NetBackup™ for Kubernetes 管理指南

版本 11.0

VERITAS
now part of Cohesity

上次更新时间： 2025-04-24

法律声明

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

技术支持

技术支持具有全球性支持中心。所有支持服务将会根据您的支持协议以及当时最新的企业技术支持政策进行交付。有关支持产品和服务以及如何联系技术支持的信息，请访问我们的网站：

https://www.veritas.com/support

您可以在下列 URL 上管理 Cohesity 帐户信息：

https://my.veritas.com

如果您对现有支持协议有疑问，请通过以下方式联系您所在地区的支持协议管理部门：

全球（日本除外）	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

文档

请确保您的文档是最新版本。每个文档都在第 2 页上显示上次更新日期。最新的文档可在 Cohesity 网站上找到：

https://sort.veritas.com/documents

文档反馈

您的反馈对我们非常重要。请提出您对本文档的改进建议，或者就本文档中的错误或疏漏进行报告。请注明所报告文本的文档标题、文档版本和章节标题。发送反馈到：

NB.docs@veritas.com

您也可以在以下 Cohesity 社区站点中查看相关文档信息或进行提问：

http://www.veritas.com/community/

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) 是一个网站，提供的信息和工具有助于自动处理及简化某些耗时的管理任务。根据具体产品，SORT 会帮助您准备安装和升级、识别您数据中心的风险并提高操作效率。要了解 SORT 为您的产品提供了哪些服务和工具，请参见数据表：

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目录

1

适用于 Kubernetes 的 NetBackup 概述

本章节包括下列主题：

概述

NetBackup Web UI 提供了以命名空间形式备份和还原 Kubernetes 应用程序的功能。在 NetBackup 环境中会自动发现 Kubernetes 群集中的可保护资产，管理员可以选择一个或多个包含所需日程表、备份和保留设置的保护计划。

NetBackup Web UI 允许您执行以下操作：

- 添加要保护的 Kubernetes 群集。
- 查看发现的命名空间。
- 管理角色的权限
- 设置资源限制以优化基础架构和网络负载。
- 管理保护组和智能组，以保护 Kubernetes 资产。
- 将命名空间和永久卷还原到相同的 Kubernetes 群集或备用 Kubernetes 群集。
- 监控备份和还原操作。
- 映像失效、映像导入和映像复制操作。

Kubernetes 支持的 NetBackup 功能

表 1-1 Kubernetes 的 NetBackup

功能	描述
自动 NetBackup Kubernetes 代理配置	添加 Kubernetes 群集和配置（如存储类和卷快照类），并且可以在支持自动部署的情况下执行数据移动器配置。
集成 NetBackup 基于角色的访问控制 (RBAC)	NetBackup Web UI 提供了 RBAC 角色，用于控制哪些 NetBackup 用户可以在 NetBackup 中管理 Kubernetes 操作。用户无需是 NetBackup 管理员即可管理 Kubernetes 操作。
授权	基于容量的授权。
保护计划	包括以下优势： ■ 使用一个保护计划保护多个 Kubernetes 命名空间。资产可以分布在多个群集上。 ■ 无需了解为 Kubernetes 资产提供保护的 Kubernetes 命令。
智能管理 Kubernetes 资产	NetBackup 自动发现 Kubernetes 群集中的命名空间、永久卷、永久卷声明等。您也可以执行手动发现。发现资产后，Kubernetes 工作负载管理员可以选择一个或多个保护计划来保护资产。 **注意：**在使用自动映像同步复制 (AIR) 的情况下，目标主服务器的已导入命名空间会将“导入的时间”显示为“**上次发现日期**”。
Kubernetes 特定凭据	用于对群集进行身份验证和管理的 Kubernetes 服务帐户。
发现 ■ 完全发现 ■ 增量发现	使用“**立即发现**”选项执行的发现始终是完全发现。 将新群集添加到 NetBackup 时执行的发现始终是完全发现。 添加 Kubernetes 群集后，将触发自动发现周期，以发现 Kubernetes 群集上可用的所有资产。当天的第一个自动发现是完全发现，后续的自动发现是增量发现。
备份功能 ■ 仅快照备份 ■ 从快照备份	以下功能可用于备份： ■ 备份完全由 NetBackup 服务器从一个中心位置进行管理。管理员可以为不同 Kubernetes 群集上的命名空间安排无人值守的自动备份。 ■ NetBackup Web UI 支持从一个界面备份和还原命名空间。 ■ 完全备份的备份计划配置。 ■ 手动备份和仅快照备份。 ■ 针对每个群集进行资源限制以提高备份性能。 ■ NetBackup 可以通过快照方法对 Kubernetes 命名空间执行备份，以实现恢复时间更短的目标。
还原功能 ■ 从快照还原 ■ 从备份副本还原	以下功能可用于还原： ■ 将 Kubernetes 命名空间和永久卷还原到不同位置。 ■ 执行并行还原作业时，使用“从备份副本还原”还原为不同的 Kubernetes 群集风格。

功能	描述
客户端数据重复数据删除支持	为 Kubernetes 启用了客户端数据重复数据删除支持功能。 有关更多详细信息，请参考《NetBackup 重复数据删除指南》中的“关于客户端重复数据删除”部分。
自动映像同步复制 (AIR)	可以将在一个 NetBackup Kubernetes 群集中生成的备份复制到一个或多个目标 NetBackup 域中的存储。这也称为 AIR。能够将备份复制到其他 NetBackup 域中的存储。 所有日程表类型都支持自动映像同步复制 (A.I.R.)。
保护有状态应用程序	使用永久卷维护其状态的 Kubernetes 应用程序可以受到保护。对于支持以下功能的容器存储接口 (CSI) 提供程序，备份和还原模式文件系统和/或块的永久卷声明 (PVC)： ■ PVC 快照功能 ■ 基于网络文件系统 (NFS) 或其他非块存储的 PVC 卷置备 ■ NetBackup 10.3 及更高版本支持备份和还原包含混合卷（VolumeMode：文件系统和块）的命名空间。
导入和验证	导入是一个两步操作，第一步为指定介质上的备份重新创建目录库条目。第二阶段导入完成后，将创建由这些映像备份的文件的目录库条目。 验证：NetBackup 可以通过将备份内容与 NetBackup 目录库中记录的内容进行比较来验证备份的内容。
Red Hat 平台的联邦信息处理标准 (FIPS) 支持	Red Hat 平台上的 NetBackup Kubernetes 可以支持符合 FIPS 的通信。
Kubernetes 的加速器备份支持	NetBackup 支持对 Kubernetes 工作负载执行加速器备份，从而缩短了备份时间。
支持执行恶意软件扫描	NetBackup 10.4 及更高版本支持通过 Kubernetes 工作负载扫描 Kubernetes 资产以查找恶意软件。
对 Kubernetes 工作负载的 OpenShift 虚拟化支持	NetBackup 版本 10.4.1 及更高版本为在 Kubernetes 群集上运行的一个或多个虚拟机所在的命名空间提供备份和还原支持。

2

部署和配置 NetBackup Kubernetes Operator

本章节包括下列主题：

NetBackup Kubernetes Operator 部署的前提条件

在部署 NetBackup Kubernetes Operator 之前，必须安装 Helm Chart 并为永久卷提供空间。

要安装最新的 Helm 版本，请运行以下命令：

1. `$ curl -fsSL -o get_helm.sh` https://raw.githubusercontent.com/helm

2. `$ chmod 700 get_helm.sh`
3. `$ ./get_helm.sh`

注意： 必须在要部署 NetBackup 的每个群集中部署 Operator。

安装新的 Helm Chart

1 要列出命名空间中的所有 Helm Chart，请运行以下命令：

```
- helm list -n <namespace>
```

2 要卸载较旧的插件，请运行以下命令：

- helm uninstall `<plugin-name> -n <namespace>`

3 要安装新插件，请运行以下命令：

- helm install `<plugin-name> <chart-path> -n <namespace>`

下面是 Helm Chart 和树结构布局：

```
netbackupkops-helm-chart/
├── charts
├── Chart.yaml
├── templates
│   ├── deployment.yaml
│   └── _helpers.tpl
└── values.yaml
```

目录结构：

```
tar --list -f netbackupkops-10.3.tar.gz
veritas_license.txt
netbackupkops.tar
netbackupkops-helm-chart/
netbackupkops-helm-chart/Chart.yaml
netbackupkops-helm-chart/values.yaml
netbackupkops-helm-chart/.helmignore
netbackupkops-helm-chart/templates/
netbackupkops-helm-chart/templates/deployment.yaml
netbackupkops-helm-chart/templates/_helpers.tpl
netbackupkops-helm-chart/charts/
```

在 NetBackup Kubernetes Operator 上部署服务软件包

配置 Helm Chart

可使用 Helm Chart 部署 NetBackup Kubernetes Operator。

必须升级 Helm Chart 才能升级 NetBackup Kubernetes Operator。

注意：安装新插件之前，必须卸载较旧的插件。

要部署 NetBackup Kubernetes Operator，请执行以下操作：

1 从 Cohesity 技术支持网站下载 tar 软件包：
https://www.veritas.com/content/support

2 将软件包提取到主目录。`netbackupkops-helm-chart` 文件夹应在主目录中。

3 要列出所有群集上下文，请运行以下命令：`kubectl config get-contexts`

4 要切换到要部署 Operator 服务的群集，请运行以下命令：

```
kubectl config use-context <cluster-context-name>
```

5 要将当前目录更改为主目录，请运行以下命令：`cd ~`

6 NetBackup 支持符合 OCI 标准的任何容器映像存储库。可以使用任何工具推送 Operator 和数据移动器映像。

如果使用专用 Docker 注册表，请按照此步骤中的说明在 NetBackup 命名空间中创建密钥 `nb-docker-cred`。否则，请跳至下一步。

- 要登录到专用 Docker 注册表，请运行以下命令：`docker login -u <user name><repo-name>`
登录后，将创建或更新包含授权令牌的 `config.json` 文件。要查看 `config.json` 文件，请运行以下命令：`cat ~/.docker/config.json`
输出如下所示：

```
{
   "auths": {
       "https://index.docker.io/v1/": {
           "auth": "c3R...zE2"
       }
   }
}
```

- 要在 NetBackup 命名空间中创建名为 `netbackupkops-docker-cred` 的密钥，请运行以下命令：

  ```
  kubectl create secret generic netbackupkops-docker-cred \
  --from-file=.dockerconfigjson=.docker/config.json \
  --type=kubernetes.io/dockerconfigjson -n netbackup
  ```

  您可以提供任何命名空间来创建密钥。
- 要检查是否已在 NetBackup 命名空间中创建 `netbackupkops-docker-cred` 密钥，请运行以下命令：

  ```
  kubectl get secrets -n netbackup
  ```
- 要将映像加载到 Docker 缓存并将映像推送到 Docker 映像存储库，请运行以下命令：
  - 为 NetBackup Kubernetes Operator 加载 tar 文件。

    ```
    <docker load -i <nameof the tar file> ./>
    ```
  - 根据要求标记加载的 docker 映像。

    ```
    docker tag <imagename:tagof the loadedimage>
    <repo-name/image-name:tag-name>
    ```
  - 将映像推送到存储库，在部署 NetBackup Kubernetes Operator 时，Kubernetes 可以从中获取映像。

    ```
    docker push <repo-name/image-name:tag-name>
    ```

注意：在该示例中，**Docker** 用作参考。可以使用任何其他提供等效功能的 CLI 工具。

7 在文本编辑器中编辑 netbackupkops-helm-chart/values.yaml，

- 将管理器部分中映像的值替换为您的映像名称和标记 repo-name/image-name:tag-name。
- 将副本的值更改为 0。

注意：按照手动步骤配置 NetBackup Kubernetes Operator 时，将副本设置为 0。

8 需要调整元数据永久卷的大小。Kubernetes Operator 的默认永久卷大小为 10 Gi。永久卷大小是可配置的。

在部署插件之前，可将存储的值从 10 Gi 更改为较大的值。这会导致 nbukops pod 具有在 pod 中装入的 PVC 的大小。

您可以在 values.yaml 中指定元数据永久卷大小。

helm-chart 下 deployment.yaml 中的永久卷声明如下所示：

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  labels:
    component: netbackup
  name: {{ .Release.Namespace }}-netbackupkops
  namespace: {{ .Release.Namespace }}
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 10Gi
```

- 在配置 Helm Chart 时的全新安装过程中。可以在 netbackupkops-helm-chart 的 deployment.yaml 中修改 PVC 存储的大小，这将导致创建初始 PVC 大小。
- 在安装后，少数存储供应商支持更新 PVC 大小（动态卷扩展）。有关更多信息，请参考 https://kubernetes.io/docs/concepts/storage/persistent-volumes

注意：可将永久卷的默认大小调整为更大的值，而不会丢失数据。建议添加支持卷扩展的存储提供商。

9 要部署 NetBackup Kubernetes Operator 服务，请运行以下命令：

```
helm install <release name of the deployment>
./netbackupkops-helm-chart -n <namespace which runs NetBackup
operator service>
```

示例： `helm install veritas-netbackupkops ./netbackupkops-helm-chart -n netbackup`

- 可根据需要更改部署的发布名称。
- 指定要运行 NetBackup Operator 服务和 NetBackup 的命名空间时，需要 `-n` 选项。

10 要检查部署的状态，请运行以下命令：

```
helm list -n <namespace which runs NetBackup operator service >
```

示例：

```
helm list -n netbackup
```

11 要检查版本历史记录，请运行以下命令：

```
helm history veritas-netbackupkops -n
```

<namespace which runs NetBackup operator service>。

示例：

```
helm history veritas-netbackupkops -n netbackup
```

Kubernetes Operator 部署的端口要求

下表显示 Kubernetes Operator 部署的端口要求。如果各个主机之间存在防火墙，则必须打开所需的通信端口。

表 2-1 必须在 NetBackup Kubernetes 群集环境中打开的端口

源	端口号	目标
主服务器	TCP 端口 443	Kubernetes 群集
介质服务器	TCP 端口 443（NetBackup 10.0 中的新增内容）。	Kubernetes 群集

注意：查看 Kubernetes 配置以确保 Kubernetes API 服务器端口未从 443 更改为非默认端口；通常为 6443 或 8443。

Kubernetes 群集	TCP 端口 443（适用于 NetBackup 版本 9.1，但不适用于版本 10.0 或更高版本）。	主服务器

注意：NetBackup Kubernetes Operator (KOps) 和 datamover pod 具有其他要求（NetBackup 10.0 中的新增内容）。

Kubernetes 群集	TCP 端口 1556 出站	主服务器
Kubernetes 群集	TCP 端口 1556 出站	介质服务器
Kubernetes 群集	TCP 端口 13724 双向（如果使用弹性网络）。	主服务器和介质服务器

升级 NetBackup Kubernetes Operator

可使用 Helm 命令升级 NetBackup Kubernetes Operator 部署。

示例：

```
helm upgrade veritas-netbackupkops ./netbackupkops-helm-chart -n
netbackup
```

为发生更改的备份 configmap 值添加备注。升级会将 Helm 值重置为默认值。升级后，必须重新修补旧的 configmap。

重要说明

- 所有组件（NBU 主服务器、介质服务器、Kubernetes Operator 和数据移动器）都必须是相同的版本。
- 现有策略继续执行备份，但必须手动还原，直到更新了 Kubernetes Operator。

注意：适用于 NetBackup 从版本 9.1 升级到 10.x 的情况

升级 NetBackup Kubernetes Operator

1. 从 Cohesity 技术支持网站下载 tar 软件包：https://www.veritas.com/support
2. 将软件包提取到主目录。`netbackupkops-helm-chart` 文件夹必须位于主目录中。
3. 要列出所有群集上下文，请运行以下命令： `kubectl config get-contexts`
4. 要切换到要部署 Operator 服务的群集，请运行以下命令：`kubectl config use-context <cluster-context-name>`
5. 要将当前目录更改为主目录，请运行以下命令：`cd ~`
6. NetBackup 支持符合 OCI 标准的任何容器映像存储库。可以使用任何工具推送 Operator 和数据移动器映像。如果使用专用 Docker 注册表，请按照此步骤中的说明在 NetBackup 命名空间中创建密钥 `nb-docker-cred`。否则，请跳至下一步。
   - 要将映像加载到 Docker 缓存并将映像推送到 Docker 映像存储库，请运行以下命令：
     - 为 NetBackup Kubernetes Operator 加载 tar 文件。
       `<docker load -i <nameof the tar file> ./>`
     - 根据要求标记加载的 docker 映像。
       `docker tag <imagename:tagof the loadedimage>`
       `<repo-name/image-name:tag-name>`

- 将映像推送到存储库，在部署 NetBackup Kubernetes Operator 时，Kubernetes 可以从中获取映像。

  ```
  docker push <repo-name/image-name:tag-name>
  ```

注意：在该示例中，docker 用作参考。可以使用任何其他提供等效功能的 CLI 工具。

7 在文本编辑器中编辑 `netbackupkops-helm-chart/values.yaml`：

- 将管理器部分中的映像值替换为您的映像名称和标记，并采用格式 `reponame/image-name:tag-name`。
- 将 `netbackup_config_pod` 部分中的 datamover 映像替换为 datamover 映像名称和标记。

8 要升级 NetBackup Kubernetes Operator，请运行以下命令：

```
helm upgrade <plugin-name> <chart-path> -n <namespace>
```

示例：

```
helm upgrade veritas-netbackupkops ./netbackupkops-helm-chart -n
netbackup
```

注意：升级 NetBackup Kubernetes Operator 会将 Helm 值重置为其默认值。如果这些值在升级后发生更改，请确保备份旧的 configmap 并重新应用任何修补程序。

删除 NetBackup Kubernetes Operator

您可以从群集中删除 NetBackup Kubernetes Operator 部署。

```
helm uninstall <plugin-name> -n <Netbackup Kubernetes Operator
Namespace>
```

注意：卸载该插件后，NetBackup Kubernetes Operator PVC 也会被删除，其中包含与基于快照的备份相关的元数据。

删除 NetBackup Kubernetes Operator 可能会导致元数据卷丢失，该卷还承载快照元数据。如果已执行任何快照，则在没有元数据的情况下，从快照副本还原操作将失败。

在 NetBackup 9.1 中，必须先手动删除较旧的快照，然后再删除关联的 Velero 快照。

在 NetBackup 10.0 中，无法使 Velero 管理的快照失效，这些快照是使用 NetBackup 9.1 创建的。当备份映像在 NetBackup 中失效时，将自动清除目录库。但是，必须手动删除 Kubernetes 服务器上的快照。

有关手动使映像失效操作的更多详细信息，请参见 https://www.veritas.com/content/support。

注意：如果不使快照失效或不删除永久卷快照，则卸载 Kubernetes Operator 后，孤立卷快照将位于 Kubernetes 群集周围。

配置 NetBackup Kubernetes 数据移动器

需要为 NetBackup Kubernetes 工作负载配置数据移动器。下载正确的数据移动器映像版本：

需要配置 NetBackup Kubernetes Operator 命名空间以支持从快照备份和从备份还原。（备份副本）。从下载中心为您的发行版本下载正确版本的数据移动器映像：`veritasnetbackup-datamover-11.0.tar`。请参见 https://www.veritas.com/content/support

配置数据移动器

1. 要将数据移动器映像推送到映像注册表，请运行以下命令：

   ```
   docker login -u <user name> <repo-name>
   ```

2. 根据提示输入密码。如果已登录，请跳过此步骤
3. 运行 `docker load -i <name of the datamover image file>`
4. 运行 `docker tag <datamover image name:tag of the loaded datamover image> <repo-name/image-name:tag-name>`

5 `docker push <repo-name/image-name:tag-name>`

注意：在该示例中，docker 用作参考。可以使用具有等效功能的任何 CLI 工具。

6 确保具有主服务器名称的 configmap 将映像值设置为在第 4 步中推送的 *<repo-name/image-name:tag-name>*。

示例

