Use o NetApp Backup and Recovery

NetApp Backup and Recovery

NetApp
February 11, 2026

Índice

Use o NetApp Backup and Recovery

Visualize a integridade da proteção no Painel de NetApp Backup and Recovery

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 NetApp Backup and Recovery . 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 do NetApp Console , selecione **Proteção** > **Backup e recuperação**.
2. Selecione um bloco de carga de trabalho (por exemplo, Microsoft SQL Server).
3. No menu Backup e Recuperação, selecione **Painel**.

   Você pode revisar os seguintes tipos de informações:

   - 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, Oracle Database 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 um snapshot das instâncias, bancos de dados, aplicativos ou máquinas virtuais 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.
     - **Fanout 3-2-1**: Armazenamento primário (disco) para storage secundário (disco) para nuvem (armazenamento de objetos). Cria múltiplas cópias de dados em diferentes sistemas de armazenamento, como ONTAP para ONTAP e ONTAP para configurações de armazenamento de objetos. Isso pode ser um armazenamento de objetos de hyperscaler de nuvem ou um armazenamento de objetos privado. Essas configurações ajudam a alcançar proteção de dados e recuperação de desastres otimizadas.

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.

   - **Ativar snapshot consistente com a VM**: Selecione se deseja ativar snapshots consistentes com a VM. Isso garante que os snapshots recém-criados sejam consistentes com o estado da máquina virtual no momento da captura do snapshot. 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 snapshots 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.

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

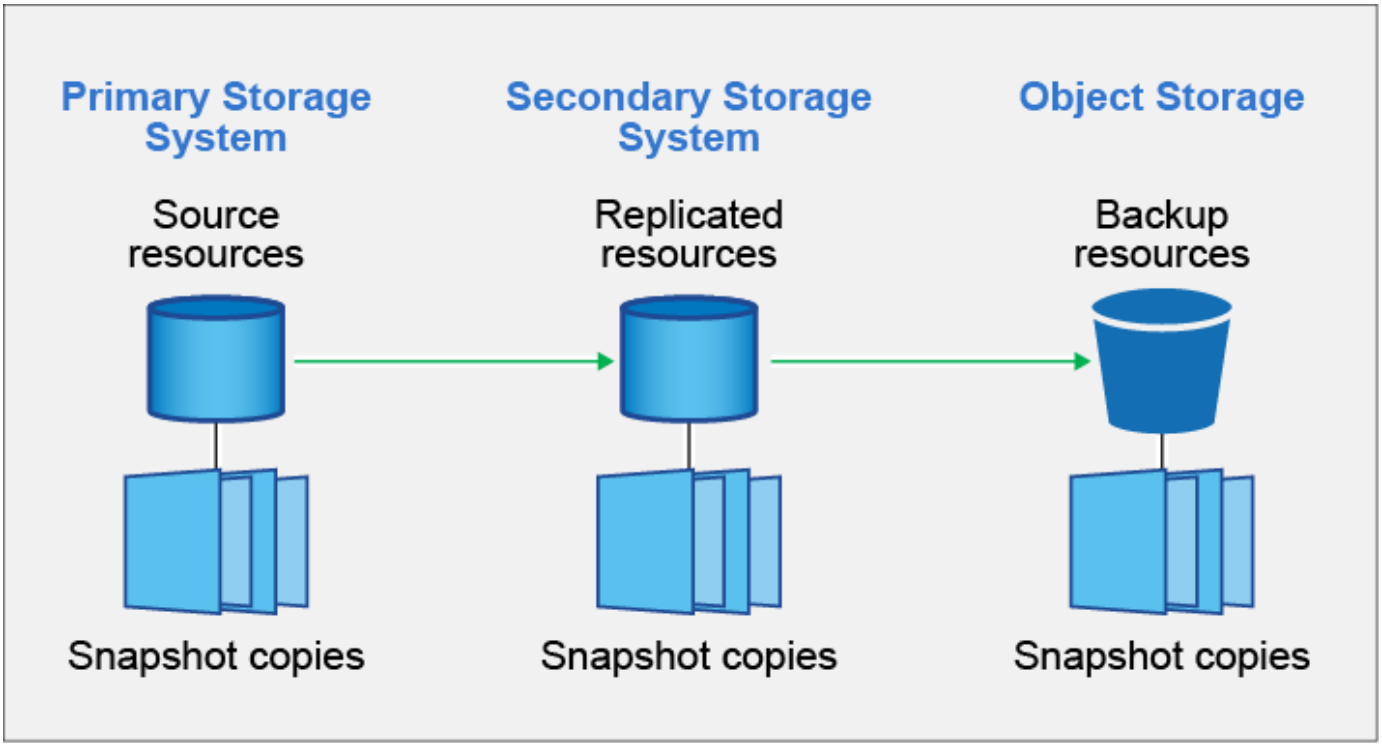
O NetApp Backup and Recovery fornece recursos de backup e restauração para proteção e arquivamento de longo prazo dos dados do seu volume ONTAP . Você pode implementar uma estratégia 3-2-1, na qual você tem 3 cópias dos seus dados de origem

em 2 sistemas de armazenamento diferentes, além de 1 cópia na nuvem.

Para alternar entre cargas de trabalho de NetApp Backup and Recovery , 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:

- Captura de tela 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 snapshots e transferindo-os para os locais de backup.

Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados protegem contra ameaças internas e externas à segurança cibernética.
- Usar diferentes tipos de mídia ajuda na recuperação caso um tipo falhe.
- Você pode restaurar rapidamente a partir da cópia local e usar as cópias externas se a cópia local estiver 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 "NetApp Replication" , 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 snapshots locais, volumes replicados ou volumes de backup em 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 fazer 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. Os snapshots 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
Cloud Volumes ONTAP no Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Blob do Azure
Cloud Volumes ONTAP no Google	Cloud Volumes ONTAP no sistema Google On-premises ONTAP	Armazenamento em nuvem do Google
Sistema ONTAP local	Sistema Cloud Volumes ONTAP ONTAP	Amazon S3, Azure Blob, Google Cloud Storage, NetApp StorageGRID , ONTAP , S3

Destinos de restauração suportados

Você pode restaurar dados do ONTAP a partir 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. Os snapshots residem no sistema de origem e só podem ser restaurados para esse mesmo sistema.

Localização do arquivo de backup		Sistema de destino
Armazenamento de Objetos (Backup)	**Sistema Secundário (Replicação)**	
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Cloud Volumes ONTAP no sistema ONTAP local da AWS
Blob do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure
Armazenamento em nuvem do Google	Cloud Volumes ONTAP no sistema Google On-premises ONTAP	Cloud Volumes ONTAP no sistema Google On-premises ONTAP
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.

A criação de snapshots ou volumes replicados é gratuita, exceto pelo espaço em disco necessário para armazená-los.

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 snapshots 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 .

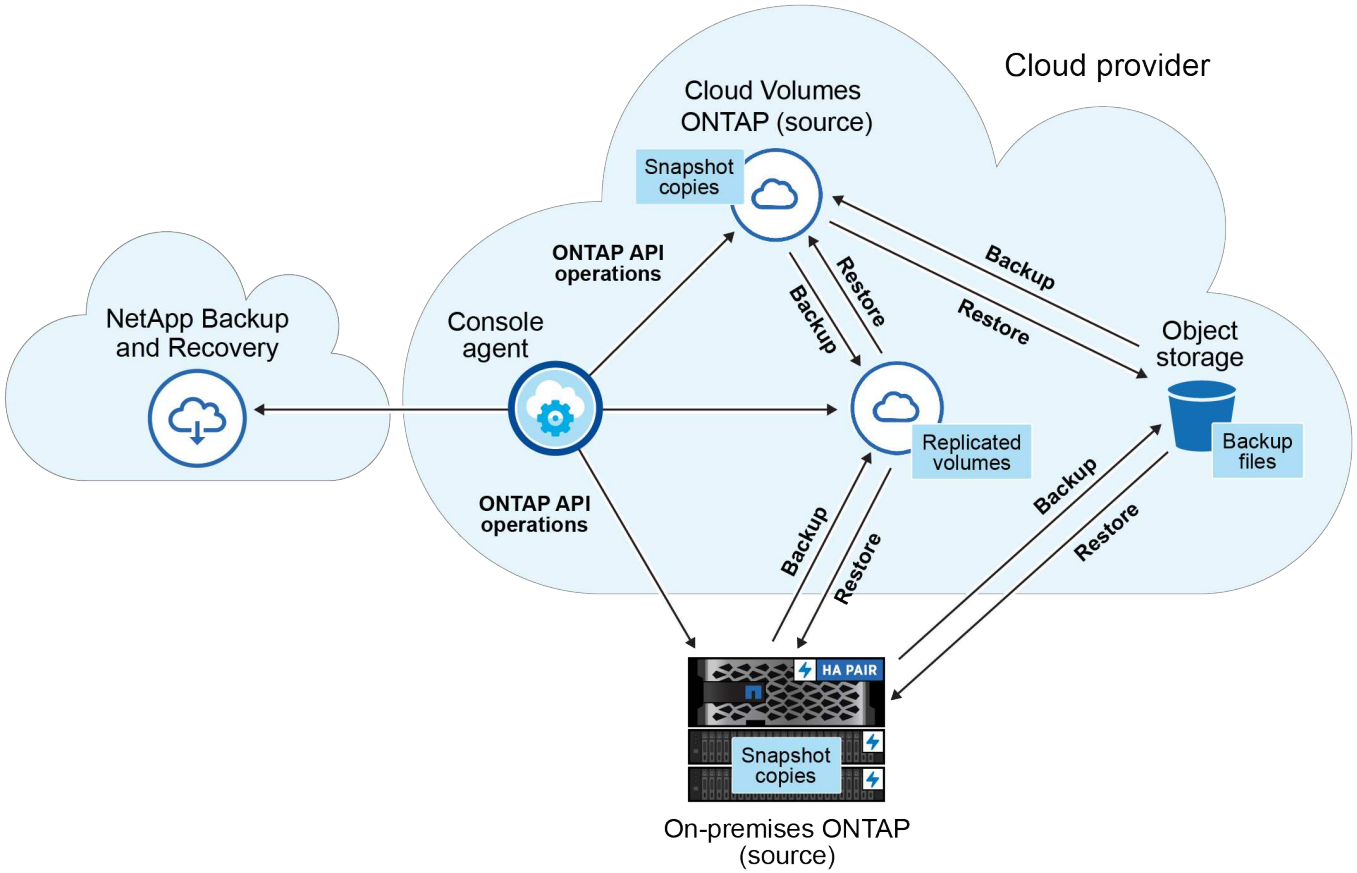
"Aprenda a configurar contratos anuais".

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:

- Os *snapshots* 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 permite 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 utiliza 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 snapshots, 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 snapshots "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 no instantâneo mais recente. As verificações agendadas podem ser desativadas para reduzir seus custos. Você pode ativar ou desativar as verificações agendadas de ransomware no snapshot mais recente usando a opção na página de 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 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 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 hierarquização 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 o Backup e a Recuperação em seus volumes, então você deve revisar suas escolhas para estar preparado.

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

Analisaremos as seguintes opções:

- Quais recursos de proteção você usará: snapshots, 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)

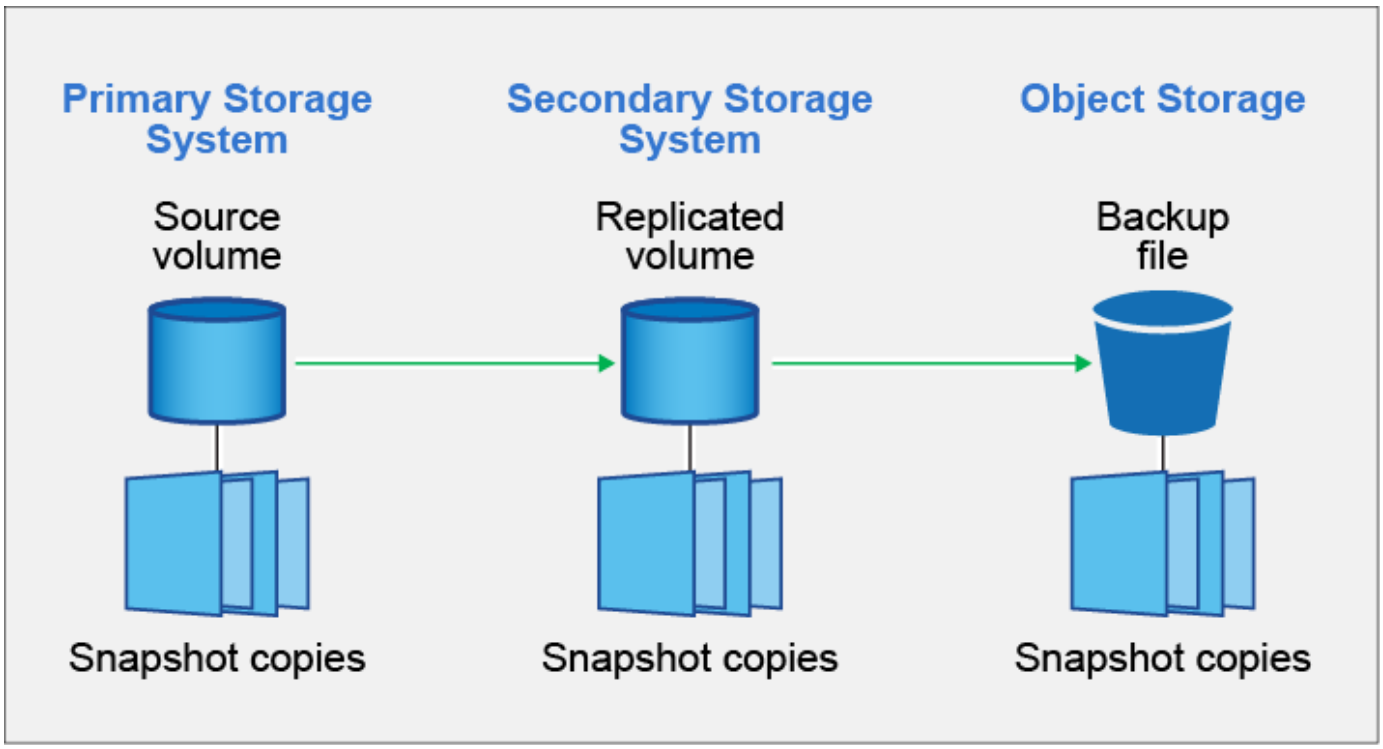
Quais recursos de proteção você usará

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 e pontual de um volume dentro do volume de origem como um instantâneo. Você pode usar o instantâneo para recuperar arquivos individuais ou para 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.

Tipo de backup	Descrição
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. Um instantâneo é uma imagem somente leitura de um volume em um determinado momento. A imagem consome um espaço de armazenamento mínimo e acarreta uma sobrecarga de desempenho insignificante, pois registra apenas as alterações feitas nos arquivos desde a última captura instantânea. O snapshot criado no seu volume é usado 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 → Instantâneo → Volume replicado → Arquivo de backup
- Volume de origem → Instantâneo → Arquivo de backup
- Volume de origem → 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.

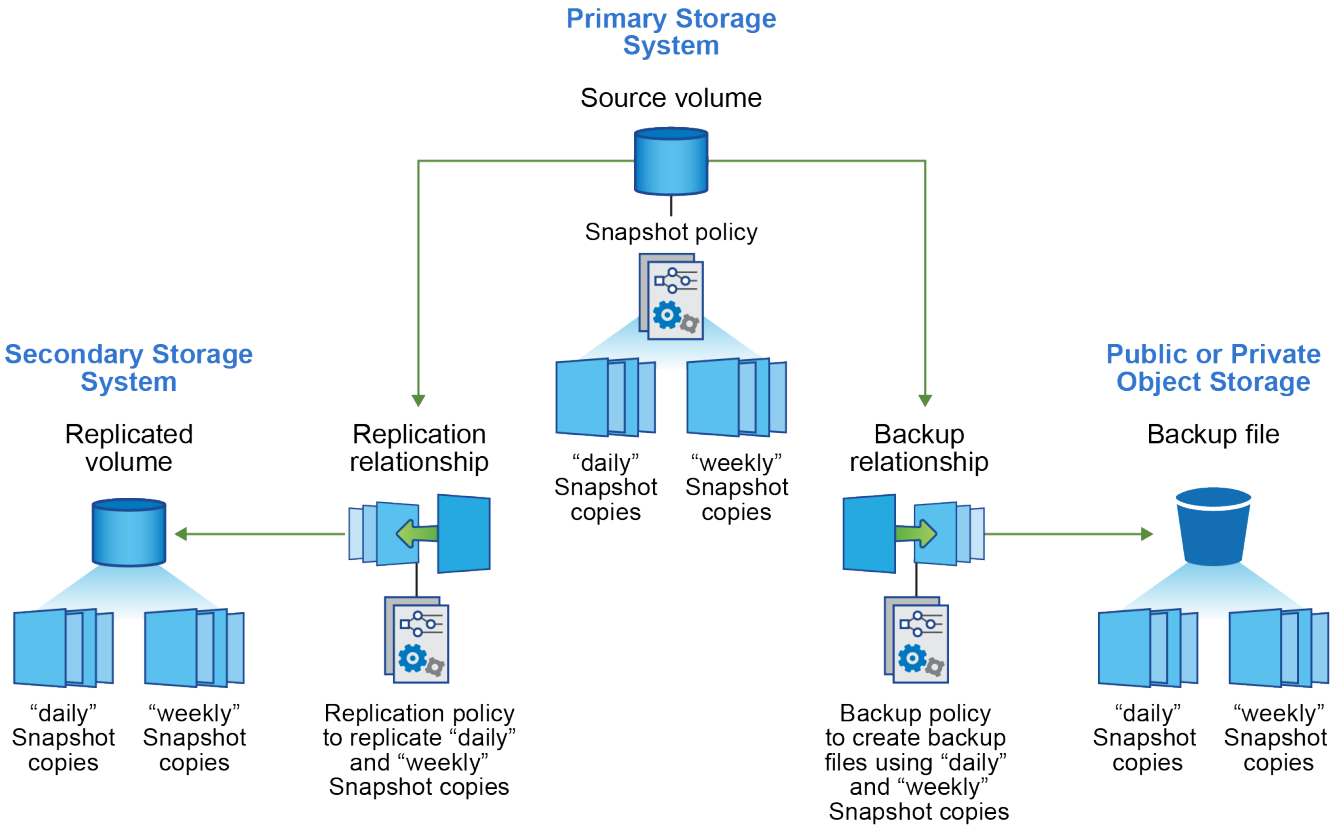
Além desses critérios, o armazenamento em nuvem oferece opções de segurança adicionais se você usar o recurso DataLock e Ransomware Resilience, além de economia de custos adicional ao selecionar classes de armazenamento de arquivamento para arquivos de backup mais antigos. "Saiba mais sobre a proteção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

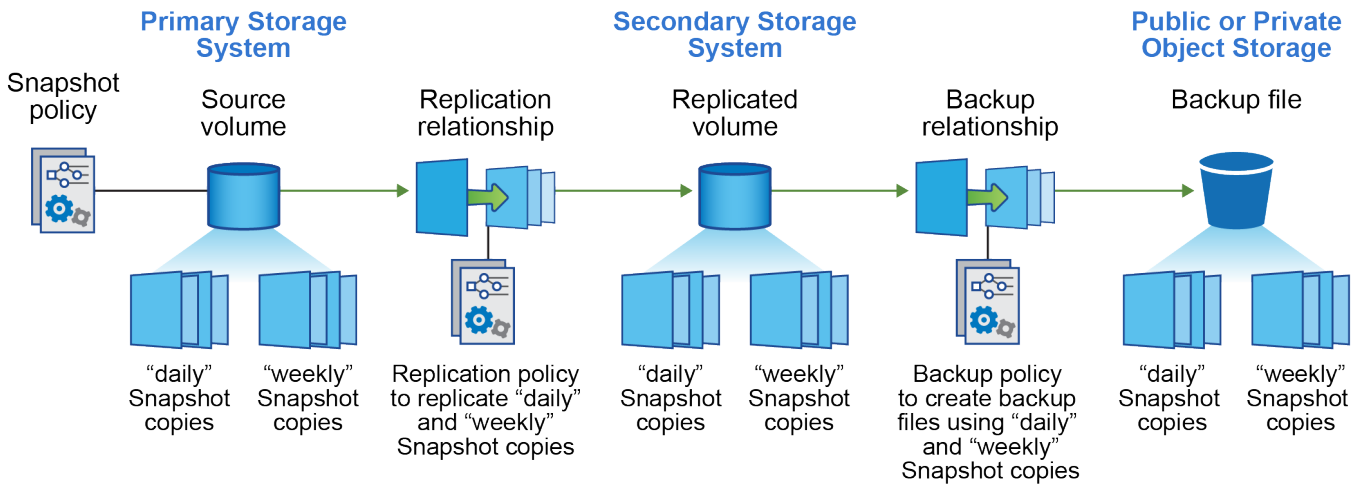
Qual arquitetura de backup você usará

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 o snapshot de forma independente tanto para o sistema de armazenamento de destino quanto para o objeto de backup na nuvem.



Uma arquitetura em **cascata** transfere primeiro o snapshot 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
O impacto no desempenho do sistema de origem é pequeno, pois ele está enviando snapshots para dois sistemas distintos.	Menor impacto no desempenho do sistema de armazenamento de origem, pois o snapshot é enviado apenas uma vez.
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 snapshots padrão cria snapshots horários, diários e semanais, retendo 6 snapshots horários, 2 diários e 2 semanais.
- A política de replicação padrão replica snapshots diários e semanais, retendo 7 snapshots diários e 52 snapshots semanais.
- A política de backup padrão replica snapshots diários e semanais, retendo 7 snapshots diários e 52 snapshots 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`
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".

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.

> ⓘ Para alternar entre cargas de trabalho de NetApp Backup and Recovery , 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:

- UI do NetApp Console
- 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 regem seus snapshots, 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 um snapshot 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 de 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.

Para alternar entre cargas de trabalho de NetApp Backup and Recovery , 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.

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 na nuvem replicados via SnapMirror para a nuvem e também habilitar a detecção de ataques de ransomware, recuperando uma cópia consistente do snapshot no armazenamento de objetos. Este recurso é compatível com AWS, Azure, Google Cloud Platform 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
Cloud Volumes ONTAP na AWS	Amazon S3
Cloud Volumes ONTAP no Azure	Blob do Azure

Sistema de origem	Destino do arquivo de backup
Cloud Volumes ONTAP no Google Cloud	Google Cloud
Sistema ONTAP local	Amazon S3 Azure Blob Google Cloud 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.
- Você não pode 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 a AWS, você pode organizar os 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 organizar 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 os snapshots históricos serão exportados como arquivos de backup e ativar ou desativar as verificações de ransomware em um sistema.

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

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

Você pode alterar as seguintes opções na página Configurações avançadas:

- Alterar as chaves de armazenamento que concedem ao seu sistema ONTAP permissão para acessar o armazenamento de objetos.
- Alterar o espaço IP do ONTAP que está conectado ao armazenamento de objetos.
- Alterar a largura de banda de rede alocada para o upload de backups para o armazenamento de objetos usando a opção Taxa Máxima de Transferência.
- Alterar se os snapshots históricos serão exportados como arquivos de backup e incluídos nos arquivos de backup iniciais 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 do sistema em nível de cluster e as configurações do provedor 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*, selecione o ••• Para visualizar as configurações do sistema, selecione **Configurar configurações avançadas > Configurações do sistema** e **Configurar configurações avançadas > Configurações do provedor** para visualizar as configurações do provedor.

   A página resultante exibe as configurações atuais desse sistema. Ao visualizar as configurações do provedor, as configurações exibidas são relevantes para o bucket selecionado na parte superior da página.

Observe que algumas opções podem não estar disponíveis dependendo da versão do ONTAP no cluster de origem e do provedor de nuvem de destino onde os backups estão armazenados.

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 **Configurar configurações avançadas > Configurações do sistema**.
3. Na página Configurações avançadas, expanda a seção **Taxa máxima de transferência**.
4. Escolha um valor entre 1 e 1.000 Mbps como taxa de transferência máxima.
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 os snapshots históricos serão exportados como arquivos de backup

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

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 **Configurar configurações avançadas > Configurações do sistema**.
3. Na página Configurações Avançadas, expanda a seção **Exportar cópias de instantâneo existentes**.
4. Selecione se deseja exportar os instantâneos existentes.
5. Selecione **Aplicar**.

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

Ao selecionar o rótulo de backup "anual" para uma política de backup de qualquer um dos seus volumes, o snapshot criado será 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 **Configurar configurações avançadas > Configurações do sistema**.
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 no instantâneo mais recente.

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.

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.

Ativar ou desativar verificações de ransomware para um sistema

Você pode ativar ou desativar as verificações de ransomware para um cluster.

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, clique em ••• para o sistema e selecione **Configurar configurações avançadas > Configurações do sistema**.
3. Na página que aparecer, 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**.

Ativar ou desativar verificações de ransomware para um provedor

Você pode ativar ou desativar as verificações de ransomware no nível do provedor usando a página de configurações do provedor. As configurações desta página são relevantes para o bucket que você selecionar na parte superior da página.

