NetBackup™ Web UI Kubernetes 管理指南

版本 **9.1**

VERITAS™

上次更新时间： 2021-06-28

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

NetBackup Web 用户界面简介

本章节包括下列主题：

关于 NetBackup Web UI

NetBackup Web 用户界面提供以下功能：

- 能够从 Web 浏览器（包括 Chrome 和 Firefox）访问主服务器。有关 Web UI 支持的浏览器的详细信息，请参见 NetBackup 软件兼容性列表。
  请注意，对于不同的浏览器，NetBackup Web UI 的行为可能有所不同。某些功能（例如日期选取器）可能并非在所有浏览器上都可用。这些不一致是浏览器功能所致，而不是由于 NetBackup 存在限制。
- 控制板，显示重要信息的简要概述。
- 基于角色的访问控制 (RBAC)，允许管理员配置用户对 NetBackup 的访问权限并委派工作负载保护任务。
- 通过保护计划、作业管理和资产保护状态可见性实现资产保护。
  另外，策略管理也适用于有限数量的策略类型。我们提供了关于这些策略类型的更多信息：
- 工作负载管理员可创建保护计划、为资产订购满足 SLO 的保护计划、监控保护状态以及执行资产的自助服务恢复。

注意：查看 NetBackup Web UI 时，使用 1280x1024 或更高的屏幕分辨率效果最佳。

NetBackup Web UI 中的访问控制

NetBackup 使用基于角色的访问控制授予对 Web UI 的访问权限。访问控制通过角色实现。

- 角色定义用户可以执行的操作以及该用户可以在 Web UI 中访问的功能。例如，访问任何工作负载资产、保护计划或凭据。
- RBAC 仅适用于 Web UI 和 API。
  Web UI 和 API 不支持 NetBackup 的其他访问控制方法，但增强的审核 (EA) 除外。

监控 NetBackup 作业

通过 NetBackup Web UI，管理员可更轻松地监控 NetBackup 作业操作，并识别需要注意的任何问题。

保护计划：用于配置日程表、存储和存储选项

保护计划具有以下优点：

- 默认的工作负载管理员可选择用于保护资产的保护计划。
- 具有必要的 RBAC 权限，工作负载管理员可创建和管理保护计划，包括所用的备份日程表和存储。
- 除了备份日程表以外，保护计划还可以包括复制和长期保留日程表。
- 从可用存储中进行选择时，会显示适用于该存储的任何其他功能。

自助服务恢复

使用 NetBackup Web UI，工作负载管理员可以轻松地恢复 VM、数据库或适用于该工作负载的其他资产类型。

术语

下表介绍了 Web 用户界面涉及的概念和术语。

表 1-1 Web 用户界面术语和概念

术语	定义
资产组	请参见*智能组*。
资产	要保护的数据，例如，物理客户端、虚拟机和数据库应用程序。

术语	定义
立即备份	资产的即时备份。NetBackup 使用选定的保护计划对资产执行一次性完全备份。此备份不会影响任何预定的备份。
智能组	允许 NetBackup 根据您指定的条件（查询）自动选择要保护的资产。智能组会自动与生产环境中的变化保持同步。这些组也称为资产组。 这些组显示在“**智能 VM 组**”或“**智能组**”选项卡下。
保护计划	保护计划定义了执行备份的时间、备份的保留期限和要使用的存储类型。设置保护计划后，可以为资产订购保护计划。
RBAC	基于角色的访问控制。角色管理员可以通过在 RBAC 中配置的角色委派或限制访问 NetBackup Web UI。 **注意：**在 RBAC 中配置的角色不控制对 NetBackup 管理控制台或 CLI 的访问。
角色	对于 RBAC，定义用户可以执行的操作，以及用户可以访问的资产或对象。例如，可以将角色配置为管理特定数据库的恢复，以及备份和还原所需的凭据。
存储	将数据备份或复制到的存储（以便长期保留）。
订购, 保护计划	用于选择资产或资产组以订购保护计划的操作。然后，根据计划中的日程表保护资产。Web UI 也将 *“订购”*称为 *“添加保护”*。
取消订购保护计划	*“取消订购”*是指删除保护或从计划中删除资产或资产组的操作。
工作负载	资产类型。例如，VMware、RHV、AHV 或云。

登录到 NetBackup Web UI

授权用户可以使用 NetBackup Web UI 从 Web 浏览器登录 NetBackup 主服务器。

可用登录选项如下：

- 使用用户名和密码登录
- 使用证书或智能卡登录
- 使用单点登录 (SSO) 进行登录

使用用户名和密码登录

只有授权用户才能登录 NetBackup Web UI。有关更多信息，请联系您的 NetBackup 安全管理员。

使用用户名和密码登录 NetBackup 主服务器

1 打开 Web 浏览器，并转到以下 URL。

https://*primaryserver*/webui/login

primaryserver 是要登录的 NetBackup 主服务器的主机名或 IP 地址。

2 输入凭据，然后单击“登录”。

例如：

适用于此类型的用户	使用此格式	示例
本地用户	*username*	**jane_doe**
Windows 用户	*DOMAIN\username*	**WINDOWS\jane_doe**
UNIX 用户	*username@domain*	**john_doe@unix**