```
apiVersion: v1
data:
  datamover.properties: image=<image-repo>/datamover:<datamover
tag>
  version: "1"
kind: ConfigMap
metadata:
  name: <Primary Server Name>
  namespace: <Netbackup Kubernetes Operator Namespace Name>
```

有关 Configmap 的更多详细信息，请参考《NetBackup for Kubernetes 管理指南》中的“受 Kubernetes Operator 支持的配置参数”部分。

自动为 Kubernetes 配置 NetBackup 保护

前提条件

在 Kubernetes 工作负载上配置 NetBackup 之前，必须运行对端口 443、1556 和 13724 具有访问权限的 NetBackup 服务器。

必须将 NetBackup Kubernetes Operator 和数据移动器映像上传到可从 Kubernetes 群集访问的容器注册表。

需要创建用于自动部署的密钥。

创建 API 密钥

1 打开 NetBackup Web UI。

2 在左侧，单击“**安全**”>“**访问密钥**”。

3 单击“**API 密钥**”选项卡。

4 单击“**添加**”。

5 在 Kubernetes 群集上，创建包含以下内容的新密钥 **nb-config-deploy-secret.yaml**。

```
apiVersion: v1
kind: Secret
metadata:
  name: <kops-namespace>-nb-config-deploy-secret
  namespace: <kops-namespace>
type: Opaque
stringData:
  apikey: <Enter the value of API key from the earlier step>
```

6 应用密钥。运行命令 `kubectl apply -f nb-config-deploy-secret.yaml`。

安装前

1 在 `netbackupkops-helm-chart/values.yaml` 中编辑以下字段。

- containers.manager.image：用于提取 NetBackup Kubernetes 控制器映像的容器注册表 URL。
- imagePullSecrets name：如果容器注册表需要身份验证才能提取映像，则该字段是映像提取密钥的名称。
- nbprimaryserver：已配置的 NetBackup 主服务器名称。
- nbsha256fingerprint：从 NetBackup Web UI 获取 SHA256 指纹。在左侧，单击“**安全**”>“**证书**”。单击“**证书颁发机构**”。
- k8sCluster：Kubernetes 群集 API 服务器的 FQDN。
- k8sPort：列出 Kubernetes API 服务器的端口。
- datamoverProperties（可选）：包括需要在 datamover pod 的 `bp.conf` 文件中指定的任何配置设置。

> **注意**：有关更多信息，请参见第 28 页的“对具有短名称的 NetBackup 服务器进行故障排除”。

Kubernetes 群集的 UI 控制台上提供了这些信息。

2 如果不存在，请运行以下命令以获取 Kubernetes 群集和 Kubernetes 端口：

`# kubectl cluster-info` Kubernetes 控制面板在 https://<Kubernetes FQDN>:6443 运行

- datamoverimage：用于提取数据移动器映像的容器注册表 URL。

- 快照和从快照备份操作需要存储参数。需要提供至少一个块或文件系统存储参数。

3 要获取存储类，请运行以下命令：

```
# kubectl get storageclasses
```

- storageclassblock：用于置备块卷的存储类。
- storageclassfilesystem：用于置备文件系统卷的存储类。

4 要获取卷快照类，请运行以下命令：

```
# kubectl get volumesnapshotclasses
```

- volumesnapshotclassblock：用于创建块卷快照的卷快照类。
- volumesnapshotclassfilesystem：用于创建文件系统卷快照的卷快照类。

5 存储类和快照类之间的映射通过 storageMap 进行管理。如果向群集添加了新的存储选项，也可以安装后在 backup-operator-configuration 的 configmap 中更新该选项。

- storageMap 是一个键-值字段字典，其中键是存储类，值是一个元组，由 snapshotClass、storageClassForBackupDataMovement、storageClassForRestoreFromBackup 组成。此字段是指定存储类和快照类之间映射的必填字段。
- snapshotclass 必须使用与存储类相同的置备程序创建，并且必须能够为存储类创建快照。所有存储类都应具有相应的 snapshotclass 条目。
- storageClassForBackupDataMovement 用于为 datamover 创建临时 PVC。它必须与使用原始存储类快照创建的原始存储类 PVC 兼容，使用此存储类创建时必须可读。Datamover 从此 PVC 读取数据，并将其发送到 NetBackup 介质服务器。storageClassForRestoreFromBackup 用于从介质服务器备份进行还原。它必须与原始存储类兼容，且来自同一置备程序。
- 一个快照类可用于为多个兼容的存储类创建快照。
- 模板

```
storageMap:
  <key - storage class name>:
    snapshotClass: [mandatory field to specify
volumesnapshotclass for creating snapshot of given key storage
 class]
    storageClassForBackupDataMovement: <optional, storage class
 used to transfer pvc backup data from k8s cluster to
NetBacup media server>
    storageClassForRestoreFromBackup: <optional, storage class
 used to restore pvc from NetBackup media server
```

```
to k8s cluster>

Note: storageClassForBackupDataMovement and
storageClassForRestoreFromBackup are optional and must be
compatible
with key storage class if they are configured different from
key storage class. If no value is specified for these
fields original
storage class would be used. These values can be changed later
 in backup-operator-configuration configmap

Example for openshift storage classes. cephfs storage class
should have corresponding snapclass as cephfs as follows
storageMap:
  ocs-storagecluster-cephfs:
    storageClassForBackupDataMovement:
ocs-storagecluster-cephfs
   storageClassForRestoreFromBackup: ocs-storagecluster-cephfs

    snapshotClass: ocs-storagecluster-cephfsplugin-snapclass
  ocs-storagecluster-ceph-rbd:
    snapshotClass: ocs-storagecluster-rbdplugin-snapclass
```

安装

要安装 helm，请运行以下命令：

```
# helm install veritas-netbackupkops <path to
netbackupkops-helm-chart> -n <kops namespace>
```

调试

要从 Kubernetes Operator 命名空间获取 config-deploy pod，请运行以下命令：

```
# kubectl get pod -n <kops namespace> | grep "config-deploy"
```

日志

要检查 pod <namespace>-netbackup-config-deploy 的日志，请运行以下命令：

```
# kubectl logs <pod-name> -n <kops namespace>
```

日志级别

用于设置配置 pod 的日志级别。可以将值设置为 DEBUG、INFO 或 ERROR。默认值设置为 INFO。

注意：有关更多详细信息，请参考《NetBackup Kubernetes 快速入门指南》。

自定义 Kubernetes 工作负载

要获取配置值，请运行以下命令：

`kubectl get configmaps <namespace>-backup-operator-configuration -n <namespace> -o yaml > {local.file}`。

要编辑配置，请运行以下命令：

`kubectl edit cm<backup-operator-configmap> -n <kops-namespace>`。

设置 `VirtualMachine=false` 可禁用资产自动发现。

注意：NetBackup 支持仅编辑“**资源**”部分下的 `VirtualMachine` 参数。

从快照备份和从备份还原操作的前提条件

1. 确认添加到 storageMap 的存储类的卷绑定模式设置为“立即”。如果 PVC 卷绑定模式为 WaitForFirstConsumer，则会影响从 PVC 创建快照。这种情况可能会导致备份作业失败。

   示例：运行命令：`# kubectl get sc`

2. 运行从快照备份和从备份副本还原操作的每个主服务器都需要使用主服务器的名称创建单独的 *ConfigMap*。

   在以下 `configmap.yaml` 示例中：

   - `backupserver.sample.domain.com` 和 `mediaserver.sample.domain.com` 是 NetBackup 主服务器和介质服务器的主机名。
   - `10.20.12.13` 和 `10.21.12.13` 这两个 IP 是 NetBackup 主服务器和介质服务器的 IP 地址。

```
apiVersion: v1
data:
  datamover.hostaliases: |
        10.20.12.13=backupserver.sample.domain.com
        10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
        image=reg.domain.com/datamover/image:latest
  version: "1"
kind: ConfigMap
metadata:
```

```
name: backupserver.sample.domain.com
namespace: kops-ns
```

- 复制 configmap.yaml 文件详细信息。
- 打开文本编辑器并粘贴 yaml 文件详细信息。
- 使用 yaml 文件扩展名将文件保存到可访问 Kubernetes 群集的主目录。

3. 使用正确的数据移动器映像指定 datamover.properties: image=reg.domain.com/datamover/image:latest。
4. 如果主服务器和连接到主服务器的介质服务器具有短名称，并且从数据移动器进行主机解析失败，请指定 datamover.hostaliases。为主服务器和介质服务器提供所有主机名到 IP 的映射。
5. 按照“在 NetBackup Kubernetes Operator 上部署服务软件包”部分第 6 点中的详细说明创建密钥，以使用专用 docker 注册表。

   创建密钥后，在创建 configmap.yaml 文件时添加以下属性。

   ```
   datamover.properties: |
   image=repo.azurecr.io/netbackup/datamover:10.0.0049
   imagePullSecret=secret_name
   ```

6. 创建 configmap.yaml 文件。运行命令：kubectl create -f configmap.yaml。
7. 如果 Kubernetes Operator 无法使用短名称解析主服务器，请参考以下准则。
   - 如果获取证书时收到以下消息：*EXIT STATUS 8500: Connection with the web service was not established*。那么，从 nbcert 日志中，验证主机名解析状态。
   - 如果主机名解析失败，则更新 values.yaml 文件，在其中添加 hostAliases。
   - 在以下 hostAliases 示例中：
     - backupserver.sample.domain.com 和 mediaserver.sample.domain.com 是 NetBackup 主服务器和介质服务器的主机名。
     - 10.20.12.13 和 10.21.12.13 这两个 IP 是 NetBackup 主服务器和介质服务器的 IP 地址。

   ```
   hostAliases:
   - hostnames:
     - backupserver.sample.domain.com
     ip: 10.20.12.13
   - hostnames:
   ```

```
  -  mediaserver.sample.domain.com
  ip: 10.21.12.13
```

在文本编辑器中复制并粘贴 hostAliases 示例详细信息，并将其添加到部署中的 hostAliases。

注意： hostAliases 部分必须添加到默认文件 ./netbackupkops-helm-chart/values.yaml 中。

hostAliases 示例：

```
2104 hostAliases;
- ip:10.15.206.7
hostnames:
- lab02-linsvr-01.demo.sample.domain.com
- lab02-linsvr-01
- ip:10.15.206.8
hostnames:
- lab02-linsvr-02.demo.sample.domain.com
- lab02-linsvr-02
imagePullSecrets:
- name:  {{ .values.netbackupKops.imagePullSecrets.name}}
```

8. 要更新 nbcertcmdtool 的 TLS 相关配置，请使用所需设置更新 deployment.yaml 文件中名称为 {{ .Release.Namespace }}-certconfigscript 的 configmap。

   例如：

```
To set TLS_MAX_VERSION,
apiVersion: v1
data:
  nbcert.sh: |
    #!/bin/sh
    mkdir -p /usr/openv/kops
    mkdir -p /usr/openv/fingerprint-dir
    mkdir -p /usr/openv/tmp
    mkdir -p /usr/openv/netbackup/logs/nbcert
    mkdir -p /usr/openv/netbackup/logs/nbcert/nobody
    mkdir -p /usr/openv/var/global
    mkdir -p /usr/openv/var/vxss
    cp -r /nbcertcmdtool /usr/openv/nbcertcmdtool
    touch /usr/openv/var/global/nbcl.conf
    touch /usr/openv/netbackup/bp.conf
```

```
    chown -R nobody:nobody /usr/openv
    echo "CLIENT_KEEP_LOG_DAYS = 90" >>
/usr/openv/netbackup/bp.conf
    echo "SERVICE_USER=nobody" >> /usr/openv/netbackup/bp.conf
    echo "MACHINE_NBU_TYPE = KUBERNETES_CLUSTER" >>
/usr/openv/netbackup/bp.conf
    echo "TLS_MAX_VERSION = TLSv1.3" >>
/usr/openv/netbackup/bp.conf
kind: ConfigMap
metadata:
  labels:
    component: netbackup
  name: {{ .Release.Namespace }}-certconfigscript
  namespace: {{ .Release.Namespace }}
```

9. 使用指纹和授权令牌创建密钥。

   有关创建密钥和 backupservercert 的更多信息，请参考《NetBackup for Kubernetes 管理指南》中的“在 NetBackup Kubernetes Operator 上部署证书”部分。

10. 创建 backupservercert 请求以获取证书。

    有关更多信息，请参考《NetBackup for Kubernetes 管理指南》中的“在 NetBackup Kubernetes Operator 上部署证书”。

    有关更多信息，请参考《NetBackup 安全和加密指南》。

注意：要成功执行从快照备份和从备份副本还原，这是必需步骤。

Kubernetes 中支持的 DTE 客户端设置

DTE_CLIENT_MODE 选项指定通过备份服务器特定的 configmap 在 datamover 上设置的传输中数据加密 (DTE) 模式。备份映像的传输中数据加密基于全局 DTE 模式和客户端 DTE 模式执行。

更新备份服务器特定的 configmap，并在其中添加 DTE_CLIENT_MODE 密钥。此密钥可以采用以下值：

- AUTOMATIC
- ON
- OFF

有关 DTE_CLIENT_MODE 的更多信息，请参考《NetBackup 管理指南，第 I 卷》中的“客户端的 DTE_CLIENT_MODE”部分。

以下是添加了 DTE_CLIENT_MODE 设置的 configmap：

```
apiVersion: v1
data:
  datamover.hostaliases: |
        10.20.12.13=backupserver.sample.domain.com
        10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
        image=reg.domain.com/datamover/image:latest
        DTE_CLIENT_MODE=ON
  version: "1"
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
  namespace: kops-ns
```

自定义 datamover 属性

可以通过在备份服务器特定的 configmap 中传递密钥值对来自定义 datamover 属性。

表 2-2 Datamover 属性

密钥名称	可能的值
VXMS_VERBOSE	范围：[0,99]
VERBOSE	范围：[0,5]
DTE_CLIENT_MODE	■ AUTOMATIC ■ ON ■ OFF
USE_CTIME_FOR_INCREMENTALS	YES/NO
USE_CTIME_FOR_DIRECTORY_INCRS	YES/NO
DO_NOT_RESET_FILE_ACCESS_TIME	YES/NO

注意：对于 NetBackup 客户端支持的任何其他配置设置，可以通过在 datamover configmap 中的 *datamover.properties* 键下添加这些配置设置，为 datamover 进行设置。这些配置将添加到 datamover 内的 `bp.conf` 文件中。

要更新 configmap，请添加键值对，如下所示：

```
apiVersion: v1
data:
  datamover.properties: |
        image=reg.domain.com/datamover/image:latest
        VERBOSE=5
        DTE_CLIENT_MODE=OFF
        VXMS_VERBOSE=5
  version: "1"
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
  namespace: kops-ns
```

从 NetBackup 10.5 开始，支持 TLS 1.3 协议。默认情况下，NetBackup 10.5 及更高版本在安全通信工作流程中使用 TLS 1.3 协议，如下所示：

- 安全代理
- 传输中数据加密 (DTE)
- 外部 KMS 服务器
- AD/LDAP 服务器
- MSDP
- 使用 cURL 进行 HTTPS 通信

要配置 TLS 相关的属性，可以在此 configmap 中更新所需的设置。有关 TLS 设置的更多详细信息，请参考此文章。

对具有短名称的 NetBackup 服务器进行故障排除

1 如果 NetBackup Kubernetes Operator 无法根据短名称解析备份服务器或介质服务器，请执行以下步骤：

- 获取证书时，如果收到消息：*退出状态 8500: 未建立与 Web 服务的连接*。然后，从 nbcert 日志中，确认主机名解析是否成功。如果解析失败，则执行以下步骤：
- 更新 Kubernetes Operator `deployment.yaml`，并在部署中添加 `hostAliases`。
- 在以下 `hostAliases` 示例中，
  - backupserver.sample.domain.com 和 mediaserver.sample.domain.com 是 NetBackup 主服务器和介质服务器的主机名。

- 10.20.12.13 和 10.21.12.13 这两个 IP 是 NetBackup 主服务器和介质服务器的 IP 地址。

```
hostAliases:
- hostnames:
  - backupserver.sample.domain.com
  ip: 10.20.12.13
- hostnames:
  -  mediaserver.sample.domain.com
  ip: 10.21.12.13
```

在文本编辑器中复制并粘贴 hostAliases 示例详细信息，并将其添加到部署中的 hostAliases。

2 如果数据移动器无法解析备份服务器或介质服务器的短名称。要解决该问题，请执行以下步骤：

- 使用备份服务器名称更新 configmap。
- 添加 *datamover.hostaliases* 字段，将 IP 地址映射到主机名。
- 在以下 `configmap.yaml` 示例中，
  - backupserver.sample.domain.com 和 mediaserver.sample.domain.com 是 NetBackup 主服务器和介质服务器的主机名。
  - 10.20.12.13 和 10.21.12.13 这两个 IP 是 NetBackup 主服务器和介质服务器的 IP 地址。

```
apiVersion: v1

data:
  datamover.hostaliases: |
        10.20.12.13=backupserver.sample.domain.com
        10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
        image=reg.domain.com/datamover/image:latest
  version: "1"
kind: configmap
metadata:
  name: backupserver.sample.domain.com
  namespace: kops-ns
```

- 复制 `configmap.yaml` 文件详细信息。
- 打开文本编辑器并粘贴 yaml 文件详细信息。
- 然后，使用 yaml 文件扩展名将其保存到可访问 Kubernetes 群集的主目录。

- 要创建 `configmap.yaml` 文件，请运行 `kubectl create -f configmap.yaml` 命令。
- 如果更新已创建的 `configmap.yaml`，则运行该命令以更新 configmap。`kubectl apply -f configmap.yaml`

datamover pod 调度机制支持

在 NetBackup 中，用户可以通过使用备份服务器特定的 ConfigMap 将网络挂接定义应用于 datamover pod，为 datamover pod 添加注释，以允许使用其他网络。

在全新安装期间使用网络挂接定义 (NAD) 为 datamover pod 添加注释

在 NetBackup Kubernetes Operator Helm 安装期间，用户可以在 `netbackupkops-helm-chart/values.yaml` 文件中指定注释，这些注释将应用于 NetBackup Kubernetes Operator 部署和 datamover pod。这是可选参数。

安装后使用网络挂接定义 (NAD) 为 datamover pod 添加注释

用户可以通过编辑备份服务器特定的 ConfigMap 来添加注释或修改现有注释。

例如

```
# kubectl get cm -n <kops-namespace>

# kubectl edit cm/<backup-server-name> -n <kops-namespace>

datamover.annotations: |

k8s.v1.cni.cncf.io/networks: whereabouts-ipvlan-conf-1
```

限制

当 datamover pod 使用专用网络时，pod 内的 hostalias 不适用于多个专用网络。如果第一个接口发生故障，连接不会回退到第二个专用备份网络。

建议使用两个接口创建一个网桥，并在此网桥上配置 multus，而不是将两个单独的专用网络接口插入 datamover。

在备份服务器 ConfigMap 中指定以下字段，以在节点上调度 datamover pod。

1. **nodeSelector**：nodeSelector 可以轻松将 pod 约束到具有特定标签的节点。

   示例：

   ```
   apiVersion: v1

   kind: ConfigMap
   ```

```
metadata:
  name: backupserver.sample.domain.com
  namespace: netbackup
data:
  datamover.hostaliases: |
    10.20.12.13=backupserver.sample.domain.com
    10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
    image=reg.domain.com/datamover/image:latest
  datamover.nodeSelector: |
    kubernetes.io/hostname: test1-l94jm-worker-k49vj
    topology.rook.io/rack: rack1
  version: "1"
```

2. **nodeName**：nodeName 是一种直接的节点选择形式，而不是亲和性或 nodeSelector。它允许您指定一个节点，在该节点上调度 pod 进行备份，从而覆盖默认调度机制。

   示例：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
  namespace: netbackup
data:
```

```
  datamover.hostaliases: |
    10.20.12.13=backupserver.sample.domain.com
    10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
    image=reg.domain.com/datamover/image:latest
  datamover.nodeName : test1-l94jm-worker-hbblk
  version: "1"
```