Passos

1. Na aba **Volumes**, selecione **Configurações de backup**.
2. Na página *Configurações de backup*, clique em ••• Para acessar o sistema, selecione **Configurar configurações avançadas > Configurações do provedor**.
3. Na parte superior da página resultante, selecione o bucket para o qual você precisa alterar as configurações.
4. Expanda a seção **Verificação de ransomware**.
5. Habilitar ou desabilitar **Verificação de ransomware**.
6. Selecione **Verificação agendada de ransomware**.
7. Opcionalmente, altere a verificação padrão semanal para dias ou semanas.
8. Defina a frequência em dias ou semanas em que a verificação deve ser executada.
9. 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.

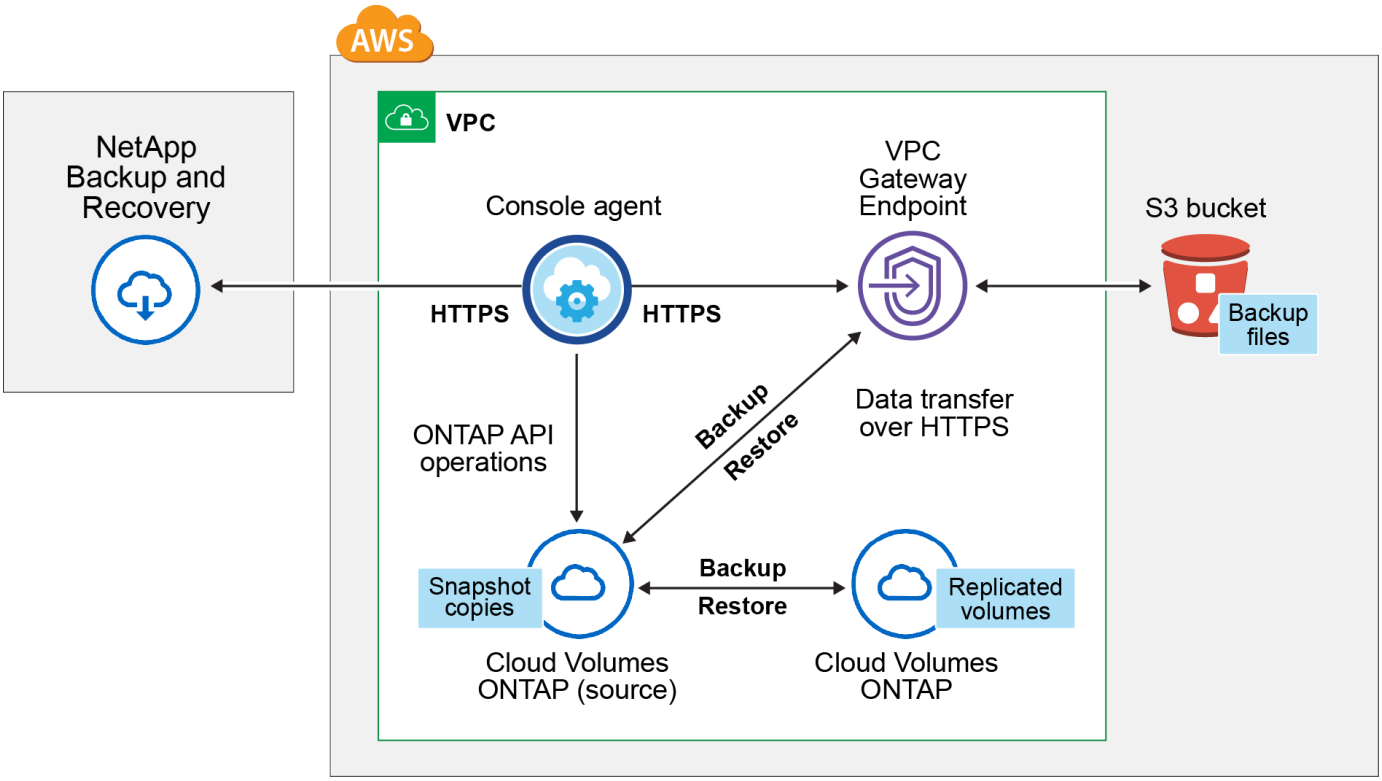
Para alternar entre cargas de trabalho de NetApp Backup and Recovery , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

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 Cloud Volumes ONTAP e de dados ONTAP locais, 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 no local, você deverá ter uma conexão da sua rede corporativa com a 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 NetApp Backup and Recovery 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 de Backup e Recuperação. Na guia Volumes, selecione **Ações**. ••• Na opção do ícone, selecione **Ativar proteção 3-2-1** para um único volume (que ainda não tenha replicação ou backup para armazenamento de objetos ativado).

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. ConsultePrepare 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 para armazenamento de objetos. Ao selecionar buckets existentes ou configurar novos buckets, você pode fazer backup de volumes em até seis buckets por cluster.
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:

   a. Digite o nome da política.
   b. Selecione até cinco programações, normalmente com frequências diferentes.
   c. Selecione **Criar**.
4. **Replicação**: Defina as seguintes opções:
   - **Destino da replicação**: Selecione o sistema de destino e a máquina virtual de armazenamento. Opcionalmente, selecione o agregado ou agregados 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:

     i. Digite o nome da política.
     ii. Selecione até cinco programações, normalmente com frequências diferentes.
     iii. Selecione **Criar**.
5. **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.

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

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

  Se você escolher um bucket existente, as informações de criptografia já estarão disponíveis, então você não precisa inseri-las agora.

- **Rede**: Configure as opções de rede para este provedor.
- **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:

  i. Digite o nome da política.

  ii. Selecione até cinco programações, normalmente com frequências diferentes.

  iii. 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" .

  iv. Selecione **Criar**.

- **Exportar snapshot existente**: Se houver snapshots 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.), esta mensagem adicional será exibida. Marque esta caixa para que todos os snapshots históricos sejam copiados para o armazenamento de objetos como arquivos de backup, garantindo 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 **Corrigir automaticamente rótulos incompatíveis em snapshots locais, replicação e backup**. Isso cria instantâneos com um rótulo que corresponde aos rótulos nas políticas de instantâneo, 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. As transferências subsequentes contêm cópias diferenciais dos dados do sistema de armazenamento primário contidos nos snapshots.

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.

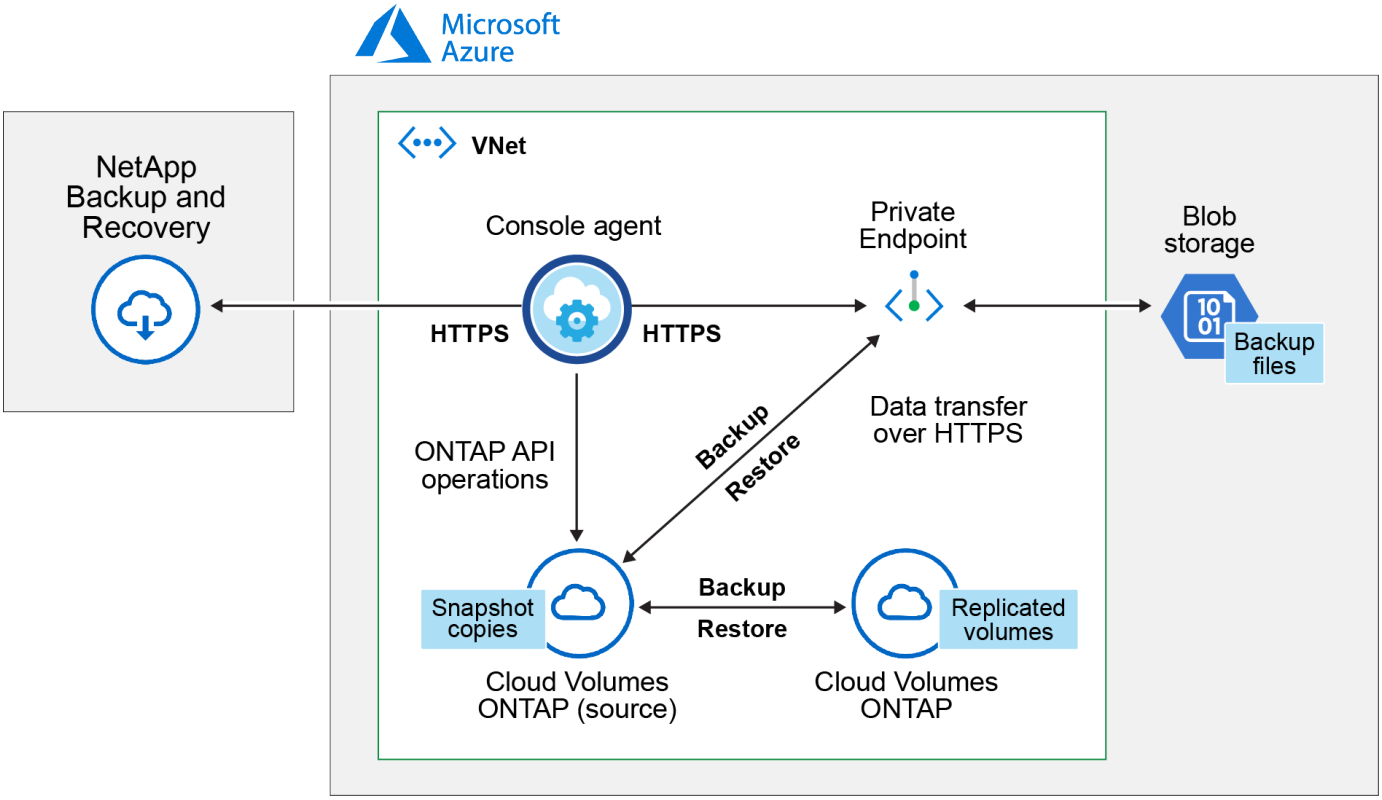
Para alternar entre cargas de trabalho de NetApp Backup and Recovery , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

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 por meio do 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 no local, você deverá ter uma conexão da sua rede corporativa com a 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 NetApp Backup and Recovery 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. ConsultePrepare 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.

   - **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 snapshots existentes para armazenamento de objetos como cópias de backup**: Se houver snapshots 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.), esta mensagem adicional será exibida. 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. As transferências subsequentes contêm cópias diferenciais dos dados de armazenamento primário contidos nos snapshots.

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.

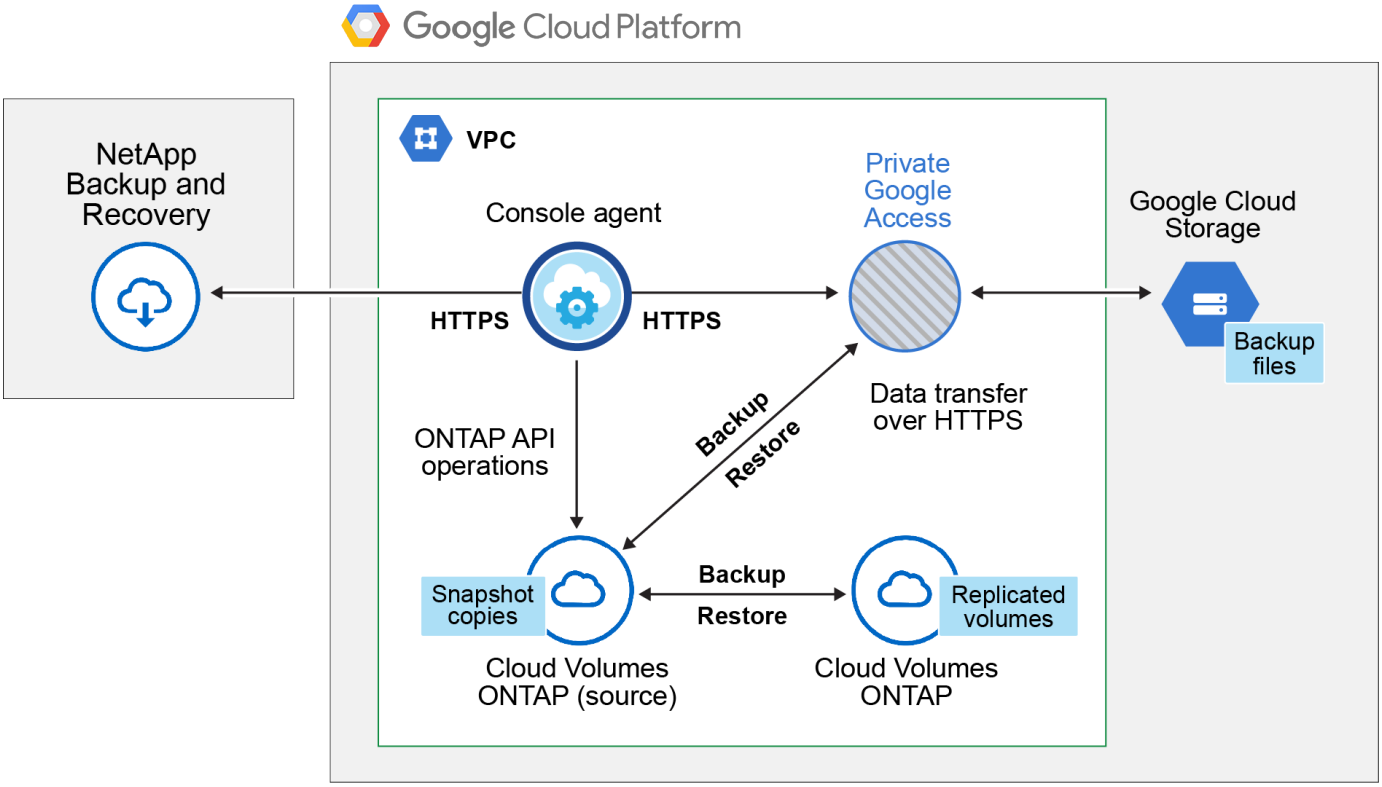
Para alternar entre cargas de trabalho de NetApp Backup and Recovery , consulte"Alterne para diferentes cargas de trabalho do NetApp Backup and Recovery" .

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 do 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 no local, você deverá ter uma conexão da sua rede corporativa com a 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 NetApp Backup and Recovery 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 snapshots existentes para armazenamento de objetos como cópias de backup**: Se houver snapshots 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.), esta mensagem adicional será exibida. 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. As transferências subsequentes contêm cópias diferenciais dos dados do sistema de armazenamento primário contidos nos snapshots.

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 os sistemas FAS, AFF e ONTAP Select .

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

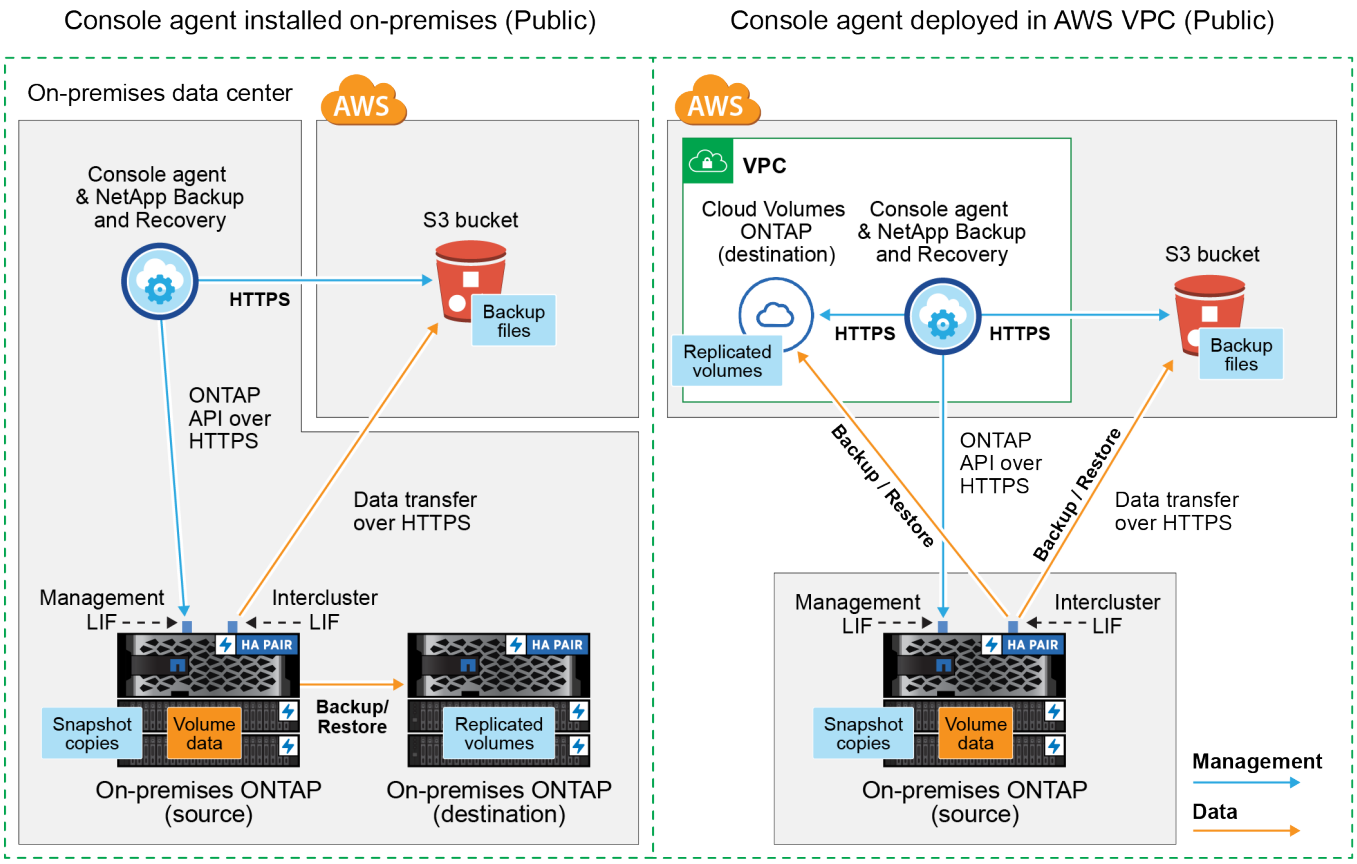
Identifique o método de conexão

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o AWS S3.

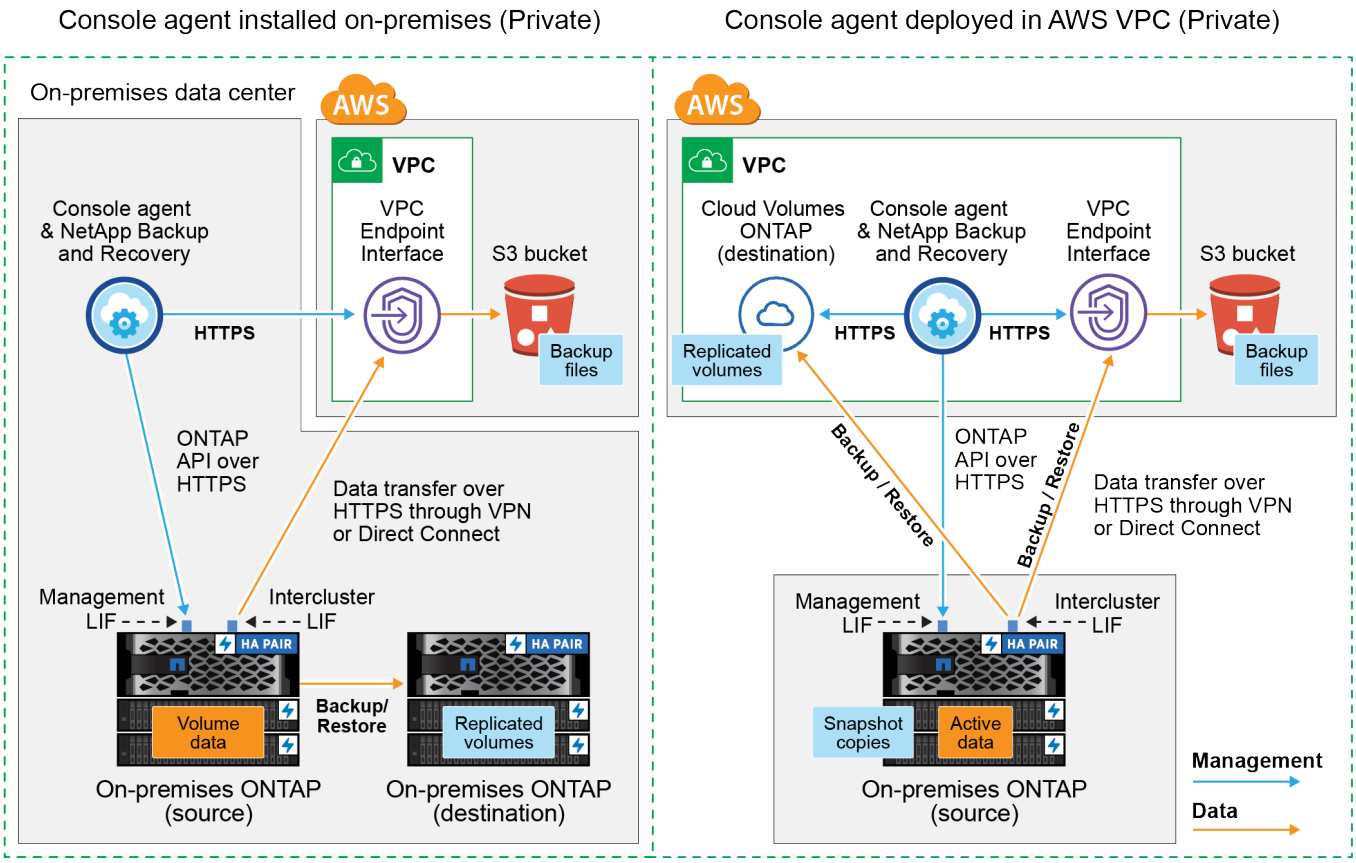
- **Conexão pública** - Conecte diretamente o sistema ONTAP ao AWS S3 usando um endpoint S3 público.
- **Conexão privada** - Use uma VPN ou AWS Direct Connect e direcione o tráfego por meio de uma interface de endpoint VPC que usa um endereço IP privado.

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

Prepare 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 seu sistema ONTAP atenda aos seguintes requisitos:

- 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 replicar dados, verifique se os sistemas de origem e destino executam versões compatíveis do ONTAP .

  "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 no local, você deverá ter uma conexão da sua rede corporativa com a 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 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 precisar usar um nome personalizado, edite o `ontapcloud-instance-policy-netapp-backup` Crie uma IAMRole para os CVOs existentes e adicione o seguinte bloco JSON às permissões do S3. `Statement` variedade. Você precisa incluir `"Resource": "arn:aws:s3:::*"` e atribuir todas as permissões necessárias que precisam ser associadas ao bucket.

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "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:::*"
  }
]
```

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 "*":

   ```
   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 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 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. ConsultePrepare 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 snapshots existentes para armazenamento de objetos como cópias de backup**: Se houver snapshots 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.), esta mensagem adicional será exibida. 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. As transferências subsequentes contêm cópias diferenciais dos dados primários contidos nos instantâneos.

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 os sistemas FAS, AFF e ONTAP Select .

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

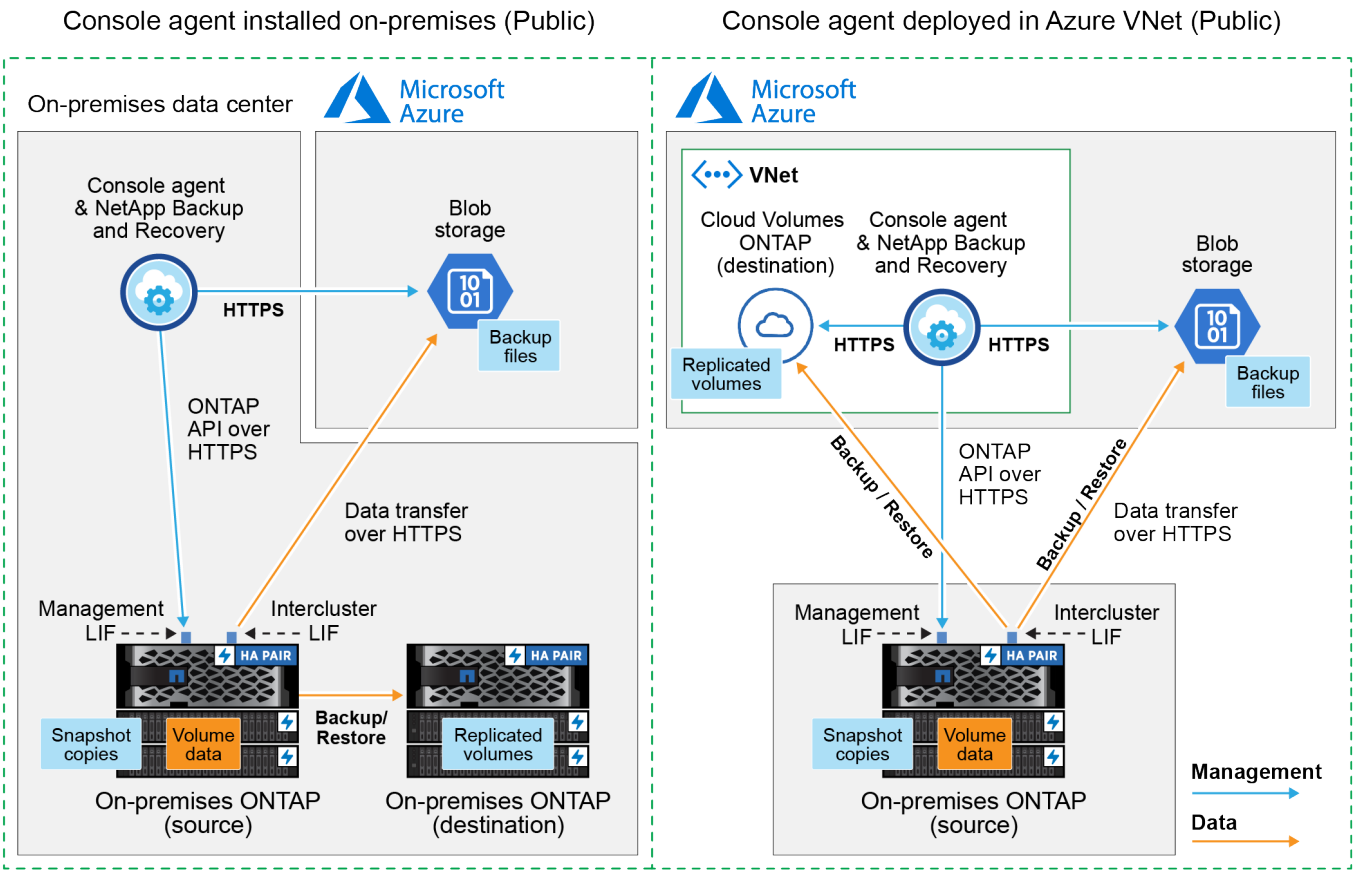
Identifique o método de conexão

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o Azure Blob.

