NetBackup™ Web UI Kubernetes 管理指南

版本 **10.1**

VERITAS™

上次更新时间： 2022-10-28

法律声明

Veritas Technologies LLC
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 Veritas 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 Veritas 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 Veritas 社区站点中查看相关文档信息或进行提问：

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

Veritas Services and Operations Readiness Tools (SORT)

Veritas 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。
- 还原命名空间和永久卷。
- 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
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。
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。 ■ 使用“从备份副本还原”还原为不同的 Kubernetes 群集风格。
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。

2

部署和配置 NetBackup Kubernetes Operator

本章节包括下列主题：

在 NetBackup Kubernetes Operator 上部署服务软件包

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 -k -fsSL -o get_helm.sh https://raw.githubusercontent.com/helm
2. #chmod +x get_helm.sh
3. #./get_helm.sh

必须在要部署 NetBackup 的每个群集中部署 Operator。

配置 Helm Chart

可使用 Helm Chart 部署 NetBackup Kubernetes Operator。

注意：由于不支持 Helm Chart 升级，因此必须安装新的 NetBackup 插件 Helm Chart。

安装新插件之前，必须卸载较旧的插件。

安装新的 Helm Chart

1 要卸载较旧的插件，请运行以下命令：

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

2 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
    └── values.yaml
```

目录结构：

```
tar --list -f netbackupkops-10.0.tar.gz
veritas_license.txt
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/development.yaml
netbackupkops-helm-chart/Charts/
```

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

1 从 Veritas 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 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
```