使用证书或智能卡登录

如果您是授权用户，则您可以使用智能卡或数字证书登录到 NetBackup Web UI。有关更多信息，请联系您的 NetBackup 安全管理员。

要使用智能卡上的数字证书以外的证书，必须先将证书上传到浏览器的证书管理器。有关更多信息，请参见浏览器文档了解相关说明，或联系您的证书管理员。

使用证书或智能卡登录

1 打开 Web 浏览器，并转到以下 URL。

https://*primaryserver*/webui/login

primaryserver 是要登录的 NetBackup 主服务器的主机名或 IP 地址。

2 单击“使用证书或智能卡登录”。

3 在浏览器提示时，选择证书。

使用单点登录 (SSO) 进行登录

如果在 NetBackup 环境中将 SAML 配置为身份提供程序，则可以使用单点登录 (SSO) 选项登录到 NetBackup Web UI。有关更多信息，请联系您的 NetBackup 安全管理员。

使用 SSO **登录** NetBackup **主服务器**

1 打开 Web 浏览器，并转到以下 URL。

https://*primaryserver*/webui/login

primaryserver 是要登录的 NetBackup 主服务器的主机名或 IP 地址。

2 单击“**使用单点登录进行登录**”。

3 执行管理员提供的步骤。

后续登录时，NetBackup 会自动登录到主服务器。

注销 NetBackup Web UI

请注意，NetBackup 会在 24 小时后自动退出 Web UI，这是用户会话所允许的最长时间。在此之后，NetBackup 要求您再次登录。如果希望更改要使用的登录选项（用户名和密码、智能卡或单点登录 (SSO)），也可以注销。

注销 NetBackup Web UI

- 在右上方，单击配置文件图标，然后单击“**注销**”。

2

监控 NetBackup

本章节包括下列主题：

NetBackup 控制板

NetBackup 控制板可用于快速查看与组织角色相关的详细信息。

表 2-1 NetBackup 控制板

控制板小组件	描述
作业	列出作业信息，包括活动和已排队作业的数量以及已尝试和已完成作业的状态。

监视作业

使用“**作业**”节点可监视 NetBackup 环境中的作业并查看特定作业的详细信息。

监视作业

1 单击要查看的作业名称。

在“**概述**”选项卡上可以查看有关作业的信息。

- “**文件列表**”包含备份映像中包括的文件。
- “**状态**”部分显示与作业相关的状态和状态码。单击状态码编号以在 Veritas 知识库中查看有关此状态码的信息。

请参见 NetBackup 状态码参考指南。

2 单击“**详细信息**”选项卡以查看有关作业的记录详细信息。可以使用下拉菜单按错误类型过滤日志。

请参见第 12 页的“过滤作业列表中的作业”。

过滤作业列表中的作业

您可以过滤作业以显示处于特定状态的作业。例如，可以显示所有活动作业或所有暂停作业。

过滤作业列表

1 单击“**作业**”。

2 在作业列表上方，单击“**过滤器**”选项。

3 在“**过滤器**”窗口中，选择过滤器选项以动态更改显示的作业。过滤器选项如下所示：

- **全部**
- **激活**
- **完成**
- **失败**
- **未完成状态**
- **部分成功**
- **排队**
- **成功**
- **已暂停状态**
- **等待重试**

4 单击“**应用过滤器**”。

5 要删除选定过滤器，单击“**全部清除**”。

3

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网络负载
- 选择保护计划以保护 Kubernetes 资产。
- 还原命名空间和永久卷。
- 监控备份和还原操作。

Kubernetes 支持的 NetBackup 功能

表 3-1 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。 ■ 能够保留或放弃部分成功的备份。 ■ 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。
备份和还原功能	以下功能可用于备份和还原： ■ 备份和还原完全由 NetBackup 服务器从一个中央位置进行管理。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。 ■ 手动备份和仅快照备份。 ■ 将 Kubernetes 命名空间和永久卷还原到不同位置。 ■ 针对每个群集进行资源限制以提高备份性能。
快照备份	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。

4

部署和配置 NetBackup Kubernetes Operator

本章节包括下列主题：

为 Kubernetes 配置群集

需要先配置群集，然后才能部署 NetBackup™ Kubernetes Operator。可以在三种不同的平台上使用 Helm Chart 部署 NetBackup Kubernetes Operator：

- Red Hat OpenShift
- Google Kubernetes Engine (GKE)
- VMware Tanzu

为 NetBackup 配置 OpenShift

在开始之前，请确保您的 OpenShift 帐户具有执行这些操作所需的权限。

要配置 OpenShift，请执行以下操作：

- 使用以下命令通过 CLI 登录到 OpenShift OC：

  ```
  oc login --token=<TOKEN> --server=<URL>
  ```

