApp Backup and Recovery em um site escuro

Ao usar o NetApp Backup and Recovery em um site sem acesso à Internet, conhecido como *modo privado*, os dados de configuração do NetApp Backup and Recovery são copiados para o bucket StorageGRID ou ONTAP S3 onde seus backups estão sendo armazenados. Se você tiver um problema com o sistema host do agente do Console, poderá implantar um novo agente do Console e restaurar os dados críticos do NetApp Backup and Recovery.

Este procedimento se aplica somente aos dados de volume ONTAP .

Quando você usa o NetApp Backup and Recovery em um ambiente SaaS onde o agente do Console é implantado no seu provedor de nuvem ou no seu próprio sistema host que tem acesso à Internet, todos os dados importantes de configuração do NetApp Backup and Recovery são armazenados em backup e protegidos na nuvem. Se você tiver um problema com o agente do Console, basta criar um novo agente do Console e adicionar seus sistemas e os detalhes do backup serão restaurados automaticamente.

Existem dois tipos de dados que são copiados:

- Banco de dados de backup e recuperação da NetApp - contém uma listagem de todos os volumes, arquivos de backup, políticas de backup e informações de configuração.
- Arquivos de catálogo indexados - contêm índices detalhados usados para a funcionalidade de pesquisa e restauração, tornando suas pesquisas muito rápidas e eficientes ao procurar dados de volume que você deseja restaurar.

É feito backup desses dados uma vez por dia à meia-noite, e no máximo 7 cópias de cada arquivo são retidas. Se o agente do Console estiver gerenciando vários sistemas ONTAP locais, os arquivos de backup e recuperação do NetApp estarão localizados no bucket do sistema que foi ativado primeiro.

Nenhum dado de volume é incluído no banco de dados do NetApp Backup and Recovery ou nos arquivos do Catálogo Indexado.

Restaurar dados de backup e recuperação do NetApp para um novo agente do Console

Se o seu agente do Console local tiver uma falha catastrófica, você precisará instalar um novo agente do Console e restaurar os dados do NetApp Backup and Recovery para o novo agente do Console.

Você precisará executar as seguintes tarefas para retornar seu sistema NetApp Backup and Recovery a um estado de funcionamento:

- Instalar um novo agente do Console
- Restaurar o banco de dados de backup e recuperação do NetApp
- Restaurar os arquivos do catálogo indexado
- Redescubra todos os seus sistemas ONTAP locais e sistemas StorageGRID na interface de usuário do NetApp Console

Depois de verificar se seu sistema está funcionando novamente, recomendamos que você crie novos arquivos de backup.

O que você vai precisar

Você precisará acessar os backups de banco de dados e índice mais recentes do bucket StorageGRID ou ONTAP S3 onde seus arquivos de backup estão sendo armazenados:

- Arquivo de banco de dados MySQL do NetApp Backup and Recovery

  Este arquivo está localizado no seguinte local no bucket `netapp-backup-<GUID>/mysql_backup/` , e é chamado `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Arquivo zip de backup do catálogo indexado

  Este arquivo está localizado no seguinte local no bucket `netapp-backup-<GUID>/catalog_backup/` , e é chamado `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Instalar um novo agente de console em um novo host Linux local

Ao instalar um novo agente do Console, certifique-se de baixar a mesma versão do software que você instalou no agente do Console original. Alterações periódicas na estrutura do banco de dados do NetApp Backup and Recovery podem tornar as versões mais recentes do software incompatíveis com os backups originais do banco de dados. Você pode "atualize o software do agente do Console para a versão mais atual após restaurar o banco de dados de backup" .

1. "Instale o agente do Console em um novo host Linux local"
2. Efetue login no Console usando as credenciais de usuário administrador que você acabou de criar.