7 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：

```
docker load -i <name of the tar file>./

docker tag <image name:tag of the loaded image>

<repo-name/image-name:tag-name>

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

8 在文本编辑器中打开 `netbackupkops-helm-chart/values.yaml` 文件，然后将 *manager* 部分中的 *image* 值替换为映像名称和标记 *repo-name/image-name:tag-name*，并保存文件。

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。

源	端口号	目标
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

无法使用 Helm 命令升级 NetBackup Kubernetes Operator 部署。

删除 NetBackup Kubernetes Operator

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

由于无法从较旧版本升级 NetBackup Kubernetes Operator 部署，您可以安装较新版本并删除较旧版本。

删除 NetBackup Kubernetes Operator 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。

在手动删除较旧的快照之前，不要删除关联的 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。

配置 NetBackup Kubernetes datamover

需要为 NetBackup Kubernetes 工作负载配置 datamover。从下载中心为您的发行版本下载正确版本的 datamover 映像：

`veritasnetbackup-datamover-10.0-0070.tar`。请参见 https://www.veritas.com/content/support

配置 datamover

1 要将 datamover 映像推送到 docker 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>`

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>*。

有关 configmap 的更多详细信息，请参见第 16 页的"从快照备份和从备份还原操作的前提条件"一节。

配置 NetBackup 快照操作的设置

在实际执行从快照备份操作之前，需要在 Kubernetes Operator 部署上配置快照操作。

1. 定义指向 CSI 插件的存储类。
2. 定义包含 CSI 驱动程序详细信息的 *VolumeSnapshotClass* 类。
3. 标记卷快照类以供 NetBackup 使用。添加以下标签 *netbackup.veritas.com/default-csi-volume-snapshot-class=true*。

注意：包含永久卷的命名空间的快照操作失败，并显示错误消息：*无法创建 Kubernetes 命名空间的快照*。

快照操作可能会由于多种原因而失败，例如，找不到带有 *volumesnapshotclass* 标签的驱动程序的有效卷快照类。

---

4. 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。

   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。

注意：要获取配置值，可以运行以下命令：`kubectl get configmaps <namespace>-backup-operator-configuration -n <namespace> -o yaml > {local.file}`

表 2-2 <namespace>-backup-operator-configuration 中受 Kubernetes Operator 支持的配置参数

配置	描述	默认值	可能的值
DaemonSets	Daemonset 是 Kubernetes 中的动态对象，由控制器管理。可以设置期望状态，该状态表示需要存在于每个节点上的特定 pod。控制循环中的 pod 调谐可将当前实际状态与期望状态进行比较。	true	true、false

配置	描述	默认值	可能的值
Deployments	Kubernetes 工作负载的部署。	true	true、false
Pods	pod 是 Kubernetes 中最小的执行单元。	true	true、false
ReplicaSets	副本集可确保应运行的 pod 副本数。可以将其视为复制控制器的替代品。	true	true、false
Secrets	密钥是包含敏感数据（如密码、令牌和凭据）的对象。	true	true、false
Services	Kubernetes 中提供的服务。	true	true、false
namespace	Kubernetes Operator 是在命名空间中部署的。	为命名空间指定的任何名称。	NetBackup 命名空间。
cleanStaleCRDurationMinutes	调用 CR 作业以清理无效 CR 的持续时间。触发无效自定义资源清理作业的间隔。	24 小时	1440 分钟
ttlCRDurationMinutes	TTL CR 持续时间	分钟	30240 分钟
livesnessProbeInitialDelay	探测初始延迟期。	分钟	60 分钟
livenessProbePeriodSeconds	探测期限。	秒	80 秒
checkNbcertdaemonStatusDurationMinutes	NB 证书后台驻留程序状态持续时间。	分钟	1440 分钟

配置	描述	默认值	可能的值
collectDataMoverLogs	由于 datamover 日志收集的内存使用率很高，建议仅在调试、故障排除或重新启动 pod 时启用日志。 在为 datamover 启用日志之前，请确保将 NetBackup Kubernetes pod 的内存限制增加到至少 2 GB 或更多。调试或故障排除完成后，可以重置为之前的值或默认值。 **注意：**仅在作业失败的情况下为收集 datamover 日志提供粒度支持。它提供了一个额外的粒度层级别 All/FailedOnly/Off。	Failed	All, Failed, None
maxRetentionDataMoverLogsInHours	datamover 日志的最大保留期限。	24 小时	72 小时
maxRetentionDataMoverInHours	它会删除超过指定时间的所有 datamover 资源。	24 小时	24 小时
cleanStaleCertFilesDurationMinutes	触发无效证书文件清理作业的间隔。	60 分钟	1440 分钟
maxRetentionInDiscoveryCacheHours	该时间（以小时为单位）决定了保留发现缓存的时间间隔。	24 小时	48 小时
pollingTimeoutInMinutes	轮询操作不断重试，超过该超时值后，操作失效并且失败。	15 分钟	15 分钟
pollingFrequencyInSecs	轮询频率。	秒	5 秒