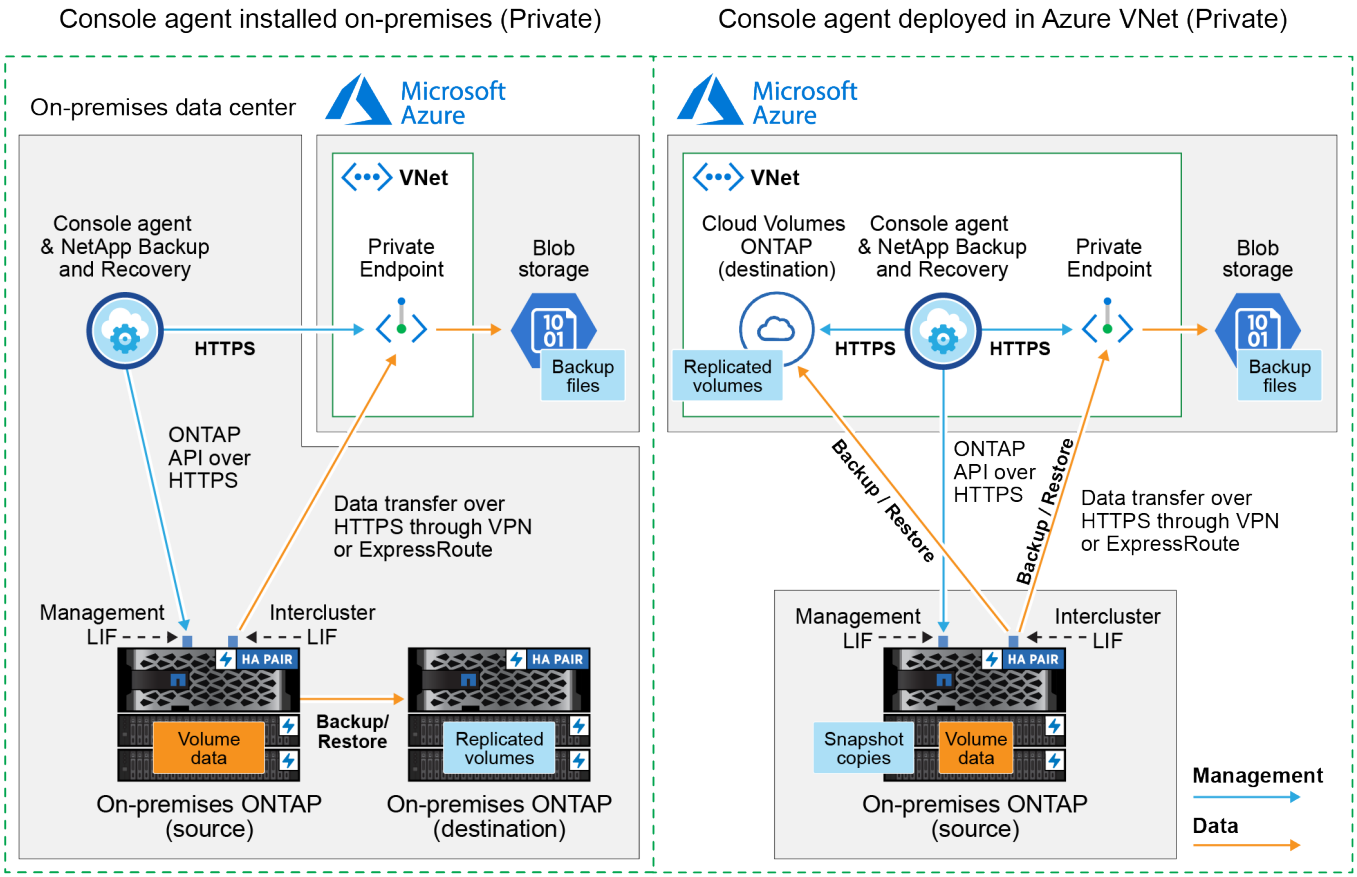
- **Conexão pública** - Conecte diretamente o sistema ONTAP ao armazenamento de Blobs do Azure usando um ponto de extremidade público do Azure.
- **Conexão privada** - Use uma VPN ou ExpressRoute e direcione o tráfego por meio de um VNet Private Endpoint que usa um endereço IP privado.

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

Prepare 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 seu sistema ONTAP atenda aos seguintes requisitos:

- 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 replicar dados, verifique se os sistemas de origem e destino executam versões compatíveis do ONTAP .

  "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 no local, você deverá ter uma conexão da sua rede corporativa com a 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. ConsultePrepare 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 snapshots existentes para armazenamento de objetos como cópias de backup**: Se houver snapshots 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.), esta mensagem adicional será exibida. 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. As transferências subsequentes contêm cópias diferenciais dos dados do sistema de armazenamento primário contidos nos snapshots.

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 os sistemas FAS, AFF e ONTAP Select .

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

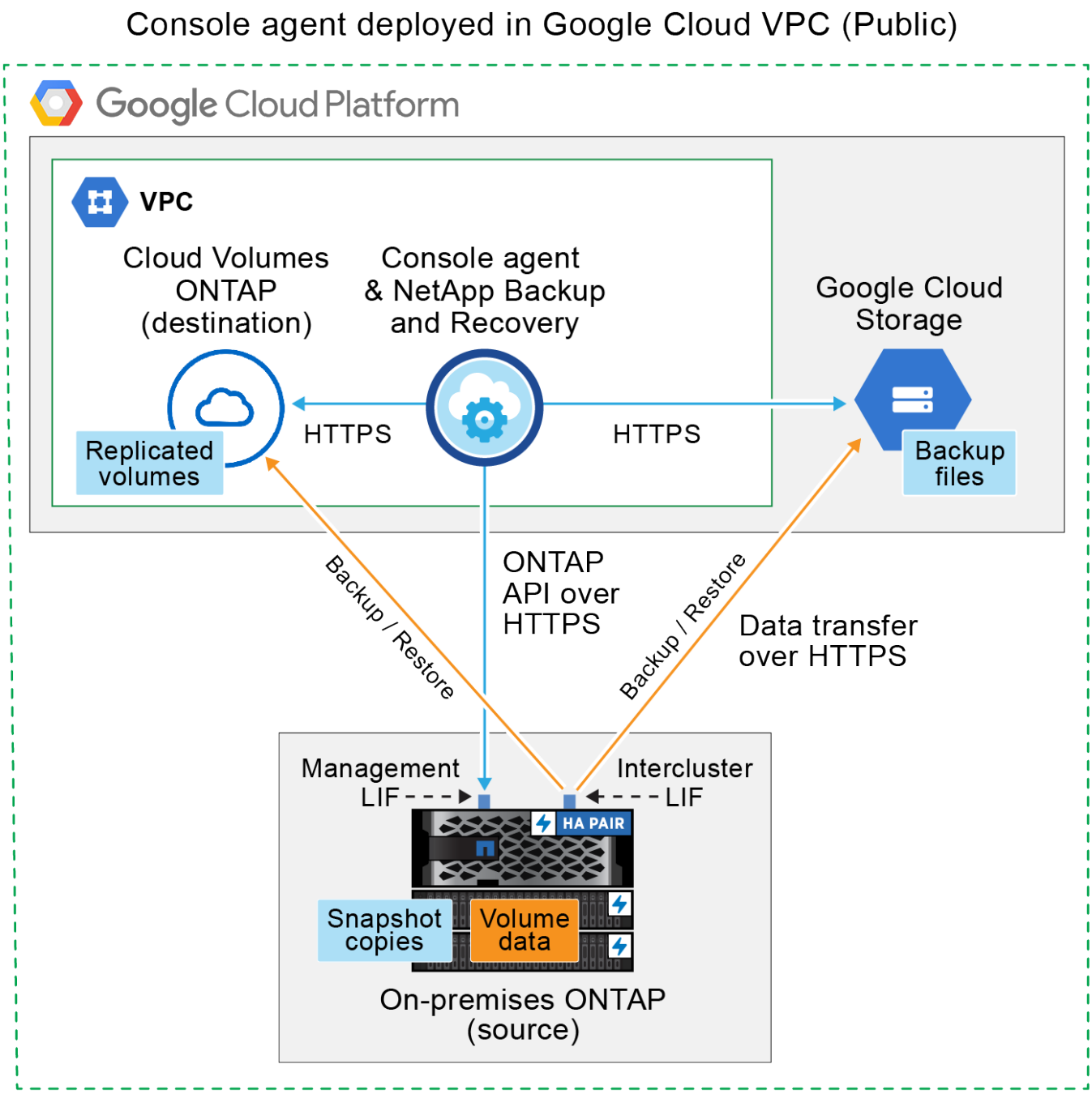
Identifique o método de conexão

Escolha qual dos dois métodos de conexão você usará ao configurar backups de sistemas ONTAP locais para o Google Cloud Storage.

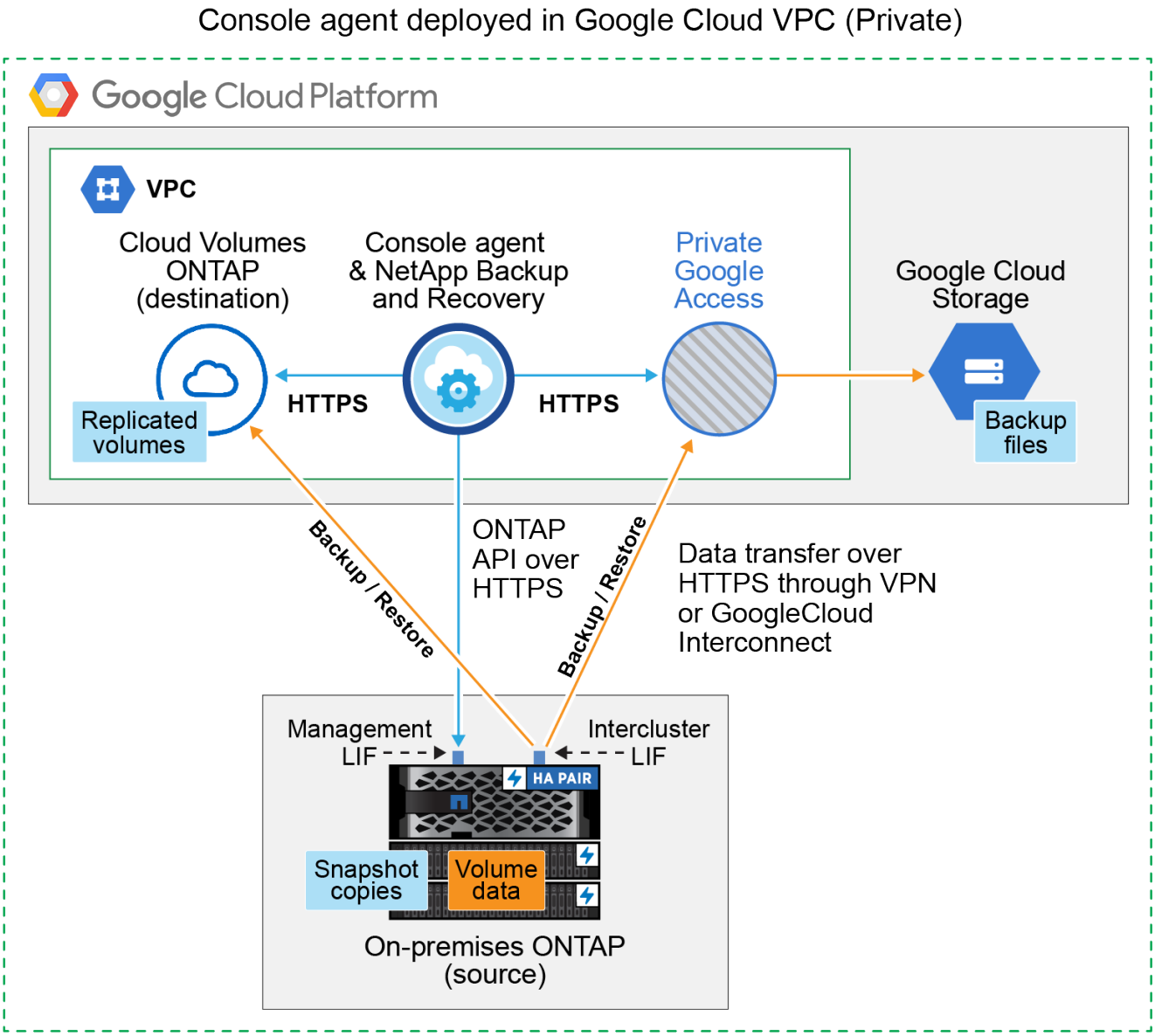
- **Conexão pública** - Conecte diretamente o sistema ONTAP ao Google Cloud Storage usando um ponto de extremidade público do Google.
- **Conexão privada** - Use uma VPN ou o Google Cloud Interconnect e direcione o tráfego por meio de uma interface de acesso privado do Google que usa um endereço IP privado.

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

Prepare 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 seu sistema ONTAP atenda aos seguintes requisitos:

- 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 replicar dados, verifique se os sistemas de origem e destino executam versões compatíveis do ONTAP .

  "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 no local, você deverá ter uma conexão da sua rede corporativa com a 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 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 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. ConsultePrepare 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 snapshots existentes para armazenamento de objetos como cópias de backup**: Se houver snapshots 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.), esta mensagem adicional será exibida. 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. As transferências subsequentes contêm cópias diferenciais dos dados do sistema de armazenamento primário contidos nos snapshots.

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.

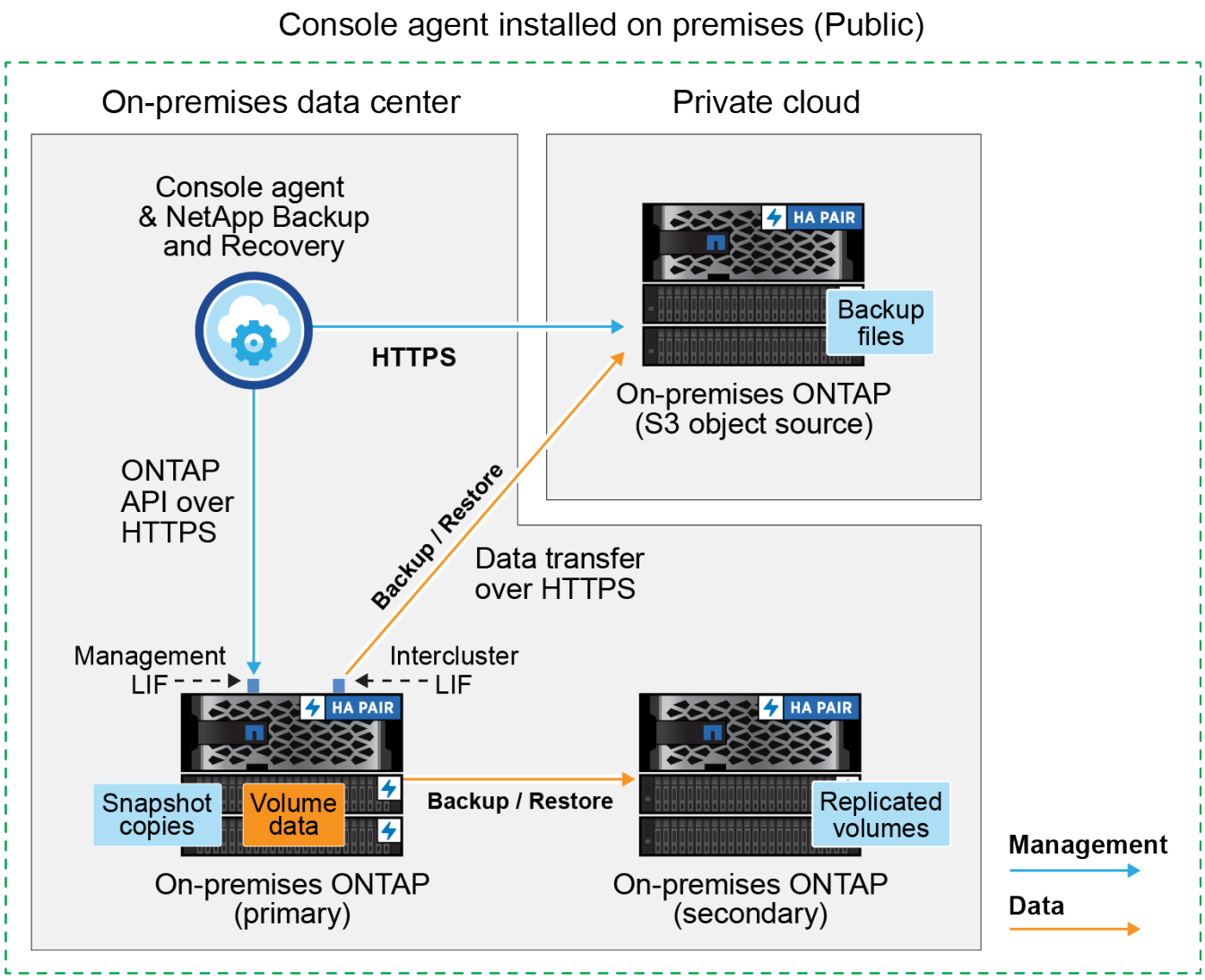
O sistema ONTAP local principal pode ser um sistema FAS, AFF ou ONTAP Select . O sistema ONTAP secundário pode ser um sistema ONTAP local ou Cloud Volumes ONTAP . O armazenamento de objetos pode estar em um sistema ONTAP local ou em um sistema Cloud Volumes ONTAP no qual você habilitou um servidor de armazenamento de objetos do Simple Storage Service (S3).

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

Identifique o método de conexão

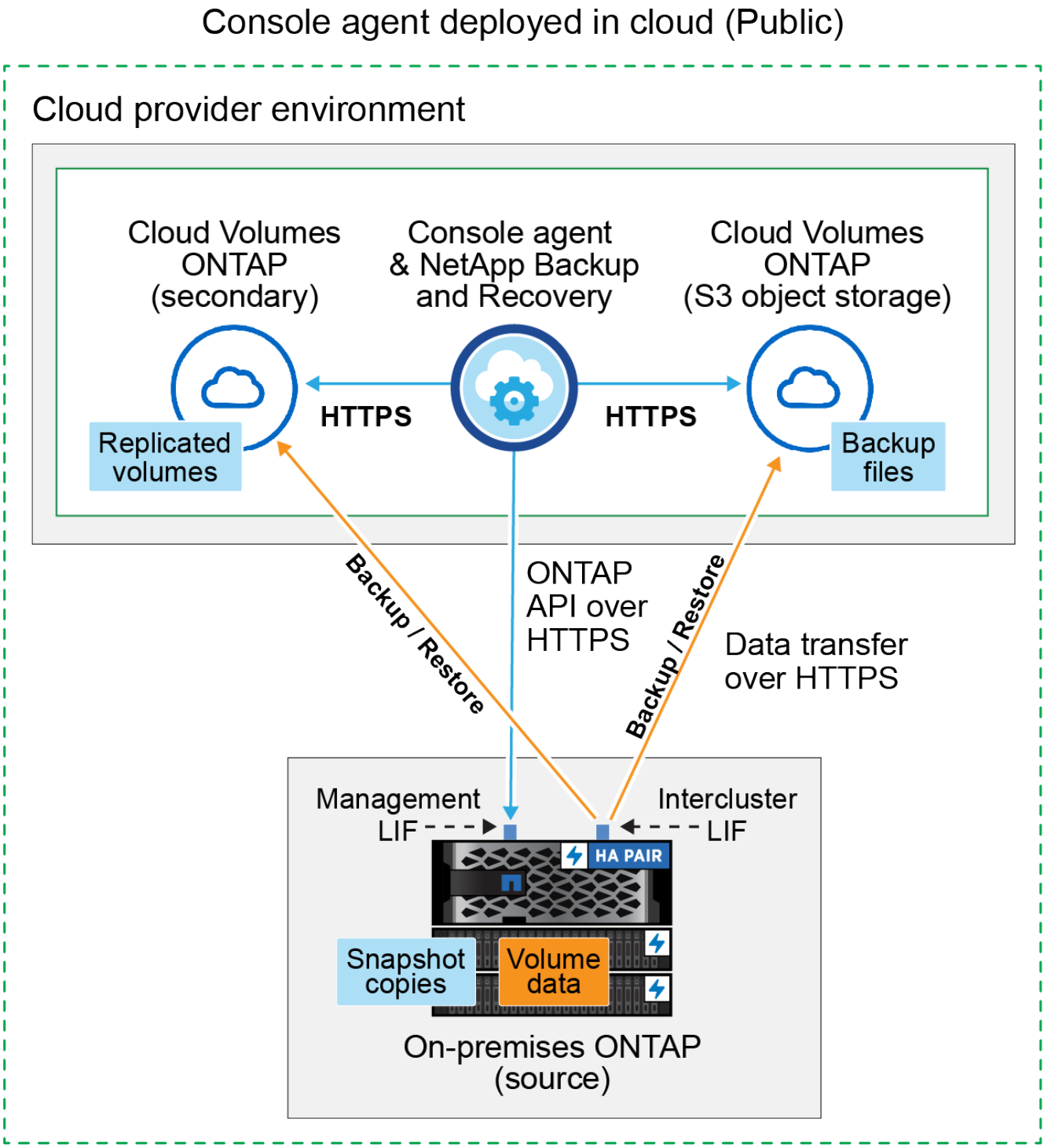
Há muitas configurações nas quais você pode criar backups para um bucket S3 em um sistema ONTAP . Dois cenários são mostrados abaixo.

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 o 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 NetApp Backup and Recovery 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 em armazenamento de objetos; nenhuma licença é necessária para criar snapshots 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

Prepare 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 seu sistema ONTAP atenda aos seguintes requisitos:

- 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 replicar dados, verifique se os sistemas de origem e destino executam versões compatíveis do ONTAP .