3. **Taint** 和 **Toleration**：Toleration 允许您调度具有类似 Taint 的 pod。Taint 和 Toleration 协同工作，确保将 pod 调度到适当节点上。如果将一个或多个 Taint 应用于节点，则该节点不得接受不能容忍这些 Taint 的任何 pod。

   示例：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
  namespace: netbackup
data:
  datamover.hostaliases: |
    10.20.12.13=backupserver.sample.domain.com
    10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
    image=reg.domain.com/datamover/image:latest
  datamover.tolerations: |
```

```
    - key: "dedicated"
      operator: "Equal"
      value: "experimental"
      effect: "NoSchedule"
  version: "1"
```

4. **亲和性与反亲和性**：节点亲和性功能类似于 nodeSelector 字段，但它更具表现力，并允许您指定软规则。pod 之间的亲和性/反亲和性允许您根据其他 pod 上的标签约束 pod。

   示例：

   - **节点亲和性**：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
  namespace: netbackup
data:
  datamover.hostaliases: |
    10.20.12.13=backupserver.sample.domain.com
    10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
    image=reg.domain.com/datamover/image:latest
  datamover.affinity: |
    nodeAffinity:
```

```
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
        - matchExpressions:
          - key: kubernetes.io/hostname
            operator: In
            values:
            - test1-l94jm-worker-hbblk
      preferredDuringSchedulingIgnoredDuringExecution:
      - weight: 1
        preference:
          matchExpressions:
          - key: beta.kubernetes.io/arch
            operator: In
            values:
            - amd64
  version: "1"
```

- **Pod 亲和性**

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
```

```
    namespace: netbackup
  data:
    datamover.hostaliases: |
      10.20.12.13=backupserver.sample.domain.com
      10.21.12.13=mediaserver.sample.domain.com
    datamover.properties: |
      image=reg.domain.com/datamover/image:latest
    datamover.affinity: |
      podAffinity:
        requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchExpressions:
            - key: component
              operator: In
              values:
              - netbackup
          topologyKey: kubernetes.io/hostname
    version: "1"
```

5. **topologySpreadConstraints**：拓扑分布约束用于控制跨故障域（如地区、区域、节点和用户定义的其他拓扑域）分布在群集中的 pod 的行为。

   示例：

```
apiVersion: v1
kind: ConfigMap
```

```
metadata:
  name: backupserver.sample.domain.com
  namespace: netbackup
data:
  datamover. hostaliases: |
    10.20.12.13=backupserver.sample.domain.com
    10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
    image=reg.domain.com/datamover/image:latest
  datamover.topologySpreadConstraints : |
    - maxSkew: 1
      topologyKey: kubernetes.io/hostname
      whenUnsatisfiable: DoNotSchedule
  version: "1"
```

- **标签**：标签是附加到对象（如 pod）的键/值对。标签用于标识与用户相关的重要对象的属性。通过标签可以组织和选择对象的子集。标签可以在创建时附加到对象，随后可以随时进行添加和修改。
  示例：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
  namespace: netbackup
```

```
data:
  datamover.hostaliases: |
    10.20.12.13=backupserver.sample.domain.com
    10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
    image=reg.domain.com/datamover/image:latest
  datamover.labels: |
    env: test
    pod: datamover
  version: "1"
```

- **注释**：用户可以使用标签或注释将元数据附加到 Kubernetes 对象。不能使用注释标识和选择对象。
  示例：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
  namespace: netbackup
data:
  datamover.hostaliases: |
    10.20.12.13=backupserver.sample.domain.com
    10.21.12.13=mediaserver.sample.domain.com
  datamover.properties: |
```

```
    image=reg.domain.com/datamover/image:latest
  datamover.annotations: |
    buildinfo: |-
      [{
            "name": "test",
            "build": "1"
      }]
    imageregistry: "https://reg.domain.com/"
  version: "1"
```

验证加速器存储类

NetBackup 支持已启用加速器的备份，可以通过在安装或升级期间使用适当的存储类在 values.yaml 中设置 *acceleratorTracklogPvcStorageClass* 键来启用此备份。

存储类必须允许创建文件模式 PVC。

例如 *acceleratorTracklogPvcStorageClass: ocs-storagecluster-ceph-rbd*

在安装和升级期间，NetBackup Kubernetes Operator 将创建文件模式 PVC 和 Pod，以检查给定的存储类是否有效。

- 如果存储类的卷绑定模式为“**立即**”，则仅当 PVC 处于“绑定”状态时，NetBackup Kubernetes Operator 才会创建 PVC 且安装成功。
- 如果存储类的卷绑定模式为 **WaitForFirstConsumer**，则会创建 datamover pod 以及 PVC。
- 如果 PVC 处于“绑定”状态且 Pod 处于“正在运行”状态，则 NetBackup Kubernetes Operator 安装成功。

3

在 NetBackup Kubernetes Operator 上部署证书

本章节包括下列主题：

在 Kubernetes Operator 上部署证书

需要部署证书才能在 datamover 和 NetBackup 介质服务器之间进行安全通信。

注意：必须先部署证书，然后才能执行“**从快照备份**”和“**从备份还原**”操作。

在创建 BackupServerCert 之前，必须先成功添加和发现群集，因为它依靠 NetBackup 传递某些 `clusterInfo` 以将状态设置为“成功”。

支持 datamover 通信的证书

datamover 促进了 NetBackup 环境中的数据移动，它通过传输层安全性 (TLS) 与介质服务器进行通信。有关更多详细信息，请参考《NetBackup™ 安全和加密指南》中的“关于 NetBackup 中的安全通信”部分。datamover 需要基于主机 ID 的证书或由 NetBackup 主服务器颁发的 ECA 签名证书，才能进行通信。引入了新的自定义资源定义 BackupServerCert，可在 NBCA（NetBackup 证书颁发机构）或 ECA（外部证书颁发机构）模式下启用证书部署操作。

自定义资源规范如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  name: backupservercert-sample-nbca
  namespace: kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: primary.server.sample.com
  certificateOperation: Create | Update | Remove
  certificateType: NBCA | ECA
  nbcaAttributes:
    nbcaCreateOptions:
      secretName: "Secret name consists of token and fingerprint"
    nbcaUpdateOptions:
      secretName: "Secret name consists of token and fingerprint"
      force: true | false
    nbcaRemoveOptions:
      hostID: "hostId of the nbca certificate. You can view on Netbackup UI"
  ecaAttributes:
    ecaCreateOptions:
      ecaSecretName: "Secret name consists of cert, key, passphrase, cacert"
      copyCertsFromSecret: true | false
      isKeyEncrypted: true | false
    ecaUpdateOptions:
      ecaCrlCheck: DISABLE | LEAF | CHAIN
      ecaCrlRefreshHours: [0,4380]
```

执行基于主机 ID 的证书操作

确保在 NBCA 模式下配置主服务器。要检查 NBCA 模式是否处于打开状态，请运行以下命令：`/usr/openv/netbackup/bin/nbcertcmd -getSecConfig -caUsage`。

输出如下所示：

```
NBCA: ON
ECA: OFF
```

基于主机 ID 的证书规范如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
```

```
  name: backupservercert-sample
  namespace: kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: primaryserver.sample.domain.com
  certificateOperation: Create | Update | Remove
  certificateType: NBCA
  nbcaAttributes:
    nbcaCreateOptions:
      secretName: "Secret name consists of token and fingerprint"
    nbcaUpdateOptions:
      secretName: "Secret name consists of token and fingerprint"
      force: true
    nbcaRemoveOptions:
      hostID: "hostId of the nbca certificate. You can view on
Netbackup UI"
```

表 3-1 基于主机 ID 的证书操作

操作类型	选项和注释
创建	secretName：包含令牌和指纹的密钥的名称。
删除	hostID：NBCA 证书的主机标识。
更新	secretName：包含令牌和指纹的密钥的名称。

为 Kubernetes Operator 创建基于主机 ID 的证书

可以使用以下过程为 Kubernetes Operator 创建基于主机 ID 的证书。

为 Kubernetes Operator 创建基于主机 ID 的证书

1 在备份服务器上，运行以下命令并获取 SHA-256 指纹。

```
/usr/openv/netbackup/bin/nbcertcmd -listCACertDetails
```

2 要创建授权令牌，请参考《NetBackup™ 安全和加密指南》中的“创建授权令牌”部分。

3 要创建重新发布令牌（如果需要），请参考《NetBackup™ 安全和加密指南》中的“创建重新发布令牌”部分。

4 使用令牌和指纹创建密钥。

5 提供令牌，因为无论安全级别如何，它都是必需项。

`Token-fingerprint-secret.yaml` 如下所示：

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-name
  namespace: kops-ns
type: Opaque
stringData:
  token: "Authorization token | Reissue token"
  fingerprint: "SHA256 Fingerprint"
```

- 复制 Token-fingerprint-secret.yaml 文件文本。
- 打开文本编辑器并粘贴 yaml 文件文本。
- 然后，使用 yaml 文件扩展名将文本保存到可以访问 Kubernetes 群集的主目录中。

6 要创建 Token-fingerprint-secret.yaml 文件，请运行以下命令：kubectl create -f Token-fingerprint-secret.yaml

7 使用 nbcaCreateOptions 创建

backupservercert 对象，然后指定密钥名称。

nbca-create-backupservercert.yaml 如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  name: backupserver-nbca-create
  namespace: kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: backupserver.sample.domain.com
  certificateOperation: Create
  certificateType: NBCA
  nbcaAttributes:
    nbcaCreateOptions:
      secretName: nbcaSecretName with token and fingerprint
```

- 复制 nbca-create-backupservercert.yaml 文件文本。
- 打开文本编辑器并粘贴 yaml 文件文本。
- 然后，使用 yaml 文件扩展名将文本保存到可以访问 Kubernetes 群集的主目录中。

8 要创建 nbca-create-backupservercert.yaml 文件，请运行以下命令：

```
kubectl create -f nbca-create-backupservercert.yaml
```

9 创建证书后，检查自定义资源状态。如果自定义资源状态为“成功”，则可以运行“**从快照备份**”作业。

注意：在启动“**从快照备份**”或“**从备份副本还原**”操作之前，需要检查 BackupServerCert 自定义资源状态是否为“成功”。

注意：续订基于主机 ID 的证书：NetBackup 主机 ID 证书会检查是否应在 24 小时周期后续订。证书将在截止日期前 180 天（6 个月）自动续订。

注意：确保检查 NetBackup 主服务器时钟和 NetBackup Kubernetes Operator 时钟是否同步。有关 CheckClockSkew 错误的更多详细信息，请参考《NetBackup™ 安全和加密指南》中的“时钟偏差对证书有效期的影响”部分。

从 Kubernetes Operator 删除主服务器证书

如果主服务器不用于运行备份和还原操作，则可以从该服务器删除证书。

从 Kubernetes Operator 删除主服务器证书。

1 登录到 NetBackup Web UI，并获取要删除的证书的主机 ID。

要获取证书的主机 ID，请参考《NetBackup™ 安全和加密指南》中的“查看基于主机 ID 的证书的详细信息”部分。

2 创建操作类型为“删除”的 backupservercert。

nbca-remove-backupservercert.yaml 文件如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  name: backupserver-nbca-domain.com
  namespace: kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: backupserver.sample.domain.com
  certificateOperation: Remove
  certificateType: NBCA
```

```
nbcaAttributes:
  nbcaRemoveOptions:
    hostID: nbcahostID
```

- 复制 nbca-remove-backupservercert.yaml 文件文本。
- 打开文本编辑器并粘贴 yaml 文件文本。
- 然后，使用 yaml 文件扩展名将文本保存到可以访问 Kubernetes 群集的主目录中。

3 要创建 nbca-remove-backupservercert.yaml 文件，请运行以下命令：

```
kubectl create -f nbca-remove-backupservercert.yaml
```

4 要吊销证书，请参考《NetBackup™ 安全和加密指南》中的“吊销基于主机 ID 的证书”部分。

注意：应用 nbca-remove-backupservercert.yaml 后，将从 Kubernetes Operator 的本地证书存储库中删除证书。但它在 NetBackup 数据库中仍然存在且有效。因此，需要吊销证书。

更新主服务器证书

以下是您可能希望更新证书的情形（假设证书可读并且存在于 Kubernetes Operator 中）：

吊销 NetBackup Kubernetes Operator 上存在的证书后，可以使用更新操作重新发布证书。要解决此问题，可以更新服务器证书，也可以删除服务器证书，然后创建新证书。

注意：如果更新证书操作失败，则必须先删除证书，然后创建新证书。

要更新 Kubernetes Operator 上的主服务器证书，请执行以下操作：

1 使用更新操作创建 backupservercert 对象：

nbca-update-backupservercert.yaml 文件如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  name: backupserver-nbca-update
  namespace:kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: backupserver.sample.domain.com
```

```
  certificateOperation: Update
  certificateType: NBCA
  nbcaAttributes:
    nbcaUpdateOptions:
    secretName: "Name of secret containing
token and fingerprint"
    force: true
```

- 复制 nbca-update-backupservercert.yaml 文件文本。
- 打开文本编辑器并粘贴 yaml 文件文本。
- 然后，使用 yaml 文件扩展名将文本保存到可以访问 Kubernetes 群集的主目录中。

2 要创建 nbca-udpate-backupservercert.yaml 文件，请运行以下命令：

```
kubectl create -f nbca-update-backupservercert.yaml
```

3 创建 backupservercert 对象后，检查自定义资源状态。

执行 ECA 证书操作

在执行外部证书颁发机构 (ECA) 的创建、更新和删除操作之前，必须在 ECA 模式下配置备份服务器。

要检查 ECA 模式是否处于打开状态，请运行以下命令：/usr/openv/netbackup/bin/nbcertcmd -getSecConfig -caUsage。

输出如下所示：

```
NBCA: ON
ECA: ON
```

要在 ECA 模式下配置备份服务器，请参考《NetBackup™ 安全和加密指南》中的“关于 NetBackup 中的外部 CA 支持”部分

ECA 证书规范如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  name: backupservercert-sample-eca
  namespace: kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: primaryserver.sample.domain.com
```

```
certificateOperation: Create | Update | Remove
certificateType: ECA
ecaAttributes:
  ecaCreateOptions:
    ecaSecretName: "Secret name consists of cert, key, passphrase,
cacert"
    copyCertsFromSecret: true | false
    isKeyEncrypted: true | false
  ecaUpdateOptions:
    ecaCrlCheck: DISABLE | LEAF | CHAIN
    ecaCrlRefreshHours: range[0,4380]
```

表 3-2 ECA 证书操作

操作类型	选项和注释
创建	■ secretName：包含证书、密钥、密码、cacert 的密钥的名称。 ■ copyCertsFromSecret：可能的值为 true 和 false。添加此选项的原因是，外部 CA 在所有主服务器中通用。可在 Kubernetes Operator 中注册相同证书，供所有主服务器使用。 因此，无需每次都复制证书和密钥。可以使用此选项控制证书和密钥的复制。 如果 ECAHealthCheck 由于证书和密钥有问题而失败，则必须再次复制证书。 ■ isKeyEncrypted：如果私钥已加密，请将此字段设置为 true，否则将其设置为 false。
删除	不适用
更新	■ ecaCrlCheck：可指定外部证书的吊销检查级别。 可能的值为 DISABLE、LEAF 和 CHAIN。 ■ ecaCrlRefreshHours 指定下载证书吊销列表的时间间隔（以小时为单位）。 可能的值范围在 0-4380 之间

创建 ECA 签名证书

NetBackup 支持在 Kubernetes Operator 中注册 ECA，以供多个主服务器使用。如果外部 CA 在主服务器中是通用的。在通信期间，必须使用证书吊销列表分发点动态获取证书吊销列表。

创建 ECA 签名证书

1 使用证书吊销列表分发点获取证书吊销列表。

2 在主目录中准备好 ECA 签名证书链、私钥和密码（如果需要）。

3 明确步骤 2 中提到的每个文件支持的不同格式（如 DER、PEM 等）。有关更多信息，请参考《NetBackup™ 安全和加密指南》中的“用于外部 CA 签名证书的配置选项”部分。

4 使用步骤 3 中提到的文件创建密钥。

- 要在私钥未加密的情况下创建密钥，请运行以下命令：`kubectl create secret generic <Name of secret> --from-file=cert_chain=<File path to ECA signed certificate chain> --from-file=key=<File path to private key> --from-file=cacert=<File path to External CA certificate> -n <Namespace where kops is deployed>`
- 要在私钥已加密的情况下创建密钥，请运行以下命令：`kubectl create secret generic <Name of secret> --from-file=cert_chain=<File path to ECA signed certificate chain> --from-file=key=<File path to private key> --from-file=cacert=<File path to External CA certificate> --from-file=passphrase=<File path to passphrase of encrypted private key> -n <Namespace where kops is deployed>`

目录结构如下所示：

```
├── cert_chain.pem
├── private
|   |___key.pem
|   |___passphrase.txt
|___trusted
      |__cacerts.pem
```

cert_chain.pem 是 ECA 签名证书链

private/key.pem 是私钥

private/passphrase.txt 是私钥的密码

trusted/cacerts.pem 是外部 CA 证书

- 要在私钥未加密的情况下创建名为 eca-secret 的密钥，请运行以下命令：`kubectl create secret generic eca-secret--from-file=cert_chain=cert_chain.pem --from-file=key=private/key.pem --from-file=cacert=trusted/cacerts.pem -n kops-ns`
- 要在私钥已加密的情况下创建名为 eca-secret 的密钥，请运行以下命令：`kubectl create secret generic eca-secret`

```
--from-file=cert_chain=cert_chain.pem
--from-file=key=private/key.pem
--from-file=cacert=trusted/cacerts.pem
--from- file=passphrase=private/passphrase.txt
-n kops-ns
```

5 创建密钥后，接下来创建 backupservercert 对象自定义资源。

eca-create-backupservercert.yaml 文件如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  name: backupservercert-eca-create
  namespace: kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: backupserver.sample.domain.com
  certificateOperation: Create
  certificateType: ECA
  ecaAttributes:
    ecaCreateOptions:
      ecaSecretName: eca-secret
      copyCertsFromSecret: true
      isKeyEncrypted: false
```

- 复制 eca-create-backupservercert.yaml 文件文本。
- 打开文本编辑器并粘贴 yaml 文件文本。
- 然后，使用 yaml 文件扩展名将文本保存到可以访问 Kubernetes 群集的主目录中。

6 要将证书和密钥复制到 Kubernetes Operator，请执行以下任一操作：

- 将 copyCertsFromSecret 设置为 true
- 将 copyCertsFromSecret 设置为 false，以避免复制 Kubernetes Operator 上现有的证书和密钥。

注意：ECA 在所有主服务器中是通用的，因此 Kubernetes Operator 需要一组证书和密钥，可根据需要在所有主服务器中注册这些证书和密钥。除非之前复制的证书和密钥出现问题，否则无需每次都复制证书和密钥。

注意：如果由于与证书和密钥相关的任何原因（ECA 已损坏、已失效或已更改）导致 ecaHealthCheck 失败，则可以使用标志确定失败原因并复制有效证书。

7 如果私钥已加密，则将 isKeyEncrypted 标志设置为 true，而对于未加密的密钥，则将其设置为 false。如果私钥已加密，请确保以私密方式提供密码。

8 使用在步骤 5 中创建的密钥名称 backupservercert yaml 设置 ecaSecretName。

9 要创建 eca-create-backupservercert.yaml 文件，请运行以下命令：kubectl create -f eca-create-backupservercert.yaml

10 创建 backupservercert 自定义资源后，检查自定义资源状态。

11 要在 NetBackup Web UI 上查看外部证书详细信息，请参考《NetBackup™ Web UI 管理指南》中的“查看域中 NetBackup 主机的外部证书信息”部分。

删除 ECA 签名证书

可以从主服务器删除 ECA 签名证书。

删除 ECA 签名证书

1 创建 backupservercert，其操作为“删除”，证书类型为 ECA。

eca-remove-backupservercert.yaml 文件如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  name: backupservercert-eca-remove
  namespace: kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: backupserver.sample.domain.com
  certificateOperation: Remove
  certificateType: ECA
```

