Proteja as cargas de trabalho do Kubernetes (visualização)

NetApp Backup and Recovery

NetApp
February 23, 2026

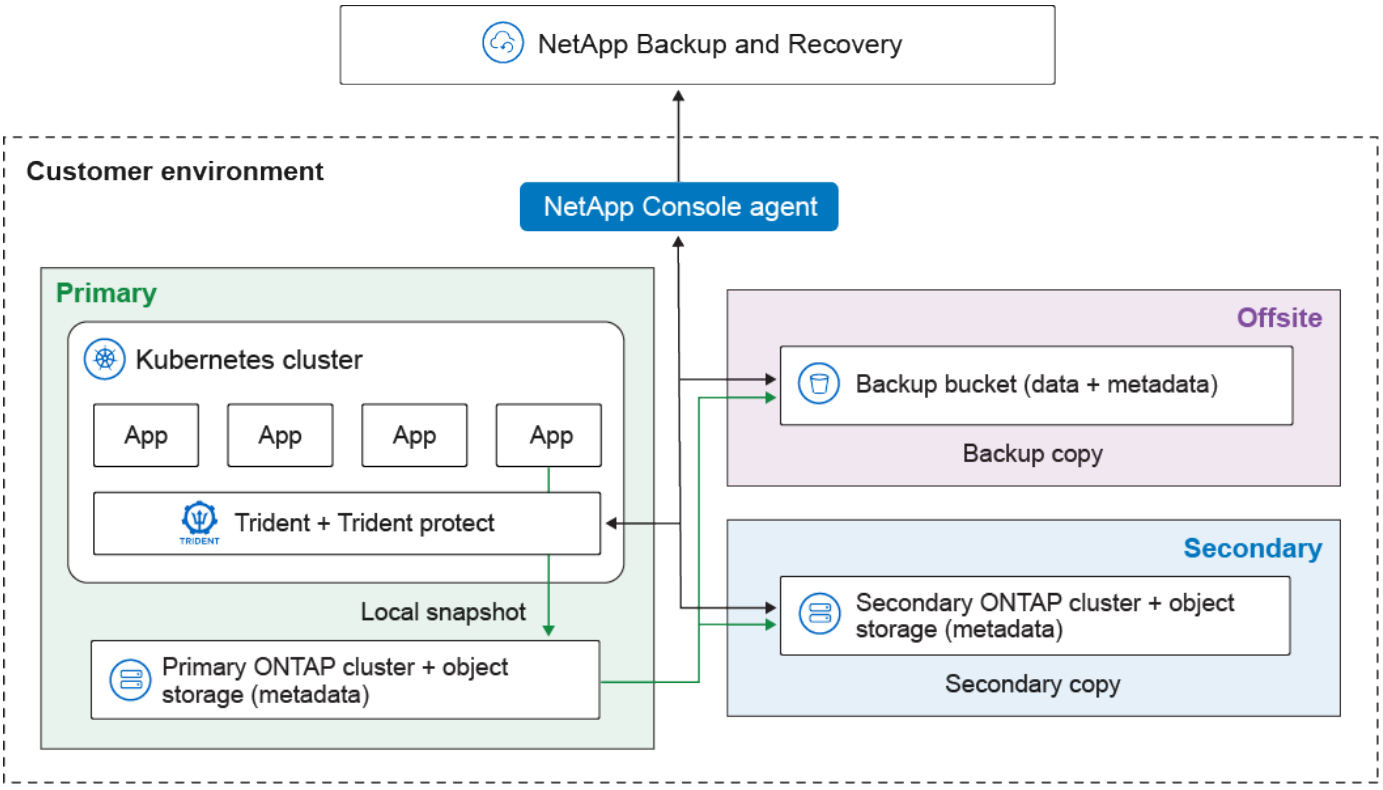
Índice

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**.

Crie e gerencie relatórios de proteção para cargas de trabalho do Kubernetes no NetApp Backup and Recovery

Em NetApp Backup and Recovery, crie relatórios de proteção para cargas de trabalho do Kubernetes para visualizar o status e os detalhes da proteção, incluindo contagens de backups bem-sucedidos e com falha, tipos de backup, informações sobre a integridade do cluster e muito mais.

Função obrigatória do NetApp Console Backup and Recovery super admin, Backup and Recovery backup admin ou Backup and Recovery restore admin. Saiba mais sobre "Funções e privilégios de backup e recuperação". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Criar um relatório de proteção

Crie um relatório de proteção para visualizar o status de proteção dos seus clusters.

Passos

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 (selecione Kubernetes na lista).
   - **Selecionar cluster**: Se você selecionou por carga de trabalho, escolha o cluster da lista para o qual deseja gerar o relatório e selecione **Aceitar**. Escolha **Selecionar tudo** para gerar um relatório para todos os clusters.
4. Defina o período 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 configuração do relatório: escolha se deseja executar o relatório apenas uma vez ou agendar a geração recorrente do relatório. Para relatórios agendados, escolha a frequência de recorrência e selecione uma data de início.

   a. Insira os detalhes de entrega por e-mail: (apenas para relatórios agendados) Se desejar que o relatório seja entregue por e-mail, insira um ou mais endereços de e-mail que devem receber o relatório agendado.

   Configure notificações por e-mail na página Configurações. Para obter detalhes sobre como configurar notificações por e-mail, consulte"Configurar definições" .

6. Selecione **Criar**.

Baixe um relatório de proteção

Faça o download de um relatório de proteção gerado, seja como um arquivo JSON ou um documento PDF, para que você possa visualizá-lo e compartilhá-lo.

Passos

1. No menu NetApp Backup and Recovery , selecione a opção **Relatórios**.
2. Na página **Relatórios**, selecione o menu **Relatórios** para ver a lista de relatórios de proteção gerados.
3. Para o relatório que você deseja baixar, selecione o ícone Ações ••• > **Baixar**.
   - Selecione **Download JSON** para baixar o relatório em formato JSON.
   - Selecione **Baixar PDF** para baixar o relatório como um documento PDF.

Visualizar um relatório de proteção

Visualize rapidamente os detalhes interativos de um relatório de proteção no NetApp Backup and Recovery. Você pode ver informações resumidas sobre tarefas, status da proteção de dados, detalhes de configuração e muito mais.

Passos

1. No menu NetApp Backup and Recovery , selecione a opção **Relatórios**.
2. Na página **Relatórios**, selecione o menu **Relatórios** para ver a lista de relatórios de proteção gerados.
3. Para o relatório que você deseja visualizar, selecione o ícone Ações ••• > **Visualizar relatório**.

   Os detalhes do relatório aparecem.

Excluir um relatório de proteção

Exclua um relatório de proteção quando não precisar mais dele.

Passos

1. No menu NetApp Backup and Recovery , selecione a opção **Relatórios**.
2. Na página **Relatórios**, selecione o menu **Relatórios** para ver a lista de relatórios de proteção gerados.
3. Para o relatório que deseja excluir, selecione o ícone Actions ••• > **Excluir**.
4. Confirme a ação selecionando **Delete**.

Informações sobre direitos autorais

Informações sobre marcas comerciais