  其中：

  - <TOKEN>：您的登录令牌
  - <URL>：您的 OpenShift 服务器 URL

注意：您可以通过登录到 OpenShift 帐户来获取令牌和 URL。在主页右上方，单击用于登录到控制台的 OpenShift 管理员帐户的名称，然后单击“**复制登录命令**”选项。在打开的新页面上，单击“**显示令牌**”以查看命令。

此命令在 `~/.kube/config` 文件中添加一个新的 kubectl 上下文，并将此新上下文设置为 kubectl 当前上下文。

为 NetBackup 配置 GKE

在开始之前，请确保您的 GKE 帐户具有执行这些操作所需的权限

前提条件：

- GKE 群集的端口号可以为 443、6443 或 8443。默认端口为 443。添加前验证安全端口号是否正确。
- 在 GKE 上创建永久卷或永久卷声明时，请指定其 `Provisioner` 为 `kubernetes.io/gce-pd` 的存储类。

要使用现有帐户登录，请执行以下操作：

1 使用以下命令通过现有用户帐户登录到 GKE 帐户：

```
gcloud auth login <account>
```

2 以交互方式或非交互方式输入登录凭据。

3 要列出所有群集并查找群集名称，请运行以下命令：

```
gcloud container clusters list
```

输出如下所示：

```
NAME                LOCATION        MASTER_VERSION    MASTER_IP

csi-cluster         us-central1-c   1.17.14-gke.400   35.238.135.170

sailor              us-central1-c   1.16.15-gke.6000  35.224.28.128

surens-cluster      us-east1-b      1.17.14-gke.1600  35.231.17.183

bw-kube-cluster-1   us-east1-c      1.16.15-gke.6000  35.196.24.132
```

4 要获取群集的凭据并将其添加到 `.kube/config`，请运行以下命令：

```
gcloud container clusters get-credentials <cluster name>
```

例如：gcloud container clusters get-credentials bw-kube-cluster-1

或者，也可以创建并使用群集的专用服务帐户进行登录。

要创建专用服务帐户，请执行以下操作：

1 要创建帐户，请运行以下命令：

```
gcloud iam service-accounts create <account name> --display-name
"<account description>"
```

例如：gcloud iam service-accounts create veritas-netbackup-k8s-sa --display-name "Veritas NetBackup K8s Service Account"

2 要列出用户，请运行以下命令：

```
gcloud iam service-accounts list --filter <email ID>@<project
ID>.gserviceaccount.com
```

例如：gcloud iam service-accounts list --filter veritas-netbackup-k8s-sa@projectID.gserviceaccount.com

3 要下载服务帐户密钥，请运行以下命令：

```
gcloud iam service-accounts keys create <key json file name>
--iam-account <e-mail address of the service account>
```

例如：gcloud iam service-accounts keys create veritas-netbackup-k8s-sa-key.json --iam-account <e-mail ID of the service account>

4 要关联角色，请运行以下命令：

```
gcloud iam roles create <role name> --project <project ID> --file
./<role name>.yaml
```

例如：gcloud iam roles create rolename --project projectID --file ./rolename.yaml

5 要激活服务帐户，请运行以下命令：

```
gcloud auth activate-service-account --project=<project ID>
--key-file=<key file name>
```

例如：gcloud auth activate-service-account --project=<YOUR PROJECT ID> --key-file=veritas-netbackup-k8s-sa-key.json

6 要列出所有群集并查找群集名称，请运行以下命令：

```
gcloud container clusters list
```

输出如下所示：

```
NAME                LOCATION       MASTER_VERSION    MASTER_IP

csi-cluster        us-central1-c  1.17.14-gke.400   35.238.135.170

sailor             us-central1-c  1.16.15-gke.6000  35.224.28.128

surens-cluster     us-east1-b     1.17.14-gke.1600  35.231.17.183

bw-kube-cluster-1  us-east1-c     1.16.15-gke.6000  35.196.24.132
```

7 要获取群集的凭据并将其添加到 .kube/config，请运行以下命令：

```
gcloud container clusters get-credentials <cluster name>
```

例如：gcloud container clusters get-credentials bw-kube-cluster-1

为 NetBackup 配置 VMware Tanzu

在开始之前，请确保您的 Tanzu 帐户具有执行这些操作所需的权限。确保已安装 TKG 客户端。

将现有 Tanzu 管理群集添加到本地 TKG 实例：

1 将 kube-tkg/config 文件从管理群集复制到本地用户主目录：~/

2 运行命令：chmod 775 ~/.kube-tkg/config

3 运行命令：export KUBECONFIG=.kube-tkg/config

4 要获取上下文列表，请运行命令：`tkg get mc`。输出如下所示：

```
  MANAGEMENT-CLUSTER-NAME  CONTEXT-NAME                STATUS
  tkg-mgmt *               tkg-mgmt-admin@tkg-mgmt    Success
  tkg1-mgmt                tkg1-mgmt-admin@tkg1-mgmt  Success
  tkg2-mgmt                tkg2-mgmt-admin@tkg2-mgmt  Success
```

