Red Hat OpenShift Data Foundation 4.12

在 VMware vSphere 上部署 OpenShift Data Foundation

使用 VMware vSphere 基础架构部署 OpenShift Data Foundation 的说明

Last Updated: 2023-12-21

Red Hat OpenShift Data Foundation 4.12 在 VMware vSphere 上部署 OpenShift Data Foundation

使用 VMware vSphere 基础架构部署 OpenShift Data Foundation 的说明

法律通告

摘要

参阅本文档，了解如何使用 Red Hat OpenShift Container Platform 在 VMware vSphere 集群上安装 Red Hat OpenShift Data Foundation。

目录

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 的信息。

对红帽文档提供反馈

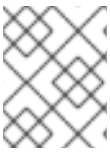
我们感谢您对文档提供反馈信息。请告诉我们如何让它更好。

要提供反馈，请创建一个 Bugzilla ticket：

1. 进入 Bugzilla 网站。
2. 在 **Component** 部分中，选择 **文档**。
3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
4. 点 **Submit Bug**。

前言

Red Hat OpenShift Data Foundation 支持在连接或断开连接的环境中的现有 Red Hat OpenShift Container Platform(RHOCP)vSp 集群上部署，以及代理环境的开箱即用支持。



注意

VMware vSphere 上均支持内部和外部 OpenShift Data Foundation 集群。如需有关部署要求的更多信息，请参阅规划部署并准备部署 OpenShift Data Foundation。

要部署 OpenShift Data Foundation，请从准备部署 OpenShift Data Foundation 章节中的要求开始，然后按照以下环境部署过程之一进行操作：

- 内部模式
  - 使用动态存储设备进行部署
  - 使用本地存储设备部署
  - 部署独立多云对象网关组件
- 外部模式

第 1 章 准备部署 OPENSHIFT 数据基础

使用动态或本地存储设备在 OpenShift Container Platform 上部署 OpenShift Data Foundation 为您提供创建内部集群资源的选项。这将会在内部置备基础服务，这有助于为应用提供额外的存储类。

在使用动态或本地存储开始部署 Red Hat OpenShift Data Foundation 前，请确保满足您的资源要求。请参阅规划部署。

1. 可选：如果要使用外部密钥管理系统 (KMS) HashiCorp Vault 启用集群范围加密，请按照以下步骤执行：
   - 确定您有有效的 Red Hat OpenShift Data Foundation Advanced 订阅。要了解 OpenShift Data Foundation 订阅如何工作，请参阅与 OpenShift Data Foundation 订阅相关的知识库文章。
   - 当为加密选择 Token 验证方法时，请参考使用 KMS 通过 Token 身份验证启用集群范围的加密。
   - 当为加密选择了 Kubernetes 验证方法时，请参考使用 KMS 使用 Kubernetes 身份验证启用集群范围的加密。
   - 确保您在 Vault 服务器上使用签名的证书。
2. 可选： 如果要使用外部密钥管理系统 (KMS) Thales CipherTrust Manager 启用集群范围的加密，您必须首先启用密钥管理互操作性协议 (KMIP)，并在服务器上使用签名证书。按照以下步骤操作：
   a. 如果 KMIP 客户端不存在，请创建一个。在用户界面中，选择 **KMIP → Client Profile → Add Profile**。
      i. 在创建配置集的过程中，将 **CipherTrust** 用户名添加到 **Common Name** 字段中。
   b. 通过进入到 **KMIP → Registration Token → New Registration Token** 来创建令牌。为下一步复制令牌。
   c. 要注册客户端，请进入到 **KMIP → Registered Clients → Add Client**。指定**名称**。粘贴上一步中的**注册令牌**，然后点**保存**。
   d. 点 **Save Private Key** 和 **Save Certificate** 下载私钥和客户端证书。
   e. 要创建新的 KMIP 接口，请进入到 **Admin Settings → Interfaces → Add Interface**。
      i. 选择 **KMIP Key Management Interoperability Protocol** 并点 **Next**。
      ii. 选择一个空闲**端口**。
      iii. 为 **Network Interface** 选择 **all**。
      iv. 为 **Interface Mode** 选择 **TLS, verify client cert, user name taken from client cert, auth request is optional**。
      v. （可选）您可以在密钥被删除时启用硬删除以删除元数据和材料。它默认是禁用的。
      vi. 选择要使用的 CA，然后点 **Save**。
   f. 要获取服务器 CA 证书，请点新创建的界面右侧的 Action 菜单(⋮)，然后点 **Download Certificate**。

g. 可选：如果要在部署过程中启用 StorageClass 加密，请创建一个密钥来充当密钥加密密钥 (KEK)：

   i. 进入到 **Keys → Add Key**。

   ii. 输入 **Key Name**。

   iii. 分别将 **Algorithm** 和 **Size** 设置为 **AES** 和 **256**。

   iv. 启用 **Create a key in Pre-Active state**，并设置激活的日期和时间。

   v. 确保在 **Key Usage** 下启用了 **Encrypt** 和 **Decrypt**。

   vi. 复制新创建的密钥的 ID，以在部署过程中用作唯一标识符。

3. 启动节点最低要求
   当不符合标准部署资源要求时，将使用最低配置部署 OpenShift Data Foundation 集群。请参阅规划指南中的资源要求部分。

4. 实现灾难恢复的要求 [技术预览]
   Red Hat OpenShift Data Foundation 支持的灾难恢复功能需要满足以下所有先决条件，才能成功实施灾难恢复解决方案：

   - 有效的 Red Hat OpenShift Data Foundation 高级订阅
   - 有效的 Red Hat Advanced Cluster Management for Kubernetes 订阅
     要了解 OpenShift Data Foundation 订阅如何工作，请参阅与 OpenShift Data Foundation 订阅相关的知识库文章。

   如需更多信息，请参阅 Configuring OpenShift Data Foundation Disaster Recovery for OpenShift Workloads 指南，以及 Red Hat Advanced Cluster Management for Kubernetes 文档中的安装指南中的 *Requirements and recommendations* 部分。

5. 有关使用本地存储设备部署，请参阅使用 本地存储设备安装 OpenShift Data Foundation 的要求。这些不适用于使用动态存储设备的部署。

1.1. 使用本地存储设备安装 OPENSHIFT DATA FOUNDATION 的要求

节点要求

集群必须至少包含三个 OpenShift Container Platform worker 节点，每个节点都有本地附加存储设备。

- 在三个选择的节点的每个节点中都至少有一个可用的原始块设备。OpenShift Data Foundation 使用一个或多个可用的原始块设备。
- 您使用的设备必须为空；磁盘中不得包含物理卷 (PV)，卷组 (VG) 或逻辑卷 (LV)。

如需更多信息，请参阅规划指南中的*资源要求*部分。

实现灾难恢复的要求 [技术预览]

Red Hat OpenShift Data Foundation 支持的灾难恢复功能需要满足以下所有先决条件，才能成功实施灾难恢复解决方案：

- 有效的 Red Hat OpenShift Data Foundation 高级订阅。
- 有效的 Red Hat Advanced Cluster Management (RHACM) for Kubernetes 订阅。

要了解 OpenShift Data Foundation 订阅如何工作，请参阅与 OpenShift Data Foundation 订阅相关的知识库文章。

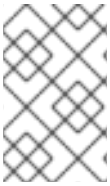
如需更多与灾难恢复相关的信息，请参阅 Configuring OpenShift Data Foundation Disaster Recovery for OpenShift Workloads 指南，以及 Red Hat Advanced Cluster Management for Kubernetes 文档中的 安装指南中的 *Requirements and recommendations* 部分。

仲裁程序扩展集群要求 [技术预览]

在这种情况下，单个集群将扩展到两个区域，并有第三个区域作为仲裁者的位置。这是一个技术预览功能，主要用于在 OpenShift Container Platform 内部部署，以及在相同的数据中心中进行部署。对于在多个数据中心上扩展部署，不建议使用这个解决方案。相反，考虑使用 Metro-DR 作为第一个选项，以便在具有低延迟网络的多个数据中心中部署任何数据丢失 DR 解决方案。

有关具体要求和说明的信息，请参阅 *为扩展集群配置 OpenShift Data Foundation* 中的知识库文章。

要了解 OpenShift Data Foundation 订阅如何工作，请参阅与 OpenShift Data Foundation 订阅相关的知识库文章。



注意

您无法同时启用 Flexible scaling 和 Arbiter，因为它们的扩展逻辑有冲突。通过灵活扩展，您可以一次向 OpenShift Data Foundation 集群添加一个节点。但在仲裁集群中，您需要在两个数据区中至少添加一个节点。

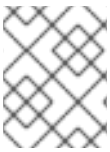
启动节点最低要求

在不满足标准部署的资源要求时，OpenShift Data Foundation 集群将使用最低配置配置。

如需更多信息，请参阅规划指南中的*资源要求*部分。

第 2 章 使用动态存储设备进行部署

使用 VMware vSphere 提供的动态存储设备（磁盘格式：精简）在 OpenShift Container Platform 上部署 OpenShift Data Foundation 为您提供了创建内部集群资源的选项。这将会在内部置备基础服务，这有助于为应用提供额外的存储类。



注意

VMware vSphere 上均支持内部和外部 OpenShift Data Foundation 集群。如需有关部署要求的更多信息，请参阅规划部署。

另外，确保已满足 准备部署 OpenShift Data Foundation 章节的要求，然后按照以下步骤使用动态存储设备进行部署：

1. 安装 Red Hat OpenShift Data Foundation Operator 。
2. 创建 OpenShift Data Foundation 集群。