- 复制 eca-remove-backupservercert.yaml 文件文本。
- 打开文本编辑器并粘贴 yaml 文件文本。

- 然后，使用 yaml 文件扩展名将文本保存到可以访问 Kubernetes 群集的主目录中。

2 要创建 `eca-remove-backupservercert.yaml` 文件，请运行以下命令：`kubectl create -f eca-remove-backupservercert.yaml`

3 创建对象后，需要检查自定义资源状态。如果失败，则可以采取必要操作。

这些步骤可从本地证书存储库中删除有关指定主服务器的外部证书详细信息。不会从系统或 NetBackup 数据库中删除证书。

如果要禁用 ECA，请参考《NetBackup™ 安全和加密指南》中的“在 NetBackup 域中禁用外部 CA”部分。

如果在 Kubernetes Operator 上为备份服务器注册了 ECA，但后来重新安装了仅支持 NBCA 的备份服务器，那么，必须从 Kubernetes Operator 中删除 ECA 注册，因为与备份服务器进行 *nbcertcmd* 通信期间，可能会对 CA 支持情况进行比较，如果不匹配，则会发生错误。

更新 ECA 签名证书

ECA 中有一些可配置的选项。可以通过更新操作配置这些选项。

更新 ECA 签名证书

1 创建操作类型为“更新”的 `backupservercert` 对象。

`eca-update-backupservercert.yaml` 文件如下所示：

```
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  name: backupservercert-eca-update
  namespace: kops-ns
spec:
  clusterName: cluster.sample.com:port
  backupServer: backupserver.sample.domain.com
  certificateOperation: Update
  certificateType: ECA
  ecaAttributes:
    ecaUpdateOptions:
      ecaCrlCheck: DISABLE | LEAF | CHAIN
      ecaCrlRefreshHours: [0,4380]
```

- 复制 `eca-update-backupservercert.yaml` 文件文本。
- 打开文本编辑器并粘贴 yaml 文件文本。

- 然后，使用 yaml 文件扩展名将文本保存到可以访问 Kubernetes 群集的主目录中。

2 要创建 `eca-update-backupservercert.yaml` 文件，请运行以下命令：`kubectl create -f eca-update-backupservercert.yaml`

3 您可以使用 ECA_CRL_CHECK 选项指定主机外部证书的吊销检查级别。还可以对外部证书禁用吊销检查。在主机通信期间，基于检查，根据证书吊销列表 (CRL) 验证证书的吊销状态。有关更多信息，请参考《NetBackup™ 安全和加密指南》中的“NetBackup 服务器和客户端的 ECA_CRL_CHECK”部分。

4 ECA_CRL_REFRESH_HOURS 选项指定从对等主机证书的证书吊销列表分发点 (CDP) 中指定的 URL 下载 CRL 的时间间隔（以小时为单位）。有关更多信息，请参考《NetBackup™ 安全和加密指南》中的“NetBackup 服务器和客户端的 ECA_CRL_REFRESH_HOURS”部分

标识证书类型

NetBackup 可帮助您标识在 Kubernetes Operator 上注册的证书类型。

标识证书类型

1 要列出 Kubernetes Operator pod，请运行以下命令： `kubectl get pods -n <namespace of Kubernetes operator>`

2 使用管理员权限登录到 Kubernetes Operator 并运行以下命令：

```
kubectl exec pod/nbu-controller-manager-7c99fb8474-hzrsl -n
<namespace of Kubernetes operator> -c netbackupkops -it -- bash
```

3 要列出具有 Kubernetes NBCA 证书的备份服务器，请运行以下命令：

```
/nbcertcmdtool/nbcertcmdtool -atLibPath/nbcertcmdtool/
-standalone -installDir "/usr/openv" -listCertDetails -NBCA
```

输出如下所示：

```
Master Server : masterserver.sample.domain.com
Host ID : b06738f0-a8c1-47bf-8d95-3b9a41b7bb0a
Issued By : /CN=broker/OU=NBCANBKOps
Serial Number : 0x508cdf4500000008
Expiry Date : Dec 22 05:46:32 2022 GMT
SHA-1 Fingerprint : 4D:7A:D9:B9:61:4E:93:29:B8:93:0B:E0:
07:0A:28:16:46:F6:39:C6
SHA-256 Fingerprint : C2:FA:AC:B5:21:6B:63:49:30:AC:4D:5E:
61:09:9A:8C:C6:40:4A:44:B6:39:7E:2B:B3:36:DE:D8:F5:D1:3D:EF
Key Strength : 2048
Subject Key Identifier : AC:C4:EF:40:7D:8D:45:B4:F1:89:DA:FB:
E7:FD:0F:FD:EC:61:12:C6
Authority Key Identifier : 01:08:CA:40:15:81:75:7B:37:9F:51:78:

B2:6A:89:A1:44:2D:82:2B
```

4 要列出具有 Kubernetes ECA 证书的备份服务器，请运行以下命令：

```
/nbcertcmdtool/nbcertcmdtool -atLibPath/nbcertcmdtool/
-standalone -installDir"/usr/openv" -listCertDetails -ECA
```

输出如下所示：

```
Subject Name : CN=ECA-KOPS,O=Veritas,OU=ECANBKOps
 Issued By : CN=ICA-2,O=Veritas,OU=ECANBKOps
 Serial Number : 0x56cf16040258d3654339b7f39817de89240d58
 Expiry Date : Dec 16 05:48:16 2022 GMT
 SHA-1 Fingerprint : 70:DE:46:72:57:56:4E:47:DB:82:8B:8D:A3:
 4B:BB:F9:8D:2C:B7:8E
 SHA-256 Fingerprint : E0:69:5F:79:A6:60:DB:7B:69:76:D3:A8:
 E6:E1:F2:0D:8C:6C:E6:4E:C4:5D:A4:77:17:5A:C2:42:89:74:15:7D
 Key Strength : 2048
 Subject Key Identifier : F0:E7:1F:8C:50:FD:4D:25:40:69:77:6C:
 2A:35:72:B6:1D:8E:E5:17
 Authority Key Identifier : D7:53:57:C7:A6:72:E3:CB:73:BD:48:51:

 2F:CB:98:A3:0B:8B:BA:5C
 Master Server : masterserver.sample.domain.com
 Host ID : b85ba9bf-02a8-439e-b787-ed52589c37d1
```

4

管理 Kubernetes 资产

本章节包括下列主题：

添加 Kubernetes 群集

在 NetBackup 中添加 Kubernetes 群集之前，必须在群集中安装和配置 Kubernetes Operator。否则，群集验证将失败，这会进一步导致群集添加操作失败。

Kubernetes Operator 配置完成后，可以在 NetBackup 中添加 Kubernetes 群集，并自动发现群集内的所有资产。

添加群集

1 在左侧，单击“**工作负载**”下的 **Kubernetes**。

2 单击“**Kubernetes 群集**”选项卡，然后单击“**添加**”。

3 在“**添加 Kubernetes 群集**”页面中，输入以下内容：

- **群集名称**：输入群集的名称。此名称应为 DNS 可解析值或 IP 地址。示例：cluster.sample.domain.com。
- **端口**：输入 Kubernetes API 服务器端口号。
- **控制器命名空间**：输入在 Kubernetes 群集中部署 NetBackup Kubernetes Operator 的命名空间。示例：kops-ns。

4 单击“**下一步**”。在“**管理凭据**”页面中，可以将凭据添加到群集。

- 要使用现有凭据，请选择“**从现有凭据中选择**”，然后单击“**下一步**”。在下一页中，选择所需的凭据，然后单击“**下一步**”。
- 要创建新凭据，请单击“**添加凭据**”，然后单击“**下一步**”。在“**管理凭据**”页面中，输入以下内容：
  - **凭据名称**：输入凭据的名称。
  - **标记**：输入要与凭据关联的标记。
  - **描述**：输入凭据的描述。
  - 要在 NetBackup 中添加 Kubernetes 群集，您需要证书颁发机构 (CA) 证书和令牌。Kubernetes 群集的授权和身份验证需要 CA 证书和备份服务帐户的令牌。要获取 CA 证书和令牌，请在 Kubernetes 群集中运行以下命令：`kubectl get secret <[namespace-name]-backup-server-secret> -n <namespace name> -o yaml.`。
    - **令牌**：输入 Base64 编码形式的身份验证令牌值。
    - **CA 证书**：输入 CA 证书文件内容。

5 单击“**下一步**”。

凭据已进行验证，验证成功后，即会添加群集。添加群集后，将运行自动发现以发现群集中的可用资产。

注意：在 NetBackup Kubernetes 版本 10.1 中，编辑群集操作失败并显示错误消息。解决此问题的建议操作是，先删除群集然后重新添加群集。

配置设置

Kubernetes 设置可用于配置 Kubernetes 部署的各个方面。

更改 Kuberentes 资源类型的资源限制

关于资源限制设置

使用此设置，可以控制可在 Kubernetes 群集上同时执行的备份数。Kubernetes 有两个不同的默认值（1 和 4），分别用于运行快照作业和从快照备份作业。

示例：

运行仅快照备份作业时，如果要保护 20 个资产并将限制设置为 5，则只有 5 个资产可以同时执行备份，其余 15 个资产将进入队列。前 5 个资产中的一个完成备份后，队列中的某个资产将会补位。

运行快照作业时，资源限制的默认值为 1。这表示每个群集只能有一个备份作业处于进行中状态，而其余资产处于排队状态。

建议配置此设置，以优化系统资源和网络资源的使用。这些设置适用于所选主服务器的所有 Kubernetes 备份。

设置资源限制

1 在左侧，“**工作负载**” > **Kubernetes**。

2 在右上方，单击“**Kubernetes 设置**” > “**资源限制**”。

3 执行以下任一操作以设置资源限制：

- 在“**每个 Kubernetes 群集的备份作业数**”旁边，单击“**编辑**”。默认情况下，限制为 1。
  这定义了每个群集并行处理的命名空间数量。另外，对于“从快照备份”作业，也适用于使用快照创建备份的第一个操作。
  默认情况下，每个群集的备份作业的资源限制为 1。
- 在“**每个 Kubernetes 群集的从快照备份作业数**”旁边，单击“**编辑**”。
  这定义了在创建快照后每个群集并行备份的命名空间数量。每个“从快照备份”作业都将在群集上的 NetBackup 命名空间中启动一个数据移动器 pod 以处理数据。
  默认情况下，每个群集的从快照备份作业的资源限制为 4。

4 在“**编辑 Kubernetes 群集**”对话框中：

- 在“**全局**”字段中输入一个值，设置所有群集的全局限制。此限制表示在群集上同时执行的 *“备份”* 作业数和 *“从快照备份”* 作业数。
- 您可以为群集添加单独的限制，以覆盖该群集的全局限制。要对群集设置单独的限制，请单击“**添加**”。
- 可以从列表中选择可用群集，然后为所选群集输入限制值。您可以为部署中的每个可用群集添加限制。
- 单击“**保存**”以保存更改。

注意：在 NetBackup 10.0 版本中，datamover pod 超过了 Kubernetes 资源限制设置。

请参见第 105 页的“datamover pod 超过 Kubernetes 资源限制 ”。

配置自动发现频率

自动发现可对群集中受 NetBackup 保护的资产计数。此设置可用于设置 NetBackup 运行自动发现的频率，以查找群集中的新资产。收集从群集中移除或删除的资产计数。

可能的值介于 5 分钟到 1 年之间。默认值为 30 分钟。

设置自动发现频率

1 在左侧，单击“**工作负载**”**> Kubernetes**。

2 在右上方，单击“**Kubernetes 设置**”**>**“**自动发现**”。

3 单击“**频率**”附近的“**编辑**”。

4 输入 NetBackup 运行自动发现前经过的小时数。单击“**保存**”。

运行完全发现和增量发现

添加 Kubernetes 群集后，将触发自动发现周期，以发现 Kubernetes 群集上可用的所有资产。当天的第一个自动发现是完全发现，后续的自动发现是增量发现。

运行发现

1 在左侧，单击“**工作负载**”**> Kubernetes**。

2 在“**Kubernetes 群集**”列表中，找到群集名称。然后单击“**操作**”**>**“**立即发现**”。

此处，增量发现仅获取自上次运行发现以来在群集中更改的 NetBackup 资产。因此，第一个发现是完全发现，所有后续发现都是增量发现。

配置权限

使用管理权限，可以为用户角色分配不同的访问权限。有关更多信息，请参见《NetBackup Web UI 管理指南》中的“管理基于角色的访问控制”一章。

资产清理

资产清理是指识别并删除未使用或过时资源的过程，以优化成本、提高安全性和保持高效运行。

可以根据特定条件自动执行资产清理。

以下是执行资产清理之前的一些常见条件：

- 资产没有备份映像。
- 未将资产订购到备份策略或保护计划。
- 资产早于可配置期限。

默认情况下，NetBackup 会清理 30 天前的资产。

设置资产期限以执行自动清理

1. 单击 **Kubernetes** 工作负载，然后单击页面右上角的“**Kubernetes 设置**”。
2. 单击“**资产清理**”。将显示资产清理页面。
3. 单击“**编辑**”并指定期限（以天为单位）。
4. 单击“**保存**”。

为资产添加保护

“**命名空间**”选项卡（“**工作负载**” > **Kubernetes**）可用于监控 Kubernetes 群集中的资产、查看其保护状态，并轻松为未受保护的资产添加保护。您还可以使用“立即备份”功能快速备份资产。此功能会为所选资产创建一次性备份，而不影响任何已计划的备份。

“命名空间”选项卡显示 NetBackup 可保护的所有已发现和已导入的 Kubernetes 资产。该选项卡显示以下信息：

- **命名空间**：显示资产的名称。
- **群集**：资产所属的群集。
- **受以下对象保护**：应用于资产的保护计划的名称。
- **上次成功备份**：资产上次成功备份的日期和时间。

可以在“**命名空间**”选项卡中执行以下操作。

为未受保护的资产添加保护

1 在左侧，单击“**工作负载**” > **Kubernetes**。

2 在资产行中选择选项。单击右上方的“**添加保护**”。或者，单击资产行中的“操作”菜单，然后单击“**添加保护**”。

3 从列表中选择保护计划，然后单击“**下一步**”。在下一页中，单击“**保护**”。

快速备份资产

1 在资产行中选择选项，然后单击右上方的“**立即备份**”。或者，单击资产行中的“操作”菜单，然后单击“**立即备份**”。

2 在下一页中，

- 如果备份已受保护的资产，请从资产已订购的计划列表中选择保护计划，然后单击“**开始备份**”。

- 如果要备份未受保护的资产，请从资产的可用计划中选择保护计划，然后单击“**开始备份**”。

扫描恶意软件

NetBackup 10.4 及更高版本支持通过 Kubernetes 工作负载扫描 Kubernetes 资产以查找恶意软件。

要触发恶意软件扫描，必须配置扫描主机。有关配置扫描主机的更多信息，请参考《NetBackup 安全和加密指南》中的“扫描主机配置”一章。

资产 (按工作负载类型)

本节介绍扫描 Kubernetes VM 资产以查找恶意软件的过程。

本节介绍扫描 VMware、通用共享、Kubernetes、Nutanix 和云 VM 资产以查找恶意软件的过程。

要扫描支持的资产以查找恶意软件，请执行以下操作：

1. 在左侧，在“**工作负载**”下选择支持的工作负载。
2. 选择已完成备份的资源。

   例如，VMware、通用共享、Kubernetes、Nutanix 和云 VM

   例如，Kubernetes

   例如，Nutanix AHV
3. 选择“**操作**”>“**扫描恶意软件**”。
4. 在“**恶意软件扫描**”页面上，执行以下操作：
   - 通过选择“**开始日期/时间**”和“**结束日期/时间**”，选择扫描的日期范围。
   - 选择“**扫描程序主机池**”
   - 从“**当前感染状态**”列表中，选择以下选项之一：
     - **未扫描**
     - **未受感染**
     - **恶意软件扫描检测到感染**
     - **文件哈希搜索检测到感染**
     - **全部**

5 单击“**扫描恶意软件**”。

注意：恶意软件扫描程序主机可以同时启动对三个映像的扫描。

6 启动扫描后，您可以看到“**恶意软件检测**”上的“**扫描状态**”，并看到以下字段：

- **未扫描**
- **未受感染**
- **受感染**
- **失败**

注意：验证失败的任何备份映像将被忽略。

- **进行中**
- **挂起**

5

管理 Kubernetes 智能组

本章节包括下列主题：

关于智能组

可根据一组过滤器（称为查询）定义智能资产组，从而创建和保护动态资产组。NetBackup 基于查询选择 Kubernetes 命名空间，然后将其添加到组中。智能组会自动反映资产环境中的更改，因此在环境中添加或删除资产时，不必手动修改组中的资产列表。

将保护计划应用于智能组时，满足查询条件的所有资产将自动受到保护。

注意：只有您的角色对需要管理的资产具有必要的 RBAC 权限时，才能创建、更新或删除智能组。NetBackup 安全管理员可以授予资产类型（群集、命名空间和 VM 组）的访问权限。请参考《NetBackup Web UI 管理指南》。

创建智能组

创建智能组

1 在左侧，单击“**工作负载**”下的 **Kubernetes**。

2 单击“**智能组**”选项卡，然后单击“**+ 添加**”。

3 为组输入名称和描述。

4 在“**群集**”部分下，单击“**添加群集**”

5 在“**添加群集**”窗口中，从列表中选择一个或多个群集，然后单击“**选择**”，所选群集即会添加到智能组中。

注意：可以跨多个群集创建智能组。确保具有在组中添加群集所需的权限。要查看和管理组，组管理员必须具有所选群集和组的查看和管理权限。

---

6 在“**选择资产**”部分下，执行以下操作之一：

- 选择“**包括所有资产**”。
  此选项使用默认查询选择所有资产，以便在保护计划运行时进行备份。
- 要仅选择满足特定条件的资产，请创建自己的查询：单击“**添加条件**”。
- 要为资产添加标签条件，请单击“**添加标签条件**”进行添加

7 要添加条件，请使用下拉列表选择关键字和运算符，然后输入值。

要更改查询的效果，请单击“**+ 条件**”并单击 **AND** 或 **OR**，然后选择条件的关键字、运算符和值。

注意：要添加标签条件，请单击“**添加标签条件**”，输入标签键和值。

注意：您可以选择在条件中仅包含标签键，不带标签值。因为值是添加标签条件的可选参数。

注意：要添加子查询，请单击“**添加子查询**”。可以添加多个级别的子查询。

---

8 要测试查询，请单击“**预览**”。

基于查询的选择过程是动态的。Kubernetes 群集中的更改可能会影响在保护计划运行时查询选择的资产。因此，查询在保护计划运行时稍后选择的资产可能与预览中当前列出的资产不同。