  "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 no local, você deverá ter uma conexão da sua rede corporativa com a 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",
"s3:GetBucketLocation"
```

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 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.
   - 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. ConsulteConsulte 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:

- **Instantâneos locais**: Cria instantâneos 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 Backup e Recuperação, 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 Backup e Recuperação, 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 snapshots existentes para armazenamento de objetos como arquivos de backup**: Se houver snapshots locais para volumes neste sistema que correspondam ao rótulo de agendamento de backup que você acabou de selecionar (por exemplo, diário, semanal etc.), esta mensagem adicional será exibida. 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. As transferências subsequentes contêm cópias diferenciais dos dados de armazenamento primário contidos nos snapshots.

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 .

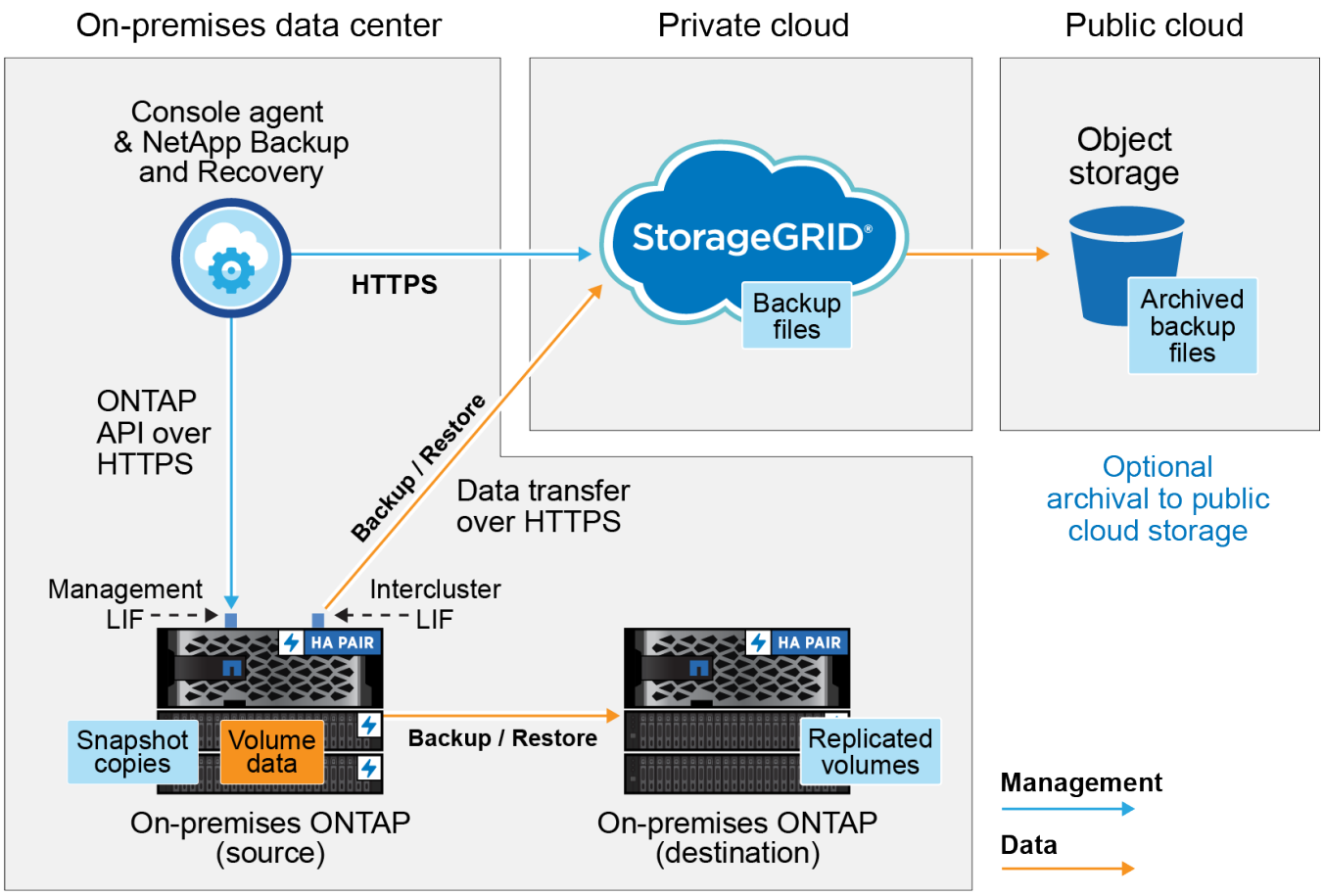
Os "sistemas ONTAP locais" incluem os sistemas FAS, AFF e ONTAP Select .

Para alternar entre cargas de trabalho de NetApp Backup and Recovery , 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 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 NetApp Backup and Recovery 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 snapshots e volumes replicados, além de criar backups para armazenamento de objetos, requer 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

Prepare 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 seu sistema ONTAP atenda aos seguintes requisitos:

- 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 replicar dados, verifique se os sistemas de origem e destino executam versões compatíveis do ONTAP .

  "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 no local, você deverá ter uma conexão da sua rede corporativa com a 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 talvez não precise. 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

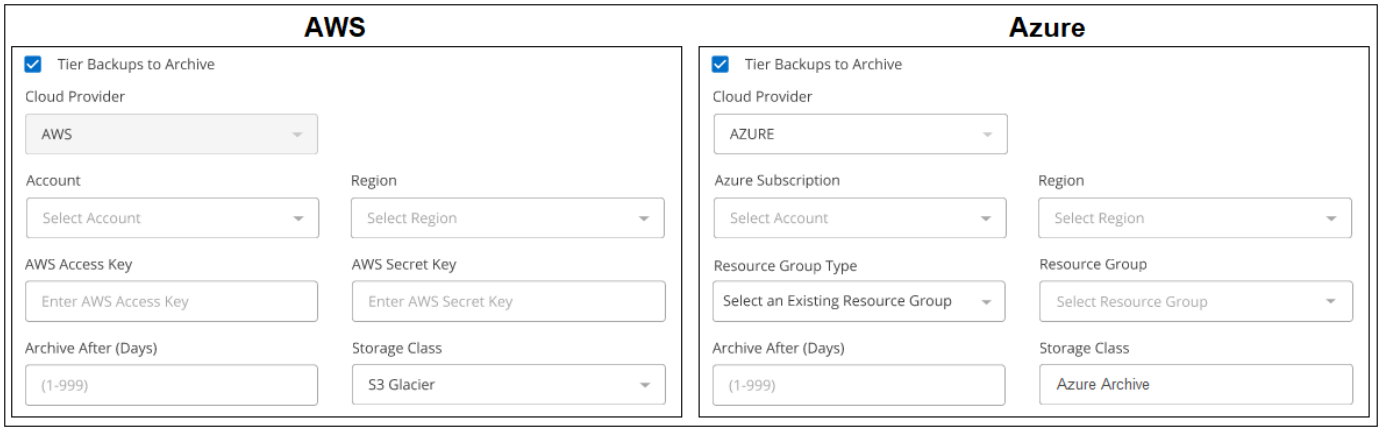
- Você precisará criar uma conta Amazon S3 para o espaço de armazenamento onde seus backups arquivados estarão localizados.
- Você pode optar por fazer backups em camadas no armazenamento AWS S3 Glacier ou S3 Glacier Deep Archive. "Saiba mais sobre as camadas de arquivamento da AWS".
- O StorageGRID 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 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 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 snapshots existentes para armazenamento de objetos como cópias de backup**: Se houver snapshots 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.), esta mensagem adicional será exibida. 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. As transferências subsequentes contêm cópias diferenciais dos dados de armazenamento primário contidos nos snapshots.

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 implementação NetApp local para outra, ou para uma solução baseada em nuvem como o Cloud Volumes ONTAP, o SnapMirror to Cloud Resync garante que os backups existentes na nuvem permaneçam intactos e operacionais.

Essa funcionalidade elimina a necessidade de um processo de redefinição de linha de base e permite que os backups 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.

O SnapMirror to Cloud Resync mantém a continuidade do backup em todos os ambientes, facilitando o gerenciamento de dados em configurações híbridas e multicloud.

Para alternar entre cargas de trabalho de NetApp Backup and Recovery , 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.
- Certifique-se de que o backup mais recente no armazenamento de objetos seja o snapshot comum entre a origem antiga, a nova origem e o armazenamento de objetos. Não utilize um snapshot comum que seja mais antigo que o snapshot mais recente armazenado no repositório de objetos.
- Tanto as políticas de snapshot quanto as de SnapMirror usadas no cluster ONTAP antigo devem ser criadas no novo cluster ONTAP antes de iniciar a operação de ressincronização. Se você usar alguma política no processo de ressincronização, também deverá criar essa política. A operação de ressincronização não cria 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 pontos de restauração. O Vol1 tem backup na nuvem usando o SnapMirror to Cloud (SM-C), mas apenas S1 e S2 estão no armazenamento de objetos.

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.

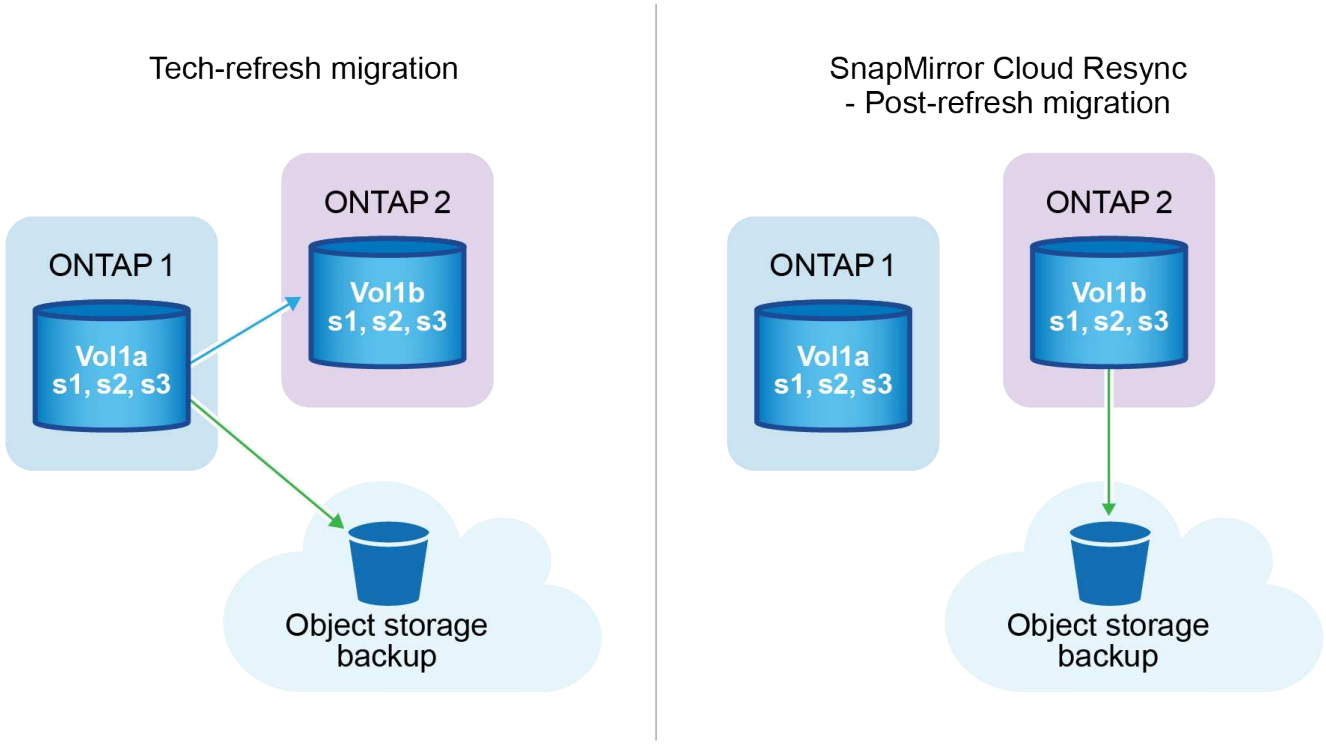
Neste ponto, você deseja continuar fazendo backup do Vol1b no mesmo ponto de extremidade da nuvem. Mas em vez de iniciar um backup completo do zero (o que levaria tempo e recursos), você usa o SnapMirror para Cloud Resync.

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 backups duplicados, economiza largura de banda e mantém os backups em execução após a migração.



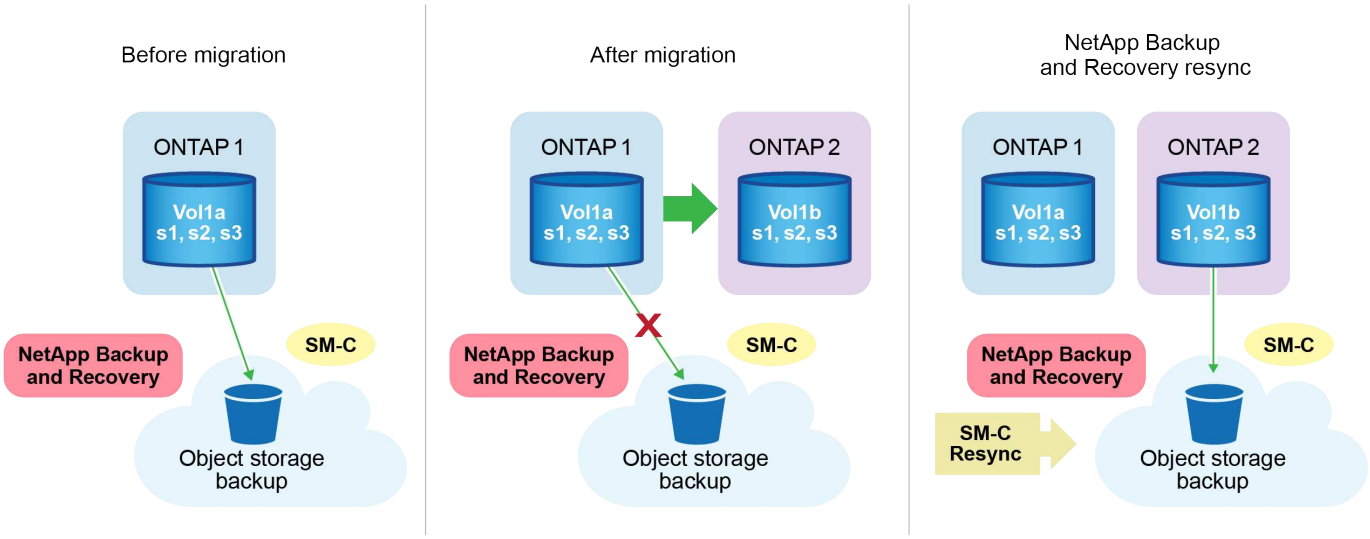
Notas de procedimento

- Migrações e atualizações de tecnologia 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 cria a relação SnapMirror entre os clusters ONTAP de origem e destino para auxiliar na movimentação de volumes.
- 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 da migração, a equipe NetApp Tech Refresh verifica esses pré-requisitos para evitar a perda de dados e garantir um processo tranquilo.

1. Garanta 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 NetApp Backup and Recovery para garantir que os detalhes do sistema de origem antigo estejam disponíveis.
3. Na página Volumes de NetApp Backup and Recovery , 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 de detalhes de 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 com o agente do Console implantado no seu provedor de nuvem ou no seu próprio host conectado à Internet, o sistema faz backup e protege todos os dados de configuração importantes na nuvem. Se você tiver um problema com o agente do Console, crie um novo agente do Console e adicione seus sistemas. Os detalhes do backup são restaurados automaticamente.

Existem dois tipos de dados que são copiados:

- Banco de dados de NetApp Backup and Recovery - 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 NetApp Backup and Recovery serão armazenados 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 NetApp Backup and Recovery para um novo agente do Console

Se o seu agente do Console local parar de funcionar, 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 NetApp Backup and Recovery
- 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 o sistema está funcionando, 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, baixe a mesma versão de software do agente original. Alterações no banco de dados do NetApp Backup and Recovery podem fazer com que versões mais recentes do software não funcionem com backups de bancos de dados antigos. 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 NetApp Backup and Recovery

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
```

8. Digite a senha.

```
mysql> show tables;
mysql> select * from volume;
```

9. Certifique-se de que os volumes exibidos sejam os mesmos que existiam em 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 NetApp Console" .