nbcertPrerequisteDirectoryAndFiles	NBCA 前提条件。	证书名称	证书名称

从快照备份和从备份还原操作的前提条件

1. 标记有效的存储类以供 NetBackup 使用，添加以下标签：*netbackup.veritas.com/default-csi-storage-class=true*。如果未找到 NetBackup

标记的存储类，则元数据映像的从快照备份作业和还原作业将失败，并显示错误消息：*No eligible storage classes found*。

要标注存储类，请运行示例中提供的以下命令：

示例 1. 运行以下命令：`# oc get sc`

名称	置备程序
ocs-storagecluster-ceph-rbd（默认值）	openshift-storage.rbd.csi.ceph.com
ocs-storagecluster-ceph-rgw	openshift-storage.ceph.rook.io/bucket
ocs-storagecluster-cephfs	openshift-storage.cephfs.csi.ceph.com
openshift-storage.noobaa.io	openshift-storage.noobaa.io/obc
thin	kubernetes.io/vsphere-volume

回收策略	卷绑定模式	允许卷扩展	时间
删除	立即	True	2d2h
删除	立即	False	2d2h
删除	立即	True	2d2h
删除	立即	False	2d2h
删除	立即	False	19h

示例 2. 运行以下命令：`# oc get sc ocs-storagecluster-ceph-rbd --show-labels`

名称	置备程序	回收策略
ocs-storagecluster-ceph-rbd（默认值）	openshift-storage.rbd.csi.ceph.com	删除

卷绑定模式	允许卷扩展	时间	标注
立即	True	2d2h	netbackup.veritas.com/default-csi-storage-class=true

示例 3. 运行以下命令：`# oc label sc ocs-storagecluster-cephfs netbackup.veritas.com/default-csi-storage-class=true`

storageclass.storage.k8s.io/ocs-storagecluster-cephfs labeled

示例 4. 运行以下命令：`oc get sc ocs-storagecluster-cephfs --show-labels`

名称	置备程序	回收策略
ocs-storagecluster-cephfs	openshift-storage.cephfs.csi.ceph.com	删除

卷绑定模式	允许卷扩展	时间	标注
立即	True	2d2h	netbackup.veritas.com/default-csi-storage-class=true

2. 标记有效的卷快照类以供 NetBackup 使用，添加以下标签：*netbackup.veritas.com/default-csi-volume-snapshot-class=true*。如果未找到 NetBackup 标记的 *VolumeSnapshotClass* 类，则元数据映像的从快照备份作业和还原作业将失败，并显示错误消息：*无法创建 Kubernetes 命名空间的快照*。

   要标注卷快照类，请运行示例中提供的以下命令：

   示例 1. 运行以下命令：`# oc get volumesnapshotclass`

名称	驱动程序
ocs-storagecluster-cephfsplugin-snapclass	openshift-storage.cephfs.csi.ceph.com
ocs-storagecluster-rbdplugin-snapclass	openshift-storage.rbd.csi.ceph.co

删除策略	时间
删除	2d2h
删除	2d2h

   示例 2. 运行以下命令：`# oc get volumesnapshotclass ocs-storagecluster-cephfsplugin-snapclass --show-labels`

名称	驱动程序
ocs-storagecluster-cephfsplugin-snapclass	openshift-storage.cephfs.csi.ceph.com

删除策略	时间
删除	2d2h

示例 3. 运行以下命令：`# oc label volumesnapshotclass ocs-storagecluster-cephfsplugin-snapclass netbackup.veritas.com/default-csi-volume-snapshot-class=true`

volumesnapshotclass.snapshot.storage.k8s.io/ocs-storagecluster-cephfsplugin-snapclass labeled

示例 4. 运行以下命令：`# oc get volumesnapshotclass ocs-storagecluster-cephfsplugin-snapclass --show-labels`

名称	驱动程序
ocs-storagecluster-cephfsplugin-snapclass	openshift-storage.cephfs.csi.ceph.com

删除策略	时间	标签
删除	2d2h	netbackup.veritas.com/default-csi-volume-snapshot-class=true

3. 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。
   - 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。

4. 使用正确的 datamover 映像指定 `datamover.properties: image=reg.domain.com/datamover/image:latest`。
5. 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 datamover 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。
6. 按照“在 NetBackup Kubernetes Operator 上部署服务软件包”部分的第 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
7. 要创建 `configmap.yaml` 文件，请运行以下命令：`kubectl create -f configmap.yaml`。
8. 如果 Kubernetes Operator 无法根据短名称解析主服务器
   - 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，验证主机名解析状态。
   - 如果主机名解析失败，则执行以下操作：
     更新 *kops 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。

注意：hostAliases 部分必须添加到默认 `./netbackupkops-helm-chart/templates/deployment.yaml` 文件的第 2104 行。

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}}
```