注意：当在“**智能组**”中使用查询时，如果查询条件包含非英文字符，则 NetBackup Web UI 可能不会显示与该查询匹配的资产的准确列表。

在任何属性上使用 `not equals` 过滤器条件所返回的资产将包括属性不存在值 (null) 的那些资产。

注意：单击“**预览**”或保存组时，如果为组选择资产，则会将查询选项视为区分大小写。

9 要保存组而不将其添加到保护计划，请单击“**添加**”。

10 要保存组并将其添加到保护计划，请单击“**添加和保护**”。

11 要为组订购保护计划，请单击“**添加保护**”。

选择组并为其应用保护计划，然后单击“**保护**”。

为所选的资产组订购保护计划成功。

向资产添加标签条件时的限制

如果组合使用条件和标签，则必须先定义命名空间条件，然后定义标签条件。

注意：对于条件，仅允许使用命名空间值。

删除智能组

删除智能组

1 在左侧，单击“**工作负载**”下的 **Kubernetes**。

2 在“**智能组**”选项卡下找到该组。

3 如果该组不受保护，则选择该组，然后单击“**删除**”。

4 如果该组受保护，则选择该组，然后单击“**删除保护**”以删除所有保护计划。

5 然后在“**智能组**”选项卡下选择该组，单击“**删除**”。

编辑智能组

可以编辑智能组的名称和描述详细信息。您可以编辑保护计划的某些设置，包括日程表备份时段和其他选项。

编辑智能组

1 在左侧，单击“**工作负载**”下的 **Kubernetes**。

2 在“**智能组**”选项卡上，单击要为其编辑保护的组。

3 执行以下操作之一：

- 单击“**编辑名称和描述**”以编辑所选组的名称和描述，然后单击“**保存**”。
- 在“**资产**”选项卡上，单击“**编辑**”以添加或删除群集。可以更新所选资产的查询条件，然后单击“**保存**”。
  可以编辑组中的群集列表，在组中添加或删除群集。还可以修改所选资产组的查询条件。
- 在“**权限**”选项卡上，单击“**添加**”可更新可用角色的权限，然后单击“**保存**”。

6

保护 Kubernetes 资产

本章节包括下列主题：

保护智能组

您可以为 Kubernetes 工作负载创建特定于 Kubernetes 的保护计划。然后，您可以为智能组订购保护计划。

使用以下过程为智能组订购保护计划。

注意：分配给您的 RBAC 角色必须提供相应的访问权限，使您可以访问要管理的智能组以及要使用的保护计划。

保护智能组

1 在左侧，单击 **Kubernetes**。

2 在“**智能组**”选项卡上，单击智能组对应的框，然后单击“**添加保护**”。

3 选择保护计划，然后单击“**下一步**”。

4 选择一个组并单击“**保护**”以订阅保护计划。

用于立即保护的“立即备份”选项

除了预定的保护计划外，还可以使用“**立即备份**”选项立即备份组，防止出现任何计划外情况。

从智能组中删除保护

可以为智能组取消订购保护计划。为智能组取消订购保护计划后，将不再执行备份。

从智能组中删除保护

1 在左侧，单击“**工作负载**”下的 **Kubernetes**。

2 在“**智能组**”选项卡上，单击要为其删除保护的组。

3 单击“**删除保护**”>“**是**”。

配置备份计划

为 Kubernetes 工作负载创建保护计划时，可以在“**添加备份计划**”对话框的“**属性**”选项卡中添加备份计划。

有关如何创建保护计划的详细信息，请参见《NetBackup Web UI 管理指南》中的“管理保护计划”部分。

为 Kubernetes 备份作业添加备份计划

1 在左侧，单击“**保护**”>“**保护计划**”，然后单击“**添加**”。

2 在“**基本属性**”中，输入“**名称**”和“**描述**”，然后从“**工作负载**”下拉列表中选择 **Kubernetes**。

3 单击“**下一步**”。在“**计划**”中，单击“**添加计划**”。

在“**添加备份计划**”选项卡中，可以配置用于保留备份和快照的选项。

4 在“**循环**”下拉列表中，指定备份频率。

5 在“**快照和备份副本**”选项中，执行以下任一操作：

- 选择“**从快照创建备份**”选项，以便为保护计划配置从快照备份。使用“**备份保留期限**”下拉列表指定从快照备份的保留期限。

注意：Kubernetes 工作负载仅支持完全备份计划。可以设置以小时、天、周、月和年为单位的备份持续时间。

默认情况下，备份保留持续时间为四周。

注意：必须选择“**从快照创建备份**”选项，才能为备份副本启用主从复制和复制选项。

- 如果不选择“**从快照创建备份**”选项，则默认情况下，将配置“**仅限快照存储**”备份以运行备份作业。
- 选择“**从快照创建备份的副本 (自动映像同步复制)**”选项，创建备份的副本。
- 选择“**从快照创建备份的复制副本**”选项，创建备份的复制副本。

6 继续按照《NetBackup Web UI 管理指南》中的“管理保护计划”部分所述，在“**启动时段**”选项卡中创建计划

7 继续按照《NetBackup Web UI 管理指南》中的“管理保护计划”部分所述，配置用于从快照备份的“**存储选项**”

配置备份选项

可以为保护计划配置备份选项。

有关如何创建保护计划的详细信息，请参见《NetBackup Web UI 管理指南》中的“管理保护计划”部分。

配置保护计划的同时配置备份选项

1 在“**备份选项**”页面的“**资源类型选择**”部分下，

- 默认情况下，“**在备份中包括所有资源类型**”选项处于选定状态，以包括备份作业的所有资源类型。
- 选择“**从备份中排除以下资源类型**”选项，从备份作业中排除资源类型。
  单击“**选择**”以从静态列表中选择资源类型。所选资源类型显示在文本字段中，您也可以使用正确的格式 (type.group) 手动输入自定义资源定义 (CRD)。可以从排除列表中删除所选资源类型。
  如果静态列表中不存在自定义资源类型定义，则可以手动输入自定义资源定义 (CRD)。例如：demo.nbu.com。

注意：在映射资源时，资源类型的排除列表优先于选定用于备份的标签。

2 在“**标签选择**”部分下，单击“**添加**”以添加标签从而映射备份的关联资源，输入标签前缀和键，然后选择运算符。系统会为备份作业映射与所包括标签关联的所有资源。

以下是可添加到标签的四种运算符：

- 输入等于某个值的标签键。
- 输入已存在的标签键（不包含任何值）。
- 输入包含在一组值中的标签键。
- 输入不包含在一组值中的标签键。

可以在一组逗号分隔值中为“in/not in”运算符添加多个值。

注意：备份时必须存在选定的标签，以确保成功应用这些条件。

注意：选择标签时，只能选择在多个标签条件之间不矛盾的任何资源类型。

“**审查**”页面显示资源类型的排除列表、要包括的选定标签以及选定的存储单元。

注意：可以编辑或删除为 Kubernetes 工作负载创建的保护计划。

无法自定义为 Kubernetes 工作负载创建的保护计划。

配置备份

NetBackup 允许您在 Kubernetes 工作负载中运行两种类型的备份作业：“仅限快照”和“从快照备份”。请按照以下步骤为 Kubernetes Operator 配置备份作业。

在 Kubernetes 工作负载上执行备份

1 在左侧，单击“**保护**”>“**保护计划**”，然后单击“**添加**”。

2 在“**基本属性**”中，输入“**名称**”和“**描述**”，然后从“**工作负载**”下拉列表中选择 **Kubernetes**。

3 单击“**下一步**”。在“**计划**”中，单击“**添加计划**”。

在“**添加备份计划**”选项卡中，可以配置用于保留备份和快照的选项。

4 在“**循环**”下拉列表中，指定备份频率。

5 在“**快照和备份副本**”选项中，执行以下任一操作：

- 选择“**从快照创建备份**”选项，以便为保护计划配置从快照备份。使用“**备份保留期限**”下拉列表指定从快照备份的保留期限。

  注意：Kubernetes 工作负载仅支持完全备份计划。可以设置以小时、天、周、月和年为单位的备份持续时间。默认情况下，备份保留持续时间为四周。

  注意：必须选择“**从快照创建备份**”选项，才能为备份副本启用主从复制和复制选项。

- 如果不选择“**从快照创建备份**”选项，则默认情况下，将配置“**仅限快照存储**”备份以运行备份作业。
- 选择“**从快照创建备份的副本 (自动映像复制)**”选项，创建备份的副本。
- 选择“**从快照创建备份的复制副本**”选项，创建备份的复制副本。

6 继续按照《NetBackup Web UI 管理指南》中的“管理保护计划”部分所述，在“**启动时段**”选项卡中创建计划

7 继续按照《NetBackup Web UI 管理指南》中的“管理保护计划”部分所述，配置用于从快照备份的“**存储选项**”

- 为“**从快照备份**”选项选择存储时，所选存储单元必须具有 NetBackup 10.0 或更高版本的介质服务器。
- 管理存储的介质服务器必须有权访问选定的 Kubernetes 群集。
- 介质服务器必须能够与 API 服务器连接。必须打开与 API 服务器对应的端口，以便从介质服务器建立出站连接。datamover pod 必须能够连接到介质服务器。

配置自动映像同步复制 (A.I.R.) 和复制

可以将在一个 NetBackup 域中生成的备份复制到一个或多个目标 NetBackup 域的存储中。此过程称为自动映像同步复制 (A.I.R.)。

NetBackup Kubernetes 支持从一个 NetBackup 域中的介质服务器重复数据删除池 (MSDP) 到另一个域中的介质服务器重复数据删除池 (MSDP) 的自动映像同步复制。NetBackup 在源域和目标域中使用存储生命周期策略 (SLP) 来管理 A.I.R. 操作。

有关配置自动映像同步复制的更多信息，请参考《NetBackup 管理指南，第 I 卷》中的“关于 NetBackup 同步复制”一章。

注意：Kubernetes A.I.R. 配置需要 10.0.1 或更高版本的 NetBackup 主服务器和介质服务器。

为 Kubernetes 备份配置自动映像同步复制 (A.I.R.) **和复制**

1 在两个 NetBackup 主服务器之间配置自动映像复制。

- 在两个主服务器之间建立信任关系以进行域间操作。
  - 登录到源主服务器，在左侧单击“**主机**”>“**主机属性**”，以在源主服务器和目标主服务器之间建立连接。
  - 选择源主服务器。如有必要，单击“**连接**”。然后，单击“**编辑主服务器**”。
  - 单击“**服务器**”。在“**可信主服务器**”选项卡上，单击“**添加**”以添加源服务器。
    - 单击“**验证证书颁发机构**”，然后单击“**下一步**”继续进行证书颁发机构验证。
    - 要创建可信主服务器，请从以下选项中进行选择：
      - 选择“**指定可信主服务器的身份验证令牌**”，为源主服务器添加现有令牌或创建新令牌。
      - 选择“**指定可信主服务器的凭据**”，为源主服务器添加用户凭据。
    - 单击“**创建信任**”。

  已成功更新主机属性的数据库。
  - 单击“**保存**”。

2 在源主服务器中配置介质服务器重复数据删除池 (MSDP) 存储，并在 MSDP 磁盘池中添加复制目标。

- 在左侧，单击“**存储**”>“**磁盘存储**”。
- 添加 MSDP 存储和磁盘池。
- 单击“**磁盘池**”选项卡，然后单击“**添加**”。
  - 选择可信主服务器和目标存储服务器。
  - 在“**用户名**”和“**密码**”字段中为复制目标服务器添加用户凭据。

- 单击“**添加**”。

3 在目标主服务器中使用“**导入**”操作创建 SLP。

- 在左侧，单击“**存储**”>“**存储生命周期策略**”。然后单击“**添加**”。
- 在“**存储生命周期策略名称**”字段中，输入策略名称，然后单击“**添加**”。
- 从“**操作**”列表中，选择“**导入**”。
- 在“**目标存储**”列表中，选择 MSDP 存储单元。
- 单击“**创建**”。

4 使用“**从快照创建备份**”选项创建 Kubernetes 保护计划，以启用复制副本选项。

在左侧，单击“**保护**”>“**保护计划**”。在“**日程表**”选项卡中，单击“**添加日程表**”。

5 在“**快照和备份副本选项**”部分中，选择“**从快照创建备份**”选项以启用主从复制和重复副本选项。

6 选择“**从快照创建备份的副本 (自动映像复制)**”选项，然后设置要保留副本的持续时间。

注意：只能在可信的 NetBackup 主服务器上创建自动映像复制。

---

7 选择“**从快照创建备份的复制副本**”选项，然后设置要保留重复副本的持续时间。

8 单击“**添加**”。

9 继续按照《NetBackup Web UI 管理指南》中的“管理保护计划”部分所述，在“**启动时段**”选项卡中创建日程表。

10 单击“**下一步**”。

11 在“**存储选项**”选项卡中，选择存储单元，以从快照备份、对副本进行同步复制或复制。

注意：对于“从快照备份”和复制，可以添加简单存储单元。但对于同步复制，必须使用导入存储生命周期策略 (SLP) 添加可信存储单元。

---

12 在所选备份选项的右侧，单击“**编辑**”以修改用于备份的所选存储单元。

- 对于副本选项，选择用于同步复制副本的主服务器。然后单击“**下一步**”。
- 选择在可信服务器中定义的导入存储生命周期策略，然后单击“**使用所选同步复制目标**”。

13 继续执行向导中的步骤。

配置存储单元

可以在保护计划中配置所有类型的存储单元以进行备份。

注意：备份作业支持存储生命周期策略 (SLP) 中支持的所有存储类型。

配置存储单元以进行备份

1 在左侧，单击“**存储**”>“**存储单元**”。

2 单击“**存储单元**”选项卡，然后单击“**添加**”以添加存储单元配置。

3 从列表中选择存储类型。

4 选择“**类别**”，然后单击“**开始**”。

5 在“**名称**”字段中输入存储单元名称。

6 在“**最大并行作业数**”字段中，选择备份作业的最大数目。

7 在“**最大片段大小**”字段中，选择存储单元片段大小的最大数值，然后单击“**下一步**”。

8 在“**磁盘池**”中，选择要在存储单元中使用的磁盘池，然后单击“**下一步**”。

9 “**只根据要求**”选项指定是否可以根据要求以独占方式使用存储单元。必须明确配置策略或计划以使用此存储单元。

10 在“**介质服务器**”选项卡中，选择要使用的介质服务器，然后单击“**下一步**”。可以让 NetBackup 自动选择介质服务器，也可以使用单选按钮手动选择介质服务器。

- 所有介质服务器都必须是 NetBackup 10.0 或更高版本
- 管理存储的所有介质服务器都必须有权访问选定的 Kubernetes 群集。
- 介质服务器必须能够与 API 服务器连接。必须打开与 API 服务器对应的端口，以便从介质服务器建立出站连接。datamover pod 必须能够连接到介质服务器。

11 查看存储单元的设置，然后单击“**保存**”。

12 要检查预定备份或立即备份作业的详细信息，请在“**活动监视器**”选项卡中单击“**作业 ID**”，以查看备份作业详细信息。对于文件模式，可以在“**作业详细信息**”部分中，查看每个映像的已备份文件总数。

卷模式支持

NetBackup Kubernetes 支持以下功能：

- 对于支持以下功能的容器存储接口 (CSI) 提供程序，备份和还原模式文件系统和/或块的永久卷声明 (PVC)：
  - PVC 快照功能。
  - 基于网络文件系统 (NFS) 或其他非块存储的 PVC 卷置备。
  - 基于块存储的 PVC 卷置备。

注意：从 NetBackup 10.3 开始，现在支持备份和还原包含混合卷（VolumeMode：文件系统和块）的命名空间。

配置应用程序一致性备份

正在运行应用程序（如数据库）的一些 pod 需要其他过程才能获取应用程序一致性备份。

应用程序一致性备份需要一种机制，来了解应用程序元数据、其内存状态以及驻留在永久性存储上的永久性数据。为了在还原期间获得正常运行状态，在所有这些 Kubernetes 资源之间进行应用程序一致性备份有助于简化恢复过程。如果仅需要崩溃一致性备份，则不需要执行这些过程。

供应商文档中记录了暂停应用程序输入和输出 (I/O) 操作的步骤，以执行应用程序一致性快照。不同应用程序有不同的步骤，因此这类过程的自定义性质非常重要。这类过程的内容由客户决定。

为使用 NetBackup 保护 Kubernetes 工作负载，方法是对备份挂钩应用应用程序 Pod 注释，以获得应用程序一致性快照。Kubernetes 注释只是元数据，可以应用于任何 Kubernetes 资源。Kubernetes 中的挂钩是用户定义的操作，可以是任何命令或多个命令。在 Kubernetes 基础架构中，将这些注释和挂钩应用于需要静默状态的任何应用程序 Pod。

在处理前（快照之前）和处理后（快照之后）使用备份挂钩。在数据保护上下文中，这通常意味着 netbackup-pre-backup 挂钩调用静默过程或命令，netbackup-post-backup 挂钩调用取消静默过程或命令。每组挂钩会指定命令以及

应用该命令的容器。请注意，这些命令不在容器上的 shell 内执行。因此，在给定示例中使用带有目录的完整命令字符串。

标识需要应用程序一致性备份的应用程序，并对一组备份挂钩应用注释，作为 Kubernetes 数据保护配置的一部分。

使用 Kubernetes 用户界面 (UI) 向 Pod 添加注释。或者，对于特定 Pod 或标签，在 Kubernetes 群集控制台上使用 `kubectl` 注释函数。应用注释的方法可能因发行版而异，基于 `kubectl` 命令在大多数发行版中的广泛应用，以下示例重点介绍该命令。

此外，可以将注释添加到基本 Kubernetes 对象（如部署资源或副本集资源）中，以确保注释包含在任何新部署的 Pod 中。Kubernetes 管理员可以动态更新注释。

标签是附加到 Kubernetes 对象（如 Pod 或服务）的键值对。标签用作具有意义且与用户相关的对象的属性。标签可以在创建时附加到对象，随后可以随时添加和修改。Kubernetes 提供集成支持，支持使用这些标签查询对象和对选定子集执行批量操作。每个对象都可以定义一组键值标签。每个密钥对于给定对象必须是唯一的。

标签元数据格式和语法的示例：

```
"metadata": {"labels": {"key1":"value1","key2":"value2"}}
```

可以指定专门的 Pod 名称，也可以指定应用于所需 Pod 组的标签。如果使用了多个注释参数，则指定正确的 JSON 格式，例如 JSON 阵列：'["item1","item2","itemn"]'`# kubectl annotate pod [ {pod_name} | -l {label=value}] -n {the-pods-namespace_name} [annotation syntax - see following]`

如果某些应用程序需要多个命令来获得所需结果，则可以将此方法与 `&&` 结合使用来联接多个命令。指定的命令不是由 Veritas 提供的，用户必须手动自定义应用程序 Pod。将 {values} 替换为环境中使用的实际名称。

注意：所有 `kubectl` 命令都必须在一行中定义。复制或粘贴以下示例时要小心。

升级到 NetBackup 10.2 后，请更新这些新的 netbackup-pre-backup 和 netbackup-post-backup 挂钩的注释，其现在包括 netbackup 前缀：

```
netbackup-pre.hook.back.velero.io/command
netbackup-pre.hook.backup.velero.io/container
netbackup-post.hook.back.velero.io/command
netbackup-post.hook.backup.velero.io/container
```

使用 Pod 名称的 MongoDB 示例

以下是用于锁定和解锁 MongoDB 4.2.23 数据库的命令：

```
# mongo --eval "db. fsyncLock ()"
```

```
# mongo --eval "db.fsyncUnlock()"
```

