



# Red Hat OpenShift Data Foundation 4.15

## 使用 Amazon Web Services 部署 OpenShift Data Foundation

有关使用 Amazon Web Services 进行云存储部署 OpenShift Data Foundation 的说明



# Red Hat OpenShift Data Foundation 4.15 使用 Amazon Web Services 部署 OpenShift Data Foundation

---

有关使用 Amazon Web Services 进行云存储部署 OpenShift Data Foundation 的说明

## 法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack<sup>®</sup> Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 摘要

请阅读本文档，了解如何使用 Red Hat OpenShift Container Platform 在 Amazon Web Services 上安装 Red Hat OpenShift Data Foundation。

---

# 目录

使开源包含更多 .....	3
对红帽文档提供反馈 .....	4
前言 .....	5
第 1 章 准备部署 OPENSIFT 数据基础 .....	6
第 2 章 使用动态存储设备部署 OPENSIFT DATA FOUNDATION .....	8
2.1. 安装 RED HAT OPENSIFT DATA FOUNDATION OPERATOR .....	8
2.2. 使用 TOKEN 验证方法通过 KMS 启用集群范围的加密 .....	9
2.3. 使用 KUBERNETES 身份验证方法通过 KMS 启用集群范围的加密 .....	10
2.4. 创建 OPENSIFT DATA FOUNDATION 集群 .....	12
2.5. 验证 OPENSIFT DATA FOUNDATION .....	16
第 3 章 部署独立多云对象网关 .....	20
3.1. 安装 RED HAT OPENSIFT DATA FOUNDATION OPERATOR .....	20
3.2. 创建独立多云对象网关 .....	21
第 4 章 查看 OPENSIFT DATA FOUNDATION 拓扑 .....	24
第 5 章 卸载 OPENSIFT DATA FOUNDATION .....	25
5.1. 以内部模式卸载 OPENSIFT DATA FOUNDATION .....	25



---

## 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。

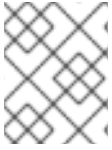
要提供反馈，请创建一个 Bugzilla ticket：

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) AWS 集群上部署，以及代理环境的开箱即用支持。



### 注意

AWS 上仅支持内部 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](#) 章节的要求开始，并根据您的要求遵循适当的部署流程：

- [使用动态存储设备进行部署](#)
- [部署独立多云对象网关组件](#)

## 第 1 章 准备部署 OPENSIFT 数据基础

使用动态存储设备在 OpenShift Container Platform 上部署 OpenShift Data Foundation 为您提供创建内部集群资源的选项。

在开始部署 Red Hat OpenShift Data Foundation 前，请按照以下步骤执行：

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](#)。

如需详细要求，请参阅 [OpenShift Workloads 配置 OpenShift Data Foundation 灾难恢复指南](#)，以及 *Red Hat Advanced Cluster Management for Kubernetes* [文档中的安装指南](#) 中的 [要求和](#) [建议](#) 部分。

## 第 2 章 使用动态存储设备部署 OPENSHIFT DATA FOUNDATION

您可以使用 Amazon Web Services(AWS)EBS（类型，**gp2-csi** 或 **gp3-csi**）提供的动态存储设备在 OpenShift Container Platform 上部署 OpenShift Data Foundation，为您提供创建内部集群资源的选项。这会导致在内部置备基础服务，这有助于为应用提供额外的存储类。

另外，可以使用 OpenShift Data Foundation 仅部署多云对象网关(MCG)组件。如需更多信息，请参阅[部署独立多云对象网关](#)。



### 注意

AWS 上仅支持内部 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 或 infrastructure 节点。
- 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。[https://access.redhat.com/documentation/zh-cn/red\\_hat\\_openshift\\_data\\_foundation/4.15/html-single/managing\\_and\\_allocating\\_storage\\_resources/index#how-to-use-dedicated-worker-nodes-for-openshift-data-foundation\\_rhddf](https://access.redhat.com/documentation/zh-cn/red_hat_openshift_data_foundation/4.15/html-single/managing_and_allocating_storage_resources/index#how-to-use-dedicated-worker-nodes-for-openshift-data-foundation_rhddf)

#### 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. 将频道更新为 **stable-4.15**。
  - 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
```

- 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。

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

- 检索 OCP 集群端点。

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

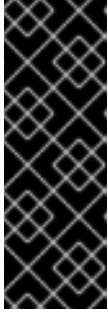
- 获取服务帐户签发者：

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

- 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="$SA_CA_CERT" \
  issuer="$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_CERT"
```

- 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
```

- 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 -
```

- 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 OPENSIFT DATA FOUNDATION 集群