2.1. 安装 RED HAT OPENSHIFT DATA FOUNDATION OPERATOR

您可以使用 Red Hat OpenShift Container Platform Operator Hub 安装 Red Hat OpenShift Data Foundation Operator。

先决条件

- 使用具有 **cluster-admin** 和 operator 安装权限的账户访问 OpenShift Container Platform 集群。
- 您必须在 Red Hat OpenShift Container Platform 集群中至少有三个 worker 节点。每个节点都应该包含一个磁盘，需要 3 个磁盘(PV)。但是，一个 PV 最终会默认未使用。这是预期的行为。
- 有关其他资源要求，请参阅规划您的部署指南。

重要

- 当您需要覆盖 OpenShift Data Foundation 的集群范围默认节点选择器时，您可以使用以下命令为 **openshift-storage** 命名空间指定空白节点选择器（在这种情况下创建 **openshift-storage** 命名空间）：

  ```
  $ oc annotate namespace openshift-storage openshift.io/node-selector=
  ```

- 将节点作为 **infra** 污点，以确保只在该节点上调度 Red Hat OpenShift Data Foundation 资源。这有助于您节省订阅成本。如需更多信息，请参阅管理和分配存储资源指南中的*如何将专用 worker 节点用于 Red Hat OpenShift Data Foundation* 部分。

流程

1. 登录 OpenShift Web 控制台。
2. 点 **Operators → OperatorHub**。
3. 在 **Filter by keyword** 框中滚动或键入 **OpenShift Data Foundation**，以查找 **OpenShift Data Foundation** Operator。

4. 点 **Install**。

5. 在 **Install Operator** 页面中设置以下选项：

   a. 更新频道为 **stable-4.12**。

   b. 安装模式是 **A specific namespace on the cluster**。

   c. Installed Namespace 为 **Operator recommended namespace openshift-storage**。如果命名空间 **openshift-storage** 不存在，它会在 Operator 安装过程中创建。

   d. 将 Approval Strategy 选为 **Automatic** 或 **Manual**。
   如果选择 **Automatic** 更新，Operator Lifecycle Manager(OLM)将自动升级 Operator 的运行实例，而无需任何干预。

   如果选择 **手动** 更新，则 OLM 会创建一个更新请求。作为集群管理员，您必须手动批准该更新请求，才能将 Operator 更新至更新的版本。

   e. 确保为 **Console 插件** 选择了 **Enable** 选项。

   f. 点 **Install**。

验证步骤

- 成功安装 Operator 后，用户界面中会显示一个带有 **Web console update is available** 信息的弹出窗口。点这个弹出窗口中的 **Refresh web console** 来反映控制台的更改。

- 在 Web 控制台中：

  - 进入到 Installed Operators，再验证 **OpenShift Data Foundation** Operator 是否显示绿色勾号，指示安装成功。

  - 进入到 **Storage**，再验证 **Data Foundation** 仪表板是否可用。

2.2. 使用 TOKEN 验证方法通过 KMS 启用集群范围的加密

您可以在密码库中启用用于令牌身份验证的键值后端路径和策略。

先决条件

- 管理员对 vault 的访问权限。

- 有效的 Red Hat OpenShift Data Foundation 高级订阅。如需更多信息，请参阅 OpenShift Data Foundation 订阅中的知识库文章。

- 仔细选择唯一路径名称作为遵循命名惯例的后端**路径**，因为它无法在以后更改。

流程

1. 在密码库中启用 Key/Value(KV)后端路径。
   对于 vault KV 机密引擎 API，版本 1：

   ```
   $ vault secrets enable -path=odf kv
   ```

   对于 vault KV 机密引擎 API，版本 2：

   ```
   -
   ```

```
$ vault secrets enable -path=odf kv-v2
```

2. 创建策略来限制用户在 secret 上执行写入或删除操作：

```
echo '
path "odf/*" {
  capabilities = ["create", "read", "update", "delete", "list"]
}
path "sys/mounts" {
capabilities = ["read"]
}'| vault policy write odf -
```

3. 创建与上述策略匹配的令牌：

```
$ vault token create -policy=odf -format json
```

2.3. 使用 KUBERNETES 身份验证方法通过 KMS 启用集群范围的加密

您可以使用密钥管理系统(KMS)为集群范围的加密启用 Kubernetes 验证方法。

先决条件

- 管理员对 Vault 的访问权限。
- 有效的 Red Hat OpenShift Data Foundation 高级订阅。如需更多信息，请参阅 OpenShift Data Foundation 订阅中的知识库文章。
- OpenShift Data Foundation 操作器必须从 Operator Hub 安装。
- 仔细选择唯一路径名称作为后端 **路径**，请仔细选择命名规则。您不能在以后更改此路径名称。

流程

1. 创建服务帐户：

```
$ oc -n openshift-storage create serviceaccount <serviceaccount_name>
```

其中, ***<serviceaccount_name>*** 指定服务帐户的名称。

例如：

```
$ oc -n openshift-storage create serviceaccount odf-vault-auth
```

2. 创建 **clusterrolebindings** 和 **clusterroles**:

```
$ oc -n openshift-storage create clusterrolebinding vault-tokenreview-binding --
clusterrole=system:auth-delegator --serviceaccount=openshift-
storage:_<serviceaccount_name>_
```

例如：

```
$ oc -n openshift-storage create clusterrolebinding vault-tokenreview-binding --
clusterrole=system:auth-delegator --serviceaccount=openshift-storage:odf-vault-auth
```

3. 为 **serviceaccount** 令牌和 CA 证书创建 secret。

```
$ cat <<EOF | oc create -f -
apiVersion: v1
kind: Secret
metadata:
  name: odf-vault-auth-token
  namespace: openshift-storage
  annotations:
    kubernetes.io/service-account.name: <serviceaccount_name>
type: kubernetes.io/service-account-token
data: {}
EOF
```

其中，***<serviceaccount_name>*** 是上一步中创建的服务帐户。

4. 从 secret 获取令牌和 CA 证书。

```
$ SA_JWT_TOKEN=$(oc -n openshift-storage get secret odf-vault-auth-token -o jsonpath="
{.data['token']}" | base64 --decode; echo)
$ SA_CA_CRT=$(oc -n openshift-storage get secret odf-vault-auth-token -o jsonpath="
{.data['ca\.crt']}" | base64 --decode; echo)
```

5. 检索 OCP 集群端点。

```
$ OCP_HOST=$(oc config view --minify --flatten -o jsonpath="{.clusters[0].cluster.server}")
```

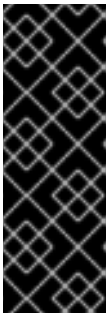
6. 获取服务帐户签发者：

```
$ oc proxy &
$ proxy_pid=$!
$ issuer="$( curl --silent http://127.0.0.1:8001/.well-known/openid-configuration | jq -r
.issuer)"
$ kill $proxy_pid
```

7. 使用上一步中收集的信息在 Vault 中设置 Kubernetes 身份验证方法：

```
$ vault auth enable kubernetes
```

```
$ vault write auth/kubernetes/config \
        token_reviewer_jwt="$SA_JWT_TOKEN" \
        kubernetes_host="$OCP_HOST" \
        kubernetes_ca_cert="$SA_CA_CRT" \
        issuer="$issuer"
```



重要

当签发者为空时，在 Vault 中配置 Kubernetes 验证方法：

```
$ vault write auth/kubernetes/config \
        token_reviewer_jwt="$SA_JWT_TOKEN" \
        kubernetes_host="$OCP_HOST" \
        kubernetes_ca_cert="$SA_CA_CRT"
```

8. 在 Vault 中启用 Key/Value(KV)后端路径。
   对于 Vault KV secret 引擎 API，版本 1：

   ```
   $ vault secrets enable -path=odf kv
   ```

   对于 Vault KV secret 引擎 API，版本 2：

   ```
   $ vault secrets enable -path=odf kv-v2
   ```

9. 创建策略来限制用户在 secret 上执行**写入**或**删除**操作：

   ```
   echo '
   path "odf/*" {
     capabilities = ["create", "read", "update", "delete", "list"]
   }
   path "sys/mounts" {
   capabilities = ["read"]
   }'| vault policy write odf -
   ```

10. 生成角色：

    ```
    $ vault write auth/kubernetes/role/odf-rook-ceph-op \
          bound_service_account_names=rook-ceph-system,rook-ceph-osd,noobaa \
          bound_service_account_namespaces=openshift-storage \
          policies=odf \
          ttl=1440h
    ```

    在创建存储系统期间配置 KMS 连接详情时，会稍后使用角色 **odf-rook-ceph-op**。

    ```
    $ vault write auth/kubernetes/role/odf-rook-ceph-osd \
          bound_service_account_names=rook-ceph-osd \
          bound_service_account_namespaces=openshift-storage \
          policies=odf \
          ttl=1440h
    ```

2.4. 创建 MULTUS 网络 [技术预览]

OpenShift Container Platform 使用 Multus CNI 插件来实现对 CNI 插件的链接。您可以在集群安装过程中配置默认 pod 网络。默认网络处理集群中的所有一般网络流量。