9. 使用指纹和授权令牌创建密钥。
10. 创建 backupservercert 请求以获取证书。

    有关更多信息，请参考《NetBackup™ 安全和加密指南》。

Kubernetes 工作负载中支持的 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《Veritas 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 2-3 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

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
```

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 datamover 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创建 *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，请运行以下命令：`kubectl create -f ConfigMap.yaml`。

管理映像组

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）。

关于映像失效

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。

关于映像导入

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

关于映像副本

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”。

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。

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，需要 CA 证书和令牌。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-token-<id>> -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。

设置 Kubernetes 资源限制

使用此设置，可以控制可在 Kubernetes 群集上同时执行的备份数。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。

例如，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，则只有五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。

例如，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。
  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**”。
  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**”。
- 必须手动输入群集名称，然后输入限制值。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。

有关更多详细信息，请参见第 68 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，并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，单击群集所在行的“操作”菜单（纵向省略号），然后单击“**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，所有后续发现都将是增量发现。

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。

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**”。

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

具有以下注意事项和限制：

- 在智能组创建的查询生成器中，第一个标签条件必须已定义[标签键]和[值]。
- 在后续条件中，可以定义[标签键]条件，也可以定义[标签键加值]条件
- 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。

配置自动映像复制 (AIR) 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 域中的存储。此过程称为自动映像复制 (AIR)。

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。

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

注意：Kubernetes AIR 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 备份配置自动映像复制 (AIR) 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。
  - 从“**主机**”选项卡中选择源主服务器，然后单击“**连接**”。
  - 单击“**编辑主服务器**”>“**服务器**”>“**可信主服务器**”>“**添加**”，以添加源服务器。
    - 单击“**验证证书颁发机构**”按钮，然后单击“**下一步**”继续进行证书颁发机构验证。
    - 有两个选项可以创建可信主服务器，请执行以下任一操作：
      - 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**”>“**存储配置**”
- 添加 MSDP 存储和磁盘池。
- 单击“**磁盘池**”>“**添加**”，以添加复制目标。
  - 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**”>“**+ 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**”。
- 在“**新建操作**”>“**属性**”>“**操作**”中，从列表中选择“**导入**”选项。
- 在“**目标存储属性**”>“**目标存储**”中，从列表中选择一个 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 **Kubernetes** 工作负载 >“**保护计划**”>“**日程表**”>“**添加备份日程表**”

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，选择要从快照备份、对副本进行主从复制或复制的存储单元。

注意：对于“从快照备份”和复制，可以添加简单存储单元。但对于主从复制，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，在“**选择复制目标**”对话框中，选择用于主从复制副本的主服务器，然后单击“**下一步**”。
- 在“**选择存储生命周期策略**”对话框中，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“**使用所选复制目标**”。

13 单击“**完成**”以使用主从复制或重复副本创建保护计划。

查看主从复制和重复副本详细信息。

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**”选项卡下的“**存储配置**”。

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，然后单击“**启动**”。

4 在“**名称**”字段中输入存储单元名称。

5 在“**最大并行作业数**”字段中，选择备份作业的最大数目。