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

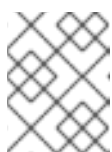
### 先决条件

- 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](#)。



## 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**。  
从 OpenShift Data Foundation 版本 4.12 开始，您可以选择 **gp2-csi** 或 **gp3-csi** 作为存储类。
  - d. 可选：选择 **Use external PostgreSQL** 复选框以使用外部 PostgreSQL **[技术预览]**。  
这为 PostgreSQL pod 是一个单点故障的多云对象网关提供了高可用性解决方案。
    - i. 提供以下连接详情：
      - 用户名
      - 密码
      - 服务器名称和端口
      - 数据库名称
    - ii. 选中 **Enable TLS/SSL** 复选框，为 Postgres 服务器启用加密。
  - e. 单击 **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. 在 **Configure performance** 部分中，选择以下性能配置集之一：
  - 精益  
在资源受限环境中使用它，且最少的资源低于推荐的资源。此配置集通过分配较少的 CPU 和较少的内存来最小化资源消耗。
  - balanced（默认）  
当推荐的资源可用时，请使用此选项。这个配置集为不同工作负载提供资源消耗和性能之间的平衡。
  - 性能

在有足够资源的环境中使用它以获得最佳性能。此配置集通过分配 ample 内存和 CPU 来为高性能量身定制，以确保对要求的工作负载进行优化执行。



### 注意

您可以选择在部署后使用 **StorageSystems** 选项卡的选项菜单中的 **Configure performance** 选项来配置性能配置集。



### 重要

在选择资源配置集前，请确保检查集群中资源的当前可用性。在资源不足的集群中选择较高的资源配置集可能会导致安装失败。

有关资源要求的更多信息，请参阅 [性能配置集的资源要求](#)。

- d. 可选：选中 **Taint nodes** 复选框，以将所选节点专用于 OpenShift Data Foundation。对于具有多个可用区的云平台，请确保节点分布在不同的位置/可用性区域。

如果选择的节点与聚合的 30 个 CPU 和 72 GiB RAM 的 OpenShift Data Foundation 集群要求不匹配，则会部署最小的集群。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。

- e. 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。

- i. 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）。

- ii. 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**，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**，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. 点击 **Next**。

b. 要启用 in-transit 加密，请选择 **In-transit encryption**。

i. 选择 **网络**。

ii. 点击 **Next**。

6. 在 **Data Protection** 页面中，如果您要为 Openshift Data Foundation 配置 Regional-DR 解决方案，然后选择 **Prepare cluster for disaster recovery (Regional-DR only)**复选框，否则点 **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**。

## 8. 单击 **Create StorageSystem**。



### 注意

如果您的部署有五个或更多节点、机架或房间，当部署中存在五个或更多个故障域时，您可以根据机架或区域的数量配置 Ceph 监控计数。在 OpenShift Web 控制台的通知面板中显示警报或 Alert Center，以指示用于增加 Ceph 监控器数量的选项。您可以使用警报中的 **Configure** 选项来配置 Ceph 监控器计数。有关更多信息，请参阅 [解决低 Ceph 监视器计数警报](#)。

### 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 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](#)。

### 其他资源

要启用 Overprovision Control 警报，请参阅 Monitoring 中的 [Alerts](#) 指南。

## 2.5. 验证 OPENSIFT DATA FOUNDATION

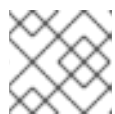
验证 OpenShift Data Foundation 是否已正确部署：

1. [验证容器集的状态](#)。
2. [验证 OpenShift Data Foundation 集群是否健康](#)。
3. [验证 Multicloud 对象网关是否健康](#)。
4. [验证 OpenShift Data Foundation 特定的存储类是否存在](#)。

### 2.5.1. 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 2.1 “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 2.1. 对应 OpenShift Data Foundation 集群的 Pod

组件	对应的 pod
OpenShift Data Foundation Operator	<ul style="list-style-type: none"> <li>● <b>ocs-operator114</b> (任何存储节点上 1 个 pod)</li> <li>● <b>ocs-metrics-exporter</b> (任何存储节点上 1 个 pod)</li> <li>● <b>odf-operator-controller-manager-*</b> (任何存储节点上 1 个 pod)</li> <li>● <b>odf-console-*</b> 任何存储节点上 1 个 pod)</li> <li>● <b>csi-addons-controller-manager-*</b> (任何存储节点上 1 个 pod)</li> </ul>
Rook-ceph Operator	<b>rook-ceph-operator-*</b> (任何存储节点上的 1 个 pod)
多云对象网关	<ul style="list-style-type: none"> <li>● <b>noobaa-operator-*</b> (任何存储节点上 1 个 pod)</li> <li>● <b>noobaa-core-*</b> (任何存储节点上 1 个 pod)</li> <li>● <b>noobaa-db-pg-*</b> (任何存储节点上 1 个 pod)</li> <li>● <b>noobaa-endpoint-*</b> (任何存储节点上 1 个 pod)</li> </ul>
MON	<b>rook-ceph-mon-*</b> (在存储节点间分布 3 个 pod)
MGR	<b>rook-ceph-mgr-*</b> (任何存储节点上的 1 个 pod)
MDS	<b>rook-ceph-mds-ocs-storagecluster-cephfilesystem-*</b> (2 个 pod 在存储节点间分布)