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":"pas
sword"}
> '
```

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*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

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 NetApp Backup and Recovery

1. Selecione cada sistema ONTAP e clique em **Exibir backups** ao lado do serviço de backup e recuperação no painel direito.

   Você deverá ver todos os backups 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 snapshots, 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.

Para alternar entre cargas de trabalho de NetApp Backup and Recovery , 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 snapshots, 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 "Instantâneos locais", "Volumes replicados" e "Backups no armazenamento de objetos".

   Cada ícone acende quando o tipo de backup correspondente está ativado e fica cinza quando o tipo de backup está inativo. Você pode posicionar o cursor sobre cada ícone para visualizar a política de backup que está sendo utilizada, bem como outras informações relevantes para cada tipo de backup.

Ativar backup em volumes adicionais em um sistema

Se você ativou o backup somente 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 guia **Volumes**, identifique o volume no qual deseja ativar os backups e selecione o menu Ações. ••• Ao final da linha, selecione **Ativar proteção 3-2-1**.
2. Na página *Definir estratégia de backup*, selecione a arquitetura de backup e, em seguida, defina as políticas e outros detalhes para snapshots 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 seus snapshots 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. No menu **Volumes**, localize o volume para o qual deseja modificar as configurações de política e selecione o menu Ações. ••• No final da linha, selecione **Editar estratégia de backup**.
2. Na página *Editar estratégia de backup*, faça alterações nas políticas de backup existentes para snapshots 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 o Ransomware Resilience* 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 estão habilitados para backup, o NetApp Backup and Recovery inicializa apenas cinco volumes por vez. Quando essas etapas forem concluídas, o processo continua em grupos de 5 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 que aparece, faça as alterações nas políticas de backup existentes para snapshots 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 o Ransomware Resilience* 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 um snapshot ou backup ad-hoc de um volume para o armazenamento de objetos. 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**.

   São exibidos os detalhes do volume e a lista de snapshots.

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 snapshots para atualizar o volume de destino. Você pode Retomar mais tarde se quiser reiniciar as atualizações incrementais.

Ação	Descrição
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 naquele 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 quaisquer arquivos de backup que tenham sido armazenados em camadas no arquivo permanente permanecerão nessa camada se você interromper o armazenamento em camadas dos backups no arquivo permanente - eles não serão movidos automaticamente de volta para a camada padrão. Somente os 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 .

Note que esta ação não afeta snapshots 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 (nos níveis de volume e sistema).

   > 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 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 (nos níveis de volume e sistema).

   > 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 um snapshot de volume ou de um backup em 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 capturas de tela 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**.

Restaurar de backups ONTAP

Restaure dados ONTAP de arquivos de backup com o NetApp Backup and Recovery

Os backups dos dados de volume do seu ONTAP são armazenados como snapshots, em volumes replicados ou em armazenamento de objetos. Você pode restaurar dados de qualquer um desses locais em um ponto específico no tempo. Com o NetApp Backup and Recovery, você pode restaurar um volume inteiro, uma pasta ou arquivos individuais conforme necessário.

Para alternar entre cargas de trabalho de NetApp Backup and Recovery , 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.

Você precisa de uma licença válida do NetApp Backup and Recovery para restaurar dados em 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
- Instantâneo → volume restaurado

Se a operação de restauração não for concluída, aguarde até que o Job Monitor mostre "Falha" antes de tentar a operação 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. Para acessar o Painel de Restauração, selecione **Backup e recuperação** no menu Console e, em seguida, selecione a guia **Restaurar**. Você também pode selecionar > **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
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
Instantâneo	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 um dos métodos de restauração, configure seu ambiente para atender aos requisitos de recursos. Consulte as seções seguintes para obter mais detalhes.

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 a partir de backups do ONTAP usando a função Pesquisar e Restaurar.

Você pode usar a função Pesquisar e Restaurar para recuperar volumes, pastas ou arquivos de backups do ONTAP . A função Pesquisar e Restaurar permite pesquisar em todos os backups (incluindo snapshots locais, volumes replicados e armazenamento de objetos) sem precisar dos nomes exatos do sistema, do volume ou do arquivo.

Restaurar a partir de snapshots locais ou volumes replicados geralmente é mais rápido e menos dispendioso do que restaurar a partir de armazenamento de objetos.

Ao restaurar um volume completo, o NetApp Backup and Recovery cria um novo volume usando os dados de backup. Você pode restaurar o sistema original, outro sistema dentro da mesma conta na nuvem ou um sistema ONTAP local. Pastas e arquivos podem ser restaurados para sua localização original, para um volume diferente no mesmo sistema, para outro sistema na mesma conta na nuvem ou para um sistema local.

As funcionalidades de restauração dependem da sua versão do ONTAP :

- **Pastas:** Usando o ONTAP 9.13.0 ou superior, você pode restaurar pastas com todos os arquivos e subpastas; em versões anteriores, você só pode restaurar os arquivos dentro da pasta.
- **Armazenamento de Arquivos:** A restauração a partir do armazenamento de arquivos (disponível no ONTAP 9.10.1 ou superior) é mais lenta e pode acarretar custos adicionais.
- **Requisitos do cluster de destino:**
  - Restauração de volume: ONTAP 9.10.1 ou superior
  - Restauração de arquivos: ONTAP 9.11.1 ou superior
  - Google Archive e StorageGRID: ONTAP 9.12.1 ou superior
  - Restauração de pastas: ONTAP 9.13.1 ou superior

"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. Os snapshots residem no sistema de origem e só podem ser restaurados nesse 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)**	
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Cloud Volumes ONTAP no sistema ONTAP local da AWS
Blob do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure
Armazenamento em nuvem do Google	Cloud Volumes ONTAP no sistema Google On-premises ONTAP	Cloud Volumes ONTAP no sistema Google On-premises ONTAP
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 .

Pesquisar e restaurar pré-requisitos

Certifique-se de que seu ambiente atenda a esses requisitos antes de ativar a função de Busca e Restauração:

- 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 entre arquivos e diretórios em diferentes snapshots.)
- A NetApp recomenda montar um volume separado no agente do console para aumentar a resiliência do recurso de Busca e Restauração. Para obter instruções, consulteMonte o volume para reindexar o catálogo. .

Pré-requisitos para a função de Busca e Restauração Legada (usando o Catálogo Indexado v1)

Os requisitos para a função Pesquisar e Restaurar ao usar a indexação legada são os seguintes:

- 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.)

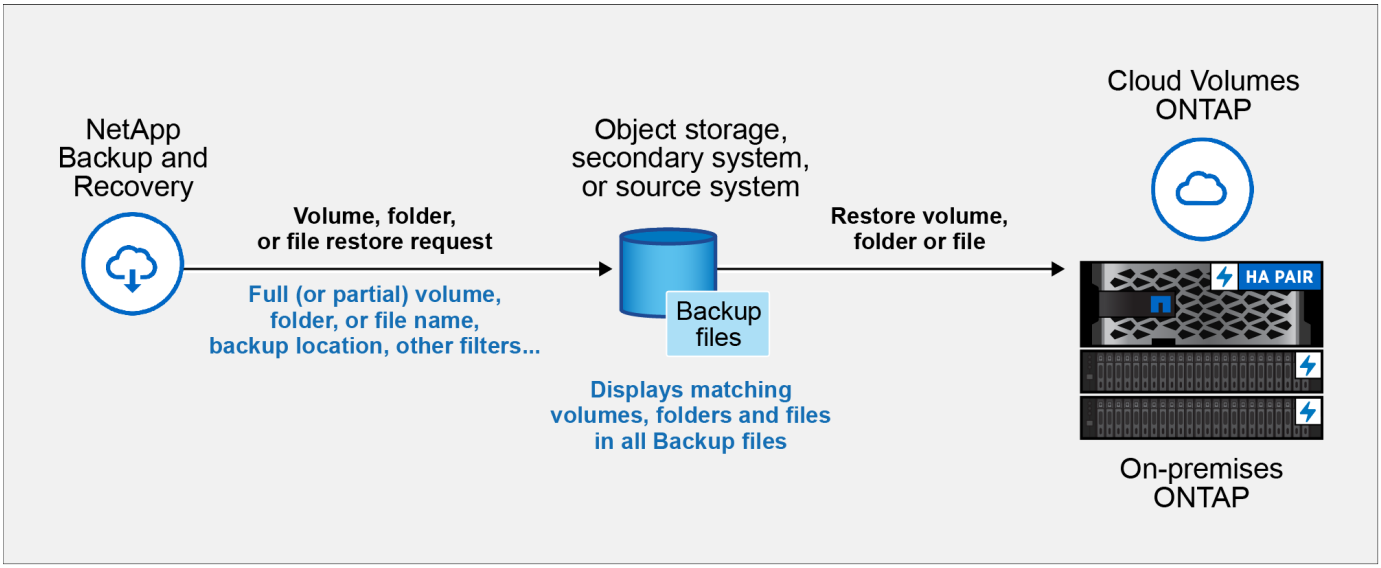
Mesmo que você esteja usando um agente do Console local, os requisitos do provedor de nuvem devem ser atendidos para permissões do agente do Console e recursos do provedor de nuvem. Veja os requisitos da AWS e do Azure acima ao usar esta implementação.

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.



Basta saber parte do nome e o NetApp Backup and Recovery pesquisa em 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

O NetApp Backup and Recovery não provisiona um bucket separado quando você usa o Catálogo Indexado. 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.

O Catálogo Indexado 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.

Etapas para habilitar a indexação de um sistema:

Se a indexação já estiver habilitada para seu sistema, vá para a próxima seção para restaurar seus dados.

Primeiro, você precisará montar um volume separado para armazenar os arquivos de catálogo. Isso evita a perda de dados caso o tamanho dos arquivos que contêm os instantâneos se torne muito grande. Isso não é necessário em todos os clusters; você pode montar qualquer volume de qualquer um dos clusters em seu ambiente. Caso contrário, a indexação poderá não funcionar corretamente.

Para o volume montado, utilize as seguintes orientações de dimensionamento:

- Utilize um volume NetApp NFS
- Armazenamento AFF recomendado com taxa de transferência de disco de 300 MB/s. A redução da capacidade de processamento afetará as buscas e outras operações.
- Habilite os snapshots do NetApp para proteger os metadados do catálogo, além dos arquivos zip de backup do catálogo.
- 50 GB por 1 bilhão de arquivos
- 20 GB para os dados do catálogo, com espaço adicional para a criação de arquivos zip e arquivos temporários.

Etapa para montar o volume para reindexar o catálogo

1. Monte o volume em `/opt/application/netapp/cbs` digitando o seguinte comando, onde:
    - `volume name` é o volume no cluster onde os arquivos de catálogo serão armazenados.
    - `/opt/application/netapp/cbs` é o caminho onde está sendo montado

    ```
    mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
    ```

    Exemplo:

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

Passos para ativar o índice

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 *Pesquisa e Restauração*, 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 snapshots ou arquivos de backup disponíveis 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 snapshots de volumes locais e volumes replicados remotos que contêm o arquivo em sua pesquisa. Você pode optar por restaurar a partir do arquivo de backup na nuvem, 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" .

Restaurar dados ONTAP usando Navegar e Restaurar

Com o NetApp Backup and Recovery, restaure dados do ONTAP usando a opção Navegar e Restaurar. Antes de restaurar, anote o nome do volume de origem, o sistema de origem, o SVM e a data do arquivo de backup. Você pode restaurar dados do ONTAP a partir de um snapshot, um volume replicado ou de backups armazenados em armazenamento de objetos.

As funcionalidades de restauração dependem da sua versão do ONTAP :

- **Pastas:** Usando o ONTAP 9.13.0 ou superior, você pode restaurar pastas com todos os arquivos e subpastas; em versões anteriores, você só pode restaurar os arquivos dentro da pasta.

- **Armazenamento de Arquivos:** A restauração a partir do armazenamento de arquivos (disponível no ONTAP 9.10.1 ou superior) é mais lenta e pode acarretar custos adicionais.
- **Requisitos do cluster de destino:**
  - Restauração de volume: ONTAP 9.10.1 ou superior
  - Restauração de arquivos: ONTAP 9.11.1 ou superior
  - Google Archive e StorageGRID: ONTAP 9.12.1 ou superior
  - Restauração de pastas: ONTAP 9.13.1 ou superior

"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. Os snapshots residem no sistema de origem e só podem ser restaurados nesse 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
Amazon S3	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Cloud Volumes ONTAP no sistema ONTAP local da AWS	Blob do Azure
Cloud Volumes ONTAP no sistema ONTAP local do Azure	Cloud Volumes ONTAP no sistema ONTAP local do Azure	Armazenamento em nuvem do Google	Cloud Volumes ONTAP no sistema Google On-premises ONTAP
Cloud Volumes ONTAP no sistema Google On-premises ONTAP	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.

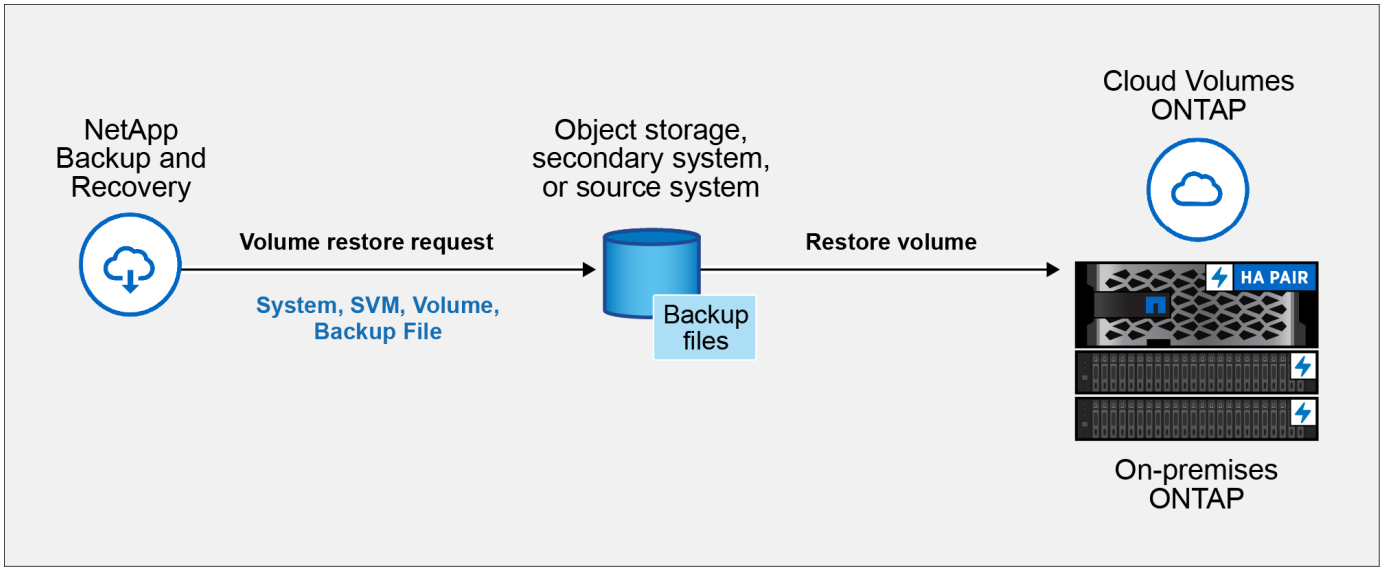
Restaurar volumes usando Navegar e Restaurar

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.



Para restaurar um volume, você precisa do nome do sistema de origem, da máquina virtual de armazenamento, do nome do volume e da data do 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 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 **Localização** mostra se o arquivo de backup (Snapshot) é **Local** (um 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.
8. 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.

9. 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**: 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.
10. 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 a restauração de arquivos e pastas a partir de um snapshot local ou de um arquivo de backup que reside em um sistema secundário (um volume replicado).

Se você selecionar vários arquivos, eles serão restaurados para o mesmo volume de destino. Para restaurar arquivos em volumes diferentes, execute o processo várias vezes.

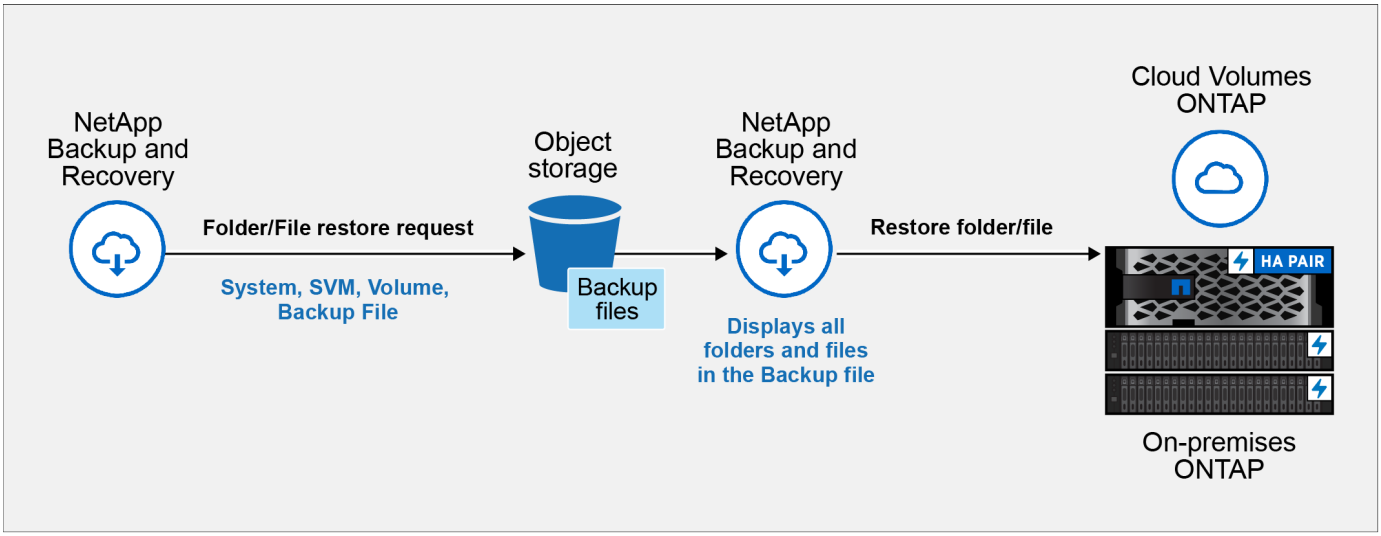
Ao usar o ONTAP 9.13.0 ou superior, você pode restaurar uma pasta junto com todos os arquivos e subpastas dentro dela. Ao usar uma versão do ONTAP anterior à 9.13.0, somente os arquivos dessa pasta são restaurados - nenhuma subpasta ou arquivo em subpastas é restaurado.

- 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" .

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.



Antes de começar

- 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.

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.
8. 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).

9. Selecione **Restaurar** para retornar ao Painel de Restauração e revisar o progresso da operação de restauração.

Proteja as cargas de trabalho do Microsoft SQL Server

Visão geral sobre como proteger cargas de trabalho do Microsoft SQL usando o NetApp Backup and Recovery

Faça backup dos dados do seu aplicativo Microsoft SQL Server de sistemas ONTAP locais para AWS, Azure ou StorageGRID usando o NetApp Backup and Recovery. O sistema cria e armazena automaticamente backups na sua conta na nuvem, seguindo suas políticas. Use uma estratégia 3-2-1: mantenha três cópias dos seus dados em dois sistemas de armazenamento e uma cópia na nuvem.

Os benefícios da abordagem 3-2-1 incluem:

- Várias cópias de dados protegem contra ameaças internas e externas à segurança cibernética.
- Usar diferentes tipos de mídia ajuda na recuperação caso um tipo falhe.
- Você pode restaurar rapidamente a partir da cópia local e usar as cópias externas se a cópia local estiver comprometida.

O NetApp Backup and Recovery utiliza o NetApp SnapMirror para sincronizar backups, criando snapshots e transferindo-os para os locais de backup.

Você pode fazer o seguinte para proteger seus dados:

- "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, crie políticas que gerenciam operações de backup e restauração. Ver"Criar políticas" para mais informações.

Destinos de backup suportados

O NetApp Backup and Recovery permite fazer 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. Os snapshots 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	N / D

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. Os snapshots residem no sistema de origem e só podem ser restaurados nesse 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 Azure Sistema ONTAP local ONTAP S3
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 de proteção de backup atuais, snapshots 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 mais detalhes, veja"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 os recursos do host do SnapCenter e exibe esses recursos na página de Inventário de NetApp Backup and Recovery . 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 você estiver acessando o Backup and Recovery pela primeira vez e tiver um sistema no Console, mas nenhum recurso descoberto, a página *Bem-vindo ao novo NetApp Backup and Recovery* será exibida com 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 NetApp Backup and Recovery

1. No menu do NetApp Console , selecione **Proteção** > **Backup e recuperação**.
2. Selecione um bloco de carga de trabalho (por exemplo, Microsoft SQL Server).
3. No menu Backup e Recuperação, selecione **Painel**.
4. 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 ou StorageGRID. O sistema cria backups automaticamente e os armazena em um repositório de objetos na sua conta na nuvem para proteção de dados.

- Para fazer backup de cargas de trabalho em um cronograma, crie políticas que gerenciem 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

Defina o caminho do log de atividades para hosts descobertos para rastrear o status da operação antes de fazer backup das cargas de trabalho.

*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. Digite o caminho do host ou navegue por uma lista de hosts ou nós para encontrar onde deseja armazenar o log do host.

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

Crie um grupo de proteção para gerenciar operações de backup e restauração para várias cargas de trabalho. Um grupo de proteção é um agrupamento lógico de cargas de trabalho.

*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 mais 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

Execute um backup sob demanda antes de fazer alterações no seu sistema para garantir que seus dados estejam protegidos.

*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

Suspenda o agendamento para interromper temporariamente os backups durante a manutenção ou solução de problemas.

*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

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.

*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 usando o NetApp Backup and Recovery. Utilize snapshots, backups replicados para armazenamento secundário ou backups em armazenamento de objetos. Restaure cargas de trabalho para o sistema original, um sistema diferente com a mesma conta de nuvem ou 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 para estes 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 se você souber o nome do arquivo, o local e a última data válida
- Restaurar para o backup mais recente

Considerações sobre restauração de armazenamento de objetos

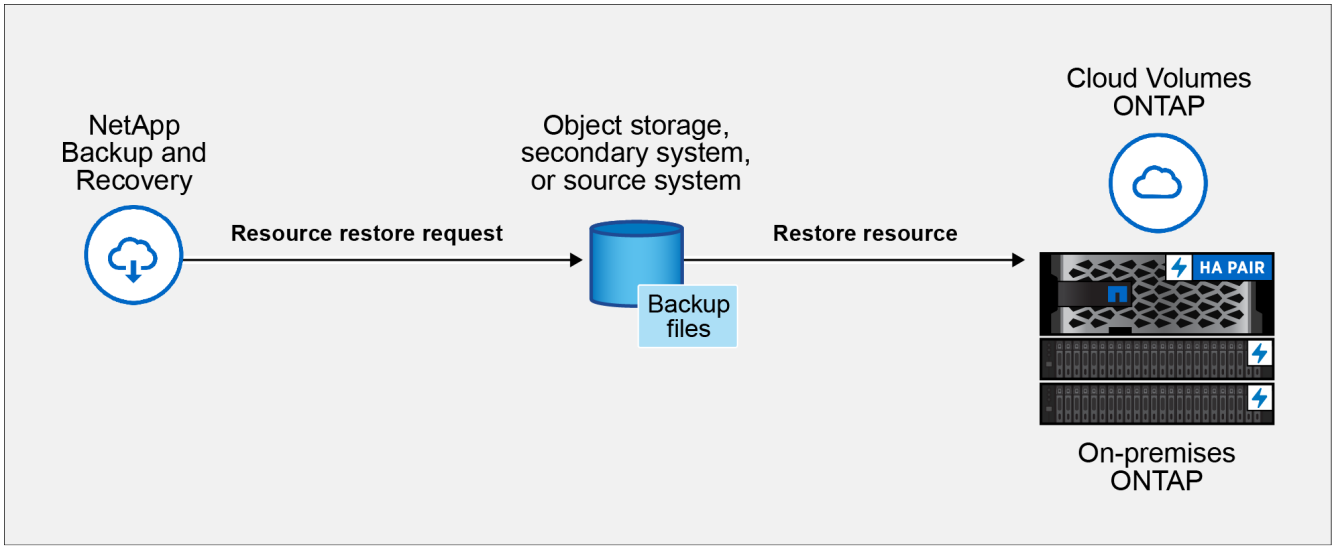
Se você selecionar um arquivo de backup no armazenamento de objetos e a Resiliência contra Ransomware estiver ativa para esse backup (se você habilitou o DataLock e a Resiliência contra Ransomware na política de backup), você será solicitado a executar uma verificação de integridade adicional no arquivo de backup antes de restaurar os dados. Recomendamos que você execute a verificação.

Você paga taxas extras ao seu provedor de nuvem para acessar o 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

Restaure cargas de trabalho usando um destes métodos:

- **Na página Restaurar**: Use esta opção para restaurar um recurso quando você não sabe seu nome, localização ou última data válida. Pesquise o instantâneo usando filtros.
- **Na página Inventário**: Use esta opção para restaurar um recurso específico quando você souber seu nome, localização e última data de validade. Navegue pela lista para encontrar o recurso.

*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 se você souber o nome do arquivo, o local e a última data válida
    - 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. No menu Bancos de dados, selecione um banco de dados com status "Protegido".
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 usando o NetApp Backup and Recovery

Clone dados de aplicativos do Microsoft SQL Server em uma VM para desenvolvimento, teste ou proteção com o NetApp Backup and Recovery. Crie clones a partir de snapshots instantâneos ou existentes de suas cargas de trabalho do 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, que 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 um snapshot e configure as opções de clonagem.
    - **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 adicione um sufixo ao nome do banco de dados clonado. Se você não adicionar 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**:
   - **Atribuição automática de ponto de montagem**: atribui automaticamente um ponto de montagem para o clone 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, adicione scripts para serem executados antes e depois da criação do clone. Esses scripts podem executar tarefas extras, 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 rótulos para ajudar você a pesquisar grupos de recursos mais tarde 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 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, adicione scripts para serem executados antes e depois da criação do clone. Esses scripts podem executar tarefas extras, 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

Ignore uma atualização de clone para mantê-lo inalterado.

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 uma política proteger o clone, tanto o clone quanto seu trabalho serão excluídos.

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 ajuda você a gerenciar seus hosts, bancos de dados e instâncias do Microsoft SQL Server. Você pode visualizar, alterar ou remover 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 logs (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 NetApp Backup and Recovery" .

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 NetApp Backup and Recovery" .
- 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 hosts com status "Não gerenciado" na coluna Hosts. O NetApp Backup and Recovery já gerencia hosts com status "Gerenciado".

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

Suspenda agendamentos para interromper operações de backup e restauração durante a manutenção do 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 atribuir as credenciais apropriadas para proteção de recursos e 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 mais detalhes, veja"Configurar as configurações de NetApp Backup and Recovery , 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

Faça backup dos seus dados agora para protegê-los 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

Restaure um banco de dados para proteger seus dados.

*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 proteger seus dados 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.

   Verifique se o ícone de instantâneo local na coluna **Localização** dessa linha aparece 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 e os detalhes do backup, incluindo a contagem de backups bem-sucedidos e com falha, tipos de backup, sistemas de armazenamento e registros de data e hora.

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**. Digite o endereço 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 cargas de trabalho VMware (sem SnapCenter Plug-in 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 protegem contra ameaças internas e externas à segurança cibernética.
- Usar diferentes tipos de mídia ajuda na recuperação caso um tipo falhe.
- Você pode restaurar rapidamente a partir da cópia local e usar as cópias externas se a cópia local estiver 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 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 fase de descoberta, o NetApp Backup and Recovery analisa as cargas de trabalho do VMware em sua organização e avalia e importa as políticas de proteção, snapshots e opções de backup e restauração existentes.

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, snapshots e opções de backup e restauração existentes do SnapCenter Plug-in for VMware vSphere.
- Exibe os recursos descobertos na página Inventário de NetApp Backup and Recovery .

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 você estiver acessando o Backup and Recovery pela primeira vez e tiver um sistema no Console, mas nenhum recurso descoberto, a página *Bem-vindo ao novo NetApp Backup and Recovery* será exibida com 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 mais detalhes, veja"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.

Continue para o Painel de NetApp Backup and Recovery

1. Para exibir o Painel de Controle, no menu Backup e Recuperação, selecione **Painel de Controle**.
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".

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 para fazer backup e restaurá-las 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 mais 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

Suspenda um grupo de proteção para pausar seus backups agendados.

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

Ao excluir um grupo de proteção, você o remove, juntamente com todos os agendamentos de backup do grupo. Exclua um grupo de proteção se não precisar mais dele.

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 mais 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**.

Restaurar cargas de trabalho do VMware

Restaure cargas de trabalho do VMware com o NetApp Backup and Recovery

Restaure cargas de trabalho do VMware a partir de snapshots, de um backup da 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 para estes pontos

Você pode restaurar dados para estes pontos:

- **Restaurar para o local original**: A VM é restaurada para o local original, na mesma implantação do vCenter, host ESXi e armazenamento de dados. A máquina virtual e todos os seus dados foram sobrescritos.
- **Restaurar para um local alternativo**: Você pode escolher um vCenter, host ESXi ou datastore diferente como destino de restauração para a VM. Isso é útil para gerenciar diferentes cópias da mesma máquina virtual em locais e estados diferentes.

Considerações sobre restauração de armazenamento de objetos

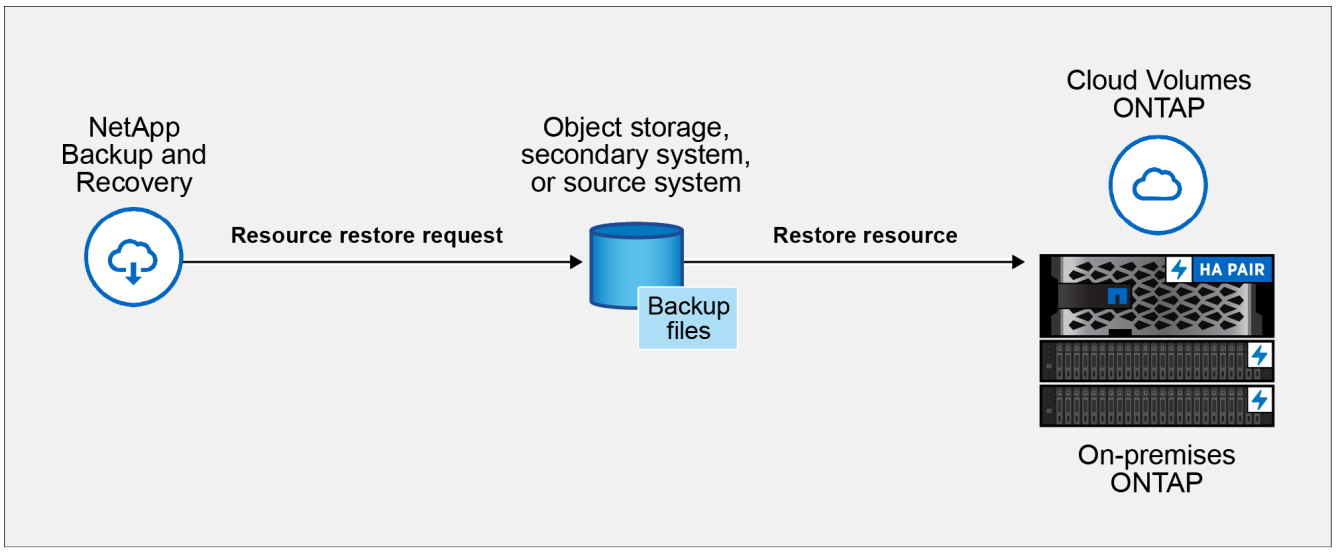
Se a Resiliência contra Ransomware estiver habilitada para um arquivo de backup no armazenamento de objetos, você será solicitado a executar uma verificação extra antes da restauração. Recomendamos realizar a verificação.

> Você pode pagar taxas extras ao seu provedor de nuvem para acessar o arquivo de backup.

Como funciona a restauração de cargas de trabalho

Ao restaurar cargas de trabalho, ocorre o seguinte:

- Ao restaurar uma carga de trabalho a partir de um snapshot local ou backup remoto, o NetApp Backup and Recovery sobrescreve a VM original se a restauração for feita para o local original e cria um *novo* recurso se a restauração for feita para um local alternativo.
- Ao restaurar uma carga de trabalho replicada, você pode restaurá-la para o sistema ONTAP local original ou para um sistema ONTAP local diferente.



- 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 (Pesquisar e Restaurar), você pode restaurar um recurso pesquisando o snapshot com filtros, mesmo que não se lembre do nome exato, local ou última data conhecida.

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 **VMware**.
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.

   Aparecerá uma lista de máquinas virtuais que correspondem aos seus critérios de pesquisa.
4. Localize na lista a máquina virtual (VM) da qual deseja restaurar e selecione o botão de menu de opções correspondente.
5. No menu que aparecer, selecione **Restaurar máquina virtual**.

   Aparece uma lista de snapshots (pontos de restauração) criados nessa máquina virtual. Por padrão, as capturas de tela mais recentes são exibidas para o período de tempo selecionado no menu suspenso **Período de tempo**.

Para cada instantâneo, os ícones iluminados na coluna **Localização** indicam os locais de armazenamento onde o instantâneo está disponível (armazenamento primário, secundário ou de objetos).

6. Ative o botão de opção correspondente ao instantâneo que deseja restaurar.
7. Selecione **Avançar**.

   Aparecem as opções de localização da captura de tela.

8. Selecione o destino de restauração para o instantâneo:
   - **Local**: Restaura o instantâneo a partir do local local.
   - **Secundário**: Restaura o snapshot a partir de um local de armazenamento remoto.
   - **Armazenamento de objetos**: Restaura o instantâneo a partir do armazenamento de objetos.

     Se optar pelo armazenamento secundário, selecione o local de destino na lista suspensa.

9. Selecione **Próximo** para continuar.
10. Escolha o destino e as configurações de restauração:

Seleção de destino

Restaurar para o local original

Ao restaurar para o local original, você não pode alterar o vCenter de destino, o host ESXi, o armazenamento de dados ou o nome da máquina virtual. A máquina virtual original é sobrescrita durante a operação de restauração.

1. Selecione o painel **Localização original**.
2. Escolha uma das seguintes opções:
   - Seção **Opções de pré-restauração**:
     - **Prescript**: Habilite esta opção para automatizar tarefas adicionais executando um script personalizado antes do início da operação de restauração. Insira o caminho completo do script que deve ser executado e quaisquer argumentos que o script receba.
   - Seção **Opções pós-restauração**:
     - **Reiniciar máquina virtual**: Habilite esta opção para reiniciar a máquina virtual após a conclusão da operação de restauração e após a aplicação do script pós-restauração.
     - **P.S.**: Habilite esta opção para automatizar tarefas adicionais executando um script personalizado após a conclusão da restauração. Insira o caminho completo do script que deve ser executado e quaisquer argumentos que o script receba.
3. Selecione **Restaurar**.

Restaurar para local alternativo

Ao restaurar para um local alternativo, você pode alterar o vCenter de destino, o host ESXi, o armazenamento de dados e o nome da VM para criar uma nova cópia da VM em um local diferente ou com um nome diferente.

1. Selecione o painel **Localização alternativa**.
2. Insira as seguintes informações:
   - Seção **Configurações de destino**:
     - **FQDN ou endereço IP do vCenter**: Selecione o servidor vCenter onde deseja restaurar o snapshot.
     - **Host ESXi**: Selecione o host onde deseja restaurar o snapshot.
     - **Rede**: Selecione a rede na qual deseja restaurar o snapshot.
     - **Repositório de dados**: Na lista suspensa, selecione o nome do repositório de dados onde deseja restaurar o snapshot.
     - **Nome da máquina virtual**: Insira o nome da máquina virtual onde você deseja restaurar o snapshot. Se o nome corresponder a uma VM já existente no armazenamento de dados, o Backup e Recuperação tornará o nome único, acrescentando um carimbo de data/hora atual.
   - Seção **Opções de pré-restauração**:
     - **Prescript**: Habilite esta opção para automatizar tarefas adicionais executando um script personalizado antes do início da operação de restauração. Insira o caminho completo do script que deve ser executado e quaisquer argumentos que o script receba.
   - Seção **Opções pós-restauração**:
     - **Reiniciar máquina virtual**: Habilite esta opção para reiniciar a máquina virtual após a conclusão da operação de restauração e após a aplicação do script pós-restauração.
     - **P.S.**: Habilite esta opção para automatizar tarefas adicionais executando um script

personalizado após a conclusão da restauração. Insira o caminho completo do script que deve ser executado e quaisquer argumentos que o script receba.

3. Selecione **Restaurar**.

Restaurar discos virtuais específicos a partir de backups.

Você pode restaurar discos virtuais existentes (VMDKs), ou discos virtuais excluídos ou desanexados, a partir de backups primários ou secundários de VMs tradicionais. Isso permite restaurar apenas dados ou aplicativos específicos da máquina virtual, evitando a necessidade de restaurar toda a máquina virtual e todos os seus discos virtuais associados em situações onde apenas dados específicos são afetados. Após a restauração do disco virtual, ele é anexado à sua máquina virtual original e fica pronto para uso.

Você pode restaurar um ou mais discos de máquina virtual (VMDKs) em uma máquina virtual para o mesmo armazenamento de dados ou para armazenamentos de dados diferentes.

Para melhorar o desempenho das operações de restauração em ambientes NFS, ative a API vStorage do aplicativo VMware para integração de matriz (VAAI).

Antes de começar

- É necessário que exista um backup.
- A VM não deve estar em trânsito.

  A VM que você deseja restaurar não deve estar no estado vMotion ou Storage vMotion.

Sobre esta tarefa

- Se o VMDK for excluído ou desanexado da VM, a operação de restauração anexará o VMDK à VM.
- Uma operação de restauração pode falhar se a camada de armazenamento do FabricPool onde a VM está localizada não estiver disponível.
- As operações de anexação e restauração conectam VMDKs usando o controlador SCSi padrão. No entanto, quando VMDKs anexados a uma VM com um disco NVMe são copiados, as operações de anexação e restauração usam o controlador NVMe, se disponível.

Passos

1. No menu NetApp Backup and Recovery , selecione **Restaurar**.
2. Na lista suspensa à direita do campo de pesquisa de nome, selecione **VMware**.
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.

   Aparecerá uma lista de máquinas virtuais que correspondem aos seus critérios de pesquisa.

4. Localize na lista a máquina virtual (VM) da qual deseja restaurar e selecione o botão de menu de opções correspondente.
5. No menu que aparecer, selecione **Restaurar discos virtuais**.

   Aparece uma lista de snapshots (pontos de restauração) criados nessa máquina virtual. Por padrão, as

capturas de tela mais recentes são exibidas para o período de tempo selecionado no menu suspenso **Período de tempo**.

Para cada instantâneo, os ícones iluminados na coluna **Localização** indicam os locais de armazenamento onde o instantâneo está disponível (armazenamento primário, secundário ou de objetos).

6. Ative o botão de opção correspondente ao instantâneo que deseja restaurar.
7. Selecione **Avançar**.

   Aparecem as opções de localização da captura de tela.

8. Selecione o destino de restauração para o instantâneo:
   - **Local**: Restaura o instantâneo a partir do local local.
   - **Secundário**: Restaura o snapshot a partir de um local de armazenamento remoto.
   - **Armazenamento de objetos**: Restaura o instantâneo a partir do armazenamento de objetos.

     Se optar pelo armazenamento secundário, selecione o local de destino na lista suspensa.

9. Selecione **Próximo** para continuar.
10. Escolha o destino e as configurações de restauração:

Seleção de destino

Restaurar para o local original

Ao restaurar para o local original, você não pode alterar o vCenter de destino, o host ESXi, o armazenamento de dados ou o nome do disco virtual. O disco virtual original foi sobrescrito.

1. Selecione o painel **Localização original**.
2. Na seção **Configurações de destino**, marque a caixa de seleção para todos os discos virtuais que você deseja restaurar.
3. Escolha uma das seguintes opções:
   - Seção **Opções de pré-restauração**:
     - **Prescript**: Habilite esta opção para automatizar tarefas adicionais executando um script personalizado antes do início da operação de restauração. Insira o caminho completo do script que deve ser executado e quaisquer argumentos que o script receba.
   - Seção **Opções pós-restauração**:
     - **P.S.**: Habilite esta opção para automatizar tarefas adicionais executando um script personalizado após a conclusão da restauração. Insira o caminho completo do script que deve ser executado e quaisquer argumentos que o script receba.
4. Selecione **Restaurar**.

Restaurar para local alternativo

Ao restaurar para um local alternativo, você pode alterar o armazenamento de dados de destino. O disco virtual é anexado à VM original após a operação de restauração, independentemente do armazenamento de dados escolhido.

1. Selecione o painel **Localização alternativa**.
2. Na seção **Configurações de destino**, marque a caixa de seleção para todos os discos virtuais que você deseja restaurar.
3. Para todos os discos virtuais que você selecionou:
   a. Selecione **Selecionar armazenamento de dados** para escolher um destino de restauração de armazenamento de dados diferente para o disco virtual.
   b. Selecione **Selecionar** para confirmar sua escolha e fechar a janela de seleção.
4. Escolha uma das seguintes opções:
   - Seção **Opções de pré-restauração**:
     - **Prescript**: Habilite esta opção para automatizar tarefas adicionais executando um script personalizado antes do início da operação de restauração. Insira o caminho completo do script que deve ser executado e quaisquer argumentos que o script receba.
   - Seção **Opções pós-restauração**:
     - **P.S.**: Habilite esta opção para automatizar tarefas adicionais executando um script personalizado após a conclusão da restauração. Insira o caminho completo do script que deve ser executado e quaisquer argumentos que o script receba.
5. Selecione **Restaurar**.

Restaurar arquivos e pastas do sistema de convidados

Você pode restaurar arquivos ou pastas de um disco de máquina virtual (VMDK) em um sistema operacional convidado Windows.

Fluxo de trabalho de restauração de convidado

As operações de restauração do sistema operacional convidado incluem as seguintes etapas:

1. Anexar

   Anexe um disco virtual a uma máquina virtual convidada e inicie uma sessão de restauração de arquivos da máquina virtual convidada.

2. Espere

   Aguarde a conclusão da operação de anexação antes de poder navegar e restaurar. Quando a operação de anexação for concluída, uma sessão de restauração de arquivos do sistema convidado será criada automaticamente.

3. Selecionar arquivos ou pastas

   Navegue pelos arquivos VMDK e selecione um ou mais arquivos ou pastas para restaurar.

4. Restaurar

   Restaurar os arquivos ou pastas selecionados para um local especificado.

Pré-requisitos para restaurar arquivos e pastas de convidados

Analise todos os requisitos antes de restaurar arquivos ou pastas de um VMDK em um sistema operacional convidado Windows.

- As ferramentas VMware devem estar instaladas e em execução.

  O NetApp Backup and Recovery utiliza informações das ferramentas VMware para estabelecer uma conexão com o sistema operacional convidado VMware.

- O sistema operacional convidado Windows deve estar executando o Windows Server 2008 R2 ou posterior.

  Para obter as informações mais recentes sobre as versões suportadas, consulte "Ferramenta de Matriz de Interoperabilidade NetApp (IMT)" .

- As credenciais para a máquina virtual de destino usam a conta de administrador local ou de domínio integrada com o nome de usuário "Administrator". Antes de iniciar a operação de restauração, configure as credenciais da máquina virtual onde deseja conectar o disco virtual. São necessárias credenciais tanto para as operações de anexação quanto para as de restauração. Usuários de grupos de trabalho podem usar a conta de administrador local integrada.

  Se você precisar usar uma conta que não seja a conta de administrador interna, mas que tenha privilégios administrativos na VM, será necessário desabilitar o UAC na VM convidada.

- Você deve saber o snapshot de backup e o VMDK para restaurar.

  O NetApp Backup and Recovery não oferece suporte à busca de arquivos ou pastas para restauração. Antes de começar, você precisa saber onde os arquivos ou pastas estão localizados no snapshot e o respectivo arquivo VMDK.

- O disco virtual a ser conectado deve estar presente em um backup do NetApp Backup and Recovery .

  O disco virtual que contém o arquivo ou pasta que você deseja restaurar deve estar em um backup de máquina virtual que foi realizado usando o NetApp Backup and Recovery.

- Para arquivos com nomes que não sejam do alfabeto inglês, você deve restaurá-los em um diretório, não como um único arquivo.

  Você pode restaurar arquivos com nomes não alfabéticos, como Kanji japonês, restaurando o diretório em que os arquivos estão localizados.

Limitações de restauração de arquivos de convidado

Antes de restaurar um arquivo ou pasta de um sistema operacional convidado, você deve estar ciente das limitações do recurso.

- Não é possível restaurar tipos de discos dinâmicos dentro de um sistema operacional convidado.
- Se você restaurar um arquivo ou pasta criptografado, o atributo de criptografia não será mantido.
- Você não pode restaurar arquivos ou pastas para uma pasta criptografada.
- Arquivos e pastas ocultos são exibidos na página de navegação de arquivos e não podem ser filtrados.
- Não é possível restaurar a partir de um sistema operacional convidado Linux.

  Não é possível restaurar arquivos e pastas de uma VM que esteja executando um sistema operacional convidado Linux. No entanto, você pode anexar um VMDK e restaurar manualmente os arquivos e pastas. Para obter as informações mais recentes sobre o sistema operacional convidado compatível, consulte o "Ferramenta de Matriz de Interoperabilidade NetApp (IMT)" .

- Não é possível restaurar de um sistema de arquivos NTFS para um sistema de arquivos FAT.

  Quando você tenta restaurar do formato NTFS para o formato FAT, o descritor de segurança NTFS não é copiado porque o sistema de arquivos FAT não oferece suporte aos atributos de segurança do Windows.

- Não é possível restaurar arquivos de convidado de um VMDK clonado ou de um VMDK não inicializado.
- Não é possível restaurar a estrutura de diretórios de um arquivo.

  Ao restaurar um arquivo de um diretório aninhado, o sistema restaura apenas o arquivo, e não sua estrutura de diretórios. Para restaurar toda a árvore de diretórios, copie o diretório de nível superior.

- Não é possível restaurar arquivos de convidado de uma VM vVol para um host alternativo.
- Não é possível restaurar arquivos de convidados criptografados.

Restaurar arquivos e pastas de convidados de VMDKs

Você pode restaurar um ou mais arquivos ou pastas de um VMDK em um sistema operacional convidado Windows.

Antes de começar

Você precisa criar credenciais para a máquina virtual convidada no NetApp Backup and Recovery antes de poder restaurar arquivos e pastas dela. O NetApp Backup and Recovery usa essas credenciais para autenticar com a máquina virtual convidada ao conectar o disco virtual.

Sobre esta tarefa

O desempenho da restauração de arquivos ou pastas convidados depende de dois fatores: o tamanho dos arquivos ou pastas que estão sendo restaurados; e o número de arquivos ou pastas que estão sendo restaurados. Restaurar um grande número de arquivos pequenos pode levar mais tempo do que o previsto em comparação à restauração de um pequeno número de arquivos grandes, se o conjunto de dados a ser restaurado for do mesmo tamanho.

Somente uma operação de anexação ou restauração pode ser executada ao mesmo tempo em uma VM. Não é possível executar operações paralelas de anexação ou restauração na mesma VM.

Com o recurso de restauração para convidados, você pode visualizar e restaurar arquivos de sistema e arquivos ocultos, além de visualizar arquivos criptografados. Não sobrescreva um arquivo de sistema existente nem restaure arquivos criptografados para uma pasta criptografada. Durante a operação de restauração, os atributos ocultos, de sistema e criptografados dos arquivos do sistema operacional convidado não são mantidos no arquivo restaurado. A visualização ou navegação em partições reservadas pode causar um erro.

Passos

1. No menu NetApp Backup and Recovery , selecione **Inventário**.
2. Selecione o menu **Máquinas virtuais**.
3. Escolha na lista uma máquina virtual que contenha os arquivos que você deseja restaurar.
4. Selecione o ícone Ações ••• para essa máquina virtual.
5. Selecione **Restaurar arquivos e pastas**.
6. Selecione um instantâneo a partir do qual deseja restaurar e, em seguida, selecione **Avançar**.
7. Escolha o local do snapshot a partir do qual deseja restaurar. Se você escolher um local secundário, selecione o instantâneo secundário na lista.
8. Selecione **Avançar**.
9. Escolha o disco virtual da lista para conectar à máquina virtual e selecione **Avançar**.
10. Na página *Selecionar credencial da máquina virtual*, se você ainda não tiver armazenado uma credencial para a máquina virtual convidada, selecione **Adicionar credenciais** e faça o seguinte:
    a. **Nome das credenciais**: Insira um nome para as credenciais.
    b. **Modo de autenticação**: Selecione **Windows**.
    c. **Agentes**: Selecione um agente de console na lista que irá gerenciar a comunicação entre o NetApp Backup and Recovery e este host.
    d. **Domínio e nome de usuário**: insira o NetBIOS ou o FQDN do domínio e o nome de usuário para as credenciais.
    e. **Senha**: Digite uma senha para a credencial.
    f. Selecione **Adicionar**.
11. Escolha uma credencial de máquina virtual para usar na autenticação com a máquina virtual convidada.

O NetApp Backup and Recovery conecta o disco virtual à máquina virtual e exibe todos os arquivos e pastas, incluindo os ocultos. Ele atribui uma letra de unidade a cada partição, incluindo as partições reservadas pelo sistema.

Os arquivos e pastas que você selecionou são listados no painel direito da tela.

12. Selecione **Avançar**.
13. Digite o caminho de compartilhamento UNC para o convidado onde os arquivos selecionados serão restaurados.
    - Exemplo de endereço IPv4: `\\10.60.136.65\c$`
    - Exemplo de endereço IPv6: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`

    Caso já existam arquivos com o mesmo nome, você pode optar por sobrescrevê-los ou ignorá-los.
14. Selecione **Restaurar**.

    Você pode visualizar o progresso da restauração na página de Monitoramento de Tarefas.

Solução de problemas de restauração de arquivos de convidado

Ao tentar restaurar um arquivo convidado, você pode encontrar qualquer um dos seguintes cenários.

A sessão de restauração do arquivo convidado está em branco

Esse problema ocorre se você criar uma sessão de restauração de arquivos em um sistema operacional convidado e o sistema operacional convidado for reiniciado durante a sessão. Os arquivos VMDK no sistema operacional convidado podem permanecer offline, portanto, a lista de sessões de restauração de arquivos do convidado fica em branco.

Para corrigir o problema, coloque manualmente os VMDKs online novamente no sistema operacional convidado. Quando os VMDKs estiverem online, a sessão de restauração do arquivo convidado exibirá o conteúdo correto.

Falha na operação de restauração de arquivo convidado e anexação de disco

Esse problema ocorre quando você inicia uma operação de restauração de arquivo convidado, mas a operação de anexação de disco falha mesmo que as ferramentas do VMware estejam em execução e as credenciais do sistema operacional convidado estejam corretas. Se isso ocorrer, o seguinte erro será retornado:

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMWare tools is running properly on system and account used is Administrator account, Error is SystemError vix error codes = (3016, 0).
```