Restaurar o banco de dados de backup e recuperação do NetApp

1. Copie o backup do MySQL do local de backup para o novo host do agente do Console. Usaremos o nome de arquivo de exemplo "CBS_DB_Backup_23_05_2023.sql" abaixo.
2. Copie o backup para o contêiner Docker do MySQL usando um dos seguintes comandos, dependendo se você estiver usando um contêiner 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. Entre no shell do contêiner MySQL usando um dos seguintes comandos, dependendo se você estiver usando um contêiner Docker ou Podman:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. No shell do contêiner, implante o "env".
5. Você precisará da senha do banco de dados MySQL, então copie o valor da chave "MYSQL_ROOT_PASSWORD".
6. Restaure o banco de dados MySQL do NetApp Backup and Recovery usando o seguinte comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verifique se o NetApp Backup and Recovery MySQL DB foi restaurado corretamente usando os seguintes comandos SQL:

```
mysql -u root -p cloud_backup
```

Digite a senha.

```
mysql> show tables;
mysql> select * from volume;
```

Verifique se os volumes exibidos são os mesmos que existiam no seu ambiente original.

Restaurar os arquivos do 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 agente do Console 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 garantir que a pasta "catalogdb1" foi criada com as subpastas "changes" e "snapshots" abaixo.

Descubra seus clusters ONTAP e sistemas StorageGRID

1. "Descubra todos os sistemas ONTAP on-prem"que estavam disponíveis no seu ambiente anterior. Isso inclui o sistema ONTAP que você usou como servidor S3.
2. "Descubra seus sistemas StorageGRID" .

Configurar os detalhes do ambiente StorageGRID

Adicione os detalhes do sistema StorageGRID associado aos seus sistemas ONTAP conforme eles foram configurados na configuração original do agente do Console usando o "APIs do console NetApp" .

As informações a seguir se aplicam a instalações em modo privado a partir do NetApp Console 3.9.xx. Para versões mais antigas, use o seguinte procedimento: "DarkSite Cloud Backup: backup e restauração de MySQL e catálogo indexado" .

Você precisará executar essas etapas para cada sistema 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 '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":"pa
ssword"}
> '
```

   Embora o endereço IP, o nome de usuário e as senhas sejam valores personalizados, o nome da conta não é. O nome da conta é sempre "account-DARKSITE1". Além disso, o nome de usuário deve usar um nome no formato de e-mail.

   Esta API retornará uma resposta como a seguinte. Você pode recuperar o token de autorização conforme 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 sistema e o X-Agent-Id usando a API tenancy/external/resource.


```
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 em "resourceIdentifier" denota o *WorkingEnvironment Id* e o valor em "agentId" denota *x-agent-id*.

3. Atualize o banco de dados do NetApp Backup and Recovery com os detalhes do sistema StorageGRID associado aos sistemas. 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 NetApp

1. Selecione cada sistema ONTAP e clique em **Exibir backups** ao lado do serviço de backup e recuperação no painel direito.

   Você poderá ver todos os backups que foram criados para seus volumes.

2. No Painel de restauração, na seção Pesquisar e restaurar, clique em **Configurações de indexação**.

   Certifique-se de que os sistemas que tinham a Catalogação Indexada habilitada anteriormente permaneçam habilitados.

3. Na página Pesquisar e restaurar, execute algumas pesquisas de catálogo para confirmar se a restauração do catálogo indexado foi concluída com sucesso.

Camadas de armazenamento de arquivo AWS compatíveis com o NetApp Backup and Recovery

O NetApp Backup and Recovery oferece suporte a duas classes de armazenamento de arquivamento S3 e à maioria das regiões.

NOTA Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery, consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Classes de armazenamento de arquivamento S3 com suporte para NetApp Backup and Recovery

Quando os arquivos de backup são criados inicialmente, eles são armazenados no armazenamento S3 *Standard*. Esta camada é otimizada para armazenar dados acessados com pouca frequência; mas isso também permite que você os acesse imediatamente. Após 30 dias, os backups passam para a classe de armazenamento S3 *Standard-Infrequent Access* para economizar custos.

Se seus clusters de origem estiverem executando o ONTAP 9.10.1 ou superior, você poderá optar por dividir os backups em camadas no armazenamento *S3 Glacier* ou *S3 Glacier Deep Archive* após um determinado número de dias (normalmente mais de 30 dias) para otimizar ainda mais os custos. Você pode definir isso como "0" ou de 1 a 999 dias. Se você definir como "0" dias, não poderá alterá-lo posteriormente para 1-999 dias.