5 要切换到 TKG 上下文，请运行命令：`tkg set mc tkg1-mgmt`

当前管理群集上下文即会切换到 **tkg1-mgmt**。

6 要检查 kubectl 上下文，请运行命令：`kubectl config get-contexts`。输出如下所示：

```
 CURRENT NAME             CLUSTER AUTHINFO   NAMESPACE
tkg1-mgmt-admin@tkg1-mgmt      tkg1-mgmt    tkg1-mgmt-admin
tkg2-mgmt-admin@tkg2-mgmt      tkg2-mgmt    tkg2-mgmt-admin
```

7 要检查本地 TKG 实例中的管理群集，请运行命令：`tkg get mc`。输出如下所示：

```
[dxxxx@xxxxxxxxx01vm1392 ~]$ tkg get mc
  MANAGEMENT-CLUSTER-NAME  CONTEXT-NAME                STATUS
  tkg-mgmt                tkg-mgmt-admin@tkg-mgmt    Success
  tkg1-mgmt *                tkg1-mgmt-admin@tkg1-mgmt  Success
  tkg2-mgmt                 tkg2-mgmt-admin@tkg2-mgmt  Success
```

8 要获取当前上下文中的所有群集，请运行命令：`tkg get clusters`。输出如下所示：

```
 NAME         NAMESPACE  STATUS  CONTROLPLANE  WORKERS  KUBERNETES

  tkg1-cluster1  default  running  3/3        3/3
v1.19.3+vmware.1
  tkg1-cluster2  default  running  3/3        3/3
v1.19.3+vmware.1
  tkg1-cluster3  default  running  3/3        3/3
v1.19.3+vmware.1
```

9 要向 kubectl 配置文件中添加凭据，请运行命令：`tkg get credentials tkg1-cluster1`

这会将工作负载群集 **tkg1-cluster1** 的凭据保存在配置文件中。要访问群集，请运行命令：`kubectl config use-context tkg1-cluster1-admin@tkg1-cluster1`

10 要切换到 **kubectl** 上下文，请运行命令：`kubectl config use-context tkg1-cluster1-admin@tkg1-cluster1`

11 要检查 kubectl 上下文，请运行命令：`kubectl config get-contexts`

输出如下所示：

```
 CURRENT NAME              CLUSTER AUTHINFO         NAMESPACE
tkg1-cluster1-admin@tkg1-cluster1   tkg1-cluster1
tkg1-cluster1-admin
tkg1-mgmt-admin@tkg1-mgmt           tkg1-mgmt
tkg1-mgmt-admin
tkg2-mgmt-admin@tkg2-mgmt           tkg2-mgmt
tkg2-mgmt-admin
```

现在，您可以在 **tkg1-cluster1** 中使用任何 kubectl 命令。

部署的前提条件

在要部署 NetBackup Kubernetes Operator的群集中下载并安装 Velero。

注意：有关支持的 Velero 版本，请参考 NetBackup 软件兼容性列表。有关 Velero 安装和配置，请参考 Velero 文档。

部署 NetBackup Kubernetes Operator

配置群集后，可以在这些群集中部署 NetBackup Kubernetes Operator。必须在要使用 NetBackup 的每个群集中部署 Operator。

配置 Helm Chart

可使用 Helm Chart 部署 NetBackup Kubernetes Operator。您可以为 NetBackup Kubernetes Operator 创建 Chart。下面是 Helm Chart 和树结构布局。

```
netbackupkops-helm-chart

    ├── charts
```

```
├── Chart.yaml
├── templates
│   └── deployment.yaml
└── values.yaml
```

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

1. 下载 Operator 服务软件包。
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 cd ~
6. 如果使用专用 Docker 注册表，请按照此步骤中的说明在 Velero 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 -d <user name> -p <password>
     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 Velero 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 velero
```

- 要检查是否已在 Velero 命名空间中创建名为 `netbackupkops-docker-cred` 的密钥，请运行以下命令： `kubectl get secrets -n velero`
- 如果使用映像 tar 文件，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>
```

- 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* 值替换为带有 (*repo-name/image-name:tag-name*) 标记的映像名称，并保存文件。

7 要部署 NetBackup Kubernetes Operator 服务，请在一行中运行以下命令：

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

例如： `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 服务的命名空间时需要 `-n` 选项。该命名空间必须与要运行 Velero 的命名空间相同。

8 要检查部署的状态，请运行以下命令：

```
helm list -n <namespace in which NetBackup operator service will
run>
```