您可以基于可用的 CNI 插件定义额外网络，并将一个或多个此类网络附加到 pod。要将额外网络接口附加到 pod，您必须创建配置来定义接口的附加方式。

您可以使用 NetworkAttachmentDefinition（NAD）自定义资源 (CR) 来指定每个接口。每个 NetworkAttachmentDefinition 中的 CNI 配置定义如何创建该接口。

OpenShift Data Foundation 使用名为 macvlan 的 CNI 插件。创建基于 macvlan 的额外网络可让主机上的 pod 通过使用物理网络接口与其他主机和那些主机上的 pod 通信。附加到基于 macvlan 的额外网络的每个 pod 都会获得一个唯一的 MAC 地址。

重要

Multus 支持是一个技术预览功能，它只受支持并在裸机和 VMWare 部署中测试。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

如需更多信息，请参阅技术预览功能支持范围。

2.4.1. 创建网络附加定义

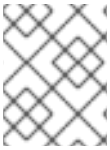
要使用 Multus，需要已使用正确网络配置的集群，请参阅推荐的网络配置和 Multus 配置要求。新创建的 NetworkAttachmentDefinition(NAD)可以在 Storage Cluster 安装过程中选择。这就是必须在存储集群之前创建它们的原因。

您可以在存储集群安装过程中选择新创建的 **NetworkAttachmentDefinition** (NAD)。这是您在创建存储集群前必须创建 NAD 的原因。

如规划指南中所述，您创建的 Multus 网络取决于您用于 OpenShift Data Foundation 流量的可用网络接口数量。可以将所有存储流量分隔到两个接口中的一个接口（一个用于默认 OpenShift SDN），或者将存储流量进一步分隔到客户端存储流量（公共）和存储复制流量（私有或集群）。

以下是同一接口上所有存储流量（公共和集群）的 **NetworkAttachmentDefinition** 示例。它要求所有可调度节点上有一个额外的接口（OpenShift 默认 SDN 在单独的网络接口上）：

```
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: ocs-public-cluster
  namespace: openshift-storage
spec:
  config: '{
   "cniVersion": "0.3.1",
   "type": "macvlan",
   "master": "ens2",
   "mode": "bridge",
   "ipam": {
        "type": "whereabouts",
        "range": "192.168.1.0/24"
   }
  }'
```



注意

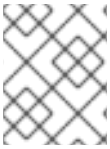
所有网络接口名称必须在附加至 Multus 网络的所有节点上相同（即 **ocs-public-cluster**的 **ens2** ）。

以下是用于单独 Multus 网络上存储流量的 **NetworkAttachmentDefinition** 示例，适用于客户端存储流量，以及用于复制流量的集群。它需要在用于托管 Object Storge Device (OSD) pod 的 OpenShift 节点上有额外两个接口，在所有其他可调度的节点上有一个额外的接口（OpenShift 默认 SDN 在单独的网络接口上）：

```
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: ocs-public
  namespace: openshift-storage
spec:
  config: '{
   "cniVersion": "0.3.1",
   "type": "macvlan",
   "master": "ens2",
   "mode": "bridge",
   "ipam": {
        "type": "whereabouts",
        "range": "192.168.1.0/24"
   }
  }'
```

NetworkAttachmentDefinition 示例：

```
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: ocs-cluster
  namespace: openshift-storage
spec:
  config: '{
   "cniVersion": "0.3.1",
   "type": "macvlan",
   "master": "ens3",
   "mode": "bridge",
   "ipam": {
        "type": "whereabouts",
        "range": "192.168.2.0/24"
   }
  }'
```



注意

所有网络接口名称必须在附加至 Multus 网络的所有节点上相同（即，**ens2** 用于 **ocs-public**，**ens3** 用于 **ocs-cluster**）。

2.5. 创建 OPENSHIFT DATA FOUNDATION 集群

安装 OpenShift Data Foundation 操作器（operator）后，创建 OpenShift Data Foundation。

先决条件

- OpenShift Data Foundation 操作器必须从 Operator Hub 安装。如需更多信息，请参阅 安装 OpenShift Data Foundation Operator。

- 对于 VMware 上的虚拟机，请确保将 **disk.EnableUUID** 选项设置为 **TRUE**。您需要具有 vCenter 帐户特权才能配置虚拟机。如需更多信息，请参阅所需的 vCenter 帐户权限。要设置 **disk.EnableUUID** 选项，请使用 **Customize hardware** 选项卡中的 **VM Options** 的 **Advanced** 选项。如需更多信息，请参阅在 vSphere 上安装。
- （可选）如果要使用厚置备的存储来获得灵活性，您必须创建一个 **zeroedthick** 或 **eagerzeroedthick** 磁盘格式的储类。如需更多信息，请参阅 VMware vSphere 对象定义。
- 如果要使用为技术预览功能的 multus 支持，在部署前您必须创建以后附加到集群的网络附加定义 (NAD)。如需更多信息，请参阅创建网络附加定义。

流程

1. 在 OpenShift Web 控制台中，点 **Operators → Installed Operators** 查看所有已安装的 Operator。
   确保所选 **项目** 为 **openshift-storage**。
2. 点 **OpenShift Data Foundation** 操作器，然后单击 **Create StorageSystem**。
3. 在 **Backing storage** 页面中，选择以下内容：
   a. 为 **Deployment 类型**选项选择 **Full Deployment**。
   b. 选择 **Use a existing StorageClass** 选项。
   c. 选择 **Storage Class**。
   默认情况下，设置为 **thin**。如果您为 thick 置备存储创建了带有 **zeroedthick** 或 **eagerzeroedthick** 磁盘格式的存储类，那么除默认的 **精简** 存储类外，还会列出该存储类。
   d. 点 **Next**。
4. 在 **Capacity and nodes** 页面中，提供必要的信息：
   a. 从下拉列表中选择 **Requested Capacity** 的值。默认设置为 **2 TiB**。

   注意

   选择初始存储容量后，集群扩展将使用所选的可用容量（原始存储的三倍）执行。

   b. 在 **Select Nodes** 部分中，选择至少三个可用节点。
   c. 可选：选中 **Taint nodes** 复选框，以将所选节点专用于 OpenShift Data Foundation。
   将 worker 节点分布到三个不同的物理节点、机架或故障域以实现高可用性。

   使用 vCenter 反关联性将 OpenShift Data Foundation 机架标签与数据中心中的物理节点和机架保持对齐，以避免在同一物理机箱上调度两个 worker 节点。

   如果选择的节点与 OpenShift Data Foundation 的一个聚合的 30 个 CPU 和 72 GiB RAM 的要求不匹配，则会部署一个最小的集群。如需最低起始节点要求，请参阅规划指南中的资源要求部分。

   选中 **Taint nodes** 复选框，使所选节点专门用于 OpenShift Data Foundation。
   d. 点 **Next**。

5. 可选：在 **Security and network** 页面中，根据您的要求进行配置：

   a. 若要启用加密，可选择为**块存储和文件存储启用数据加密。**

   b. 选择其中一个加密级别或两个都选：

   - **集群范围的加密**
     加密整个集群（块和文件）。

   - **StorageClass 加密**
     使用启用加密的存储类创建加密的持久性卷（仅块）。

   c. 可选：选择 **Connect to an external key management service** 复选框。这是集群范围加密的可选选项。

      i. 从 **Key Management Service Provider** 下拉列表中，选择 **Vault** 或 **Thales CipherTrust Manager (using KMIP)**。如果选择了 **Vault**，请进入下一步。如果您选择了 **Thales CipherTrust Manager （using KMIP）**，请转到步骤 iii。

      ii. 选择**身份验证方法**。

      使用令牌验证方法

      - 输入唯一的**连接名称** , Vault 服务器的主机**地址**（'https://<hostname 或 ip>'），**端口**号和**令牌**。
      - 展开 **Advanced Settings**，以根据您的 **Vault** 配置输入其他设置和证书详情：
        - 在 **后端路径**中输入为 OpenShift Data Foundation 专用且唯一的 Key Value secret 路径。
        - （可选）输入 **TLS 服务器名称**和 **Vault Enterprise 命名空间**。
        - 上传对应的 PEM 编码证书文件，以提供 **CA 证书**、**客户端证书**和**客户端私钥**。
        - 点 **Save** 并跳过步骤 iv。