Os dados nessas camadas não podem ser acessados imediatamente quando necessário e exigirão um custo de recuperação mais alto, então você precisa considerar com que frequência precisará restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre restauração de dados do armazenamento de arquivo.

- Se você não selecionar nenhuma camada de arquivamento em sua primeira política de backup ao ativar o NetApp Backup and Recovery, o *S3 Glacier* será sua única opção de arquivamento para políticas futuras.
- Se você selecionar *S3 Glacier* na sua primeira política de backup, poderá mudar para a camada *S3 Glacier Deep Archive* para futuras políticas de backup para esse cluster.
- Se você selecionar *S3 Glacier Deep Archive* na sua primeira política de backup, essa camada será a única camada de arquivamento disponível para futuras políticas de backup para esse cluster.

Observe que, ao configurar o NetApp Backup and Recovery 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 arquivo

Embora armazenar arquivos de backup mais antigos em armazenamento de arquivo seja muito mais barato do que o armazenamento Standard ou Standard-IA, acessar dados de um arquivo de backup em armazenamento de arquivo para operações de restauração levará mais tempo 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. O S3 Glacier Deep Archive custa menos que o S3 Glacier:

Camada de arquivo	Restaurar Prioridade e Custo		
	Alto	**Padrão**	**Baixo**
Geleira S3	Recuperação mais rápida, custo mais alto	Recuperação mais lenta, menor custo	Recuperação mais lenta, menor custo
Arquivo S3 Glacier Deep		Recuperação mais rápida, custo mais alto	Recuperação mais lenta, menor custo

Cada método tem uma taxa diferente de recuperação por GB e por solicitação. Para obter preços detalhados do S3 Glacier por região da AWS, visite o "Página de preços do Amazon S3" .

Quanto tempo levará para restaurar meus objetos arquivados no Amazon S3 Glacier?

Há 2 partes que compõem o tempo total de restauração:

- **Tempo de recuperação**: O tempo para recuperar o arquivo de backup do arquivo morto e colocá-lo no armazenamento padrão. Às vezes, isso é chamado de período de "reidratação". O tempo de recuperação é diferente dependendo da prioridade de restauração escolhida.

Camada de arquivo	Restaurar prioridade e tempo de recuperação		
	Alto	**Padrão**	**Baixo**
Geleira S3	3-5 minutos	3-5 horas	5-12 horas
Arquivo S3 Glacier Deep		12 horas	48 horas

- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento padrão. Desta vez não é diferente da operação típica de restauração diretamente do armazenamento padrão, quando não se usa uma camada de arquivamento.

Para obter mais informações sobre as opções de recuperação do Amazon S3 Glacier e do S3 Glacier Deep Archive, consulte "Perguntas frequentes da Amazon sobre essas classes de armazenamento" .

Camadas de acesso ao arquivo do Azure com suporte ao NetApp Backup and Recovery

O NetApp Backup and Recovery oferece suporte a uma camada de acesso de arquivamento do Azure e à maioria das regiões.

NOTA Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery, consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Camadas de acesso do Azure Blob com suporte para backup e recuperação do NetApp

Quando os arquivos de backup são criados inicialmente, eles são armazenados na camada de acesso *Cool*. Esta camada é otimizada para armazenar dados que são acessados com pouca frequência, mas que podem ser acessados imediatamente quando necessário.

Se seus clusters de origem estiverem executando o ONTAP 9.10.1 ou superior, você poderá optar por dividir os backups em camadas do armazenamento *Cool* para o *Azure Archive* após um determinado número de dias (normalmente mais de 30 dias) para otimizar ainda mais os custos. Os dados nesta camada não podem ser acessados imediatamente quando necessário e exigirão um custo de recuperação mais alto, então você precisa considerar com que frequência pode precisar restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre restauração de dados do armazenamento de arquivo.