Para corrigir o problema, reinicie o serviço VMware Tools Windows no sistema operacional convidado e tente novamente a operação de restauração do arquivo convidado.

Os backups não são desanexados após a sessão de restauração do arquivo convidado ser descontinuada

Esse problema ocorre quando você executa uma operação de restauração de arquivo convidado a partir de um backup consistente com VM. Enquanto a sessão de restauração do arquivo convidado estiver ativa, outro backup consistente com a VM será executado para a mesma VM. Quando a sessão de restauração de arquivos do convidado é desconectada, manual ou automaticamente após 24 horas, os backups da sessão não são desanexados.

Para corrigir o problema, desvincule manualmente os VMDKs que foram anexados da sessão de restauração de arquivo guest ativa.

Proteja cargas de trabalho do KVM (visualização)

Visão geral das cargas de trabalho de proteção do KVM

Proteja suas VMs KVM gerenciadas e pools de armazenamento com o NetApp Backup and Recovery. O NetApp Backup and Recovery oferece operações de backup e restauração rápidas, com uso eficiente de espaço, consistentes em caso de falha e consistentes com a máquina virtual. Seus hosts KVM e VMs devem ser gerenciados por uma plataforma de gerenciamento como o Apache CloudStack antes que você possa protegê-los usando o Backup e Recuperação.

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 protegem contra ameaças internas e externas à segurança cibernética.
- Usar diferentes tipos de mídia ajuda na recuperação caso um tipo falhe.
- Você pode restaurar rapidamente a partir da cópia local e usar as cópias externas se a cópia local estiver 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 descobrir os hosts KVM e as máquinas virtuais

antes de protegê-los. Seus hosts KVM e VMs devem ser gerenciados por uma plataforma de gerenciamento como o Apache CloudStack antes que você possa adicioná-los ao Backup e Recuperação.

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" .

Adicione uma plataforma de gerenciamento, um host KVM e descubra recursos.

Adicione informações sobre a plataforma de gerenciamento e o host KVM e permita que o NetApp Backup and Recovery descubra as cargas de trabalho.

Passos

1. No menu do NetApp Console , selecione **Proteção > Backup e recuperação**.
2. Em **Cargas de trabalho**, selecione o bloco **KVM**.

   Se você estiver acessando o Backup and Recovery pela primeira vez e tiver um sistema no Console, mas nenhum recurso descoberto, a página *Bem-vindo ao novo NetApp Backup and Recovery* será exibida com 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 integrou sua plataforma de gerenciamento com o Backup e Recuperação, selecione **Adicionar plataforma de gerenciamento**.
      i. Insira as seguintes informações:
         - **Endereço IP ou FQDN da plataforma de gerenciamento**: Insira o endereço IP ou o nome de domínio totalmente qualificado da plataforma de gerenciamento.
         - **Chave de API**: Insira a chave de API a ser usada para autenticar as solicitações de API.
         - **Chave secreta**: Insira a chave secreta a ser usada para autenticar as solicitações da API.
         - **Porta**: Insira a porta a ser usada para comunicação entre o Backup e Recuperação e a plataforma de gerenciamento.
         - **Agentes**: Selecione um agente de console para facilitar a comunicação entre o Backup e Recuperação e a plataforma de gerenciamento.
      ii. Ao terminar, selecione **Adicionar**.
   c. **Configurações do KVM**: Adicione um novo host KVM inserindo as seguintes informações:
      - **Nome de domínio totalmente qualificado (FQDN) ou endereço IP do KVM**: Insira o FQDN ou o endereço IP do host.
      - **Credenciais**: Insira o nome de usuário e a senha do host KVM.
      - **Agente de console**: Selecione o agente de console a ser usado para comunicação entre o Backup e Recuperação e o host KVM.
      - **Número da porta**: Insira a porta a ser usada para comunicação entre o Backup e Recuperação e o host KVM.
      - **Plataforma de gerenciamento**: Se o host KVM for gerenciado e você tiver adicionado a plataforma de gerenciamento ao Backup e Recuperação, selecione a plataforma de gerenciamento

na lista.

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 NetApp Backup and Recovery

Passos

1. No menu do NetApp Console , selecione **Proteção** > **Backup e recuperação**.
2. Selecione um bloco de carga de trabalho (por exemplo, Microsoft SQL Server).
3. No menu Backup e Recuperação, selecione **Painel**.
4. 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 mais 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 a partir de snapshots, 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 para estes 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 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 **Próximo** para continuar.
9. Escolha o destino e as configurações de restauração:

Seleção de destino

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 a pré-visualização de cargas de trabalho KVM.

Proteja as cargas de trabalho do Hyper-V

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 uso eficiente de espaço, consistentes em caso de falha e consistentes com a máquina virtual, tanto para instâncias autônomas quanto para instâncias de cluster FCI. Você também pode proteger máquinas virtuais Hyper-V provisionadas pelo System Center Virtual Machine Manager (SCVMM) e hospedadas em um compartilhamento CIFS.

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 protegem contra ameaças internas e externas à segurança cibernética.
- 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 ajuda você a restaurar dados rapidamente, e você pode usar as cópias externas se a cópia no local estiver 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 descobrir máquinas virtuais Hyper-V antes 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 inserindo o FQDN ou endereço IP do host, as credenciais, o agente do console e o número da porta. Se o FQDN não puder ser resolvido pelo

agente do Console, use o endereço IP em vez disso. Para clusters FCI, insira o endereço IP de gerenciamento do cluster FCI.

4. Selecione **Descobrir**.

Este processo pode levar alguns minutos.

Resultado

Depois que o NetApp Backup and Recovery descobre recursos, a página Inventário exibe a carga de trabalho do Hyper-V na lista de cargas de trabalho.

Continue para o Painel de NetApp Backup and Recovery

Passos

1. No menu do NetApp Console , selecione **Proteção** > **Backup e recuperação**.
2. Selecione um bloco de carga de trabalho (por exemplo, Microsoft SQL Server).
3. No menu Backup e Recuperação, selecione **Painel**.
4. 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. Crie um grupo de proteção para fazer backup e restaurar cargas de trabalho em conjunto.

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 o menu **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.

Editar um grupo de proteção

Edite um grupo de proteção para alterar seu nome ou configurações. Você pode querer editar um grupo de proteção se os recursos do grupo tiverem sido alterados.

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 deseja editar.
6. Selecione o ícone Ações ••• > **Editar**.
7. Altere quaisquer configurações do grupo de proteção, como o nome ou quais máquinas virtuais estão no grupo.
8. Selecione **Avançar**.
9. Altere a política de proteção, se necessário. Ao terminar, selecione **Próximo**.
10. Revise a configuração e selecione **Enviar**.

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 mais 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

Use o backup sob demanda para que seus dados estejam protegidos antes de fazer alterações no sistema.

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**.

   O backup usa a mesma política que você atribuiu 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 a partir de snapshots, de um backup da 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 para estes pontos

Você pode restaurar dados para estes pontos:

- Restaurar para o local original
- Restaurar para um local alternativo

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 **Próximo** para continuar.
8. Escolha o destino e as configurações de restauração:

Seleção de destino

Restaurar para o local original

Ao restaurar para o local original, você pode visualizar as configurações de destino expandindo a seção **Configurações de destino**, mas não poderá alterá-las.

1. Na seção **Opções pós-restauração**, considere a seguinte opção:
   - **Iniciar a máquina virtual**: Habilite esta opção para iniciar a nova máquina virtual após a restauração.
2. Selecione **Restaurar**.

Restaurar para local alternativo

1. Na seção **Configurações de destino**, insira as seguintes informações:
   - **Nome de domínio totalmente qualificado (FQDN) ou endereço IP do Hyper-V**: Insira o nome de domínio totalmente qualificado ou o endereço IP do host Hyper-V de destino.
   - **Rede**: Selecione a rede de destino onde deseja restaurar o snapshot.
   - **Nome da máquina virtual**: Insira o nome da máquina virtual que você deseja restaurar.
   - **Local de destino**: Insira a pasta de destino ou o compartilhamento CIFS que deve conter os dados restaurados.
2. Na seção **Opções de pré-restauração**, considere as seguintes opções:
   - **Restauração rápida**: Ative esta opção para disponibilizar a máquina virtual restaurada imediatamente. Apenas os arquivos necessários para executar a máquina virtual são restaurados do armazenamento de objetos, em vez do volume inteiro.
3. Na seção **Opções pós-restauração**, considere as seguintes opções:
   - **Iniciar a máquina virtual**: Habilite esta opção para iniciar a nova máquina virtual após a restauração.
4. Selecione **Restaurar**.

Proteger cargas de trabalho do Oracle Database (Prévia)

Visão geral da proteção de cargas de trabalho do Oracle Database

Proteja bancos de dados e logs do Oracle usando NetApp Backup and Recovery. Obtenha backups e restaurações rápidos, com uso eficiente de espaço, consistentes com falhas e consistentes com o banco de dados. Faça backup de cargas de trabalho do Oracle Database no AWS S3, NetApp StorageGRID, Azure Blob Storage ou ONTAP S3. Restaure backups 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 protegem contra ameaças internas e externas à segurança cibernética.
- Usar diferentes tipos de mídia ajuda na recuperação caso um tipo falhe.
- Você pode restaurar rapidamente a partir da cópia local e usar as cópias externas se a cópia local estiver 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 NetApp Backup and Recovery para executar as seguintes tarefas relacionadas às cargas de trabalho do Oracle Database:

- "Descubra cargas de trabalho do Oracle Database"
- "Criar e gerenciar grupos de proteção para cargas de trabalho do Oracle Database"
- "Fazer backup das cargas de trabalho do Oracle Database"
- "Restaurar cargas de trabalho do Oracle Database"

Descubra as cargas de trabalho do Oracle Database em 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. Em **Cargas de trabalho**, selecione o bloco **Oracle**.

   Se você estiver acessando o Backup and Recovery pela primeira vez e tiver um sistema no Console, mas nenhum recurso descoberto, a página *Bem-vindo ao novo NetApp Backup and Recovery* será exibida com 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 NetApp Backup and Recovery

1. No menu do NetApp Console , selecione **Proteção** > **Backup e recuperação**.
2. Selecione um bloco de carga de trabalho (por exemplo, Microsoft SQL Server).
3. No menu Backup e Recuperação, selecione **Painel**.
4. 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 Oracle Database com NetApp Backup e 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.
- Faça backup de um grupo de proteção agora. Veja "Faça backup das cargas de trabalho do Oracle Database 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 mais 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 das cargas de trabalho do Oracle Database usando NetApp Backup and Recovery

Use o NetApp Backup and Recovery para fazer backup de grupos de proteção ou bancos de dados do Oracle Database de sistemas ONTAP locais para armazenamento em nuvem, incluindo Amazon S3, NetApp StorageGRID, Microsoft Azure Blob Storage ou ONTAP S3. O NetApp Backup and Recovery faz backup de bancos de dados e dados de log em cada grupo de proteção.

> ⓘ Para fazer backup de grupos de proteção ou bancos de dados individuais em um agendamento, crie políticas que gerenciem 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. Consulte "Crie e gerencie grupos de proteção para cargas de trabalho do Oracle Database com NetApp Backup e Recovery" para mais 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

Execute um backup sob demanda antes de fazer alterações no sistema para garantir que seus dados estejam protegidos.

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. Em **Cargas de trabalho**, selecione o bloco **Oracle**.
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**.