例如：

```
helm list -n netbackup
```

9 要检查发布历史记录，请运行以下命令：`helm history veritas-netbackupkops -n <namespace in which NetBackup operator service will run>`

例如：

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

升级 NetBackup Kubernetes 操作员部署

您可以使用 Helm 命令升级 NetBackup Kubernetes 操作员部署。

```
helm upgrade <release name> ./<directory of the chart> -n <namespace>
```

例如：`helm upgrade veritas-netbackupkops ./nbukops-helm-chart -n netbackup`

删除 NetBackup Kubernetes Operator部署

您可以根据需要从群集中删除 NetBackup Kubernetes Operator部署。

要删除 NetBackup Kubernetes Operator部署，请运行以下命令：

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

例如： `helm uninstall veritas-netbackupkops -n netbackup`

NetBackup 端的 Operator 配置

NetBackup 9.1 引入了两个新的默认 RBAC 角色：

- **默认 NetBackup Kubernetes Operator**：此角色为在 Kubernetes 群集中运行的 Operator 提供了与 NetBackup Web 服务通信所需的权限。安全管理员或 NetBackup 管理员可以为此角色分配所需的用户。此 API 密钥的权限有限，随角色一起定义。Kubernetes 群集结尾处的配置中需要 API 密钥和 CA 证书。

  注意：请与安全管理员或 NetBackup 管理员联系，获取 NetBackup CA 证书。

- **默认 Kubernetes 管理员**：此角色具有 NetBackup Web UI 和 API 所需的所有权限。

Kubernetes 端的 Operator 配置

要运行 NetBackup Kubernetes Operator，必须在 Kubernetes 群集所需的配置中创建 Kubernetes 密钥资源。该密钥的文件名必须与配置的主服务器相同，且命名空间必须是运行 NetBackup Kubernetes Operator 的相同命名空间。Kubernetes 群集结尾处的配置中需要 NetBackup 主服务器的 API 密钥和 CA 证书。

注意：请与安全管理员或 NetBackup 管理员联系，获取 NetBackup CA 证书。

密钥的格式如下。提供尖括号中指定的值：

```
apiVersion: v1
kind: Secret
metadata:
  name: <NetBackp primary server host name or IP address.>>
  namespace: <Namespace name where the NetBackup Kubernetes operator
 is deployed>>


type: Opaque
stringData:
  apiKey: <API key of the primary server>>
  caCert: "<CA certificate of the primary server>>"
```

请与安全管理员联系，索取 API 密钥和 CA 证书。

获取用于添加群集的令牌

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
```

选择没有注释字段的令牌

以下是示例 CA 证书：