这可转换为以下单个命令，用于为 MongoDB 设置备份前挂钩和备份后挂钩。请注意用于转义特殊字符的特殊语法，以及用作 JSON 格式一部分的方括号 ([])、单引号、双引号和逗号 (,)：

```
# kubectl annotate pod {mongodb-pod-name} -n {mongodb namespace}
netbackup-pre.hook.back.velero.io/command='["/bin/bash", "-c", "mongo
--eval \"db.fsyncLock()\""]'
netbackup-pre.hook.backup.velero.io/container={mongodb-pod-name}
netbackup-post.hook.backup.velero.io/command='["/bin/bash","-c","mongo
--eval \"db.fsyncUnlock()\""]'
netbackup-post.hook.backup.velero.io/container={mongodb-pod-name}
```

使用标签的 MySQL 示例

以下是用于静默和取消静默 MySQL 数据库的命令：

```
# mysql -uroot -ppassword -e "flush tables with read lock"
```

```
# mysql -uroot -ppassword -e "unlock tables"
```

这可转换为以下单个命令，用于为 MySQL 设置备份前挂钩和备份后挂钩。在此示例中，我们使用标签而不是 Pod 名称，因此该标签可以一次为多个 Pod 添加注释。请注意用于转义特殊字符的特殊语法，以及用作 JSON 格式一部分的方括号 ([])、单引号、双引号和逗号 (,)：

```
# kubectl annotate pod -l label=value -n {mysql namespace}
netbackup-pre.hook.backup.velero.io/command='["/bin/bash", "-c",
"mysql -uroot -ppassword -e \"flush tables with read lock\""]'
netbackup-pre.hook.backup.velero.io/container={mysql container name}
netbackup-post.hook.backup.velero.io/command='["/bin/bash", "-c",
"mysql -uroot -ppassword -e \"unlock tables\""]'
netbackup-post.hook.backup.velero.io/container={mysql container name}
```

使用标签的 Postgres 示例

以下是用于静默和取消静默 PostgreSQL 数据库的命令：

```
# Psql -U postgres -c "SELECT pg_start_backup('tagvalue');"
```

```
# psql -U postgres -c \"SELECT pg_stop_backup();"
```

这可转换为以下单个命令，用于为 Postgres 设置备份前挂钩和备份后挂钩。在此示例中，我们使用标签而不是 Pod 名称，因此该标签可以一次为多个匹配的 Pod 添加注释。标签可以应用于任何 Kubernetes 对象，在这种情况下，我们使用标签提供另一种方法来修改特定容器并仅选择某些 Pod。请注意用于转义特殊字符的特殊语法，以及用作 JSON 格式一部分的方括号 ([])、单引号、双引号和逗号 (,)：

```
# kubectl annotate pod -l app=app-postgresql -n {postgres namespace}
netbackup-pre.hook.backup.velero.io/command='["/bin/bash", "-c",
"psql -U postgres -c \"SELECT
pg_start_backup(quote_literal($EPOCHSECONDS));\""]'
netbackup-pre.hook.backup.velero.io/container={postgres container
name} netbackup-post.hook.backup.velero.io/command='["/bin/bash",
"-c", "psql -U postgres -c \"SELECT pg_stop_backup();\""]'
netbackup-post.hook.backup.velero.io/container={postgres container
name}
```

不带容器挂钩的 NGINX 应用程序示例

以下是用于静默和取消静默 Nginx 应用程序的命令：

```
# /sbin/fsfreeze --freeze /var/log/nginx
```

```
# /sbin/fsfreeze --unfreeze /var/log/nginx
```

这可转换为以下单个命令，用于为 NGINX 设置备份前挂钩和备份后挂钩。在此示例中，我们将忽略容器挂钩，这将修改默认情况下与 Pod 名称匹配的第一个容器。请注意用于转义特殊字符的特殊语法，以及用作 JSON 格式一部分的方括号 ([])、单引号、双引号和逗号 (,)：

```
# kubectl annotate pod {nginx-pod-name} -n {nginx namespace}
netbackup-pre.hook.backup.velero.io/command='["/sbin/fsfreeze",
"--freeze", "/var/log/nginx"]'
netbackup-post.hook.backup.velero.io/command='["/sbin/fsfreeze",
"--unfreeze", "/var/log/nginx"]'
```

Cassandra 示例

以下是用于静默和取消静默 Cassandra 数据库的命令：

```
# nodetool flush
```

```
# nodetool verify
```

这可转换为以下单个命令，用于为 Cassandra 设置备份前挂钩和备份后挂钩。请注意用于转义特殊字符的特殊语法，以及用作 JSON 格式一部分的方括号 ([])、单引号 (')、双引号 (“”) 和逗号 (,)：

```
# kubectl annotate pod {cassandra-pod} -n {Cassandra namespace}
netbackup-pre.hook.backup.velero.io/command='["/bin/bash", "-c",
"nodetool flush"]'
netbackup-pre.hook.backup.velero.io/container={cassandra-pod}
netbackup-post.hook.backup.velero.io/command='["/bin/bash", "-c",
"nodetool verify"]'
netbackup-post.hook.backup.velero.io/container={cassandra-pod}
```

注意：提供的示例仅用作初始指南，每个工作负载的具体要求必须包括备份、工作负载和 Kubernetes 管理员之间的协作。

目前，Kubernetes 不支持在出错时使用挂钩。如果用户指定的命令失败，则备份快照不会继续。

用于返回退出状态的命令的默认超时值为 30 秒。但是，可以使用具有 Pod 注释的以下挂钩来更改此值：

```
netbackup-pre.hook.backup.velero.io/timeout=#in-seconds#

netbackup-post.hook.backup.velero.io/timeout=#in-seconds#
```

7

管理映像组

本章节包括下列主题：

关于映像组

对于每个 Kubernetes 恢复点，将创建一个映像组。映像组可能包括多个映像，具体取决于命名空间中符合条件的永久卷声明数量。

会为元数据创建单独的映像，并为每个永久卷声明创建一个映像。

恢复点详细信息 API 用于获取有关映像组的所有备份 ID、资源名称、复制完成状态的详细信息。

为了支持在 Kubernetes 工作负载上执行从快照备份操作，将创建多个备份映像，以针对单个命名空间执行从快照备份。

对于 Kubernetes 备份操作，将为每个永久卷创建单独的备份映像。创建的所有映像必须分组在一起，才能成功执行某些操作（还原、删除、导入等）。

映像失效

要回收失效映像占用的存储空间，需要删除这些映像。

以下是与映像失效相关的要点。

对于包含多个映像的恢复点：

- 如果已使映像组中的单个映像失效，这不会导致剩余映像自动失效。必须明确使映像组中的所有映像失效。
- 如果已使一些映像失效，则恢复点将处于未完成状态。未完成的恢复点不支持还原操作。

- 如果更改了任何映像的失效时间，则必须更改其余映像的失效时间。否则，与恢复点对应的映像的失效时间将产生偏差，导致某个时间点的恢复点处于未完成状态。

映像导入

Kubernetes 恢复点可能包含多个映像。要执行还原操作，必须导入与恢复点对应的所有映像。否则，恢复点将标记为“未完成”，并且不会执行还原。

有关更多信息，请参考《NetBackup™ 管理指南，第 I 卷》中的“关于导入备份映像”部分

映像副本

可以使用两种类型的备份操作创建映像副本：

1. “**快照**”是默认副本，并标记为副本 1。
2. “**从快照备份**”标记为副本 2。

只要触发任何立即备份操作或预定备份，就会创建“**快照**”。但是，“**从快照备份**”是可选的，因为这取决于在创建保护计划时是否选择了“**从快照备份**”选项。

映像组由元数据和永久卷声明 (PVC) 的资产映像组成。每个副本有一个对应于命名空间的映像，以及一个对应于命名空间中每个 PVC 的映像。

恢复点详细信息 API 用于标识映像的副本完成状态。此 API 还详细介绍了相应副本中存在的所有备份 ID 和资源名称。映像副本的此状态（“完成”或“未完成”）有助于还原功能运行，因为如果有人尝试从未完成的映像副本还原资产，则会引发错误。

未完成的映像副本

在以下情况下，会显示未完成的映像：

1. 在执行快照作业或从快照备份作业时，相应的副本显示为未完成的副本。
2. 如果任何 PVC 的备份活动失败，则将该副本标记为“未完成”。
3. 如果某个副本的子映像失效（具有多个子映像），则将该副本标记为“未完成”。

8

在 NetBackup 中保护 Rancher 管理的群集

本章节包括下列主题：

使用自动配置在 NetBackup 中添加 Rancher 管理的 RKE 群集

请按以下步骤使用自动配置在 NetBackup 中添加 Rancher 管理的 RKE 群集。

使用自动配置在 NetBackup **中添加** Rancher **管理的** RKE **群集**

注意：提取全球 Rancher 管理服务器证书。此 CA 证书可以是 Rancher 生成的默认证书，也可以在创建管理服务器期间使用其他/外部 CA（认证颁发机构）进行配置。

---

1 提取 CA 证书：导航到 **Rancher Management Server UI** > 打开左侧面板 **Global Settings** > 在 **CA Certs** 下，单击 **Show CA Certs** 按钮。将完整的 CA 证书值提取到临时文件。

注意：确保提取包含起始行和结尾行的完整值。

---

2 CA 证书值将添加到密钥中，该密钥是在安装 Kubernetes Operator Helm 之前创建的

3 提取令牌：打开 **Rancher Management Server UI** > 打开左侧面板 > 在 **Explore Cluster** 部分中 > 导航到要保护的群集 > 单击右上角的 **Download KubeConfig** 图标。

4 使用此图标下载群集的 **KubeConfig**，并且该文件内存在令牌字段。

5 从下载的 Kubeconfig 文件提取“令牌:”值（不带双引号 " "）。

6 此配置过程依赖于具有以下命名模式的密钥：
`(<kops-namespace>-nb-config-deploy-secret)`。

密钥包含在步骤 1 和 3 中提取的值。

7 使用以下格式创建 yaml 文件 `nb-config-deploy-secret. yaml`，然后在所有字段中输入值。

```
apiVersion: v1
kind: secret
metadata:
   name: <kops-namespce>-nb-config-deploy-secret
   namespace:  <kops-namespace>

type: Opaque
stringData:
#All the 3 fields are mandatory here to add a Rancher managed
RKF2 cluster in NetBackup
     apikey:
A_YoUkgYQwPLUkmyj9Q6A1-6RX8RNY-PtYX0SukbqCwIK-osPz8qVm9zCL9phje

     k8stoken:
kubeconfig-user-mvvgcm8sq8:nrscvn8hj46t24r2tjrxd2kn8tzo2bg4kj8waxpw36k8ktrchp826

     k8scacert: |
-------BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIBATANBgkqhkiG9w0BAQwIgYDVQQDDBtpbmdy
ZXNzLW9wZXJhdG9yQDE2ODc1MzY4NjgWHhcNMjMwNjIzMTYxNDI3WhcNMjUwNjIy
XtXqbaBGrXIuCCo90mxv4g==
-------END CERTIFICATE------
```

8 运行命令：`kubectl apply -f nb-config-deploy-secret. yaml`

9 有关 Helm Chart 的 values.yaml 文件中的其余输入，请参考《Kubernetes 快速入门指南》的“自动配置”部分，并输入完整设置所需的所有值。

10 如果在 `values.yaml` 文件中添加了所有必要的简化安装输入，则在 NetBackup Kubernetes Operator Chart 上运行 Helm 安装命令，并且自动配置 pod **<kops-namespace>-netbackup-config-deploy** 应启动。

11 查看 **<kops-namespace>-netbackup-config-deploy** 日志，以确定 config-deploy pod 是否选取了更新的密钥值。

12 **config-deploy** pod 执行其任务后，群集将成功添加到 NetBackup 中，并且发现请求正在进行或已成功完成。从 NetBackup Web UI 执行另一个凭据验证和手动发现，以确保该过程正常工作。

在 NetBackup 中手动添加 Rancher 管理的 RKE 群集

请按以下步骤在 NetBackup 中手动添加 Rancher 管理的 RKE 群集。

为 NetBackup 创建 Kubernetes 凭据

导航到 NetBackup Web UI > “凭据管理” > “指定的凭据” > “添加” > “添加凭据” > 选择 NetBackup 作为凭据存储 > 在 “类别” 字段中选择 Kubernetes，输入之前从全局 Rancher 管理平台 UI 提取的令牌和 CA 证书，然后保存此凭据。

在 NetBackup 中手动添加 Rancher 管理的 RKE 群集

1 **外部 CA 证书**：如果使用不同的 CA（认证颁发机构）配置证书以进行外部访问，则 NetBackup 需要外部 CA 证书才能与群集成功通信。

- 导航到 **Rancher Management Server UI** > 打开左侧面板 **Global Settings** > 在 **cacerts** 下，单击 **showcacerts** 按钮。
  将此完整的 CA 证书值提取到临时文件
- 例如，`<cacert-value-file>`

2 **服务帐户 CA 证书**：

注意：必须执行以下步骤，因为与群集中可用的服务帐户 CA 证书相比，为 Kubernetes API 服务器的外部访问配置了不同的 CA（认证颁发机构）。因此，必须将这两个 CA 证书组合在一起。

要获取服务帐户 CA 证书，请在 Linux 群集主机上运行以下命令。

- 使用以下命令获取 Kubernetes Operator 命名空间中可用的服务帐户密钥名称：

```
kubectl describe serviceaccount <kopsnamespace>-backup-server
-n <kopsnamespace> | grep Tokens | cut -d ":" -f 2
```

- 使用以下命令从此服务帐户密钥获取 base64 解码格式的 CA 证书：

```
kubectl get secret <output-from-previous-command> -n
<kopsnamespace> -o jsonpath='{. data.ca\.crt}' | base64 -d
```

此命令的全部输出必须附加到步骤 1 中创建的临时文件。

3 将步骤 2 之后生成的输出附加到 `<cacert-value-file>` 文件末尾。已提取必要的外部和内部 CA 证书值，这些值在 **<cacert-value-file>** 文件中可用。CA 证书值是 base64 解码格式，在 NetBackup 上创建凭据时，必须再次对其进行编码。

4 令牌：**Rancher Management Server UI** > 打开左侧面板 > 在 **EXPLORE CLUSTER** 部分中 > 导航到要保护的群集 > 右上角的 **Kubeconfig** 图标。

- 将“令牌:”值（不带双引号 " "）从下载的 Kubeconfig 文件（使用 **Download KubeConfig**）提取到临时文件 **<token-value-file>**。
- 这两个字段 **token** 和 **cacert** 都需要采用 base64 编码格式，才能在 NetBackup for Kubernetes 中添加指定凭据。
- 使用以下 base64 命令获取这两个提取值的 base64 编码版本：

  #在此步骤中使用 Linux VM 对这些值进行编码 #注意：标志 -w0 具有数位 0，而不是符号 0。
  #对于 CA 证书：
  Cat <cacert-value-file>| base64 -w0
  将此输出粘贴到 NetBackup 凭据创建页面中的“CA 证书”字段中。
  #对于令牌：
  将此输出粘贴到 NetBackup Web UI 凭据创建页面的“令牌”字段中。

- 在 NetBackup Web UI >“**凭据管理**”>“**指定的凭据**”>“**添加**”中使用这些值，以在 NetBackup 中添加有效的 Rancher 凭据。
- 创建凭据后，使用以下群集信息输出中显示的名称在 NetBackup 中添加 Kubernetes 群集。

要获取群集信息输出，请运行以下命令

1 群集信息输出必须采用以下示例格式：`[root@master-0~] # kubectl cluster-info`

2 Kubernetes 控制面板运行于：
https://<rancher-hostname>/k8s/clusters/c-m-zjrfft56

3 CoreDNS 运行于：https://<rancher-hostname>/k8s/clusters/c-m-zjrfft56/api/v1/namespaces/kube-system/services/rke2-coredns-rke2-coredns:udp-53/proxy

4 从提到的输出中提取整个 API 服务器端点（包含 https://），其应采用以下模式：https://<rancher-hostname>/k8s/clusters/c-m-zjrfft56

5 在 NetBackup Web UI >“**工作负载**”> **Kubernetes** >“**Kubernetes 群集**”>“**添加群集**”中，添加整个 Rancher 群集名称。

6 在“**添加 Kubernetes 群集**”页面上，选择与 URL 或端点关联的选项，以允许基于端点（包含 https:// ）添加群集。

注意：不能编辑使用基于端点的方法添加的群集名称。只能删除和重新添加此类群集名称。

7 在 NetBackup Web UI 上的输入字段（端点或 URL ）中输入上述提取的群集信息输出。

8 继续操作，然后选择或创建步骤 1-4 中准备的凭据。

9 验证凭据并成功添加群集后，它将触发自动验证和发现。

10 在自动发现成功后，用户会尝试手动验证凭据并执行发现操作，以确保一切正常。

11 在 NetBackup 中添加 Rancher 管理的群集。

12 创建备份服务器证书密钥和数据移动器的 configmap，以设置从快照备份 (BFS) 功能。

然后，根据建议的设置指南继续执行其余配置步骤。

9

恢复 Kubernetes 资产

本章节包括下列主题：

浏览并验证恢复点

NetBackup 10.0 及更高版本支持使用从快照还原和从备份副本还原操作恢复 Kubernetes 资产。

注意：恢复后，新创建的命名空间、永久卷和其他资源将获取系统生成的新 UID。

NetBackup 通过 Kubernetes 工作负载中的备份副本状态（“完成”或“未完成”）帮助您执行备份映像验证。NetBackup 不允许从未完成的备份副本运行还原操作。

与 Kubernetes 命名空间对应的恢复点包含多个映像。恢复点可能未完成，因为某些映像的副本可能不可用。此类恢复点标记为“未完成”。

执行恢复点验证

1 在左侧，单击“**工作负载**”下的 **Kubernetes**

2 在“**命名空间**”选项卡中，单击要恢复的资产的命名空间。

3 单击“**恢复点**”选项卡。

4 “**恢复点**”选项卡显示所有恢复点以及备份的日期、时间和副本数。

单击恢复点旁边的“副本数”按钮，可查看位置、默认副本、副本类型和状态（是否完成）。

状态（是否完成）可帮助您验证选定的恢复点，以运行还原操作。

导致备份副本未完成的原因可能有多种：正在进行备份、映像失效、硬件故障或网络通信问题。

从快照还原

NetBackup 具有从快照还原功能，可以使用单个还原作业还原恢复点中的所有备份映像。可以在活动监视器中查看“从快照还原”作业。

从快照还原

1 在左侧，单击“**工作负载**”**> Kubernetes**。

2 在“**命名空间**”选项卡中，单击要恢复的资产的命名空间。

3 单击“**恢复点**”选项卡。

“**恢复点**”选项卡显示所有恢复点以及备份的日期、时间和副本数。可以设置过滤器来过滤显示的恢复点。单击“**日期**”列中的日期以查看恢复点的详细信息。“**恢复点详细信息**”对话框显示已备份的资源，如 ConfigMap、密钥、永久卷、pod 等。有关这些资源的详细信息，请参见 https://kubernetes.io/docs/reference/kubernetes-api/

4 找到要还原的恢复点。

5 在“**副本数**”列中，单击“**# 个副本**”按钮。例如，如果有两个副本，该按钮将显示为“**2 个副本**”。

6 在副本列表中，找到“**快照**”副本。然后单击“**操作**”**>**“**还原**”。

注意：通过选择“**允许选择受恶意软件影响的恢复点**”选项，为所有受感染副本启用“**还原**”选项。

---

7 在“**恢复目标**”页面中，目标群集是自动填充的。

注意：快照副本不支持备用群集还原。

---

8 在“**指定目标命名空间**”下，选择以下任一选项进行还原：

- 选择“**使用原始命名空间**”，可使用备份的原始命名空间进行还原。默认情况下，此选项处于选中状态。
- 选择“**使用备用命名空间**”，可使用备用命名空间进行还原，然后单击“**下一步**”。