> O NetApp Backup and Recovery usa a mesma política para o backup e o 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. Em **Cargas de trabalho**, selecione o bloco **Oracle**.
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 a partir de snapshots, 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 para estes 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 **Próximo** para continuar.
9. Escolha o destino e as configurações de restauração:

Seleção de destino

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 a prévia de cargas de trabalho do Oracle Database.

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 Oracle Database

Se você configurar a política de proteção para um banco de dados para reter logs de arquivamento, poderá montar pontos de recuperação para visualizar o histórico de alterações do 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**.

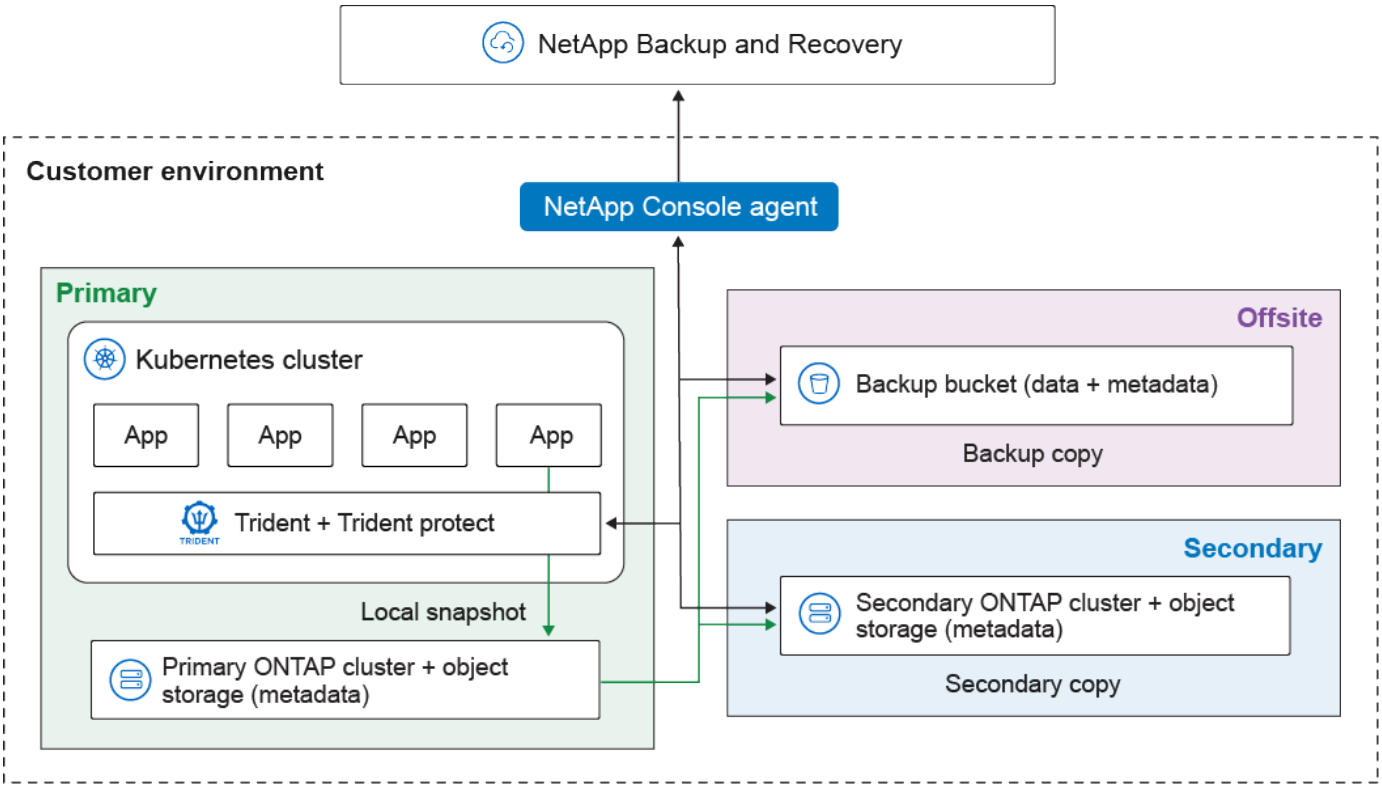
   Uma lista de pontos de recuperação para esse banco de dados é exibida.
7. Escolha um ponto de recuperação da lista e selecione o ícone Ações ••• > **Desmontar**.
8. Confirme a ação selecionando **Desmontar**.

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 descobrir cargas de trabalho do Kubernetes antes de protegê-las.

*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, descubra cargas de trabalho do Kubernetes em seu ambiente. Adicionar uma carga de trabalho adiciona um cluster Kubernetes ao NetApp Backup and Recovery. Você pode então adicionar aplicativos e proteger os recursos do cluster.

> Ao descobrir um cluster que está atualmente protegido com Trident Protect, quaisquer agendamentos de backup usados com Trident Protect são desativados durante o processo de descoberta (os agendamentos de backup do Trident Protect não são compatíveis com Backup and Recovery). Para proteger os aplicativos do cluster, "crie uma nova política de proteção" ou associe os aplicativos a uma política existente. Você pode então remover os agendamentos de backup do Trident Protect, se necessário.

Passos

1. Faça um dos seguintes:
   - Se você estiver descobrindo cargas de trabalho do Kubernetes pela primeira vez, no NetApp Backup and Recovery, em **Cargas de trabalho**, selecione o bloco **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 Trident Protect
   - Crie um segredo do Kubernetes
   - Adicionar um repositório Helm
   - Instale ou atualize 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 NetApp Backup and Recovery

Siga estas etapas para visualizar o Painel de NetApp Backup and Recovery .

1. No menu do NetApp Console , selecione **Proteção** > **Backup e recuperação**.
2. Selecione um bloco de carga de trabalho (por exemplo, Microsoft SQL Server).
3. No menu Backup e Recuperação, selecione **Painel**.
4. 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

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" .

Adicione um aplicativo usando a interface web

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.

Adicionar um aplicativo usando um CR

Passos

1. Crie o arquivo CR do aplicativo de destino:
   a. Crie o arquivo de recurso personalizado (CR) e dê um nome a ele (por exemplo, `my-app-`

`name.yaml`).

b. Configurar os seguintes atributos:

- **metadata.name**: (*Obrigatório*) O nome do recurso personalizado do aplicativo. Anote o nome escolhido, pois outros arquivos CR necessários para operações de proteção fazem referência a esse valor.
- **spec.includedNamespaces**: (*Obrigatório*) Use o seletor de namespace e rótulo para especificar os namespaces e recursos que o aplicativo utiliza. O namespace do aplicativo deve fazer parte desta lista. O seletor de rótulo é opcional e pode ser usado para filtrar recursos dentro de cada namespace especificado.
- **spec.includedClusterScopedResources**: (*Opcional*) Use este atributo para especificar recursos com escopo de cluster a serem incluídos na definição do aplicativo. Este atributo permite selecionar esses recursos com base em seu grupo, versão, tipo e rótulos.
  - **groupVersionKind**: (*Obrigatório*) Especifica o grupo de API, a versão e o tipo do recurso com escopo de cluster.
  - **labelSelector**: (Opcional) Filtra os recursos com escopo de cluster com base em seus rótulos.

c. Configurar as seguintes anotações, se necessário:

- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**: (*Opcional*) Esta anotação só se aplica a aplicações definidas a partir de máquinas virtuais, como em KubeVirt ambientes, onde o congelamento do sistema de arquivos ocorre antes dos snapshots. Especifique se esta aplicação pode gravar no sistema de arquivos durante um snapshot. Se definida como true, a aplicação ignora a configuração global e pode gravar no sistema de arquivos durante um snapshot. Se definida como false, a aplicação ignora a configuração global e o sistema de arquivos é congelado durante um snapshot. Se especificada, mas a aplicação não tiver máquinas virtuais na definição da aplicação, a anotação será ignorada. Se não especificada, a aplicação segue a "configuração global de congelamento do sistema de arquivos".
- **protect.trident.netapp.io/protection-command**: (opcional) Use esta anotação para instruir o NetApp Backup and Recovery a proteger ou parar de proteger o aplicativo. Os valores possíveis são `protect` ou `unprotect`.
- **protect.trident.netapp.io/protection-policy-name**: (opcional) Use esta anotação para especificar o nome da política de proteção do NetApp Backup and Recovery que você deseja usar para proteger este aplicativo. Esta política de proteção já deve existir no NetApp Backup and Recovery.

Se você precisar aplicar essa anotação depois que um aplicativo já tiver sido criado, pode usar o seguinte comando:

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
Exemplo YAML:

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
    protect.trident.netapp.io/protection-command: "protect"
    protect.trident.netapp.io/protection-policy-name: "policy-name"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. (Opcional) Adicione filtragem que inclua ou exclua recursos marcados com rótulos específicos:

   - **resourceFilter.resourceSelectionCriteria**: (obrigatório para filtragem) Use `Include` ou `Exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:

     - **resourceFilter.resourceMatchers**: Uma matriz de objetos resourceMatcher. Se você definir vários elementos nesta matriz, eles correspondem como uma operação OR, e os campos dentro de cada elemento (group, kind, version) correspondem como uma operação AND.
       - **resourceMatchers[].group**: (*Opcional*) Grupo do recurso a ser filtrado.
       - **resourceMatchers[].kind**: (*Opcional*) Tipo do recurso a ser filtrado.
       - **resourceMatchers[].version**: (Opcional) Versão do recurso a ser filtrado.

- **resourceMatchers[].names**: (*Opcional*) Nomes no campo metadata.name do Kubernetes do recurso a ser filtrado.
- **resourceMatchers[].namespaces**: (*Opcional*) Namespaces no campo metadata.name do Kubernetes do recurso a ser filtrado.
- **resourceMatchers[].labelSelectors**: (*Opcional*) String seletora de rótulo no campo metadata.name do Kubernetes do recurso, conforme definido no "Documentação do Kubernetes". Por exemplo: `"trident.netapp.io/os=linux"`.

> Quando ambos `resourceFilter` e `labelSelector` são usados, `resourceFilter` é executado primeiro e, em seguida, `labelSelector` é aplicado aos recursos resultantes.

Por exemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

2. Após criar a CR do aplicativo para corresponder ao seu ambiente, aplique a CR. Por exemplo:

```
kubectl apply -f my-app-name.yaml
```

Faça backup de aplicativos Kubernetes agora usando a interface web de Backup and Recovery

NetApp Backup and Recovery permite que você faça backup manual de aplicativos Kubernetes usando a interface web.

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" .

Faça backup de um aplicativo Kubernetes agora usando a interface web

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.

Faça backup de aplicativos Kubernetes agora usando recursos personalizados em Backup and Recovery

NetApp Backup and Recovery permite que você faça backup manual de aplicativos Kubernetes usando recursos personalizados (CRs).

Faça backup de um aplicativo Kubernetes agora usando recursos personalizados

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.

> Os recursos com escopo de cluster são incluídos em um backup, Snapshot ou clone se forem explicitamente referenciados na definição do aplicativo ou se tiverem referências a qualquer um dos namespaces do aplicativo.

Antes de começar

Certifique-se de que o tempo de expiração do token de sessão da AWS seja suficiente para quaisquer operações de backup do s3 de longa duração. Se o token expirar durante a operação de backup, a operação pode falhar.

- Consulte o "Documentação da API AWS" para mais informações sobre como verificar a expiração do token de sessão atual.
- Consulte "Documentação do AWS IAM" para obter mais informações sobre credenciais com recursos da AWS.

Crie um snapshot local usando um recurso personalizado

Para criar um Snapshot da sua aplicação Kubernetes e armazená-lo localmente, utilize o recurso personalizado Snapshot com atributos específicos.

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `local-snapshot-cr.yaml`.
2. No arquivo que você criou, configure os seguintes atributos:
   - **metadata.name**: (*Obrigatório*) O nome deste recurso personalizado; escolha um nome único e adequado ao seu ambiente.
   - **spec.applicationRef**: o nome do aplicativo no Kubernetes para o qual será criado o Snapshot.
   - **spec.appVaultRef**: (*Obrigatório*) O nome do AppVault onde o conteúdo do Snapshot (metadados) deve ser armazenado.
   - **spec.reclaimPolicy**: (*Opcional*) Define o que acontece com o AppArchive de um snapshot quando o CR do snapshot é excluído. Isso significa que mesmo quando definido como `Retain`, o snapshot será excluído. Opções válidas:
     - `Retain` (padrão)
     - `Delete`

```
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  namespace: my-app-namespace
  name: local-snapshot-cr
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  reclaimPolicy: Retain
```

3. Após preencher o `local-snapshot-cr.yaml` file com os valores corretos, aplique a CR:

```
kubectl apply -f local-snapshot-cr.yaml
```

Faça backup de um aplicativo em um armazenamento de objetos usando um recurso personalizado

Crie um CR de backup com atributos específicos para fazer backup do seu aplicativo em um object store.

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `object-store-backup-cr.yaml`.
2. No arquivo que você criou, configure os seguintes atributos:
   - **metadata.name**: (*Obrigatório*) O nome deste recurso personalizado; escolha um nome único e adequado ao seu ambiente.
   - **spec.applicationRef**: (*Obrigatório*) O nome do aplicativo Kubernetes a ser feito backup.
   - **spec.appVaultRef**: (*Obrigatório, mutuamente exclusivo com spec.appVaultTargetsRef*) Se você usar o mesmo bucket para armazenar o snapshot e o backup, este é o nome do AppVault onde o conteúdo do backup deve ser armazenado.

- **spec.appVaultTargetsRef**: (*Obrigatório, mutuamente exclusivo com spec.appVaultRef*) Se você usar buckets diferentes para armazenar o snapshot e o backup, este é o nome do AppVault onde o conteúdo do backup deve ser armazenado.
- **spec.dataMover**: (*Opcional*) Uma string indicando qual ferramenta de backup usar para a operação de backup. O valor diferencia maiúsculas de minúsculas e deve ser `CBS`.
- **spec.reclaimPolicy**: (*Opcional*) Define o que acontece com o conteúdo do backup (metadados/dados do volume) quando o CR de backup é excluído. Valores possíveis:
  - `Delete`
  - `Retain` (padrão)
- **spec.cleanupSnapshot**: (*Obrigatório*) Garante que o snapshot temporário criado pelo CR de backup não seja excluído após a conclusão da operação de backup. Valor recomendado: `false`.

Exemplo de YAML ao usar o mesmo bucket para armazenar o snapshot e o backup:

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

Exemplo de YAML ao usar buckets diferentes para armazenar o snapshot e o backup:

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: object-store-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

3. Após preencher o arquivo `object-store-backup-cr.yaml` com os valores corretos, aplique a CR:

```
kubectl apply -f object-store-backup-cr.yaml
```

Crie um backup 3-2-1 fanout usando um recurso personalizado

O backup usando uma arquitetura de distribuição 3-2-1 copia um backup para storage secundário, bem como para um armazenamento de objetos. Para criar um backup 3-2-1 de distribuição, crie um Backup CR com atributos específicos.

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `3-2-1-fanout-backup-cr.yaml`.
2. No arquivo que você criou, configure os seguintes atributos:
   - **metadata.name**: (*Obrigatório*) O nome deste recurso personalizado; escolha um nome único e adequado ao seu ambiente.
   - **spec.applicationRef**: (*Obrigatório*) O nome do aplicativo Kubernetes a ser feito backup.
   - **spec.appVaultTargetsRef**: (*Obrigatório*) O nome do AppVault onde o conteúdo do backup deve ser armazenado.
   - **spec.dataMover**: (*Opcional*) Uma string indicando qual ferramenta de backup usar para a operação de backup. O valor diferencia maiúsculas de minúsculas e deve ser `CBS`.
   - **spec.reclaimPolicy**: (*Opcional*) Define o que acontece com o conteúdo do backup (metadados/dados do volume) quando o CR de backup é excluído. Valores possíveis:
     - `Delete`
     - `Retain` (padrão)
   - **spec.cleanupSnapshot**: (*Obrigatório*) Garante que o snapshot temporário criado pelo CR de backup não seja excluído após a conclusão da operação de backup. Valor recomendado: `false`.
   - **spec.replicateSnapshot**: (*Obrigatório*) Instrui o NetApp Backup and Recovery a replicar o Snapshot para storage secundário. Valor obrigatório: `true`.
   - **spec.replicateSnapshotReclaimPolicy**: (*Opcional*) Define o que acontece com o snapshot replicado quando ele é excluído. Valores possíveis:
     - `Delete`
     - `Retain` (padrão)

     Exemplo YAML:

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: 3-2-1-fanout-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
  replicateSnapshot: true
  replicateSnapshotReclaimPolicy: Retain
```

3. Após preencher o `3-2-1-fanout-backup-cr.yaml` file com os valores corretos, aplique a CR:

```
kubectl apply -f 3-2-1-fanout-backup-cr.yaml
```

Anotações de backup suportadas

A tabela a seguir descreve as anotações que você pode usar ao criar um backup CR.

Anotação	Tipo	Descrição	Valor padrão
protect.trident.netapp.io/backup-completo	string	Especifica se um backup deve ser não incremental. Defina como `true` para criar um backup não incremental. A melhor prática é realizar um backup completo periodicamente e, em seguida, realizar backups incrementais entre os backups completos para minimizar o risco associado às restaurações.	"false"
protect.trident.netapp.io/snapshot-completion-timeout	string	O tempo máximo permitido para a conclusão geral da operação de Snapshot.	"60m"
protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout	string	Tempo máximo permitido para que os snapshots de volume atinjam o estado pronto para uso.	"30m"
protect.trident.netapp.io/volume-snapshots-created-timeout	string	O tempo máximo permitido para que snapshots de volume sejam criados.	"5m"
protect.trident.netapp.io/pvc-bind-timeout-sec	string	Tempo máximo (em segundos) de espera para que quaisquer PersistentVolumeClaims (PVCs) recém-criadas atinjam a `Bound` fase antes que a operação falhe.	"1200" (20 minutos)

Restaurar aplicativos Kubernetes

Restaurar aplicações Kubernetes usando a interface web

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.

Antes de começar

Se você estiver restaurando um aplicativo que foi copiado usando Trident Protect, certifique-se de que Trident Protect esteja instalado tanto no cluster de origem quanto no cluster de destino.

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 menu NetApp Backup e Recuperação, selecione **Restaurar**.
2. Escolha um aplicativo Kubernetes da lista e selecione **Visualizar e restaurar** para esse aplicativo.

   A lista de pontos de restauração é exibida.

3. Selecione o botão **Restaurar** para o ponto de recuperação que deseja usar.

Configurações gerais

1. Escolha o local de origem do qual restaurar.
2. Escolha o cluster de destino na lista **Cluster**.

   Restaurar um snapshot local criado pelo Trident Protect para um cluster diferente não é suportado no momento.

3. Escolha restaurar nos namespaces originais ou em novos namespaces.
4. Se você optar por restaurar para novos namespaces, insira o namespace ou namespaces de destino a serem usados.
5. 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. Expanda a seção **Configurações de destino** e escolha restaurar para a classe de armazenamento padrão, para uma classe de armazenamento diferente ou, se estiver restaurando para um cluster diferente, mapear as classes de armazenamento para o cluster de destino.
2. Se você optar por restaurar para uma classe de armazenamento diferente, selecione uma classe de armazenamento de destino que corresponda a cada classe de armazenamento de origem.
3. Opcionalmente, se estiver restaurando um backup ou snapshot criado com Trident Protect, visualize os detalhes do AppVault usado como o bucket de armazenamento para a operação de restauração. Se houver uma alteração no seu ambiente ou no status do AppVault, selecione **Sincronizar App Vault** para atualizar os detalhes.

   Se você precisar criar um AppVault em um cluster Kubernetes para facilitar a restauração de um backup ou snapshot criado usando Trident Protect, consulte "Use objetos do Trident Protect AppVault para gerenciar buckets".

4. Opcionalmente, expanda a seção **Scripts de restauração** e habilite a opção **Pós-script** para escolher um modelo de gancho de execução que será executado após a conclusão da operação de restauração. Se necessário, insira quaisquer argumentos que o script precise e adicione seletores de rótulo para filtrar recursos com base nos rótulos dos recursos.
5. Selecione **Restaurar**.

Restaurar aplicativos Kubernetes usando um recurso personalizado

Você pode usar recursos personalizados para restaurar seus aplicativos a partir de um snapshot ou backup. A restauração a partir de um snapshot existente será mais rápida

ao restaurar o aplicativo para o mesmo cluster.

- Ao restaurar um aplicativo, todos os ganchos de execução configurados para o aplicativo são restaurados juntamente com o aplicativo. Se houver um gancho de execução pós-restauração, ele é executado automaticamente como parte da operação de restauração.
- A restauração a partir de um backup para um namespace diferente ou para o namespace original é suportada para volumes qtree. No entanto, a restauração a partir de um snapshot para um namespace diferente ou para o namespace original não é suportada para volumes qtree.
- Você pode usar configurações avançadas para personalizar as operações de restauração. Para saber mais, consulte "Use configurações avançadas de restauração de recursos personalizados".

Restaurar um backup para um namespace diferente

Ao restaurar um backup para um namespace diferente usando uma BackupRestore CR, NetApp Backup and Recovery restaura o aplicativo em um novo namespace e cria uma CR de aplicativo para o aplicativo restaurado. Para proteger o aplicativo restaurado, crie backups ou snapshots sob demanda, ou estabeleça um cronograma de proteção.

- Restaurar um backup para um namespace diferente com recursos existentes não alterará nenhum recurso que compartilhe nomes com aqueles no backup. Para restaurar todos os recursos do backup, exclua e recrie o namespace de destino ou restaure o backup para um novo namespace.
- Ao usar uma CR para restaurar em um novo namespace, você deve criar manualmente o namespace de destino antes de aplicar a CR. NetApp Backup and Recovery cria namespaces automaticamente somente quando se usa a CLI.

Antes de começar

Certifique-se de que o tempo de expiração do token de sessão da AWS seja suficiente para quaisquer operações de restauração do s3 de longa duração. Se o token expirar durante a operação de restauração, a operação pode falhar.

- Consulte o "Documentação da API AWS" para mais informações sobre como verificar a expiração do token de sessão atual.
- Consulte "Documentação do AWS IAM" para obter mais informações sobre credenciais com recursos da AWS.

Ao restaurar backups usando Kopia como o data mover, você pode opcionalmente especificar anotações no CR para controlar o comportamento do armazenamento temporário usado pelo Kopia. Consulte a "Documentação Kopia" para mais informações sobre as opções que você pode configurar.

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `trident-protect-backup-restore-cr.yaml`.
2. No arquivo que você criou, configure os seguintes atributos:
   - **metadata.name**: (*Obrigatório*) O nome deste recurso personalizado; escolha um nome único e adequado ao seu ambiente.

- **spec.appArchivePath**: O caminho dentro do AppVault onde o conteúdo do backup está armazenado. Você pode usar o seguinte comando para encontrar esse caminho:

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.appVaultRef**: (*Obrigatório*) O nome do AppVault onde o conteúdo do backup está armazenado.
- **spec.namespaceMapping**: O mapeamento do namespace de origem da operação de restauração para o namespace de destino. Substitua `my-source-namespace` e `my-destination-namespace` pelas informações do seu ambiente.

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. (*Opcional*) Se precisar selecionar apenas determinados recursos do aplicativo para restaurar, adicione filtros que incluam ou excluam recursos marcados com rótulos específicos:

> ⓘ Trident Protect seleciona alguns recursos automaticamente devido à sua relação com os recursos que você seleciona. Por exemplo, se você selecionar um recurso de reivindicação de volume persistente e ele tiver um pod associado, Trident Protect também restaurará o pod associado.

- **resourceFilter.resourceSelectionCriteria**: (obrigatório para filtragem) Use `Include` ou `Exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:
  - **resourceFilter.resourceMatchers**: Uma matriz de objetos resourceMatcher. Se você definir vários elementos nesta matriz, eles correspondem como uma operação OR, e os campos dentro de cada elemento (group, kind, version) correspondem como uma operação AND.
    - **resourceMatchers[].group**: (*Opcional*) Grupo do recurso a ser filtrado.
    - **resourceMatchers[].kind**: (*Opcional*) Tipo do recurso a ser filtrado.
    - **resourceMatchers[].version**: (Opcional) Versão do recurso a ser filtrado.
    - **resourceMatchers[].names**: (*Opcional*) Nomes no campo metadata.name do Kubernetes do recurso a ser filtrado.
    - **resourceMatchers[].namespaces**: (*Opcional*) Namespaces no campo metadata.name do Kubernetes do recurso a ser filtrado.
    - **resourceMatchers[].labelSelectors**: (*Opcional*) String seletora de rótulo no campo metadata.name do Kubernetes do recurso, conforme definido no "Documentação do

Kubernetes". Por exemplo: `"trident.netapp.io/os=linux"`.

Por exemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Após preencher o `trident-protect-backup-restore-cr.yaml` file com os valores corretos, aplique a CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Restaurar um backup para o namespace original

Você pode restaurar um backup para o namespace original a qualquer momento.

Antes de começar

Certifique-se de que o tempo de expiração do token de sessão da AWS seja suficiente para quaisquer operações de restauração do s3 de longa duração. Se o token expirar durante a operação de restauração, a operação pode falhar.

- Consulte o "Documentação da API AWS" para mais informações sobre como verificar a expiração do token de sessão atual.
- Consulte "Documentação do AWS IAM" para obter mais informações sobre credenciais com recursos da AWS.

> ⓘ Ao restaurar backups usando Kopia como o data mover, você pode opcionalmente especificar anotações no CR para controlar o comportamento do armazenamento temporário usado pelo Kopia. Consulte a "Documentação Kopia" para mais informações sobre as opções que você pode configurar.

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `trident-protect-backup-ipr-cr.yaml`.
2. No arquivo que você criou, configure os seguintes atributos:
   - **metadata.name**: (*Obrigatório*) O nome deste recurso personalizado; escolha um nome único e adequado ao seu ambiente.
   - **spec.appArchivePath**: O caminho dentro do AppVault onde o conteúdo do backup está armazenado. Você pode usar o seguinte comando para encontrar esse caminho:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef**: (*Obrigatório*) O nome do AppVault onde o conteúdo do backup está armazenado.

     Por exemplo:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. (*Opcional*) Se precisar selecionar apenas determinados recursos do aplicativo para restaurar, adicione filtros que incluam ou excluam recursos marcados com rótulos específicos:

   Trident Protect seleciona alguns recursos automaticamente devido à sua relação com os recursos que você seleciona. Por exemplo, se você selecionar um recurso de reivindicação de volume persistente e ele tiver um pod associado, Trident Protect também restaurará o pod associado.

   - **resourceFilter.resourceSelectionCriteria**: (obrigatório para filtragem) Use `Include` ou `Exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:
     - **resourceFilter.resourceMatchers**: Uma matriz de objetos resourceMatcher. Se você definir vários elementos nesta matriz, eles correspondem como uma operação OR, e os campos dentro de cada elemento (group, kind, version) correspondem como uma operação AND.
       - **resourceMatchers[].group**: (*Opcional*) Grupo do recurso a ser filtrado.
       - **resourceMatchers[].kind**: (*Opcional*) Tipo do recurso a ser filtrado.
       - **resourceMatchers[].version**: (Opcional) Versão do recurso a ser filtrado.
       - **resourceMatchers[].names**: (*Opcional*) Nomes no campo metadata.name do Kubernetes do recurso a ser filtrado.
       - **resourceMatchers[].namespaces**: (*Opcional*) Namespaces no campo metadata.name do Kubernetes do recurso a ser filtrado.

- **resourceMatchers[].labelSelectors**: (*Opcional*) String seletora de rótulo no campo metadata.name do Kubernetes do recurso, conforme definido no "Documentação do Kubernetes". Por exemplo: `"trident.netapp.io/os=linux"`.

  Por exemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Após preencher o arquivo `trident-protect-backup-ipr-cr.yaml` com os valores corretos, aplique a CR:

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

Restaurar um backup em um cluster diferente

Você pode restaurar um backup em um cluster diferente se houver um problema com o cluster original.

- Ao restaurar backups usando Kopia como o data mover, você pode opcionalmente especificar anotações no CR para controlar o comportamento do armazenamento temporário usado pelo Kopia. Consulte a "Documentação Kopia" para mais informações sobre as opções que você pode configurar.
- Ao usar uma CR para restaurar em um novo namespace, você deve criar manualmente o namespace de destino antes de aplicar a CR.

Antes de começar

Certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O cluster de destino tem Trident Protect instalado.
- O cluster de destino tem acesso ao caminho do bucket do mesmo AppVault que o cluster de origem, onde o backup está armazenado.

- Certifique-se de que o tempo de expiração do token de sessão da AWS seja suficiente para quaisquer operações de restauração de longa duração. Se o token expirar durante a operação de restauração, a operação pode falhar.
  - Consulte o "Documentação da API AWS" para mais informações sobre como verificar a expiração do token de sessão atual.
  - Consulte "Documentação da AWS" para obter mais informações sobre credenciais com recursos da AWS.

Passos

1. Verifique a disponibilidade do AppVault CR no cluster de destino usando o plugin Trident Protect CLI:

```
tridentctl-protect get appvault --context <destination_cluster_name>
```

> Certifique-se de que o namespace destinado à restauração do aplicativo exista no cluster de destino.

2. Visualize o conteúdo do backup disponível AppVault do cluster de destino:

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

Executar este comando exibe os backups disponíveis no AppVault, incluindo seus clusters de origem, nomes de aplicativos correspondentes, carimbos de data/hora e caminhos de arquivamento.

Exemplo de saída:

```
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |         TIMESTAMP
|    PATH     |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
```

3. Restaure o aplicativo no cluster de destino usando o nome AppVault e o caminho do arquivo:
4. Crie o arquivo de recurso personalizado (CR) e nomeie-o `trident-protect-backup-restore-cr.yaml`.

5. No arquivo que você criou, configure os seguintes atributos:

   - **metadata.name**: (*Obrigatório*) O nome deste recurso personalizado; escolha um nome único e adequado ao seu ambiente.
   - **spec.appVaultRef**: (*Obrigatório*) O nome do AppVault onde o conteúdo do backup está armazenado.
   - **spec.appArchivePath**: O caminho dentro do AppVault onde o conteúdo do backup está armazenado. Você pode usar o seguinte comando para encontrar esse caminho:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

     Se o BackupRestore CR não estiver disponível, você pode usar o comando mencionado na etapa 2 para visualizar o conteúdo do backup.

   - **spec.namespaceMapping**: O mapeamento do namespace de origem da operação de restauração para o namespace de destino. Substitua `my-source-namespace` e `my-destination-namespace` pelas informações do seu ambiente.

     Por exemplo:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

6. Após preencher o `trident-protect-backup-restore-cr.yaml` file com os valores corretos, aplique a CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Restaurar um snapshot para um namespace diferente

Você pode restaurar dados de um snapshot usando um arquivo de recurso personalizado (CR) para um namespace diferente ou para o namespace de origem original. Ao restaurar um snapshot para um namespace diferente usando um SnapshotRestore CR, NetApp Backup and Recovery restaura o aplicativo em um novo namespace e cria um CR de aplicativo para o aplicativo restaurado. Para proteger o aplicativo restaurado, crie backups ou snapshots sob demanda, ou estabeleça um agendamento de proteção.

- SnapshotRestore é compatível com o atributo `spec.storageClassMapping`, mas somente quando as classes de armazenamento de origem e destino usam o mesmo backend de armazenamento. Se você tentar restaurar para uma `StorageClass` que usa um backend de armazenamento diferente, a operação de restauração falhará.
- Ao usar uma CR para restaurar em um novo namespace, você deve criar manualmente o namespace de destino antes de aplicar a CR.

Antes de começar

Certifique-se de que o tempo de expiração do token de sessão da AWS seja suficiente para quaisquer operações de restauração do s3 de longa duração. Se o token expirar durante a operação de restauração, a operação pode falhar.

- Consulte o "Documentação da API AWS" para mais informações sobre como verificar a expiração do token de sessão atual.
- Consulte "Documentação do AWS IAM" para obter mais informações sobre credenciais com recursos da AWS.

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `trident-protect-snapshot-restore-cr.yaml`.
2. No arquivo que você criou, configure os seguintes atributos:
   - **metadata.name**: (*Obrigatório*) O nome deste recurso personalizado; escolha um nome único e adequado ao seu ambiente.
   - **spec.appVaultRef**: (*Obrigatório*) O nome do AppVault onde o conteúdo do snapshot está armazenado.
   - **spec.appArchivePath**: O caminho dentro do AppVault onde o conteúdo do snapshot está armazenado. Você pode usar o seguinte comando para encontrar esse caminho:

     ```
     kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.namespaceMapping**: O mapeamento do namespace de origem da operação de restauração para o namespace de destino. Substitua `my-source-namespace` e `my-destination-namespace` pelas informações do seu ambiente.

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
       namespaceMapping: [{"source": "my-source-namespace", "destination":
     "my-destination-namespace"}]
     ```

3. (*Opcional*) Se precisar selecionar apenas determinados recursos do aplicativo para restaurar, adicione filtros que incluam ou excluam recursos marcados com rótulos específicos:

> Trident Protect seleciona alguns recursos automaticamente devido à sua relação com os recursos que você seleciona. Por exemplo, se você selecionar um recurso de reivindicação de volume persistente e ele tiver um pod associado, Trident Protect também restaurará o pod associado.

   - **resourceFilter.resourceSelectionCriteria**: (obrigatório para filtragem) Use `Include` ou `Exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:
     - **resourceFilter.resourceMatchers**: Uma matriz de objetos resourceMatcher. Se você definir vários elementos nesta matriz, eles correspondem como uma operação OR, e os campos dentro de cada elemento (group, kind, version) correspondem como uma operação AND.
       - **resourceMatchers[].group**: (*Opcional*) Grupo do recurso a ser filtrado.
       - **resourceMatchers[].kind**: (*Opcional*) Tipo do recurso a ser filtrado.
       - **resourceMatchers[].version**: (Opcional) Versão do recurso a ser filtrado.
       - **resourceMatchers[].names**: (*Opcional*) Nomes no campo metadata.name do Kubernetes do recurso a ser filtrado.
       - **resourceMatchers[].namespaces**: (*Opcional*) Namespaces no campo metadata.name do Kubernetes do recurso a ser filtrado.
       - **resourceMatchers[].labelSelectors**: (*Opcional*) String seletora de rótulo no campo metadata.name do Kubernetes do recurso, conforme definido no "Documentação do Kubernetes". Por exemplo: `"trident.netapp.io/os=linux"`.

         Por exemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Após preencher o arquivo `trident-protect-snapshot-restore-cr.yaml` com os valores corretos, aplique a CR:

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

Restaurar um snapshot para o namespace original

Você pode restaurar um snapshot para o namespace original a qualquer momento.

Antes de começar

Certifique-se de que o tempo de expiração do token de sessão da AWS seja suficiente para quaisquer operações de restauração do s3 de longa duração. Se o token expirar durante a operação de restauração, a operação pode falhar.

- Consulte o "Documentação da API AWS" para mais informações sobre como verificar a expiração do token de sessão atual.
- Consulte "Documentação do AWS IAM" para obter mais informações sobre credenciais com recursos da AWS.

Passos

1. Crie o arquivo de recurso personalizado (CR) e nomeie-o `trident-protect-snapshot-ipr-cr.yaml`.
2. No arquivo que você criou, configure os seguintes atributos:
   - **metadata.name**: (*Obrigatório*) O nome deste recurso personalizado; escolha um nome único e adequado ao seu ambiente.
   - **spec.appVaultRef**: (*Obrigatório*) O nome do AppVault onde o conteúdo do snapshot está armazenado.
   - **spec.appArchivePath**: O caminho dentro do AppVault onde o conteúdo do snapshot está armazenado. Você pode usar o seguinte comando para encontrar esse caminho:

     ```
     kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotInplaceRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
     ```
3. (*Opcional*) Se precisar selecionar apenas determinados recursos do aplicativo para restaurar, adicione filtros que incluam ou excluam recursos marcados com rótulos específicos:

> Trident Protect seleciona alguns recursos automaticamente devido à sua relação com os recursos que você seleciona. Por exemplo, se você selecionar um recurso de reivindicação de volume persistente e ele tiver um pod associado, Trident Protect também restaurará o pod associado.

- **resourceFilter.resourceSelectionCriteria**: (obrigatório para filtragem) Use `Include` ou `Exclude` para incluir ou excluir um recurso definido em resourceMatchers. Adicione os seguintes parâmetros resourceMatchers para definir os recursos a serem incluídos ou excluídos:
  - **resourceFilter.resourceMatchers**: Uma matriz de objetos resourceMatcher. Se você definir vários elementos nesta matriz, eles correspondem como uma operação OR, e os campos dentro de cada elemento (group, kind, version) correspondem como uma operação AND.
    - **resourceMatchers[].group**: (*Opcional*) Grupo do recurso a ser filtrado.
    - **resourceMatchers[].kind**: (*Opcional*) Tipo do recurso a ser filtrado.
    - **resourceMatchers[].version**: (Opcional) Versão do recurso a ser filtrado.
    - **resourceMatchers[].names**: (*Opcional*) Nomes no campo metadata.name do Kubernetes do recurso a ser filtrado.
    - **resourceMatchers[].namespaces**: (*Opcional*) Namespaces no campo metadata.name do Kubernetes do recurso a ser filtrado.
    - **resourceMatchers[].labelSelectors**: (*Opcional*) String seletora de rótulo no campo metadata.name do Kubernetes do recurso, conforme definido no "Documentação do Kubernetes". Por exemplo: `"trident.netapp.io/os=linux"`.

      Por exemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Após preencher o arquivo `trident-protect-snapshot-ipr-cr.yaml` com os valores corretos, aplique a CR:

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

Use configurações avançadas de restauração de recursos personalizados

Você pode personalizar as operações de restauração usando configurações avançadas, como anotações, configurações de namespace e opções de armazenamento para atender às suas necessidades específicas.

Anotações e rótulos de namespace durante operações de restauração e failover

Durante as operações de restauração e failover, os rótulos e anotações no namespace de destino são ajustados para corresponder aos rótulos e anotações no namespace de origem. Rótulos ou anotações do namespace de origem que não existem no namespace de destino são adicionados, e quaisquer rótulos ou anotações já existentes são sobrescritos para corresponder ao valor do namespace de origem. Rótulos ou anotações que existem apenas no namespace de destino permanecem inalterados.

> Se você usa Red Hat OpenShift, é importante observar o papel crucial das anotações de namespace em ambientes OpenShift. As anotações de namespace garantem que os pods restaurados sigam as permissões e configurações de segurança apropriadas definidas pelas restrições de contexto de segurança (SCCs) do OpenShift e possam acessar volumes sem problemas de permissão. Para mais informações, consulte o "OpenShift security context constraints documentação".

Você pode impedir que anotações específicas no namespace de destino sejam sobrescritas definindo a variável de ambiente do Kubernetes `RESTORE_SKIP_NAMESPACE_ANNOTATIONS` antes de executar a operação de restauração ou failover. Por exemplo:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values
```

> Ao executar uma operação de restauração ou failover, quaisquer anotações e rótulos de namespace especificados em `restoreSkipNamespaceAnnotations` e `restoreSkipNamespaceLabels` são excluídos da operação de restauração ou failover. Certifique-se de que essas configurações sejam definidas durante a instalação inicial do Helm. Para saber mais, consulte "Configurar configurações adicionais do helm chart do Trident Protect".

Se você instalou o aplicativo de origem usando Helm com a `--create-namespace` flag, um tratamento especial é dado à chave de rótulo `name`. Durante o processo de restauração ou failover, Trident Protect copia esse rótulo para o namespace de destino, mas atualiza o valor para o valor do namespace de destino se o valor da origem corresponder ao namespace de origem. Se esse valor não corresponder ao namespace de origem, ele é copiado para o namespace de destino sem alterações.

Exemplo

O exemplo a seguir apresenta um namespace de origem e um de destino, cada um com anotações e rótulos diferentes. Você pode ver o estado do namespace de destino antes e depois da operação, e como as anotações e os rótulos são combinados ou sobrescritos no namespace de destino.

Antes da operação de restauração ou failover

A tabela a seguir ilustra o estado dos namespaces de origem e destino do exemplo antes da operação de restauração ou failover:

Espaço de nomes	Anotações	Etiquetas
Namespace ns-1 (fonte)	• annotation.one/key: "valoratualizado" • anotação.dois/chave: "true"	• ambiente=produção • compliance=hipaa • name=ns-1
Espaço de nomes ns-2 (destino)	• annotation.one/key: "true" • anotação.three/chave: "falso"	• role=database

Após a operação de restauração

A tabela a seguir ilustra o estado do namespace de destino de exemplo após a operação de restauração ou failover. Algumas chaves foram adicionadas, outras foram sobrescritas e o `name` rótulo foi atualizado para corresponder ao namespace de destino:

Espaço de nomes	Anotações	Etiquetas
Espaço de nomes ns-2 (destino)	• annotation.one/key: "valoratualizado" • anotação.dois/chave: "true" • anotação.three/chave: "falso"	• name=ns-2 • compliance=hipaa • ambiente=produção • role=database

Campos suportados

Esta seção descreve os campos adicionais disponíveis para operações de restauração.

Mapeamento de classe de armazenamento

O `spec.storageClassMapping` atributo define um mapeamento de uma classe de armazenamento presente na aplicação de origem para uma nova classe de armazenamento no cluster de destino. Você pode usar isso ao migrar aplicações entre clusters com classes de armazenamento diferentes ou ao alterar o backend de armazenamento para operações de BackupRestore.

Exemplo:

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

Anotações suportadas

Esta seção lista as anotações suportadas para configurar diversos comportamentos no sistema. Se uma anotação não for definida explicitamente pelo usuário, o sistema usará o valor padrão.

Anotação	Tipo	Descrição	Valor padrão
protect.trident.netapp.io/data-mover-timeout-sec	string	O tempo máximo (em segundos) permitido para a operação de movimentação de dados ficar parada.	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	string	O limite máximo de tamanho (em megabytes) para o cache de conteúdo do Kopia.	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	string	Tempo máximo (em segundos) de espera para que qualquer PersistentVolumeClaims (PVC) recém-criado atinja a `Bound` fase antes que a operação falhe. Aplica-se a todos os tipos de CR de restauração (BackupRestore, BackupInplaceRestore, SnapshotRestore, SnapshotInplaceRestore). Use um valor maior se o seu backend de armazenamento ou cluster exigir mais tempo com frequência.	"1200" (20 minutos)

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

Para parar de proteger um cluster do Kubernetes, desative a proteção e exclua os aplicativos associados e, em seguida, remova o cluster do NetApp Backup and Recovery. O NetApp Backup and Recovery não exclui o cluster ou seus recursos; ele apenas remove o cluster do inventário do NetApp Console .

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.

> Não é possível remover a proteção de um aplicativo enquanto as operações de proteção ainda estiverem em execução. Aguarde a conclusão da operação ou, como solução alternativa, remover o ponto de restauração a operação de proteção em execução está usando. Você pode então remover a proteção do aplicativo.

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

Exclua um aplicativo que você não precisa mais. O NetApp Backup and Recovery interrompe a proteção e remove todos os backups e snapshots de aplicativos excluídos.

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**.

Remover um ponto de recuperação para um aplicativo Kubernetes

Pode ser necessário remover um ponto de recuperação de um aplicativo se você precisar desprotegê-lo e operações de proteção estiverem em execução.

Passos

1. No menu NetApp Backup e Recuperação, selecione **Restaurar**.
2. Escolha um aplicativo Kubernetes da lista e selecione **Visualizar e restaurar** para esse aplicativo.

   A lista de pontos de restauração é exibida.

3. Escolha o ponto de recuperação que deseja excluir e selecione o ícone Ações ••• > **Excluir ponto de recuperação** para excluí-lo.

Gerenciar modelos de ganchos de execução de NetApp Backup and Recovery para cargas de trabalho do Kubernetes

Um gancho de execução é uma ação personalizada que é executada com uma operação de proteção de dados em um aplicativo Kubernetes gerenciado. Por exemplo, crie snapshots consistentes com o aplicativo usando um gancho de execução para pausar transações de banco de dados antes de um snapshot e retomá-las depois. Ao criar um modelo de gancho de execução, especifique o tipo de gancho, o script a ser executado e filtros para contêineres de destino. Use o modelo para vincular ganchos de execução aos seus aplicativos.

NetApp Backup and Recovery congela e descongela sistemas de arquivos para aplicações como KubeVirt durante a proteção de dados. Você pode desativar esse comportamento globalmente ou para aplicações específicas usando a 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 vários ganchos de pré-operação personalizados, mas sua ordem de execução 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. O NetApp Backup and Recovery executa quaisquer ganchos de execução de pré-operação personalizados aplicáveis nos contêineres apropriados. Você pode criar vários ganchos pós-operação personalizados, mas a ordem de execução deles não é garantida nem configurável.

Se você criar vários ganchos do mesmo tipo, a ordem de execução deles não será garantida. Ganchos de diferentes tipos sempre são executados na ordem especificada. 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

Teste os scripts de execução antes de habilitá-los na produção. Use 'kubectl exec' para testar scripts e, em seguida, verifique snapshots e backups clonando o aplicativo em um namespace temporário e restaurando-o.

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.

Ganchos de execução podem reduzir ou desabilitar a funcionalidade do aplicativo. Faça com que seus ganchos personalizados sejam executados o mais rápido possível. 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.

> Os modelos que você cria aqui só podem ser usados ao proteger cargas de trabalho do Kubernetes.

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**.

   Depois de criar o modelo, ele 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 snapshots locais, replicações e trabalhos de backup que você iniciar. Acompanhe os trabalhos de restauração que você inicia. Veja os trabalhos concluídos, em andamento ou que falharam para ajudar a diagnosticar problemas. Ative as notificações por e-mail no Centro de Notificações do NetApp Console para se manter informado sobre a atividade do sistema quando não estiver conectado. Use a Linha do Tempo do Console para ver detalhes de todas as ações iniciadas na IU ou na API.

O NetApp Backup and Recovery mantém as informações do trabalho por 15 dias e, em seguida, exclui as informações do trabalho e as remove do 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, reinicie 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 do usuário, Carga de trabalho, Nome da política, Rótulo do instantâneo), selecione o sinal de mais.

Pesquise e filtre a lista de empregos

Na página de Monitoramento de Tarefas, você pode filtrar as operações usando diversos filtros, como política, rótulo do snapshot, tipo de operação (proteção, restauração, retenção ou outro) e tipo de proteção (snapshot 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 filtrar ou classificar os resultados. 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)

Monitore os fluxos de retenção (*ciclo de vida do backup*) para verificar backups, mantê-los seguros e dar suporte a auditorias. Identifique quando as cópias de backup expiram para rastrear o ciclo de vida.

Uma tarefa de ciclo de vida de backup rastreia todos os snapshots que foram excluídos ou que estão na fila para serem excluídos. A partir do ONTAP 9.13, você pode visualizar todos os tipos de trabalho denominados "Retenção" na página de Monitoramento de Trabalhos.

O tipo de tarefa "Retenção" captura todas as tarefas de exclusão de snapshots iniciadas 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.

Você pode visualizar alertas na Central de Notificações e configurar o Console para enviar alertas por e-mail sobre atividades importantes do sistema, mesmo quando você não estiver conectado. "Saiba mais sobre o Centro de Notificações e como enviar e-mails de alerta para tarefas de backup e restauração" .

A Central de Notificações exibe inúmeros eventos de snapshot, replicação, backup na nuvem e restauração, mas apenas alguns eventos acionam alertas por e-mail:

Tipo de operação	Evento	Alerta gerado	E-mail enviado
Ativação	Falha na ativação do backup e recuperação do sistema	Sim	Sim
Ativação	Falha na edição de backup e recuperação do sistema	Sim	Sim
Ativação	Volume agora associado à política de instantâneo	Sim	Sim
Ativação	Backup de volume ou estado modificado	Sim	Sim
Ativação	Ativação do recurso de backup e recuperação concluída com sucesso para o sistema.	Sim	Sim
Ativação	Falha no backup de volume ad-hoc	Sim	Sim
Ativação	Backup de volume ad-hoc concluído com sucesso.	Sim	Não
Ativação	Falha no backup de vários volumes	Sim	Sim

Tipo de operação	Evento	Alerta gerado	E-mail enviado
Operações Cron	Verificando se há rótulos de instantâneo ausentes	Sim	Sim
Operações Cron	Falha ao enviar o token de segurança para o ONTAP para este sistema.	Sim	Sim
Eventos Pub/Sub	Falha na conexão	Sim	Não
Eventos Pub/Sub	Falha ao excluir um instantâneo agendado.	Sim	Não
Eventos Pub/Sub	Falha no backup agendado do volume	Sim	Não
Eventos Pub/Sub	Restauração do volume concluída com sucesso.	Sim	Não
Eventos Pub/Sub	A restauração do volume falhou	Sim	Não
Ransomware	Possível ataque de ransomware identificado em cópia de segurança.	Sim	Sim
Ransomware	Possível ataque de ransomware identificado na cópia de segurança deste sistema.	Sim	Sim
Instantâneo local	Falha na tarefa de criação de snapshot ad hoc do NetApp Backup and Recovery	Sim	Sim
Replicação	Modificação da relação de replicação da falha de volume	Sim	Sim
Replicação	Falha na tarefa de replicação ad hoc do NetApp Backup and Recovery	Sim	Sim
Replicação	Falha na tarefa de pausa de replicação do NetApp Backup and Recovery	Sim	Não
Replicação	Falha na tarefa de interrupção da replicação do NetApp Backup and Recovery	Sim	Não
Replicação	Falha na tarefa de ressincronização de replicação do NetApp Backup and Recovery	Sim	Não
Replicação	Falha na tarefa de interrupção da replicação do NetApp Backup and Recovery	Sim	Não
Replicação	Falha na tarefa de ressincronização reversa da replicação do NetApp Backup and Recovery	Sim	Sim
Replicação	Falha na exclusão da tarefa de replicação do NetApp Backup and Recovery	Sim	Sim
Operações-alvo	Falha ao restaurar para um destino local ou na nuvem	Sim	Sim
Operações-alvo	falha de restauração sob demanda	Sim	Sim

Tipo de operação	Evento	Alerta gerado	E-mail enviado
Operações do sistema	Falha na criação de snapshot de volume ad-hoc	Sim	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". Por padrão, o sistema não configura outros usuários e destinatários para receber e-mails de notificação. Configure alertas por e-mail para qualquer usuário do Console na sua conta do NetApp Cloud ou para outros destinatários que precisam saber sobre 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.

O agente do Console inclui a funcionalidade de NetApp Backup and Recovery .

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`
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`

Informações sobre direitos autorais

Informações sobre marcas comerciais