```
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURCakNDQWU2
Z0F3SUJBZ0lCQVRBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd0VR
WURWUVFERXdwdGFXNXAKYTNWaVpVTkJNQjRYRFRJd01URXhPVEV3
TURZeU1sb1hEVE13TVRFeE9ERXdNRFl5TWxvd0ZURVRNQkVHQTF
VRQpBeE1LYldsdWFXdDFZbVZEUVRDQ0FTSXdEUVlKS29aSWh2Y05
BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTklaClduc0MvTEpjaUV
NOGx0ZnU0dzFPcmNaeTVZemhOTXoxQWV0V09xRmUrQ0VxblFVY3h
mVEpwOElWMFRTei9yYmYKSHVBdWlmWTd2ZGxNdC9zREJUbDlIMGF
xUkxLdG9KMDZaUHVBRzN0WjA5Nm1VUzV5bXYzRktWV2kvaVMyYz
I0ZQpFc2NENTBRaTRyYUM5YTlHK1NuSWVRNXYrQzZGUU9vYnBuS
ERXOTNIMlRpK3gyaEMrTHVoSndVVlRldG1EbzkyCktHendENU5OU
kV0L1FPYnVtaTN0QnFPMTdpSThua2xwb0tBd0RYQWlYd2ZjeFpQ
RXNrKytkajRBNVo2bWFGRHMKMUxxVkQ3ZFpkYk1vM08rTDJ6bzB
KdFIzWXYzenY3L0tYM0JDVmdzQWduQWdNeWJUYWMyenRRYzhsWH
hwLzZxcAowbTRPT0h0ME1KYnRSMmo4bWJrQ0F3RUFBYU5oTUY4d
0RnWURWUjBQQVFIL0JBUURBZ0trTUIwR0ExVWRKUVFXCk1CUUdD
Q3NHQVFVRkJ3TUNCZ2dyQmdFRkJRY0RBVEFQQmdOVkhSTUJBZjh
```

FQlRBREFRSC9NQjBHQTFVZERnUVcKQkJSUkVNM3JxQjhFTjRJW
FFiQ3RJd2hhb3hzeW1EQU5CZ2txaGtpRzl3MEJBUXNGQUFPQ0F
RRUFsY2ZURGNObwpoZi9EM3BQYmx6V3BXUm5xbUc2aTF5eG0wT
2V3OUJWMjhVeDc0S1ppcGEvUm5valpaVDlRdmwvcmg3YW5rRHd
NCllDSlVsZUNHVWJkc1dwRHpycFlqa0lJVlMybHkxeHpUWkNLY0
FWOENEWWkzdjdHdWswR2R2SXc0VENndk5XajIKanBDbC9QWkFp
ZUFXdTlYL2R4THU1S01FN05uTnlGNWx4Uy85cTVvMkRUSS8reD
RncEQwQ09rQVl3SDZ4SzViUgp2WGNabFJ3NmNlMWlTZG43dVE1
V1dxcU50ZEQ1MHRNRHlzWERqUzI4WVh6WjlRYThkMEVnR1E1dW
JMZnZZdzJkCm9xcmZIZjN6bitYajNFVUg0eXROROkdOc1hMN0t4
NVdtNjNjTGlrSzBLV1dOQjMwdVpsVEljUXIyenQ2MGFjK28KbC9
0dFhsUWdoaGUwaFE9PQotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==

以下是示例令牌：

ZXlKaGJHY2lPaUpTVXpJMU5pSXNJbXRwWkNJNkluRjZNMUl5UlR
reWJVSmFkbTFqV1Zaa1FtNVNkbkZwWjFSSWIzWmpTa1ZhWm5KSV
NVSnBRVEJUWVhjaWZRLmV5SnBjM01pT2lKcmRXSmxjbTVsZEdW
ekwzTmxjblpwWTJWaFkyTnZkVzUwSWl3aWEzVmlaWEp1WlhSbGN
5NXBieTl6WlhKMmFXTmxZV05qYjNWdWRDOXVZVzFsYzNCaFkyVW
lPaUoyWld4bGNtOGlMQ0pyZFdKbGNtNWxkR1Z6TG1sdkwzTmxjbl
pwWTJWaFkyTnZkVzUwTDNObFkzSmxkQzV1WVcxbElqb2lkbVZz
WlhKdkxXSmhZMnQxY0MxelpYSjJaWEl0ZEc5clpXNHRhSEpqT0
cwaUxDSnJkV0psY201bGRHVnpMbWx2TDNObGNuWnBZMlZoWTJOd
mRXNTBMM05sY25acFkyVXRZV05qYjNWdWRDNXVZVzFsSWpvaWRt
VnNaWEp2TFdKaFkydDFjQzF6WlhKMlpYSWlMQ0pyZFdKbGNtNWx
kR1Z6TG1sdkwzTmxjblpwWTJWaFkyTnZkVzUwTDNObGNuWnBZMl
V0WVdOamIzVnVkQzUxYVdRaU9pSTFNVEptWldNd09DMWlaRFV5T
FRRd01HRXRZV1V3TWkwMlpUbGpaVGhpWmpObE1Ea2lMQ0p6ZFdJ
aU9pSnplWE4wWlcwNmMyVnlkbWxqWldGalkyOTFiblE2ZG1Wc1p
YSnZPblpsYkdWeWJ5MWlZV05yZFhBdGMyVnlkbVZ5SW4wLnFEWm
t2bDNmSHlabTQzNUQyakZGX2Q5MlA2RkdFb1R0Mmx2V1J6RGR5V
GItYngxSnZ3S25Wa1M0MGswRF9jeGlMcEx5X3liNGVqelZJM2dz
UG0xM0hJUlV2bWhiSEZaUzhlX0FvOTdnbGhOd3VpQlhncjRjNW0
3dUd3eGVKOWs4eERWazVhUVhUalM4cWJlMHB4QXhpVG9EOUt4aF
BtMTVoNy1EaUtjbHBlZEJkZ2N1V2JHenRuci1uXzAzYUFFbkY3Y
zU2c1Z5N1VrV2ZUQXZMZXBZUG9jZkJoRjY3cUR4eEMza2d0S2U4
SnJUNlItclgxYWRnQVhnRnJ5WDJYNGM0RUI3WE14NFd6SFMzQXR
RdEFqNno3eEVMNXQ4eHlQZ1EtMnlpeGJudzVUTXVac1JLcnZyak
1OX2FxUTRDTEJlM29BWEVXaEdJaW1uaXgydkdpNVVVdw==

关于失效的映像

为了回收失效的 Kubernetes 映像所占用的存储空间，NetBackup 会创建 `deletebackuprequest` 自定义资源，向 Velero 提交删除请求。但是，NetBackup 不会等待删除完成或跟踪删除请求状态。Velero 接受删除请求并执行删除。

您可以通过列出 Kubernetes 群集内的 `deletebackuprequest.velero.io` CRS 来跟踪删除请求的进度。删除 Velero 备份后，`deletebackuprequest` CR 也随之删除。

注意：仅支持通过 CLI 和 API 手动使映像失效，不支持通过 Web UI 和 Java UI 执行此操作。

5

管理 Kubernetes 资产

本章节包括下列主题：

添加 Kubernetes 群集

可以在 NetBackup 中添加 Kubernetes 群集，并自动发现群集内的所有资产。为了在添加群集后执行资产发现，需要为群集添加 Operator 配置。

请参见第 23 页的“Kubernetes 端的 Operator 配置”。

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。