9 在“**选择要恢复的资源类型**”下，选择以下任一资源类型进行还原：

- 选择“**所有资源类型**”，可恢复所有资源类型。默认情况下，此选项处于选中状态。
- 选择“**恢复所选的资源类型**”，可仅恢复所选的资源类型。

注意：“**选择要恢复的资源类型**”选项适用于高级用户。如果在选择要还原的资源时不够谨慎，还原后您可能无法获得命名空间的全部功能。

---

10 在“**选择要恢复的永久卷声明**”下，选择以下任一永久卷声明进行恢复：

- 选择“**所有永久卷声明**”，可恢复所有永久卷声明。默认情况下，此选项处于选中状态。
- 选择“**恢复所选的永久卷声明**”，可恢复所选的永久卷声明。

注意：如果未在“**恢复所选的资源类型**”中选择任何选项，则会选择“包括空的永久卷声明”选项，并且不会还原任何永久卷声明。

如果未在“**恢复所选的永久卷声明**”中选择任何选项，则在“**恢复选项**”部分中，将会包括空的永久卷声明，并且不会还原任何永久卷声明。

注意：“**仅还原永久卷**”可在所选的永久卷声明中进行切换，以便仅还原永久卷。此设置不会创建相应的永久卷声明。

---

11 单击“**失败策略**”部分，可查看要恢复的失败策略选项。

12 在“**选择失败策略以执行恢复**”下，选择以下任一失败策略进行恢复：

注意：如果在还原元数据或 PVC 期间出现失败，还原作业将根据所选的失败策略运行。

- 如果出现任何失败，选择“**快速失败**”终止还原。

- 选择“**继续**”，可继续还原下一个 PVC。如果父映像（第一个映像）还原失败，则还原作业将终止。
- 选择“**重试**”，可指定元数据或 PVC 还原的重试计数。如果即使在重试后还原仍失败，则还原作业将终止。

注意：“**活动监视器**”中将显示所选的失败策略。

13 单击“**下一步**”。

14 在“**恢复选项**”页面中，单击“**启动恢复**”以提交恢复条目。

15 在“**活动监视器**”中，单击“**作业 ID**”以查看还原作业详细信息。

注意：NetBackup Kubernetes 还原使用单个作业来还原所有永久卷声明和命名空间。可在“**活动监视器**”中查看日志，以跟踪永久卷、永久卷声明或元数据的还原。

从备份副本还原

如果所选命名空间中有多个 PVC，则使用 NetBackup 从备份还原将并行进行。启动还原时，作业将创建父-子层次（如果命名空间至少有一个 PVC 要还原）。父作业充当编排程序并监控子作业的状态。第一个子作业还原元数据，之后 PVC 将并行还原。

注意：如果元数据还原失败，则不会提交其他作业进行还原操作。成功还原元数据后，PVC 将批量并行还原。

可以按照“从快照还原”中所述的相同过程，选择“**备份**”作为副本类型。还可以还原到备用目标群集。

从备份副本还原

1 在左侧，单击“**工作负载**” **> Kubernetes**。

2 在“**命名空间**”选项卡中，单击要恢复的资产的命名空间。单击“**恢复点**”选项卡。

3 “**恢复点**”选项卡显示所有恢复点以及备份的日期、时间和副本数。可以设置过滤器来过滤显示的恢复点。单击“**日期**”列中的日期可查看恢复点的详细信息。“**恢复点详细信息**”对话框显示已备份的资源，如 `ConfigMap`、密钥、永久卷、pod 等。有关这些资源的详细信息，请参见 https://kubernetes.io/docs/reference。

4 找到要还原的恢复点。

5 在“**副本数**”列中，单击“**# 个副本**”按钮。例如，如果有两个副本，该按钮将显示为“**2 个副本**”。

6 在副本列表中，找到“**备份**”副本。然后单击“**操作**”**>**“**还原**”。

注意：通过选择“**允许选择受恶意软件影响的恢复点**”选项，为所有受感染副本启用“**还原**”选项。

---

7 在“**恢复目标**”页面中，将资产恢复到同一源群集，源群集是自动填充的。单击“**下一步**”。

8 在“**指定目标命名空间**”下，从以下选项中进行选择：

- 选择“**使用原始命名空间**”，可使用原始命名空间。
- 选择“**使用备用命名空间**”并输入备用命名空间。

  单击“**下一步**”。

9 在“**选择要恢复的资源类型**”下，从以下资源类型中进行选择：

- 选择“**所有资源类型**”，可恢复所有资源类型。
- 选择“**恢复所选的资源类型**”，可仅恢复所选的资源类型。

10 在“**选择要恢复的永久卷声明**”下，从以下选项中进行选择：

- 选择“**所有永久卷声明**”，可恢复所有永久卷声明。
- 选择“**恢复所选的永久卷声明**”，可恢复所选的永久卷声明。

注意：如果未在“**恢复所选的资源类型**”中选择任何选项，则会选择“包括空的永久卷声明”选项，并且不会还原任何永久卷声明。

如果未在“**恢复所选的永久卷声明**”中选择任何选项，则在“**恢复选项**”部分中，将会包括空的永久卷声明，并且不会还原任何永久卷声明。

注意：“**仅还原永久卷**”可切换所选的永久卷声明，以便仅还原永久卷。此设置不会创建相应的永久卷声明。

11 单击“**失败策略**”部分，可查看要恢复的失败策略选项。

12 在“**选择失败策略以执行恢复**”下，选择以下任一失败策略进行恢复：

注意：如果还原元数据或 PVC 时出现任何失败，还原作业将根据所选的失败策略运行。

- 如果出现任何失败，选择“**快速失败**”终止还原。
  - 此还原失败策略可帮助您在首次失败时终止还原作业。
  - 允许当前批处理中剩余的所有活动还原作业完成，并且不再提交其他批处理进行还原。
- 选择“**继续**”，可继续还原下一个 PVC。如果父映像（第一个映像）还原失败，则还原作业将终止。
  - 如果正在进行批处理的任何 PVC 还原失败，此策略可帮助您继续还原剩余的 PVC。
  - 如果元数据还原失败，最终作业将标记为失败，并且不会提交任何 PVC 进行还原。
  - 在这种情况下，标记为“部分成功”状态的最终作业和具有“失败”状态的 PVC 列表将显示在父作业的“**活动监视器**”选项卡中。
- 选择“**重试**”，可指定元数据或 PVC 还原的重试计数。如果即使在重试后还原仍失败，则还原作业将终止。
  - 此失败策略可帮助您重试失败的 PVC/元数据的还原作业，该策略在还原作业开始时进行配置。
  - 如果即使重试次数达到上限，还原作业仍失败，则该作业将标记为失败，并且不会再提交其他批处理进行还原。

注意：“**活动监视器**”中将显示所选的失败策略。

- 单击“**下一步**”。

13 单击“**启动恢复**”以提交恢复条目。

14 在“**活动监视器**”中，单击“**作业 ID**”以查看还原作业详细信息。

15 在“**作业详细信息**”页面上，单击“**详细信息**”选项卡。将显示还原作业顺序（还原前作业、数据移动作业和还原后作业）。

注意：可以取消父作业以取消还原操作。父作业将终止所有活动的子还原作业。

配置更改

并行 PVC 还原的批处理大小可在 bp.conf 中配置。用户可以在 `bp.conf` 文件中添加 `KUBERNETES_RESTORE_FROM_BACKUP_COPY_PARALLEL_RESTORE_BATCH_SIZE` 项，以设置所需的批处理大小。这是一个可选项，如果未定义，则其值为 5。

可为批处理大小分配的最小值为 1，而最大值为 100。

可以在 NetBackup 主服务器上使用 `bpsetconfig` 命令更新批处理大小。

10

关于增量式备份和还原

本章节包括下列主题：

对 Kubernetes 的增量式备份和还原支持

NetBackup Kubernetes 10.4 及更高版本在备份时支持使用差异式、累积式和自动备份日程表。

增量式备份显著缩短了 NetBackup 中的备份时段。在此方法中，NetBackup 仅备份自后续完全备份以来更改的数据。

增量式备份支持

增量式备份仅支持文件系统类型的永久卷。无论日程表类型为何，块类型的永久卷备份始终是完全备份。

注意：由于存储类限制，快照副本始终是完全备份。除了快照副本外，从快照备份、复制副本都支持增量式备份。

还原作业

从完整的恢复点还原将执行时间点还原。该恢复点之前的所有数据都将还原。

如果“**完整**”字段显示“**否**”，则无法从该恢复点进行还原。

映像链验证

将对恢复点副本执行映像链验证操作，且验证结果将反映在每个备份副本的恢复点的“**完整**”字段中。

当恢复点的所有相关映像都存在时，“**完整**”字段设置为“**是**”。

注意：如果增量式备份链不完整或映像组中缺少任何映像，则“**完整**”字段标记为“否”(Complete = No)。

自动映像同步复制 (A.I.R.) 限制

仅完全备份日程表备份作业支持 A.I.R.。差异增量式备份日程表、累积增量式备份日程表或自动备份日程表不支持 A.I.R. 功能。

从手动导入还原

手动导入的增量式映像可从有效恢复点 (Complete = Yes) 进行还原。

手动导入故障排除

手动导入后，如果恢复点标记为“**不完整**”，则映像链可能会因手动导入操作期间遗漏了映像而中断。

为手动导入操作重新创建映像链

1 打开文件 `/usr/openv/netbackup/logs/bpdbm/root{dateformat}.log` 并查找关于 **之前备份关系的行**. `To restore the relationship`，了解手动导入操作遗漏了哪些映像。

2 导入遗漏的映像，然后运行以下命令创建新的映像链。

```
`bpimage -update -id <backupid> -previous_backupid <previous
backup id>`
```

ctime 和 mtime 标志

NetBackup 客户端的 USE_CTIME_FOR_INCREMENTALS 选项：

- USE_CTIME_FOR_INCREMENTALS 条目可更改 NetBackup 确定文件是否已更改的方式。通过该条目，客户端软件可以在增量式备份期间使用修改时间和索引节点更改时间两者来确定文件是否已更改（mtime 和 ctime）。

NetBackup 客户端的 DO_NOT_RESET_FILE_ACCESS_TIME 选项：

- DO_NOT_RESET_FILE_ACCESS_TIME 条目指定在备份文件时，文件的访问时间 (Atime) 显示备份时间。默认情况下，NetBackup 保留访问时间。NetBackup 会重置备份的上一个值。
- 设置数据移动器属性：用户必须在 Kubernetes 群集上 NetBackupKOps 命名空间下创建的 NetBackup 主服务器特定 ConfigMap 中设置或更新标志。
- 示例：

```
apiVersion: v1
data:
  datamover.properties: |
```

```
    image=reg.domain.com/datamover/image:latest
    VERBOSE=5
    VXMS_VERBOSE=5
    USE_CTIME_FOR_INCREMENTALS=YES
    DO_NOT_RESET_FILE_ACCESS_TIME=YES
     version: "1"
kind: ConfigMap
metadata:
  name: backupserver.sample.domain.com
  namespace: <NetBackupKOps-Namespace>
```

保护计划

NetBackup Kubernetes 工作负载支持以下备份日程表。

- 自动
- 完全
- 差异增量式
- 累积增量式

具有不同日程表的保护计划可以按如下配置。

使用不同的日程表类型进行备份

1. 在保护计划中，选择备份类型（完全备份、差异增量式备份、累积增量式备份、自动备份）。
2. 在“配置快照的日程表”下，提供“循环”值和“快照保留”值。

   提供“从快照备份”保留期限的值。
3. 在“启动时段”选项卡中，设置日程表时间，然后单击“**添加**”。
4. 在“**日程表和保留**”部分下，单击“**添加日程表**”以在同一保护计划中添加多个日程表（差异增量式备份日程表、累积增量式备份日程表）。
5. 选择存储并按照剩余步骤运行备份作业。

自动日程表

- 对于自动类型日程表，在创建保护计划后，根据快照循环值确定日程表。
- 如果循环值小于一周，则创建一个差异式备份日程表和完全备份日程表。

建议

- 对于增量式备份日程表，遵循保护计划中“保留”值的建议。

  - 要对任何副本（快照、从快照备份、复制）执行从恢复点还原，建议将副本的保留持续时间设长一点。
  - 例如，要从备份副本还原，从快照备份的保留期限必须大于快照副本。否则，备份副本将失效，恢复点将标记为 `COMPLETE = NO`。
  - 在此类情况下，NetBackup Web UI 中将显示如下警告：
    - **建议将备份保留期限设置为大于快照保留期限。**
    - **建议将复制保留期限设置为大于备份保留期限。**
- 务必添加完全备份日程表和累积式备份日程表。否则，每个累积式备份都将作为完全备份执行。
- 默认情况下，对于增量式备份类型，始终启用“从快照备份”选项。

11

启用基于加速器的备份

本章节包括下列主题：

关于 Kubernetes 工作负载的 NetBackup 加速器支持

NetBackup 加速器缩短了 Kubernetes 群集备份的备份时间。

对于 Kubernetes 备份，选择支持加速器的存储类型时，将激活加速器功能。例如，MSDP、OpenStorage、CloudStorage 和 MSDP-C（Azure 和 AWS）以及支持“启用加速器”备份的 Kubernetes 群集。

注意：仅文件模式 PVC 支持已启用加速器的备份。

启用对特定 Kubernetes 群集的加速器支持

NetBackup Kubernetes Operator `values.yaml` 有一个条目

`acceleratorTracklogPvcStorageClass:` `None`

要启用加速器，请指定有效的存储类名称，以便为加速器备份生成跟踪日志。存储类可帮助创建一个文件模式卷，该卷可用于 Kubernetes 群集中的任何工作节点。

注意：如果 *acceleratorTracklogPvcStorageClass* 设置为 None 并且选择启用加速器的存储，则不会运行加速器备份作业。升级到 NetBackup 10.4 版本后，*acceleratorTracklogPvcStorageClass* 的默认值为 None。

有关更多详细信息，请参考《NetBackup for Kubernetes 管理指南》中的“验证加速器存储类”部分。

加速器跟踪日志存储类的资源限制和存储要求

- 每个 Kubernetes 群集的“从快照备份”作业数的默认值为 4。
- 如果 4 个采用加速器的“从快照备份”作业同时运行以备份 4 个 PVC，则这些作业会占用一些存储。
- 根据以下计算，每个 PVC 都需要一些空间来创建跟踪日志。跟踪日志大小（字节）= 2 *（（PVC 中的文件数 * 200）+（PVC 中已用磁盘总空间 (KiB/128KiB) * 20））
- 同时运行 4 个“从快照备份”作业所需的存储 = 4 个 PVC 的跟踪日志大小之和。

  因此，如果更改了每个 Kubernetes 群集的“从快照备份”作业数，则存储要求也会更改。
- 在运行备份作业之前，请确保有足够的存储可用。为避免存储问题，可以使用弹性存储。

备份流

NetBackup 加速器可创建备份流，如下所示：

- 如果命名空间没有任何先前备份，NetBackup 将执行完全备份。
- 对于下一个备份作业，NetBackup 将标识自上一次备份以来发生更改的数据。备份中仅包括已更改的块和标题的信息，用于创建完全备份。
- 备份完成后，数据移动器上的 bpbkar 将更新跟踪日志。数据移动器内的跟踪日志路径 - *usr/openv/netbackup/track/<primary server>/<storage server>/<k8s cluster name>_<namespace uuid>_<pvc uuid>/<policy>/<backup selection>*
- 然后，该跟踪日志将以内联方式传输到主服务器的以下位置：*/usr/openv/netbackup/db/track/<primary server>/<storage server>/<k8s cluster name>_<namespace uuid>_<pvc uuid>/<policy>/<backup selection>*
- 启动下一个加速器备份作业时，将从主服务器获取跟踪日志以标识更改的文件。然后，将使用新内容进行更新并传回主服务器。

控制主服务器上跟踪日志的磁盘空间

要继续执行已启用加速器的备份，NetBackup 预计会因处理跟踪日志而出现磁盘已满的情况。由于可用空间较少，主服务器上的加速器跟踪日志可能会成为一个问题。

默认情况下，如果系统上的可用空间少于 5 GB 或 5%，NetBackup 将阻止加速器备份。

NetBackup 提供了两个配置设置来控制主机上用于启动加速器备份的可用磁盘空间量：

- ACCELERATOR_TRACKLOG_FREE_SPACE_MB
- ACCELERATOR_TRACKLOG_FREE_SPACE_PERCENT

每个设置的默认值分别为 5120 MB 和 5%。要使备份在空间不足时快速失败，请在主服务器的 `bp.conf` 文件中配置这些值。

存储类行为对加速器的影响

存储类行为对加速器的影响如下所述：

- 对于已启用加速器的 Kubernetes 备份，NetBackup 根据更改的数据量显示优化建议。
  但是，完成后续加速器作业的持续时间可能与完成完全备份作业的持续时间相似。
- 发生这种情况的原因是存储类行为，即无论文件的数据或元数据是否更改，文件的 `INODE` 和 `CTIME` 都会更改。
- 这是由于存储类的内部实现造成的。有关更多详细信息，请参考客户门户站点上的 Red Hat 知识库文章：https://access.redhat.com/solutions/7036388

关于加速器强制的重新扫描

NetBackup“加速器强制的重新扫描”功能支持可防止备份映像损坏问题。当使用“加速器强制的重新扫描”时，将备份所选备份目标中的所有数据。

要执行“加速器强制的重新扫描”作业，请手动运行 `ForcedRescan` 命令。当使用“加速器强制的重新扫描”时，将备份所选备份目标中的所有数据。

此备份类似于首次为某个策略进行的加速器备份。该备份的持续时间类似于非加速器完全备份的持续时间。强制重新扫描可增强安全性，并为下一次加速器备份建立基线。此功能可防止任何潜在的损坏，如校验和验证失败。

有关使用强制重新扫描的建议：

- 要手动启动备份并强制重新扫描，请在命令提示符或Linux终端运行以下命令：
  `bpbackup -i -p <policy_name> -s ForcedRescan`
- 例如，
  `bpbackup -i -p msdp_10mins_FRS+5d990ab5-f791-474f-885a-ae0c30f31c98 -s ForcedRescan`
  可以使用以下 API 启动强制重新扫描日程表：
  `POST admin/manual-backup`

加速器备份失败的警告和可能原因

警告	消息	推荐的操作
此 NetBackup 介质服务器版本不支持 Kubernetes 加速器备份功能，将执行未加速的备份。	介质服务器版本低于 10.4。	将介质服务器升级到 10.4 或更高版本。
由于客户端版本较低或客户端上未配置跟踪日志 PVC 的存储类，导致客户端不支持加速器。但是，客户端将执行未加速的备份。	NetBackup Kubernetes Operator 版本低于 10.4，或者客户端上未配置跟踪日志 PVC 的存储类。	将 NetBackup Kubernetes Operator 和数据移动器升级到 10.4 或更高版本。 确保在 Kubernetes Operator 中正确配置了跟踪日志 PVC 的存储类。

12

在 Kubernetes 中启用 FIPS 模式

本章节包括下列主题：

在 Kubernetes 中启用联邦信息处理标准 (FIPS) 模式

NetBackup Kubernetes 10.3 版本为基于 RedHat 的 NetBackup 部署提供 FIPS 支持。NetBackup、Kubernetes Operator 和数据移动器中涉及的所有 Kubernetes 工作负载组件都必须在 FIPS 模式下运行。要实现 FIPS 支持，所有这些组件都需要满足某些要求。