      使用 Kubernetes 验证方法

      - 输入唯一的 Vault **Connection Name**, Vault 服务器的主机**地址**（'https://<hostname 或 ip>'）、**端口**号和**角色**名称。
      - 展开 **Advanced Settings**，以根据您的 **Vault** 配置输入其他设置和证书详情：
        - 在 **后端路径**中输入为 OpenShift Data Foundation 专用且唯一的 Key Value secret 路径。
        - 可选：输入 **TLS Server Name** 和 **Authentication Path**（如果适用）。
        - 上传对应的 PEM 编码证书文件，以提供 **CA 证书**、**客户端证书**和**客户端私钥**。
        - 点 **Save** 并跳过步骤 iv。

      iii. 要使用 **Thales CipherTrust Manager (using KMIP)** 作为 KMS 供应商，请按照以下步骤执行：

A. 在项目中输入密钥管理服务的唯一**连接名称**。

B. 在 **Address** 和 **Port** 部分中，输入 Thales CipherTrust Manager 的 IP 以及在其中启用了 KMIP 接口的端口。例如：

- **地址**: 123.34.3.2
- **端口** ：5696

C. 上传 **客户端证书**、**CA 证书**和 **客户端私钥**。

D. 如果启用了 StorageClass 加密，请输入用于加密和解密的唯一标识符。

E. **TLS Server** 字段是可选的，并在没有 KMIP 端点的 DNS 条目时使用。例如，**kmip_all_<port>.ciphertrustmanager.local**。

iv. 选择 **网络**。

d. 如果使用一个单一网络，选择 **Default** (SDN)；如果使用多个网络借口，选择 **Custom** (Multus) Network。

i. 从下拉菜单中选择**公共网络接口**。

ii. 从下拉菜单中选择**集群网络接口**。

注意

如果您只使用一个额外网络接口，请选择单个 **NetworkAttachementDefinition**，即 **ocs-public-cluster** 用于 **公共网络接口**，并将 **Cluster Network Interface** 留空。

iii. 点 **Next**。

6. 在 **Review and create** 页面中，检查配置详情。
若要修改任何配置设置，请单击 **Back**。

7. 单击 **Create StorageSystem**。

验证步骤

- 验证已安装存储集群的最终状态：

a. 在 OpenShift Web 控制台中，导航到 **Installed Operators → OpenShift Data Foundation → Storage System → ocs-storagecluster-storagesystem → Resources**。

b. 验证 **StorageCluster** 的 **Status** 是否为 **Ready**，并且旁边有一个绿色勾号标记。

1. 要验证 OpenShift 数据基础的所有组件是否已成功安装，请参阅验证您的 OpenShift Data Foundation 部署。

2. 要验证多网络(Multus)，请参阅验证 Multus 网络。

其他资源

要启用 Overprovision Control 警报，请参阅 Monitoring 中的 Alerts 指南。

第 3 章 使用本地存储设备部署

使用本地存储设备在 OpenShift Container Platform 上部署 OpenShift Data Foundation 为您提供创建内部集群资源的选项。这将会在内部置备基础服务，这有助于为应用提供额外的存储类。

使用本节在已安装 OpenShift Container Platform 的 VMware 上部署 OpenShift Data Foundation。

另外，在执行后续步骤前，请确保您已满足 准备部署 OpenShift Data Foundation 章节的要求。

1. 安装 Local Storage Operator
2. 安装 Red Hat OpenShift Data Foundation Operator 。
3. 创建 OpenShift Data Foundation 集群。

3.1. 安装 LOCAL STORAGE OPERATOR

在本地存储设备上创建 Red Hat OpenShift Data Foundation 集群前，请先从 Operator Hub 安装 Local Storage Operator。

流程

1. 登录 OpenShift Web 控制台。
2. 点 **Operators → OperatorHub**。
3. 在 **Filter by keyword** 框中键入 **local storage**，从操作器列表中搜索 **Local Storage operator** 并单击它。
4. 在 **Install Operator** 页面中设置以下选项：
   a. 将频道更新为 **4.12** 或 **stable**。
   b. 安装模式是 **A specific namespace on the cluster**。
   c. Installed Namespace 为 **Operator recommended namespace openshift-local-storage**。
   d. 将批准更新为 **Automatic**。
5. 点 **Install**。

验证步骤

- 验证 Local Storage Operator 是否显示绿色勾号，代表安装成功。

3.2. 安装 RED HAT OPENSHIFT DATA FOUNDATION OPERATOR

您可以使用 Red Hat OpenShift Container Platform Operator Hub 安装 Red Hat OpenShift Data Foundation Operator。

先决条件

- 使用具有 **cluster-admin** 和 operator 安装权限的账户访问 OpenShift Container Platform 集群。

- 您必须在 Red Hat OpenShift Container Platform 集群中至少有三个 worker 节点。每个节点都应该包含一个磁盘，需要 3 个磁盘(PV)。但是，一个 PV 最终会默认未使用。这是预期的行为。
- 有关其他资源要求，请参阅规划您的部署指南。

重要

- 当您需要覆盖 OpenShift Data Foundation 的集群范围默认节点选择器时，您可以使用以下命令为 **openshift-storage** 命名空间指定空白节点选择器（在这种情况下创建 **openshift-storage** 命名空间）：

```
$ oc annotate namespace openshift-storage openshift.io/node-selector=
```

- 将节点作为 **infra** 污点，以确保只在该节点上调度 Red Hat OpenShift Data Foundation 资源。这有助于您节省订阅成本。如需更多信息，请参阅管理和分配存储资源指南中的*如何将专用 worker 节点用于 Red Hat OpenShift Data Foundation* 部分。

流程

1. 登录 OpenShift Web 控制台。
2. 点 **Operators → OperatorHub**。
3. 在 **Filter by keyword** 框中滚动或键入 **OpenShift Data Foundation**，以查找 **OpenShift Data Foundation** Operator。
4. 点 **Install**。
5. 在 **Install Operator** 页面中设置以下选项：
   a. 更新频道为 **stable-4.12**。
   b. 安装模式是 **A specific namespace on the cluster**。
   c. Installed Namespace 为 **Operator recommended namespace openshift-storage**。如果命名空间 **openshift-storage** 不存在，它会在 Operator 安装过程中创建。
   d. 将 Approval Strategy 选为 **Automatic** 或 **Manual**。
   如果选择 **Automatic** 更新，Operator Lifecycle Manager(OLM)将自动升级 Operator 的运行实例，而无需任何干预。

   如果选择 **手动** 更新，则 OLM 会创建一个更新请求。作为集群管理员，您必须手动批准该更新请求，才能将 Operator 更新至更新的版本。
   e. 确保为 **Console 插件** 选择了 **Enable** 选项。
   f. 点 **Install**。

验证步骤

- 成功安装 Operator 后，用户界面中会显示一个带有 **Web console update is available** 信息的弹出窗口。点这个弹出窗口中的 **Refresh web console** 来反映控制台的更改。
- 在 Web 控制台中：

- 进入到 Installed Operators，再验证 **OpenShift Data Foundation** Operator 是否显示绿色勾号，指示安装成功。
- 进入到 **Storage**，再验证 **Data Foundation** 仪表板是否可用。

3.3. 创建 MULTUS 网络 [技术预览]

OpenShift Container Platform 使用 Multus CNI 插件来实现对 CNI 插件的链接。您可以在集群安装过程中配置默认 pod 网络。默认网络处理集群中的所有一般网络流量。

您可以基于可用的 CNI 插件定义额外网络，并将一个或多个此类网络附加到 pod。要将额外网络接口附加到 pod，您必须创建配置来定义接口的附加方式。

您可以使用 NetworkAttachmentDefinition（NAD）自定义资源 (CR) 来指定每个接口。每个 NetworkAttachmentDefinition 中的 CNI 配置定义如何创建该接口。

OpenShift Data Foundation 使用名为 macvlan 的 CNI 插件。创建基于 macvlan 的额外网络可让主机上的 pod 通过使用物理网络接口与其他主机和那些主机上的 pod 通信。附加到基于 macvlan 的额外网络的每个 pod 都会获得一个唯一的 MAC 地址。

重要

Multus 支持是一个技术预览功能，它只受支持并在裸机和 VMWare 部署中测试。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

如需更多信息，请参阅技术预览功能支持范围。

3.3.1. 创建网络附加定义

要使用 Multus，需要已使用正确网络配置的集群，请参阅推荐的网络配置和 Multus 配置要求。新创建的 NetworkAttachmentDefinition(NAD)可以在 Storage Cluster 安装过程中选择。这就是必须在存储集群之前创建它们的原因。

您可以在存储集群安装过程中选择新创建的 **NetworkAttachmentDefinition** (NAD)。这是您在创建存储集群前必须创建 NAD 的原因。

如规划指南中所述，您创建的 Multus 网络取决于您用于 OpenShift Data Foundation 流量的可用网络接口数量。可以将所有存储流量分隔到两个接口中的一个接口（一个用于默认 OpenShift SDN），或者将存储流量进一步分隔到客户端存储流量（公共）和存储复制流量（私有或集群）。

以下是同一接口上所有存储流量（公共和集群）的 **NetworkAttachmentDefinition** 示例。它要求所有可调度节点上有一个额外的接口（OpenShift 默认 SDN 在单独的网络接口上）：

```
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: ocs-public-cluster
  namespace: openshift-storage
spec:
  config: '{
   "cniVersion": "0.3.1",
   "type": "macvlan",
   "master": "ens2",
```

```
 "mode": "bridge",
 "ipam": {
      "type": "whereabouts",
      "range": "192.168.1.0/24"
 }
}'
```

注意

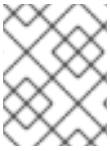
所有网络接口名称必须在附加至 Multus 网络的所有节点上相同（即 **ocs-public-cluster**的 **ens2** ）。

以下是用于单独 Multus 网络上存储流量的 **NetworkAttachmentDefinition** 示例，适用于客户端存储流量，以及用于复制流量的集群。它需要在用于托管 Object Storge Device (OSD) pod 的 OpenShift 节点上有额外两个接口，在所有其他可调度的节点上有一个额外的接口（OpenShift 默认 SDN 在单独的网络接口上）：

```
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: ocs-public
  namespace: openshift-storage
spec:
  config: '{
   "cniVersion": "0.3.1",
   "type": "macvlan",
   "master": "ens2",
   "mode": "bridge",
   "ipam": {
        "type": "whereabouts",
        "range": "192.168.1.0/24"
   }
  }'
```