- **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。

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。
  - **令牌**：输入 Base64 编码形式的身份验证令牌值。
    请参见第 24 页的“获取用于添加群集的令牌”。
  - **CA 证书**：输入 CA 证书文件内容。
    请参见第 24 页的“获取用于添加群集的令牌”。

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。

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。例如，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。

此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 在“**每个 Kubernetes 群集的备份作业数**”旁边，单击“**编辑**”。

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。
- 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**”。

- 从列表中选择一个群集并输入限制值。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。

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**”。

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。

管理 Kubernetes 资产

“**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**”。

6

保护 Kubernetes 资产

本章节包括下列主题：

Kubernetes 保护计划

与其他 NetBackup 工作负载一样，您需要创建保护计划来保护 Kubernetes 工作负载。Kubernetes 保护计划：

- 不需要在保护计划中指定任何存储。
- 仅支持完全备份日程表。

为 Kubernetes 保护计划配置备份选项

Kubernetes 保护计划支持区分部分成功的备份，并根据需要保留或放弃它们。部分成功的备份可能未成功备份您想要备份的所有资源。您可以决定是保留还是放弃此类备份，并针对每个保护计划分别指定此设置。

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。

要在为 Kubernetes 配置保护计划的同时配置备份选项，请在“**备份选项**”页面中选择“**如果任何资源无法得到保护，则备份作业失败**”选项。此设置会放弃任何部分成功的备份作业。

7

恢复 Kubernetes 资产

本章节包括下列主题：

恢复 Kubernetes 资产

使用 NetBackup，您可以恢复 Kubernetes 命名空间和永久卷。

注意：在 NetBackup 9.1 中，仅适用于 Google Cloud Platform (GCP) 的 Velero 插件支持独占恢复永久卷。

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。

恢复命名空间

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和时间。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、命名空间、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/workload-resources/。
4. 在要恢复的恢复点所在行中，单击省略号菜单（三个点）。要恢复命名空间，请单击“**还原命名空间**”。

5 在“**恢复目标**”页面中，要将资产恢复到同一个源群集，单击“**下一步**”。要恢复到其他群集，单击“**选择群集**”。在“**选择群集**”对话框中，选择目标群集，然后单击“**选择**”。单击“**下一步**”。

注意：如果选择的目标群集与原始群集不同，则两个群集上的 Velero 插件使用的对象存储必须相同。

6 在“**恢复选项**”页面上，执行以下操作：

- 要恢复到原始命名空间，请选择“**使用原始命名空间**”。要将资产还原到其他命名空间，选择“**使用备用命名空间**”，然后输入新的命名空间名称。该名称应遵循命名空间名称的 Kubernetes 规范。
- 如果已存在相同命名空间仍要允许还原，请选择“**如果命名空间已存在，请继续还原**”。此选项可帮助您还原已存在的命名空间中任何缺少的资源。如果群集内的资产缺少资源，而备份副本中存在此资源，可以使用此选项还原该资产中缺少的资源。此选项不会重写资产中的任何现有资源，而是仅还原缺少的资源。
- 要还原资产内的所有资源，请选择“**恢复所有资源**”。要还原资产的所选资源类型，请选择“**选择资源类型**”，然后选择要恢复的资源类型。请注意，您不能还原单独的资源或实例，而需要选择可能包含任意数量单独资源或实例的多个资源类型。

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

7 单击“**下一步**”。

8 在“**恢复概览**”页面中，查看已选择的所有恢复选项。要返回并更改任何设置，请单击“**上一步**”。更改所有参数后，请单击“**启动恢复**”。

恢复永久卷

1 执行上述过程的步骤 1-3。

2 在要恢复的恢复点所在行中，单击省略号菜单（三个点）。要恢复永久卷，请单击“**还原永久卷**”。

3 在“**恢复目标**”页面中，要将永久卷恢复到同一个源群集，请单击“**下一步**”。要恢复到其他群集，单击“**选择群集**”。在“**选择群集**”对话框中，选择目标群集，然后单击“**选择**”。单击“**下一步**”。

注意：如果选择的目标群集与原始群集不同，则两个群集上的 Velero 插件使用的对象存储必须相同。

---

4 在“**恢复选项**”页面上，执行以下任一操作：

- 要恢复到原始命名空间，请选择“**使用原始命名空间**”。如果已存在相同命名空间仍要允许还原，请选择“**如果命名空间已存在，请继续还原**”。此选项可帮助您还原已存在的命名空间中任何缺少的永久卷。如果群集内的资产缺少任何永久卷，而备份副本中存在相同的永久卷，可以使用此选项还原该资产中缺少的永久卷。此选项不会重写资产中的任何现有永久卷，而是仅还原缺少的永久卷。
- 选择“**使用临时系统生成的命名空间**”，以使用系统生成的唯一命名空间。还原操作完成后，会删除命名空间。要优先还原永久卷数据而不是命名空间时，请使用此选项。

5 单击“**下一步**”。

6 在“**恢复概览**”页面中，查看已选择的所有恢复选项。要更正任何设置，请针对该选项单击“**编辑**”，或单击“**上一步**”。所有参数均正确后，单击“**启动恢复**”。

8

对 Kubernetes 问题进行故障排除

本章节包括下列主题：

使用短主机名连接到主服务器

必须可从 NetBackup Kubernetes Operator 访问 NetBackup 主服务器。NetBackup 主服务器名称可以是 FQDN 或短主机名，此名称应该能在 NetBackup Kubernetes Operator 中解析。

可以在 Velero 控制器管理器部署中使用 hostAliases，以便可从 NetBackup Kubernetes Operator 访问基于短主机名的 NetBackup 主服务器。