系统要求

以下是在 NetBackup Kubernetes 工作负载中实现 FIPS 支持需满足的系统要求。

名称	参数

NetBackup 主服务器和介质服务器	■ 主服务器和介质服务器必须部署在 NetBackup 10.2.1 上，该版本具有已启用 FIPS 的基础 RHEL-8 系统。
	■ RHEL 操作系统版本必须高于 RHEL 8。
	■ 可以使用以下命令检查 RedHat 计算机的版本：
	`cat /etc/Redhat-release`
	■ 可以使用以下命令检查基础系统是否已启用 FIPS：
	`FIPS-MODE-SETUP--CHECK`
	■ 有关更多详细信息，可以使用以下命令检查手册页条目：
	`fips-mode-setup`

名称	参数
Kubernetes 群集	■ 必须在启用 FIPS 的模式下部署 Kubernetes 群集。 ■ 在 FIPS 模式下部署 Kubernetes 群集的过程与供应商相关。 ■ 例如，在启用 FIPS 的情况下部署 Openshift

配置参数

以下是 NetBackup Kubernetes 工作负载中 FIPS 模式的配置参数。

配置	参数
NetBackup 主服务器和介质服务器	启用 NetBackup 进程以在 FIPS 模式下运行： ■ 使用以下密钥更新 <Netbackup-Installation-Path>/netbackup/bp.conf：*NB_FIPS_MODE = ENABLE* ■ 有关 FIPS 模式下 NetBackup 的更多信息，请参考《NetBackup™ 安全和加密指南》中的“在 NetBackup 域中配置 FIPS 模式”部分
NetBackup Kubernetes Operator	执行以下任一操作以启用 FIPS 模式： ■ 在 Helm Chart 的 values.yaml 文件中将 **fipsMode** 参数的值更新为 **ENABLE**。 ■ 在 backup-operator 中将 **NB_FIPS_MODE** 参数的值更新为 **ENABLE**。

注意：确保运行 NetBackup Kubernetes 工作负载的所有系统都符合 FIPS 标准。

FIPS 故障排除

对自动映像同步复制 (AIR) 操作的影响：

- 对于启用了 FIPS 的环境中的 AIR，您需要执行其他配置。
- 在支持站点上更新 <KB-Article>。
- 在命令行界面 (CLI) 中运行以下命令：

```
/usr/openv/java/jre/bin/keytool/keytool -storetype BCFKS
-providerpath
/usr/openv/wmc/webserver/lib/ccj-3.0.1.jar -providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvider
-importcert -trustcacerts -file <target CA certificate file (pem
encoded)> -keystore
```

```
NB_INSTALL_DIR/var/global/wsl/credentials/cacerts.bcfks -storepass
<password from the /usr/openv/var/global/jkskey file>
-alias <alias name of the trusted certificate entry to be added>
```

13

对 Kubernetes 问题进行故障排除

本章节包括下列主题：

主服务器升级期间出错：NBCheck 失败

NetBackup 主服务器从 9.1 版升级到 10.0 版失败，并出现非关键 NBCheck 错误。

错误消息：该测试发现了 {{no. of policies}} 个活动的 Kubernetes 策略。如果 NetBackup 实例有任何活动的 Kubernetes 策略，则此测试失败。

推荐的操作：在将 NetBackup 升级到 10.0 版本之前，停用主服务器上的所有活动 Kubernetes 策略。

有关更多详细信息，请参见 https://www.veritas.com/content/support

旧映像还原期间出错：操作失败

对于使用 NetBackup 9.1 版本创建的较旧映像，Kubernetes 还原操作失败。

错误消息：低于 10.0 版的 NetBackup 的备份映像不支持还原操作。

推荐的操作：使用 Velero 命令还原较旧映像。Velero 是一个开源工具，用于安全地进行备份和还原、执行灾难恢复以及迁移 Kubernetes 群集资源和永久卷。因此，要从 Velero 还原旧映像，前提条件是在群集中进行安装。

从 NetBackup 管理员 Web UI 获取备份名称/备份 ID，并在 Velero 命令中使用它以进行还原。

有关更多详细信息，请参见 https://www.veritas.com/content/support

永久卷恢复 API 期间出错

在 NetBackup Kubernetes Operator 10.0 版上，永久卷恢复 API 已删除且不受支持。在较旧版本的 NetBackup 上，此 API 用于还原永久卷。因此，如果已升级 NetBackup 10.0 版，并使用永久卷恢复 API 进行还原，则还原操作将失败。

错误消息：由于重新设计了 NetBackup Kubernetes 恢复过程，Kubernetes 永久卷恢复 API 不再使用，并且已从产品中删除。

推荐的操作：在 NetBackup Kubernetes Operator 10.0 版中，升级 NetBackup 以从备份中恢复选定的资源。因此，如果要恢复永久卷或永久卷声明，则可以从 NetBackup 中选择永久卷并恢复到目标命名空间。

有关更多详细信息，请参见 https://www.veritas.com/content/support

还原期间出错：最终作业状态显示部分失败

最终还原作业状态为部分失败，并出现一些特定于资源 RoleBinding 的警告。

对于 API 组 `groupauthorization.openshift.io` 和 `rbac.authorization.Kubernetes.io`，显示了特定于资源 RoleBinding 的警告。因为 RoleBinding 是使用控制器自动管理的，并且是在我们创建新命名空间时创建的。

推荐的操作：可以从还原中排除相关的 RoleBinding 资源，或忽略生成的警告。

在同一命名空间上进行还原时出错

如果所选 PVC 已存在于命名空间中，则在原始命名空间上还原 PVC 可能会失败。

推荐的操作：

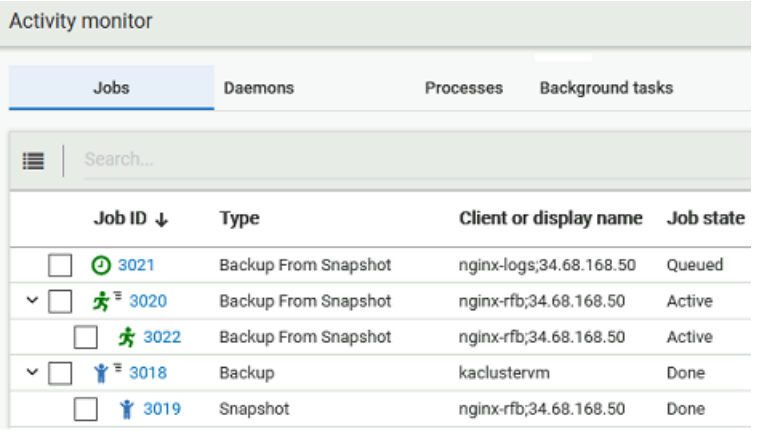
- 可以使用备用命名空间进行还原
- 运行还原操作时，可以在“**恢复选项**”中选择不与现有 PVC 重叠的 PVC。

datamover pod 超过 Kubernetes 资源限制

NetBackup 使用两个资源限制属性控制 Kubernetes 工作负载上正在进行的备份作业总数。在 NetBackup 10.0 版中，datamover pod 超出了为每个 Kubernetes 群集设置的“**备份**”和“**从快照备份**”资源限制。

以下是资源限制问题的示例

情形 1



每个 Kubernetes 群集的从快照备份作业的资源限制设置为 1。

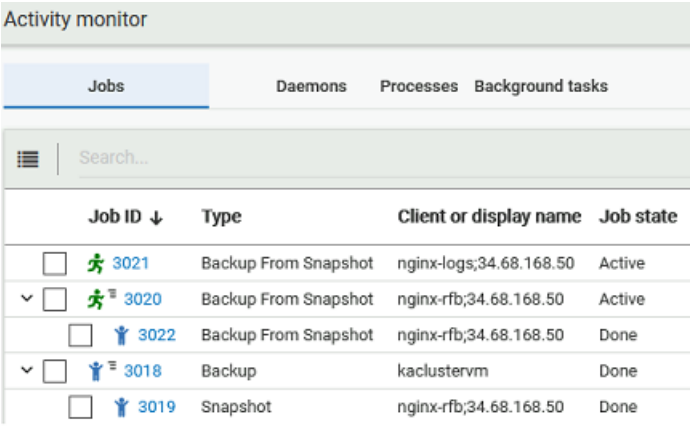
作业 ID 3020 和 3021 是从快照备份的父作业。datamover pod 创建及其清理过程是备份作业生命周期的一部分。

作业 ID 3022 是子作业，其中数据从群集移动到存储单元。

根据资源限制设置，当作业 ID 3022 处于正在运行状态时，作业 ID 3021 将继续处于排队状态。备份作业 ID 3022 完成后，父作业 ID 3021 将启动。

请注意，作业 ID 3020 仍在进行中，因为我们正在清理 datamover pod 并完成父作业 ID 3020 的生命周期。

情形 2



在此阶段，我们可能会遇到 2 个 datamover pod 在 NetBackup Kubernetes Operator 部署命名空间中同时运行。因为作为作业 ID 3020 的一部分创建的 datamover pod 仍未清理，但我们已经开始为作业 3021 创建 datamover pod。

在触发了多个从快照备份作业的繁忙环境中，较低的资源限制值设置可能会导致备份作业大部分时间处于排队状态。

但是，如果资源限制设置较高，我们可能会发现 datamover pod 可能会超过资源限制中指定的计数。这可能会导致 Kubernetes 群集中出现资源匮乏。

当数据移动作业（如 3022）并行运行时，会按顺序处理清理活动。数据移动所需的时间加上清理 datamover 资源所需的时间，如果比较接近备份 PVC/命名空间数据所需的时间，则将导致作业完成时产生较长的延迟。

如果数据移动和清理资源的总持续时间接近备份作业的时间。然后，永久卷或命名空间数据的备份作业可能会导致作业完成产生延迟。

推荐的操作：确保查看系统资源和性能，并相应地设置资源限制值。此措施将有助于所有备份作业实现最佳性能。

还原期间出错：高负载群集上的作业失败

负载较重的 Kubernetes 群集上的还原作业失败。

错误消息：ERR - Unable to initialize VxMS, cannot write data to socket, Connection reset by peer.

Error bpbrm (pid=712755) from client cluster.sample.domain.com: ERR - Unable to initialize VxMS.

Error bptm (pid=712795) cannot write data to socket, Connection reset by peer.

推荐的操作：如果在还原操作期间遇到此问题，则应在负载较轻的群集上或在群集空闲时运行还原操作。

为特定群集创建的自定义 Kubernetes 角色无法查看作业

为具有特定 Kubernetes 群集的 Kubernetes 工作负载创建自定义 RBAC 角色时，系统管理员必须明确提供查看 Kubernetes 作业的权限，否则所有 Kubernetes 特定作业都将不可见。

如果系统管理员未提供查看 Kubernetes 作业的权限，则用户可以查看以下作业：

- 仅层次结构视图中的还原作业。
- 仅列表视图中的快照和还原作业。

如果创建的自定义 Kubernetes 角色无法查看特定 Kubernetes 群集的作业。然后，执行以下步骤以提供查看权限。

提供查看权限

1 在左侧，单击“**工作负载**”下的 **Kubernetes**。

2 在右侧，单击“**Kubernetes 设置**”>“**管理权限**”。

3 单击相应角色旁边的纵向省略号，然后选择“**编辑**”。

4 在“**编辑权限**”中，选择角色的“**编辑**”和“**查看作业**”权限，然后单击“**保存**”。

Kubernetes 自定义角色用户将能够在层级视图和列表视图中查看备份、快照、还原和从快照备份作业。

假设：

- 如果已升级设置，则用户可以查看以下内容：
  - 仅现有作业的层次结构视图中的还原作业。
  - 仅现有作业的列表视图中的快照和还原作业。
- 如果创建的 Kubernetes 自定义角色具有所选 Kubernetes 群集的权限，则用户只能**取消**和**重新启动**快照作业上的操作。

从 OperatorHub 还原安装的应用程序时，Openshift 会创建空白非选定的 PVC

在 Openshift 环境中，通过 OperatorHub 目录库源安装应用程序。当用户尝试从此类应用程序命名空间的备份执行选择性 PVC 还原时，反而会创建所有 PVC。

出现此问题是因为，Openshift 环境会在目标命名空间中置备非选定的 PVC，并设置所需的大小。

注意：对于此类应用程序，PVC 会根据部署配置自动置备，即使用户未选择它们进行还原也是如此。

如果超过 Kubernetes 节点上的 PID 限制，NetBackup Kubernetes Operator 将变得无响应

在 Linux 系统中，有一个以 PID 1 身份运行的 initd 或系统进程来接收僵尸进程。没有此类 initd 进程的容器会不断生成僵尸进程。

在一定的时间段后，这些僵尸进程会累积，然后达到在 Kubernetes 节点上设置的 PID 的最大限制。

在 NetBackup Kubernetes Operator 中，nbcertcmdtool 会生成子进程以执行证书相关操作。操作完成后，这些进程将变为孤儿进程，并且不会被接收。最终达到最大 PID 限制，NetBackup Kubernetes Operator 变得无响应。

Error message: login pod/nbukops-controller-manager-67f5498bbb-gn9zw -c netbackupkops -n nbukops ERRO[0005] exec failed: container_linux.go:380: starting container process caused: read init-p: connection reset by peer a command that is terminated with exit code 1.

推荐的操作：

- 要解决超过 PID 限制的问题，可以使用 Initd 脚本。Initd 脚本充当控制器 pod 的父进程或入口点脚本。
  作为父进程，它在子进程完成后将僵尸进程附加到自身，以终止持久性僵尸进程。它还帮助您正常关闭容器。Initd 脚本在 NBUKOPs 内部版本 10.0.1 中可用。
- 使用以下步骤删除现有的 nbcertcmdtool 僵尸进程：

1. 描述 NetBackup Operator pod 并找到正在运行控制器 pod 的 Kubernetes 节点。运行命令：

   ```
   kubectl describe -c netbackupkops <NB k8s operator pod name> -n
   <namespace>
   ```

2. 登录到 Kubernetes 节点，运行以下命令：

   ```
   kubectl debug node/nodename
   ```

3. 终止 nbcertcmdtool 僵尸进程，运行以下命令：

   ```
   ps -ef | grep "\[nbcertcmdtool\] <defunct>” | awk '{print $3}'
   | xargs kill -9
   ```

注意：这些步骤将终止该工作节点的所有僵尸进程，但会暂时解决这个问题。要获得永久解决方案，必须部署带有 Initd 脚本的新 KOps 内部版本。

在 NetBackup Kubernetes 10.1 中编辑群集时失败

Kubernetes 编辑群集操作存在问题，在 NetBackup Kubernetes 10.1 版本中不起作用。

推荐的操作：要编辑群集，必须先从保护计划中删除 Kubernetes 群集，然后再添加群集。

对于大型 PVC，备份或还原失败

对于大型 PVC，如果未在配置的轮询超时中绑定 PVC，则从快照备份和从快照还原/从备份还原将失败。出现此问题是因为，大型卷快照水化所用的时间超过默认超时值（15 分钟）。

从快照备份

对于大型 PVC（例如：1.5 TB），从快照备份失败，错误代码为 34

错误消息：

Error nbcs (pid=250908) failed to setup the data mover instance for tracklog pvc operation.

Error nbcs (pid=250908) unable to initialize the tracklog data mover instance, data mover pod status: Pending reason:Failed message:Error: context deadline exceeded.

从快照还原或从备份还原

对于大型 PVC（例如：100 GB），从快照还原失败，错误代码为 5

错误消息：

Error nbcs (pid=29228) timeout occurred while waiting for the persistent volume claim pvc-sample status to be in the bound phase

推荐的操作：

在备份 Operator **configmap** 中增加轮询超时。

- **Configmap 名称**：<kops-name>-backup-operator-configuration
- **要更新的项**：pollingTimeoutInMinutes

将命名空间文件模式 PVC 还原到不同文件系统时部分失败

将命名空间文件模式 PVC 还原到不同文件系统会使得命名空间卷部分成功。在这种情况下，将文件系统对象（文件/目录）还原到源文件系统以外的其他文件系统会导致还原失败，因为元数据不兼容。因此，此操作显示为部分成功的还原。

Error message: 7:38:57 AM - Error bpbrm (pid=30171) client restore EXIT STATUS 1: the requested operation was partially successful.

推荐的操作：查看目标文件系统，其中显示已就绪的文件。由于文件已还原，数据没有实际问题。此部分失败以警告形式进行报告，指出元数据还原存在问题，操作员必须意识到这一点。

从备份副本还原失败并显示映像不一致错误

将旧版介质服务器用于存储时，从备份副本还原失败并显示映像不一致错误。例如：用于存储的介质服务器版本低于 10.1.1，用于从备份副本还原的 NetBackup 版本为 10.1.1。

Error message: Sep 22, 2022 3:12:55 PM - Info tar (pid=1459) done. status: 229: events out of sequence - image inconsistency Sep 22, 2022 3:12:55 PM - Error bpbrm (pid=16523) client restore EXIT STATUS 229: events out of sequence - image inconsistency

推荐的操作：对于包含所有 Kubernetes 工作流程的基于 Kubernetes 文件系统的备份，必须始终使用主服务器、介质服务器和 NetBackup Kubernetes Operator 版本 10.1.1。

NetBackup 主服务器、介质服务器和 Kubernetes 服务器之间的连接检查。

要检查 NetBackup 主服务器与其他主机之间的连接，可以参考以下命令。

- 打开所需端口以方便与 NetBackup 主服务器通信后，可以运行以下命令。
- 要检查 NetBackup 主服务器/介质服务器与 Kubernetes 群集之间的连接，请从 Kubernetes Operator pod 运行以下命令。

  ```
  curl -v telnet://<netbackup-server-host>:<port-no>
  ```

- 要检查 NetBackup 主服务器与 Kubernetes 群集之间的连接，请从 NetBackup 主服务器主机运行以下命令。

  ```
  curl -v telnet://<kubernetes-api-server-host>:<port-no>
  ```

注意：对这两个命令的响应必须表明已成功建立连接。

没有可用于跟踪日志的空间时，加速器备份过程中出错

如果没有足够的空间来存储跟踪日志，则“从快照备份”作业将失败，并显示错误“套接字写入失败 (24)”。

错误消息：存在重复，状态码为 24（套接字写入失败）。

推荐的操作：存储跟踪日志的路径上必须有足够的存储空间，才能成功运行备份作业。

由于跟踪日志 PVC 创建失败导致加速器备份期间出错

如果在创建跟踪日志 PVC 时出现错误，则“从快照备份”作业将失败。跟踪日志 PVC 创建可能会因以下多种原因而失败：

- 提供的存储类无效。
- 没有足够的空间可用于 PVC 创建。

推荐的操作：

- 检查是否有足够的空间可用于创建具有所需大小的 PVC。
- 检查 Kubernetes 群集上是否正确配置了存储类。

由于加速器存储类无效导致加速器备份期间出错

如果为加速器备份作业提供的存储类无效，则跟踪日志 PVC 创建将失败。等待 PVC 状态到达绑定阶段时出错。

错误消息：StorageClass.storage.k8s.io cstor-storage-class-x2 not found

Jan 11, 2024 2:12:54 AM - Error nbcs (pid=92639) StorageClass.storage.k8s.io cstor-storage-class-x2 not found

推荐的操作：在备份操作员 configmap 中提供有效的存储类，然后重新运行备份作业。

启动跟踪日志 pod 时出错

错误消息：无法初始化跟踪日志数据移动器实例。

推荐的操作：使用 describe 命令检查 Kubernetes 群集上的 pod 创建日志，获取错误详细信息。

设置跟踪日志 PVC 操作的数据移动器实例失败

错误消息：无法获取跟踪日志数据移动器 pod 状态和事件。

推荐的操作：使用 describe 命令检查 Kubernetes 群集上的 pod 创建日志，获取错误详细信息。

从 configmap 读取跟踪日志存储类时出错

错误消息：无法获取跟踪日志的存储类。

推荐的操作：检查是否正确配置了 NetBackup Kubernetes Operator。