Observe que, ao configurar o NetApp Backup and Recovery com esse tipo de regra de ciclo de vida, você não deve configurar nenhuma regra de ciclo de vida ao configurar o contêiner na sua conta do Azure.

"Saiba mais sobre as camadas de acesso do Azure Blob" .

Restaurar dados do armazenamento de arquivo

Embora armazenar arquivos de backup mais antigos no armazenamento de arquivo seja muito mais barato do que no armazenamento frio, acessar dados de um arquivo de backup no Azure Archive para operações de restauração levará mais tempo e custará mais dinheiro.

Quanto custa restaurar dados do Arquivo do Azure?

Há duas prioridades de restauração que você pode escolher ao recuperar dados do Arquivo do Azure:

- **Alto**: Recuperação mais rápida, custo mais alto
- **Padrão**: Recuperação mais lenta, menor custo

Cada método tem uma taxa diferente de recuperação por GB e por solicitação. Para obter preços detalhados do Azure Archive por 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 Arquivo do Azure?

Existem 2 partes que compõem o tempo de restauração:

- **Tempo de recuperação**: o tempo para recuperar o arquivo de backup arquivado do Azure Archive e colocá-lo no armazenamento frio. Às vezes, isso é chamado de período de "reidratação". O tempo de recuperação é diferente dependendo da prioridade de restauração escolhida:
  - **Alto**: < 1 hora
  - **Padrão**: < 15 horas
- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento Cool. Desta vez não é diferente da operação típica de restauração diretamente do armazenamento Cool, quando não se usa uma camada de arquivamento.

Para obter mais informações sobre as opções de recuperação do Azure Archive, consulte "estas perguntas frequentes do Azure" .

Camadas de armazenamento de arquivo do Google compatíveis com o NetApp Backup and Recovery

O NetApp Backup and Recovery oferece suporte a uma classe de armazenamento de arquivamento do Google e à maioria das regiões.

NOTA Para alternar entre as versões da interface de usuário do NetApp Backup and Recovery, consulte"Mudar para a interface de usuário anterior do NetApp Backup and Recovery" .

Classes de armazenamento de arquivamento do Google com suporte para NetApp Backup and Recovery

Quando os arquivos de backup são criados inicialmente, eles são armazenados no armazenamento *Padrão*. Esta camada é otimizada para armazenar dados acessados com pouca frequência; mas isso também permite que você os acesse imediatamente.

Se o seu cluster local estiver usando o ONTAP 9.12.1 ou superior, você poderá optar por colocar backups mais antigos em camadas no armazenamento *Archive* na interface do NetApp Backup and Recovery após um determinado número de dias (normalmente mais de 30 dias) para otimizar ainda mais os custos. Os dados nessa camada exigirão um custo de recuperação mais alto, então você precisa considerar com que frequência precisará restaurar dados desses arquivos de backup arquivados. Consulte a seção nesta página sobre restauração de dados do armazenamento de arquivo.

Observe que, ao configurar o NetApp Backup and Recovery 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 do Google.

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

Restaurar dados do armazenamento de arquivo

Embora armazenar arquivos de backup mais antigos no armazenamento de arquivo seja muito mais barato do que o armazenamento padrão, acessar dados de um arquivo de backup no armazenamento de arquivo 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?

Há 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 no armazenamento padrão. Às vezes, isso é chamado de período de "reidratação". Ao contrário das soluções de armazenamento "mais frias" fornecidas por outros provedores de nuvem, seus dados ficam acessíveis em milissegundos.
- **Tempo de restauração**: O tempo para restaurar os dados do arquivo de backup no armazenamento padrão. Desta vez não é diferente da operação típica de restauração diretamente do armazenamento padrão, quando não se usa uma camada de arquivamento.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

"https://www.netapp.com/company/legal/copyright/"

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

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 e licenças de terceiros usados no software NetApp .

- "Aviso para o NetApp Console"
- "Aviso sobre o NetApp Backup and Recovery"
- "Aviso para restauração de arquivo único"

Informações sobre direitos autorais

Informações sobre marcas comerciais