NetworkAttachmentDefinition 示例：

```
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: ocs-cluster
  namespace: openshift-storage
spec:
  config: '{
   "cniVersion": "0.3.1",
   "type": "macvlan",
   "master": "ens3",
   "mode": "bridge",
   "ipam": {
        "type": "whereabouts",
        "range": "192.168.2.0/24"
   }
  }'
```



注意

所有网络接口名称必须在附加至 Multus 网络的所有节点上相同（即，**ens2** 用于 **ocs-public**，**ens3** 用于 **ocs-cluster**）。

3.4. 在 VMWARE VSPHERE 上创建 OPENSHIFT DATA FOUNDATION

VMware vSphere 支持以下三种类型的本地存储：

- 虚拟机磁盘 (VMDK)
- 原始设备映射 (RDM)
- VMDirectPath I/O

先决条件

- 确保满足使用本地存储设备安装 OpenShift Data Foundation 的要求部分中的所有要求。
- 您必须至少有三个 worker 节点，其存储类型和大小与每个节点相同，才能在 VMware 上使用本地存储设备。
- 对于 VMware vSphere 上的虚拟机，请确保将 **disk.EnableUUID** 选项设置为 **TRUE**。您需要具有 vCenter 帐户特权才能配置虚拟机。如需更多信息，请参阅所需的 vCenter 帐户权限。要设置 **disk.EnableUUID** 选项，请使用 **Customize hardware** 选项卡中的 **VM Options** 的 **Advanced** 选项。如需更多信息，请参阅在 vSphere 上安装。
- 如果要使用为技术预览功能的 multus 支持，在部署前您必须创建以后附加到集群的网络附加定义 (NAD)。如需更多信息，请参阅 Multi network 插件(Multus)支持 和创建网络附加定义。

流程

1. 在 OpenShift Web 控制台中，点 **Operators → Installed Operators** 查看所有已安装的 Operator。
   确保所选 **项目** 为 **openshift-storage**。
2. 单击 **OpenShift Data Foundation** 操作器，然后单击 **Create StorageSystem**。
3. 在 Backing storage 页面中，执行以下操作：
   a. 为**部署类型**选择选择**完全部署**。
   b. 选择 **Create a new StorageClass using the local storage devices**选项。
   c. 点 Next。

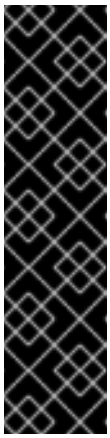
   注意

   如果还没有安装，系统会提示您安装 Local Storage Operator。点 **Install** 并按照以下步骤进行操作，如 Installing Local Storage Operator 所述。

4. 在 Create local volume set 页面中，提供以下信息：
   a. 为 **LocalVolumeSet** 和 **StorageClass** 输入一个名称。
   默认情况下，存储类名称会出现本地卷集名称。您可以更改名称。

b. 任选以下一项：

- **所有节点上的磁盘**，以使用与所有节点上所选过滤器匹配的可用磁盘。
- **选定节点上的磁盘**，以使用仅与所选节点上的所选过滤器匹配的可用磁盘。



重要

- 只有在您使用 3 个或更多节点创建的存储集群分布到 3 个可用区的最低要求时，才会启用灵活的扩展功能。
  有关灵活扩展的信息，请参阅知识库文章 *在启用灵活扩展时使用 YAML 扩展 OpenShift Data Foundation 集群*。
- 灵活扩展功能会在部署时启用，以后无法启用或禁用。
- 如果选择的节点与 OpenShift Data Foundation 的一个聚合的 30 个 CPU 和 72 GiB RAM 的要求不匹配，则会部署一个最小的集群。
  如需最低起始节点要求，请参阅规划指南中的资源要求部分。

c. 从可用 **Disk Type** 列表中，选择 **SSD/NVMe**。

d. 展开 **Advanced** 部分并设置以下选项：

卷模式	默认会选择块。
设备类型	从下拉列表中选择一个或多个设备类型。
磁盘大小	为设备设置最小 100GB 大小，以及需要包含的设备的最大可用大小。
磁盘限制上限	这表示节点上可以创建的 PV 数量上限。如果此字段留空，则为匹配节点上的所有可用磁盘创建 PV。

e. 点 **Next**。
此时会显示一个用于确认创建 LocalVolumeSet 的弹出窗口。

f. 单击 **Yes** 以继续。

5. 在 Capacity 和 nodes 页面中，配置以下内容：

a. **可用的原始容量**会根据与存储类关联的所有附加磁盘填充容量值。这将需要一些时间才能出现。**Selected nodes** 列表根据存储类显示节点。

b. 可选：选中 **Taint nodes** 复选框，以将所选节点专用于 OpenShift Data Foundation。

c. 点 **Next**。

6. 可选：在 Security and network 页面中，根据您的要求进行配置：

a. 若要启用加密，可选择为**块存储和文件存储启用数据加密。**

b. 选择以下**加密级别**之一：

- **Cluster-wide encryption** 来加密整个集群（块存储和文件存储）。
- **Storage class encryption** 以使用加密启用的存储类创建加密的持久性卷（仅限块）。

c. 可选：选择 **Connect to an external key management service**复选框。这是集群范围加密的可选选项。

i. 从 **Key Management Service Provider**下拉列表中，选择 **Vault** 或 **Thales CipherTrust Manager (using KMIP)**。如果选择了 **Vault**，请进入下一步。如果您选择了 **Thales CipherTrust Manager （using KMIP）**，请转到步骤 iii。

ii. 选择**身份验证方法**。

使用令牌验证方法

- 输入唯一的**连接名称** , Vault 服务器的主机**地址**（'https://<hostname 或 ip>'），**端口**号和**令牌**。
- 展开 **Advanced Settings**，以根据您的 **Vault** 配置输入其他设置和证书详情：
  - 在 **后端路径**中输入为 OpenShift Data Foundation 专用且唯一的 Key Value secret 路径。
  - （可选）输入 **TLS 服务器名称**和 **Vault Enterprise 命名空间**。
  - 上传对应的 PEM 编码证书文件，以提供 **CA 证书**、**客户端证书**和**客户端私钥**。
  - 点 **Save** 并跳过步骤 iv。

使用 Kubernetes 验证方法

- 输入唯一的 Vault **Connection Name**, Vault 服务器的主机**地址**（'https://<hostname 或 ip>'）、**端口**号和**角色**名称。
- 展开 **Advanced Settings**，以根据您的 **Vault** 配置输入其他设置和证书详情：
  - 在 **后端路径**中输入为 OpenShift Data Foundation 专用且唯一的 Key Value secret 路径。
  - 可选：输入 **TLS Server Name** 和 **Authentication Path**（如果适用）。
  - 上传对应的 PEM 编码证书文件，以提供 **CA 证书**、**客户端证书**和**客户端私钥**。
  - 点 **Save** 并跳过步骤 iv。

iii. 要使用 **Thales CipherTrust Manager (using KMIP)** 作为 KMS 供应商，请按照以下步骤执行：

A. 在项目中输入密钥管理服务的唯一**连接名称**。

B. 在 **Address** 和 **Port** 部分中，输入 Thales CipherTrust Manager 的 IP 以及在其中启用了 KMIP 接口的端口。例如：

- **地址**: 123.34.3.2
- **端口** ：5696

C. 上传 **客户端证书**、**CA 证书**和 **客户端私钥**。

D. 如果启用了 StorageClass 加密，请输入用于加密和解密的唯一标识符。

E. **TLS Server** 字段是可选的，并在没有 KMIP 端点的 DNS 条目时使用。例如，**kmip_all_<port>.ciphertrustmanager.local**。

iv. 选择 **网络**。

d. 任选以下一项：

- 如果您使用的是单一网络，请选择 **Default(SDN)**。
- 如果您使用多个网络接口，请选择 **Custom(Multus)**。
  i. 从下拉菜单中选择**公共网络接口**。
  ii. 从下拉菜单中选择**集群网络接口**。

注意

如果您只使用一个额外网络接口，请选择单个 **NetworkAttachementDefinition**，即**ocs-public-cluster** 用于公共网络接口，并将 Cluster Network Interface 留空。

e. 点 **Next**。

7. 在 Review and create 页面中，检查配置详情。
   - 若要修改任何配置设置，请单击 **Back** 以返回到上一配置页面。
8. 单击 **Create StorageSystem**。

验证步骤

- 验证已安装存储集群的最终状态：
  a. 在 OpenShift Web 控制台中，导航到 **Installed Operators → OpenShift Data Foundation → Storage System → ocs-storagecluster-storagesystem → Resources**。
  b. 验证 **StorageCluster** 的 **Status** 是否为 **Ready**，并且旁边有一个绿色勾号标记。
- 要验证是否在存储集群中启用了灵活的扩展，请执行以下步骤（对于仲裁模式，请禁用灵活的扩展）：
  1. 在 OpenShift Web 控制台中，导航到 **Installed Operators → OpenShift Data Foundation → Storage System → ocs-storagecluster-storagesystem → Resources**。
  2. 在 YAML 选项卡中，在 **spec** 部分搜索键 **flexibleScaling**，在 **status** 部分搜索 **failureDomain**。如果 **flexible scaling** 为 true，**failureDomain** 被设置为 host，则启用灵活的扩展功能。

```
spec:
flexibleScaling: true
[…]
status:
failureDomain: host
```