6 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**”。

7 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**”。

8 “**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。

9 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。

10 查看存储单元的设置，然后单击“**保存**”。

7

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 NetBackup Web UI 中查看从快照还原作业。

运行从快照还原

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。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/

注意：在 NetBackup Web UI 上，会在 Kubernetes 资产的“**恢复点**”选项卡下添加新的“**副本数**”列。此列显示副本总数。

注意：默认情况下，对于新安装的 NetBackup 版本 10.0，“**副本数**”列对您可见。

如果 NetBackup 主服务器从版本 9.1 升级到 10.0，且您是已访问“**恢复点**”选项卡的现有用户，则“**副本数**”列对您不可见。

注意：可以使用“**恢复点**”页面上的“**显示或隐藏列**”选项启用“**副本数**”列的可见性。

---

4 在具有“**快照**”类型和已完成副本的恢复点行中，单击“**副本数**”，单击省略号菜单（三个点），以进行还原。

5 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。

6 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**”。

7 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。

8 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“**恢复所选的永久卷声明**”中选择任何选项，请单击“下一步”，然后在“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。

如果未在“**恢复所选的永久卷声明**”中选择任何选项，单击“**下一步**”，然后在“**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。这不会创建相应的永久卷声明。

9 单击“**失败策略**”部分，可查看要恢复的失败策略选项。

10 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。
- 单击“**继续**”以继续还原下一个 PVC，如果父映像（第一个映像）还原失败，则还原作业将终止。
- 单击“**重试**”以指定元数据或 PVC 还原的重试计数。如果即使重试后还原仍然失败，则还原作业将终止。

注意：活动监视器上将显示所选的失败策略。

11 单击“**下一步**”。

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

13 在“**活动监视器**”选项卡中，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**”上查看日志，以跟踪要还原的永久卷、永久卷声明或元数据。

从备份副本还原

NetBackup 10.0 及更高版本允许您从备份副本进行还原。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**”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。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

---

注意：在 NetBackup Web UI 上，会在 Kubernetes 资产的“**恢复点**”选项卡下添加新的“**副本数**”列。此列显示副本总数。

注意：默认情况下，如果您新安装了 NetBackup 10.0 版，则“**副本数**”列对您可见。

但是，如果 NetBackup 主服务器从版本 9.1 升级到 10.0，且您是已访问“**恢复点**”选项卡的现有用户，则“**副本数**”列对您不可见。

注意：可以使用“**恢复点**”页面上的“**显示或隐藏列**”选项启用“**副本数**”列的可见性。

---

4 在具有“**备份**”类型和已完成副本的恢复点行中，单击“**副本数**”，单击省略号菜单（三个点），以进行还原。

5 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**”

6 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**”，可使用原始命名空间。默认情况下，此选项处于选中状态。
- 选择“**使用备用命名空间**”并输入备用命名空间，然后单击“**下一步**”。

7 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。

8 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“**恢复所选的永久卷声明**”中选择任何选项，请单击“下一步”，然后在“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。

如果未在“**恢复所选的永久卷声明**”中选择任何选项，单击“**下一步**”，然后在“**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。这不会创建相应的永久卷声明。

---

9 单击“**失败策略**”部分，可查看要恢复的失败策略选项。

10 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。
  终止还原
- 单击“**继续**”以继续还原下一个 PVC，如果父映像（第一个映像）还原失败，则还原作业将终止。
- 单击“**重试**”以指定元数据或 PVC 还原的重试计数。如果即使重试后还原仍然失败，则还原作业将终止。

  注意：活动监视器上将显示所选的失败策略。

- 单击“**下一步**”

11 单击“**启动恢复**”以提交恢复条目。

12 在“**活动监视器**”选项卡中，单击“**作业 ID**”以查看还原作业详细信息。

13 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：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，以跟踪要还原的永久卷、永久卷声明或元数据。

注意：NetBackup 10.0 版不支持取消还原作业。

注意：NetBackup 10.0 及更高版本仅在“**从备份副本还原**”作业中支持备用群集还原。在某些情况下，由于群集上的对象版本不同，还原到备用群集可能会部分失败。

8

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：

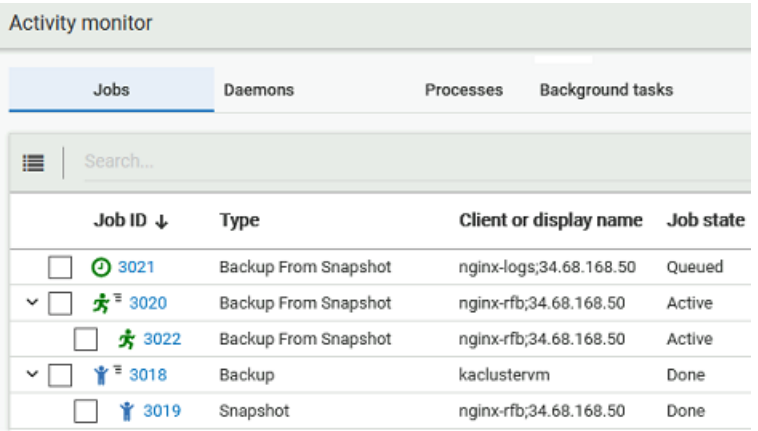
- 可以使用备用命名空间进行还原
- 运行还原操作时，可以在“**恢复选项**”中选择不与现有 PVC 重叠的 PVC。

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。

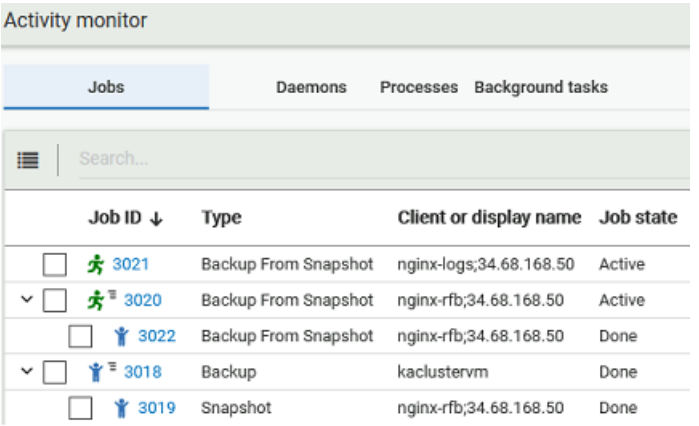
作业 ID 3020 和 3021 是从快照备份的父作业。datamover pod 创建及其清理过程是备份作业生命周期的一部分。

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。