组件	对应的 pod
CSI	<ul style="list-style-type: none"> <li>● <b>cephfs</b> <ul style="list-style-type: none"> <li>○ <b>csi-cephfsplugin-*</b> (每个存储节点上 1 个 pod)</li> <li>○ <b>csi-cephfsplugin-provisioner-*</b> (2 个 pod 在存储节点间分布)</li> </ul> </li> <li>● <b>rbd</b> <ul style="list-style-type: none"> <li>○ <b>csi-rbdplugin-*</b> (每个存储节点上 1 个 pod)</li> <li>○ <b>csi-rbdplugin-provisioner-*</b> (2 个 pod 在存储节点间分布)</li> </ul> </li> </ul>
rook-ceph-crashcollector	<p><b>rook-ceph-crashcollector-*</b></p> <p>(每个存储节点上 1 个 pod)</p>
OSD	<ul style="list-style-type: none"> <li>● <b>rook-ceph-osd-*</b> (每个设备 1 个 pod)</li> <li>● <b>rook-ceph-osd-prepare-ocs-deviceset-*</b> (每个设备 1 个 pod)</li> </ul>

## 2.5.2. 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](#)。

## 2.5.3. 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](#)。

#### 2.5.4. 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**

## 第 3 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。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

### 3.1. 安装 RED HAT OPENSIFT 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 或 infrastructure 节点。
- 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。[https://access.redhat.com/documentation/zh-cn/red\\_hat\\_openshift\\_data\\_foundation/4.15/html-single/managing\\_and\\_allocating\\_storage\\_resources/index#how-to-use-dedicated-worker-nodes-for-openshift-data-foundation\\_rhddf](https://access.redhat.com/documentation/zh-cn/red_hat_openshift_data_foundation/4.15/html-single/managing_and_allocating_storage_resources/index#how-to-use-dedicated-worker-nodes-for-openshift-data-foundation_rhddf)

#### 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. 将频道更新为 **stable-4.15**。
  - 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** 仪表盘是否可用。

## 3.2. 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**，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**，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	<ul style="list-style-type: none"> <li>● <b>ocs-operator114</b> (任何存储节点上 1 个 pod)</li> <li>● <b>ocs-metrics-exporter</b> (任何存储节点上 1 个 pod)</li> <li>● <b>odf-operator-controller-manager-*</b> (任何存储节点上 1 个 pod)</li> <li>● <b>odf-console-*</b> 任何存储节点上 1 个 pod)</li> <li>● <b>csi-addons-controller-manager-*</b> (任何存储节点上 1 个 pod)</li> </ul>
Rook-ceph Operator	<p><b>rook-ceph-operator-*</b></p> <p>(任何存储节点上的 1 个 pod)</p>
多云对象网关	<ul style="list-style-type: none"> <li>● <b>noobaa-operator-*</b> (任何存储节点上 1 个 pod)</li> <li>● <b>noobaa-core-*</b> (任何存储节点上 1 个 pod)</li> <li>● <b>noobaa-db-pg-*</b> (任何存储节点上 1 个 pod)</li> <li>● <b>noobaa-endpoint-*</b> (任何存储节点上 1 个 pod)</li> </ul>

## 第 4 章 查看 OPENSIFT DATA FOUNDATION 拓扑

拓扑显示 OpenShift Data Foundation 存储集群在各种抽象级别映射的视觉化，并可让您与这些层交互。视图还显示了各种元素如何一起编写存储集群。

### 流程

1. 在 OpenShift Web 控制台中，进入到 **Storage → Data Foundation → Topology**。  
视图显示存储集群及其内部区域。您可以查看区域中由循环实体描述的节点，这些实体由点行表示。每个项目或资源的标签包含基本信息，如状态和健康或指示警报。
2. 选择一个节点来查看右侧面板中的节点详情。您还可以通过点 search/preview decorator 图标来访问节点内的资源或部署。
3. 查看部署详情
  - a. 点节点上的 preview decorator。在节点上面会显示一个模态窗口，它会显示与该节点关联的所有部署及其状态。
  - b. 点模型左上角的 **Back to main view** 按钮，以关闭并返回上视图。
  - c. 选择特定的部署来查看它的更多信息。所有相关数据都会在侧面面板中显示。
4. 点 **Resources** 选项卡查看 pod 信息。此选项卡深入了解问题，并提供有助于更好地进行故障排除的粒度。
5. 点 pod 链接查看 OpenShift Container Platform 上的 pod 信息页面。该链接在新窗口中打开。

## 第 5 章 卸载 OPENSIFT DATA FOUNDATION

### 5.1. 以内部模式卸载 OPENSIFT 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](#)。