- 要验证 OpenShift 数据基础的所有组件是否已成功安装，请参阅验证您的 OpenShift Data Foundation 部署。

- 要验证多网络(Multus)，请参阅验证 Multus 网络。

其他资源

- 若要扩展初始集群的容量，请参阅扩展存储指南。

第 4 章 验证 OPENSHIFT DATA FOUNDATION

使用本节验证 OpenShift Data Foundation 是否已正确部署。

4.1. 验证 POD 的状态

流程

1. 从 OpenShift Web 控制台点 **Workloads → Pods**。
2. 从 **Project** 下拉列表中选择 **openshift-storage**。

注意

如果禁用 **Show default projects** 选项，请使用切换按钮列出所有默认项目。

有关每个组件预期的 pod 数量及其变化取决于节点数量的更多信息，请参阅 表 4.1 "对应 OpenShift Data Foundation 集群的 Pod"。

3. 为 Running 和 Completed pod 设置过滤器，以验证以下 pod 是否处于 **Running** 和 **Completed** 状态：

表 4.1. 对应 OpenShift Data Foundation 集群的 Pod

组件	对应的 pod
OpenShift Data Foundation Operator	• **ocs-operator114**（任何存储节点上 1 个 pod） • **ocs-metrics-exporter**（任何存储节点上 1 个 pod） • **odf-operator-controller-manager-***（任何存储节点上 1 个 pod） • **odf-console-*** 任何存储节点上 1 个 pod） • **csi-addons-controller-manager-***（任何存储节点上 1 个 pod）
Rook-ceph Operator	**rook-ceph-operator-*** （任何存储节点上的 1 个 pod）

组件	对应的 pod
多云对象网关	• **noobaa-operator-*** （任何存储节点上 1 个 pod） • **noobaa-core-*** (任何存储节点上 1 个 pod) • **noobaa-db-pg-*** (任何存储节点上 1 个 pod) • **noobaa-endpoint-*** (任何存储节点上 1 个 pod)
MON	**rook-ceph-mon-*** （在存储节点间分布 3 个 pod）
MGR	**rook-ceph-mgr-*** （任何存储节点上的 1 个 pod）
MDS	**rook-ceph-mds-ocs-storagecluster-cephfilesystem-*** （2 个 pod 在存储节点间分布）
RGW	**rook-ceph-rgw-ocs-storagecluster-cephobjectstore-*** （任何存储节点上的 1 个 pod）

CSI	• **cephfs**
	  ◦ **csi-cephfsplugin-*** （每个存储节点上 1 个 pod）
	  ◦ **csi-cephfsplugin-provisioner-*** （2 个 pod 在存储节点间分布）
	• **rbd**
	  ◦ **csi-rbdplugin-*** （每个存储节点上 1 个 pod）
	  ◦ **csi-rbdplugin-provisioner-*** （2 个 pod 在存储节点间分布）

rook-ceph-crashcollector	**rook-ceph-crashcollector-*** （每个存储节点上 1 个 pod）

组件	对应的 pod
OSD	• **rook-ceph-osd-*** (每个设备 1 个 pod) • **rook-ceph-osd-prepare-ocs-deviceset-*** （每个设备 1 个 pod）

4.2. 验证 OPENSHIFT DATA FOUNDATION 集群是否健康

流程

1. 在 OpenShift Web 控制台中，点 **Storage → Data Foundation**。
2. 在 **Overview** 选项卡的 **Status** 卡中，点 **Storage System**，然后点弹出框中的存储系统链接。
3. 在 **Block and File** 选项卡的 **Status** 卡中，验证 *Storage Cluster* 是否具有绿色勾号。
4. 在 **Details** 卡中，验证是否显示集群信息。

如需有关使用 **Block and File** 仪表板的 OpenShift Data Foundation 集群健康的更多信息，请参阅 监控 OpenShift Data Foundation。

4.3. 验证 MULTICLOUD 对象网关是否健康

流程

1. 在 OpenShift Web 控制台中，点 **Storage → Data Foundation**。
2. 在 **Overview** 选项卡的 **Status** 卡中，点 **Storage System**，然后点弹出框中的存储系统链接。
   a. 在 **Object** 选项卡的 **Status** 卡 中，验证 *Object Service* 和 *数据弹性* 都具有绿色勾号。
   b. 在 **Details** 卡中，验证是否显示了 MCG 信息。

如需有关使用对象服务仪表板的 OpenShift Data Foundation 集群健康的更多信息，请参阅监控 OpenShift Data Foundation。

4.4. 验证特定的存储类是否存在

流程

1. 从 OpenShift Web 控制台左侧窗格中，点击 **Storage → Storage Classes**。
2. 验证是否在创建 OpenShift Data Foundation 集群时创建了以下存储类：
   - **ocs-storagecluster-ceph-rbd**
   - **ocs-storagecluster-cephfs**
   - **openshift-storage.noobaa.io**
   - **ocs-storagecluster-ceph-rgw**

4.5. 验证 MULTUS 网络

要确定 Multus 是否在集群中工作，请验证 Multus 网络。

流程

根据您的网络配置选择，OpenShift Data Foundation 操作器将执行以下操作之一：

- 如果为公共网络接口只选择了一个 NetworkAttachmentDefinition（如 **ocs-public-cluster**），则应用程序 Pod 和 OpenShift Data Foundation 集群之间的流量将在此网络上发生。此外，集群也将自行配置，以也使用此网络在 OSD 之间复制和重新平衡流量。
- 如果在存储集群安装过程中，分别为公共网络接口和集群网络接口选择了 NetworkAttachmentDefinition（如 **ocs-public** 和 **ocs-cluster**），则客户端存储流量将位于公共网络和集群网络中，用于在 OSD 之间复制和重新平衡流量。

要验证网络配置是否正确，请完成以下步骤：

在 OpenShift 控制台中，导航到 **Installed Operators → OpenShift Data Foundation → Storage System → ocs-storagecluster-storagesystem → Resources → ocs-storagecluster**。

在 YAML 选项卡中，在 **spec** 部分搜索 **network**，并确保您的网络接口选择配置正确。本例用于将客户端存储流量与存储复制流量分隔开。

输出示例：

```
[..]
spec:
  [..]
  network:
    ipFamily: IPv4
    provider: multus
    selectors:
      cluster: openshift-storage/ocs-cluster
      public: openshift-storage/ocs-public
  [..]
```

要使用命令行界面验证网络配置是否正确，请运行以下命令：

```
$ oc get storagecluster ocs-storagecluster \
-n openshift-storage \
-o=jsonpath='{.spec.network}{"\n"}'
```

输出示例：

```
{"ipFamily":"IPv4","provider":"multus","selectors":{"cluster":"openshift-storage/ocs-cluster","public":"openshift-storage/ocs-public"}}
```

确认 OSD pod 使用正确的网络

在 **openshift-storage** 命名空间中，使用其中一个 OSD pod 验证 pod 是否与正确的网络连接。本例用于将客户端存储流量与存储复制流量分隔开。

注意

如果两者都已创建，只有 OSD pod 将连接到 Multus 公共网络和集群网络。所有其他 OCS pod 将连接到 Multus 公共网络。

```
$ oc get -n openshift-storage $(oc get pods -n openshift-storage -o name -l app=rook-ceph-osd | grep 'osd-0') -o=jsonpath='{.metadata.annotations.k8s\.v1\.cni\.cncf\.io/network-status}{"\n"}'
```

输出示例：

```
[{
    "name": "openshift-sdn",
    "interface": "eth0",
    "ips": [
        "10.129.2.30"
    ],
    "default": true,
    "dns": {}
},{
    "name": "openshift-storage/ocs-cluster",
    "interface": "net1",
    "ips": [
        "192.168.2.1"
    ],
    "mac": "e2:04:c6:81:52:f1",
    "dns": {}
},{
    "name": "openshift-storage/ocs-public",
    "interface": "net2",
    "ips": [
        "192.168.1.1"
    ],
    "mac": "ee:a0:b6:a4:07:94",
    "dns": {}
}]
```

若要使用命令行界面确认 OSD pod 使用正确的网络，可运行以下命令（需要 jq 实用程序）：

```
$ oc get -n openshift-storage $(oc get pods -n openshift-storage -o name -l app=rook-ceph-osd | grep 'osd-0') -o=jsonpath='{.metadata.annotations.k8s\.v1\.cni\.cncf\.io/network-status}{"\n"}' | jq -r '.[].name'
```

输出示例：

```
openshift-sdn
openshift-storage/ocs-cluster
openshift-storage/ocs-public
```

第 5 章 部署独立多云对象网关

仅通过 OpenShift Data Foundation 部署多云对象网关组件可为部署提供灵活性，并有助于减少资源消耗。您可以使用动态存储设备或使用本地存储设备部署 Multicloud 对象网关组件。

5.1. 使用动态存储设备部署独立多云对象网关

使用这个部分来只部署独立 Multicloud 对象网关组件，它涉及以下步骤：

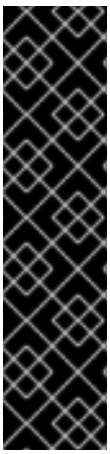
- 安装 Red Hat OpenShift Data Foundation Operator
- 创建独立多云对象网关

5.1.1. 安装 Red Hat OpenShift Data Foundation Operator

您可以使用 Red Hat OpenShift Container Platform Operator Hub 安装 Red Hat OpenShift Data Foundation Operator。