```
hostAliases:
- hostnames:
  - falcon
    ip: 10.x.x.x
```

群集发现失败

发现协调器 (NetBackup Kubernetes Operator) 将资产数据发布到 NetBackup。要执行此任务，Operator 需要密钥文件中存在 API 密钥和 caCert。

推荐的操作：

- 确保部署了 NetBackup Kubernetes Operator 的命名空间中存在与 NetBackup 主服务器同名的密钥。
- 请确保该密钥文件与 NetBackup Kubernetes Operator Pod 在同一命名空间中。
- 确保 API 密钥和 CA 证书有效。

备份期间出错：命名空间已标记为删除

当您尝试备份的命名空间已从 Kubernetes 群集中删除时，将显示此错误。NetBackup 资产服务还会从资产数据库中删除该资产。但是，如果有可用于该命名空间的备份，则资产服务不会删除资产，而是将其标记为 DELETED。在这种情况下，我们不希望备份此类资产或命名空间。

推荐的操作：验证群集上是否存在命名空间。

还原期间出错：最终作业状态为部分失败

最终作业状态为部分失败，并出现一些专门针对资源 RoleBinding 的警告。

这些警告专门针对 API 组授权的资源 RoleBinding。引发 `openshift.io` 和 `rbac.authorization.Kubernetes.io` 的原因是这些 RoleBinding 由控制器自动管理，并在我们创建新命名空间时创建。

推荐的操作：您可以通过从还原中排除相关的 RoleBinding 资源来避免这些警告。

备份停滞在“正在进行中”状态

情形 1：如果 Kubernetes 群集中运行的 Velero pod 在备份作业运行时重新启动，则会发生这种情况。

推荐的操作：

按照 Velero 文档中的这些步骤确定作业是停滞还是运行缓慢。请参见 Velero 文档。删除 NetBackup 备份 ("backups.netbackup.veritas.com") CRD 作业和 Velero 备份 ("backups.velero.io") CRD 作业。

情形 2：快照处于 *UploadFailed* 状态或上传失败，这可能导致重试上传任务。

推荐的操作：

通过查看 datamanager 日志（在处理节点上）和备份驱动程序日志来确定问题的原因，以确定上传错误的根本原因。要启用 NetBackup 作业，请删除 NetBackup 备份 CR ("backups.netbackup.veritas.com")，这会将备份作业标记为失败。还要清理相应的 velero 备份作业 ("backups.velero.io")、快照作业 ("snapshots.backupdriver.cnsdp.vmware.com") 和上传作业 ("uploads.datamover.cnsdp.vmware.com")。

还原停滞在“正在进行中”状态

如果正在运行还原作业时，Kubernetes 群集中正在运行的 Velero Pod 重新启动，则会出现此问题。

推荐的操作：

对于适用于 vSphere 的 Velero 插件，

如果还原包含永久卷，请验证与还原作业对应的 CloneFromSnapshot ("clonefromsnapshots.backupdriver.cnsdp.vmware.com") CRD 的状态。如果下载请求 ("downloads.datamover.cnsdp.vmware.com") 失败，则对象存储访问或还原的目标命名空间可能会有问题。该命名空间中可能已经包含同名的现有永久卷声明。删除 NetBackup 还原 ("restores.netbackup.veritas.com") CRD 作业和 Velero 还原 ("restores.velero.io") CRD 作业以及对应的 clonefromsnapshot CRD（如果适用）。可以选择删除对应的数据移动工具下载 ("downloads.datamover.cnsdp.vmware.com") CRD。

对于适用于 GCP 的 Velero 插件：

删除 NetBackup 还原 ("restores.netbackup.veritas.com") CRD 作业和 Velero 还原 ("restores.velero.io") CRD 作业。或者，删除相应的下载 ("downloadrequests.velero.io") CRD。