先决条件

- 使用具有 **cluster-admin** 和 operator 安装权限的账户访问 OpenShift Container Platform 集群。
- 您必须在 Red Hat OpenShift Container Platform 集群中至少有三个 worker 节点。每个节点都应该包含一个磁盘，需要 3 个磁盘(PV)。但是，一个 PV 最终会默认未使用。这是预期的行为。
- 有关其他资源要求，请参阅规划您的部署指南。



重要

- 当您需要覆盖 OpenShift Data Foundation 的集群范围默认节点选择器时，您可以使用以下命令为 **openshift-storage** 命名空间指定空白节点选择器（在这种情况下创建 **openshift-storage** 命名空间）：

```
$ oc annotate namespace openshift-storage openshift.io/node-selector=
```

- 将节点作为 **infra** 污点，以确保只在该节点上调度 Red Hat OpenShift Data Foundation 资源。这有助于您节省订阅成本。如需更多信息，请参阅管理和分配存储资源指南中的*如何将专用 worker 节点用于 Red Hat OpenShift Data Foundation* 部分。

流程

1. 登录 OpenShift Web 控制台。
2. 点 **Operators → OperatorHub**。
3. 在 **Filter by keyword** 框中滚动或键入 **OpenShift Data Foundation**，以查找 **OpenShift Data Foundation** Operator。
4. 点 **Install**。
5. 在 **Install Operator** 页面中设置以下选项：
    a. 更新频道为 **stable-4.12**。

b. 安装模式是 **A specific namespace on the cluster**。

c. Installed Namespace 为 **Operator recommended namespace openshift-storage**。如果命名空间 **openshift-storage** 不存在，它会在 Operator 安装过程中创建。

d. 将 Approval Strategy 选为 **Automatic** 或 **Manual**。
如果选择 **Automatic** 更新，Operator Lifecycle Manager(OLM)将自动升级 Operator 的运行实例，而无需任何干预。

如果选择 **手动** 更新，则 OLM 会创建一个更新请求。作为集群管理员，您必须手动批准该更新请求，才能将 Operator 更新至更新的版本。

e. 确保为 **Console 插件** 选择了 **Enable** 选项。

f. 点 **Install**。

验证步骤

- 成功安装 Operator 后，用户界面中会显示一个带有 **Web console update is available** 信息的弹出窗口。点这个弹出窗口中的 **Refresh web console** 来反映控制台的更改。
- 在 Web 控制台中：
  - 进入到 Installed Operators，再验证 **OpenShift Data Foundation** Operator 是否显示绿色勾号，指示安装成功。
  - 进入到 **Storage**，再验证 **Data Foundation** 仪表板是否可用。

5.1.2. 创建独立多云对象网关

在部署 OpenShift Data Foundation 时，您只能创建独立多云对象网关组件。

先决条件

- 确保已安装 OpenShift Data Foundation Operator。

流程

1. 在 OpenShift Web 控制台中，点 **Operators → Installed Operators** 查看所有已安装的 Operator。
确保所选 **项目** 为 **openshift-storage**。
2. 单击 **OpenShift Data Foundation** operator，然后单击 **Create StorageSystem**。
3. 在 **Backing storage** 页面中，选择以下内容：
   a. 为 **Deployment 类型**选择 **Multicloud Object Gateway**。
   b. 选择 **Use a existing StorageClass** 选项。
   c. 点 **Next**。
4. 可选：选择 **Connect to an external key management service**复选框。这是集群范围加密的可选选项。
   a. 从 **Key Management Service Provider**下拉列表中，选择 **Vault** 或 **Thales CipherTrust Manager (using KMIP)**。如果选择了 **Vault**，请进入下一步。如果您选择了 **Thales**

CipherTrust Manager（using KMIP），请转到步骤 iii。

b. 选择**身份验证方法**。

使用令牌验证方法

- 输入唯一的**连接名称** , Vault 服务器的主机**地址**（'https://<hostname 或 ip>'），**端口**号和**令牌**。
- 展开 **Advanced Settings**，以根据您的 **Vault** 配置输入其他设置和证书详情：
  - 在 **后端路径**中输入为 OpenShift Data Foundation 专用且唯一的 Key Value secret 路径。
  - （可选）输入 **TLS 服务器名称**和 **Vault Enterprise 命名空间**。
  - 上传对应的 PEM 编码证书文件，以提供 **CA 证书**、**客户端证书**和**客户端私钥**。
  - 点 **Save** 并跳过步骤 iv。

使用 Kubernetes 验证方法

- 输入唯一的 Vault **Connection Name**, Vault 服务器的主机**地址**（'https://<hostname 或 ip>'）、**端口**号和**角色**名称。
- 展开 **Advanced Settings**，以根据您的 **Vault** 配置输入其他设置和证书详情：
  - 在 **后端路径**中输入为 OpenShift Data Foundation 专用且唯一的 Key Value secret 路径。
  - 可选：输入 **TLS Server Name** 和 **Authentication Path**（如果适用）。
  - 上传对应的 PEM 编码证书文件，以提供 **CA 证书**、**客户端证书**和**客户端私钥**。
  - 点 **Save** 并跳过步骤 iv。

c. 要使用 **Thales CipherTrust Manager (using KMIP)** 作为 KMS 供应商，请按照以下步骤执行：

i. 在项目中输入密钥管理服务的唯一**连接名称**。

ii. 在 **Address** 和 **Port** 部分中，输入 Thales CipherTrust Manager 的 IP 以及在其中启用了 KMIP 接口的端口。例如：

- **地址**: 123.34.3.2
- **端口** ：5696

iii. 上传 **客户端证书**、**CA 证书**和 **客户端私钥**。

iv. 如果启用了 StorageClass 加密，请输入用于加密和解密的唯一标识符。

v. **TLS Server** 字段是可选的，并在没有 KMIP 端点的 DNS 条目时使用。例如，**kmip_all_<port>.ciphertrustmanager.local**。

d. 选择 **网络**。

e. 点 **Next**。

5. 在 **Review and create** 页面中，查看配置详情：
   若要修改任何配置设置，请单击 **Back**。

6. 单击 **Create StorageSystem**。

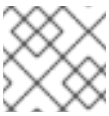
验证步骤

验证 OpenShift Data Foundation 集群是否健康

1. 在 OpenShift Web 控制台中，点 **Storage → Data Foundation**。
2. 在 **Overview** 选项卡的 **Status** 卡中，点 **Storage System**，然后点弹出框中的存储系统链接。
   a. 在 **Object** 选项卡的 **Status 卡** 中，验证 *Object Service* 和 *数据弹性* 都具有绿色勾号。
   b. 在 **Details** 卡中，验证是否显示了 MCG 信息。

验证 pod 的状态

1. 从 OpenShift Web 控制台点 **Workloads → Pods**。
2. 从 **Project** 下拉列表中选择 **openshift-storage**，再验证以下 pod 处于 **Running** 状态。



注意

如果禁用 **Show default projects** 选项，请使用切换按钮列出所有默认项目。

组件	对应的 pod
OpenShift Data Foundation Operator	• **ocs-operator114**（任何存储节点上 1 个 pod） • **ocs-metrics-exporter**（任何存储节点上 1 个 pod） • **odf-operator-controller-manager-***（任何存储节点上 1 个 pod） • **odf-console-*** 任何存储节点上 1 个 pod） • **csi-addons-controller-manager-***（任何存储节点上 1 个 pod）
Rook-ceph Operator	**rook-ceph-operator-*** （任何存储节点上的 1 个 pod）

组件	对应的 pod
多云对象网关	• **noobaa-operator-*** （任何存储节点上 1 个 pod） • **noobaa-core-*** (任何存储节点上 1 个 pod) • **noobaa-db-pg-*** (任何存储节点上 1 个 pod) • **noobaa-endpoint-*** (任何存储节点上 1 个 pod)

5.2. 使用本地存储设备部署独立多云对象网关

使用这个部分来只部署独立 Multicloud 对象网关组件，它涉及以下步骤：

- 安装 Local Storage Operator
- 安装 Red Hat OpenShift Data Foundation Operator
- 创建独立多云对象网关

5.2.1. 安装 Local Storage Operator

在本地存储设备上创建 Red Hat OpenShift Data Foundation 集群前，请先从 Operator Hub 安装 Local Storage Operator。

流程

1. 登录 OpenShift Web 控制台。
2. 点 **Operators → OperatorHub**。
3. 在 **Filter by keyword** 框中键入 **local storage**，从操作器列表中搜索 **Local Storage operator** 并单击它。
4. 在 **Install Operator** 页面中设置以下选项：
   a. 将频道更新为 **4.12** 或 **stable**。
   b. 安装模式是 **A specific namespace on the cluster**。
   c. Installed Namespace 为 **Operator recommended namespace openshift-local-storage**。
   d. 将批准更新为 **Automatic**。
5. 点 **Install**。

验证步骤

- 验证 Local Storage Operator 是否显示绿色勾号，代表安装成功。

5.2.2. 安装 Red Hat OpenShift Data Foundation Operator

您可以使用 Red Hat OpenShift Container Platform Operator Hub 安装 Red Hat OpenShift Data Foundation Operator。

先决条件

- 使用具有 **cluster-admin** 和 operator 安装权限的账户访问 OpenShift Container Platform 集群。
- 您必须在 Red Hat OpenShift Container Platform 集群中至少有三个 worker 节点。每个节点都应该包含一个磁盘，需要 3 个磁盘(PV)。但是，一个 PV 最终会默认未使用。这是预期的行为。
- 有关其他资源要求，请参阅规划您的部署指南。

重要

- 当您需要覆盖 OpenShift Data Foundation 的集群范围默认节点选择器时，您可以使用以下命令为 **openshift-storage** 命名空间指定空白节点选择器（在这种情况下创建 **openshift-storage** 命名空间）：

```
$ oc annotate namespace openshift-storage openshift.io/node-selector=
```

- 将节点作为 **infra** 污点，以确保只在该节点上调度 Red Hat OpenShift Data Foundation 资源。这有助于您节省订阅成本。如需更多信息，请参阅管理和分配存储资源指南中的*如何将专用 worker 节点用于 Red Hat OpenShift Data Foundation* 部分。

流程

1. 登录 OpenShift Web 控制台。
2. 点 **Operators → OperatorHub**。
3. 在 **Filter by keyword** 框中滚动或键入 **OpenShift Data Foundation**，以查找 **OpenShift Data Foundation** Operator。
4. 点 **Install**。
5. 在 **Install Operator** 页面中设置以下选项：
   a. 更新频道为 **stable-4.12**。
   b. 安装模式是 **A specific namespace on the cluster**。
   c. Installed Namespace 为 **Operator recommended namespace openshift-storage**。如果命名空间 **openshift-storage** 不存在，它会在 Operator 安装过程中创建。
   d. 将 Approval Strategy 选为 **Automatic** 或 **Manual**。
   如果选择 **Automatic** 更新，Operator Lifecycle Manager(OLM)将自动升级 Operator 的运行实例，而无需任何干预。

   如果选择 **手动** 更新，则 OLM 会创建一个更新请求。作为集群管理员，您必须手动批准该更新请求，才能将 Operator 更新至更新的版本。
   e. 确保为 **Console 插件** 选择了 **Enable** 选项。
   f. 点 **Install**。

验证步骤

- 成功安装 Operator 后，用户界面中会显示一个带有 **Web console update is available** 信息的弹出窗口。点这个弹出窗口中的 **Refresh web console** 来反映控制台的更改。
- 在 Web 控制台中：
  - 进入到 Installed Operators，再验证 **OpenShift Data Foundation** Operator 是否显示绿色勾号，指示安装成功。
  - 进入到 **Storage**，再验证 **Data Foundation** 仪表板是否可用。

5.2.3. 创建独立多云对象网关

在部署 OpenShift Data Foundation 时，您只能创建独立多云对象网关组件。

先决条件

- 确保已安装 OpenShift Data Foundation Operator。

流程

1. 在 OpenShift Web 控制台中，点 **Operators → Installed Operators** 查看所有已安装的 Operator。
   确保所选 **项目** 为 **openshift-storage**。
2. 单击 **OpenShift Data Foundation** operator，然后单击 **Create StorageSystem**。
3. 在 **Backing storage** 页面中，选择以下内容：
   a. 为 **Deployment 类型**选择 **Multicloud Object Gateway**。
   b. 选择 **Create a new StorageClass using the local storage devices**选项。
   c. 点 **Next**。

注意

如果还没有安装，系统会提示您安装 Local Storage Operator。点 **Install** 并按照 Installing Local Storage Operator 中所述的步骤进行操作。

4. 在 **Create local volume set** 页面中，提供以下信息：
   a. 为 **LocalVolumeSet** 和 **StorageClass** 输入一个名称。
   默认情况下，存储类名称会出现本地卷集名称。您可以更改名称。
   b. 选择以下任意一项：
      - **所有节点上的磁盘**
        使用与所有节点上所选过滤器匹配的可用磁盘。
      - **所选节点上的磁盘**
        仅在所选节点上使用与所选过滤器匹配的可用磁盘。
   c. 从可用 **Disk Type** 列表中，选择 **SSD/NVMe**。

d. 展开 **Advanced** 部分并设置以下选项：

卷模式	文件系统会被默认选择。始终为**卷模式**选择 Filesystem。
设备类型	从下拉列表中选择一个或多个设备类型。
磁盘大小	为设备设置最小 100GB 大小，以及需要包含的设备的最大可用大小。
磁盘限制上限	这表示节点上可以创建的 PV 数量上限。如果此字段留空，则为匹配节点上的所有可用磁盘创建 PV。

e. 点 **Next**。
此时会显示一个用于确认创建 LocalVolumeSet 的弹出窗口。

f. 单击 **Yes** 以继续。

5. 在 **Capacity 和 nodes** 页面中，配置以下内容：

a. **可用的原始容量**会根据与存储类关联的所有附加磁盘填充容量值。这将需要一些时间才能出现。**Selected nodes** 列表根据存储类显示节点。

b. 点 **Next**。

6. 可选：选择 **Connect to an external key management service**复选框。这是集群范围加密的可选选项。

a. 从 **Key Management Service Provider**下拉列表中，选择 **Vault** 或 **Thales CipherTrust Manager (using KMIP)**。如果选择了 **Vault**，请进入下一步。如果您选择了 **Thales CipherTrust Manager （using KMIP）**，请转到步骤 iii。

b. 选择**身份验证方法**。

使用令牌验证方法

- 输入唯一的**连接名称** , Vault 服务器的主机**地址**（'https://<hostname 或 ip>'），**端口**号和**令牌**。
- 展开 **Advanced Settings**，以根据您的 **Vault** 配置输入其他设置和证书详情：
  - 在 **后端路径**中输入为 OpenShift Data Foundation 专用且唯一的 Key Value secret 路径。
  - （可选）输入 **TLS 服务器名称**和 **Vault Enterprise 命名空间**。
  - 上传对应的 PEM 编码证书文件，以提供 **CA 证书**、**客户端证书**和**客户端私钥**。
  - 点 **Save** 并跳过步骤 iv。

使用 Kubernetes 验证方法

- 输入唯一的 Vault **Connection Name**, Vault 服务器的主机**地址**（'https://<hostname 或 ip>'）、**端口**号和**角色**名称。
- 展开 **Advanced Settings**，以根据您的 **Vault** 配置输入其他设置和证书详情：

- 在 **后端路径**中输入为 OpenShift Data Foundation 专用且唯一的 Key Value secret 路径。
- 可选：输入 **TLS Server Name** 和 **Authentication Path**（如果适用）。
- 上传对应的 PEM 编码证书文件，以提供 **CA 证书**、**客户端证书**和**客户端私钥**。
- 点 **Save** 并跳过步骤 iv。

c. 要使用 **Thales CipherTrust Manager (using KMIP)** 作为 KMS 供应商，请按照以下步骤执行：

i. 在项目中输入密钥管理服务的唯一**连接名称**。

ii. 在 **Address** 和 **Port** 部分中，输入 Thales CipherTrust Manager 的 IP 以及在其中启用了 KMIP 接口的端口。例如：

- **地址**: 123.34.3.2
- **端口** ：5696

iii. 上传 **客户端证书**、**CA 证书**和 **客户端私钥**。

iv. 如果启用了 StorageClass 加密，请输入用于加密和解密的唯一标识符。

v. **TLS Server** 字段是可选的，并在没有 KMIP 端点的 DNS 条目时使用。例如，**kmip_all_<port>.ciphertrustmanager.local**。

d. 选择 **网络**。

e. 点 **Next**。

7. 在 **Review and create** 页面中，查看配置详情：
若要修改任何配置设置，请单击 **Back**。

8. 单击 **Create StorageSystem**。

验证步骤

验证 OpenShift Data Foundation 集群是否健康

1. 在 OpenShift Web 控制台中，点 **Storage → Data Foundation**。
2. 在 **Overview** 选项卡的 **Status** 卡中，点 **Storage System**，然后点弹出框中的存储系统链接。
   a. 在 **Object** 选项卡的 **Status 卡** 中，验证 *Object Service* 和 *数据弹性* 都具有绿色勾号。
   b. 在 **Details** 卡中，验证是否显示了 MCG 信息。

验证 pod 的状态

1. 从 OpenShift Web 控制台点 **Workloads → Pods**。
2. 从 **Project** 下拉列表中选择 **openshift-storage**，再验证以下 pod 处于 **Running** 状态。

注意

如果禁用 **Show default projects**选项，请使用切换按钮列出所有默认项目。

组件	对应的 pod
OpenShift Data Foundation Operator	• **ocs-operator114**（任何存储节点上 1 个 pod） • **ocs-metrics-exporter**（任何存储节点上 1 个 pod） • **odf-operator-controller-manager-***（任何存储节点上 1 个 pod） • **odf-console-*** 任何存储节点上 1 个 pod） • **csi-addons-controller-manager-***（任何存储节点上 1 个 pod）
Rook-ceph Operator	**rook-ceph-operator-*** （任何存储节点上的 1 个 pod）
多云对象网关	• **noobaa-operator-***（任何存储节点上 1 个 pod） • **noobaa-core-*** (任何存储节点上 1 个 pod) • **noobaa-db-pg-*** (任何存储节点上 1 个 pod) • **noobaa-endpoint-*** (任何存储节点上 1 个 pod)

第 6 章 卸载 OPENSHIFT DATA FOUNDATION

6.1. 以内部模式卸载 OPENSHIFT DATA FOUNDATION

要以内部模式卸载 OpenShift Data Foundation，请参阅 有关卸载 OpenShift Data Foundation 的知识库文章。