Red Hat OpenShift Data Foundation 4.12

使用 Microsoft Azure 部署 OpenShift Data Foundation

使用 Microsoft Azure 部署 OpenShift Data Foundation 的说明

Last Updated: 2023-11-08

Red Hat OpenShift Data Foundation 4.12 使用 Microsoft Azure 部署 OpenShift Data Foundation

使用 Microsoft Azure 部署 OpenShift Data Foundation 的说明

法律通告

摘要

有关如何在 Microsoft Azure 上使用 Red Hat OpenShift Container Platform 安装和管理 Red Hat OpenShift Data Foundation 的说明，请参阅此文档。

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。

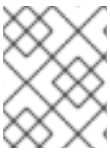
对红帽文档提供反馈

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。提供反馈：

- 关于特定内容的简单评论：
  1. 请确定您使用 *Multi-page HTML* 格式查看文档。另外，确定 **Feedback** 按钮出现在文档页的右上方。
  2. 用鼠标指针高亮显示您想评论的文本部分。
  3. 点在高亮文本上弹出的 **Add Feedback**。
  4. 按照显示的步骤操作。
- 要提交更复杂的反馈，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 支持在现有 Red Hat OpenShift Container Platform(RHOCP)Azure 集群上进行部署。



注意

Microsoft Azure 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。

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：

- 在 Microsoft Azure 上部署 OpenShift Data Foundation
- 部署独立多云对象网关组件

第 1 章 准备部署 OPENSHIFT 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。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。

在开始部署 OpenShift Data Foundation 前，请按照以下步骤操作：

1. 设置 chrony 服务器。请参阅 配置 chrony 时间服务 并使用知识库解决方案来创建允许所有流量的规则。

2. 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。

   注意

   如果您使用 Thales CipherTrust Manager 作为 KMS，您将在部署过程中启用它。

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。

第 2 章 在 MICROSOFT AZURE 和 AZURE RED HAT OPENSHIFT 上部署 OPENSHIFT DATA FOUNDATION

您可以使用 Microsoft Azure 安装程序置备的基础架构(IPI)提供的动态存储设备（type: **managed-csi**）在 OpenShift Container Platform 上部署 OpenShift Data Foundation，以便您创建内部集群资源。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

Microsoft Azure 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。

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：

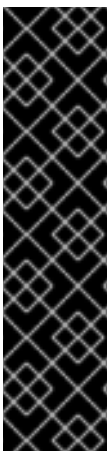
1. 安装 Red Hat OpenShift Data Foundation Operator 。
2. 创建 OpenShift Data Foundation 集群

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。
- 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 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，请参阅使用 Operator Hub 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**。

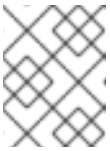
   b. 选择 **Use a existing StorageClass** 选项。

   c. 选择 **Storage Class**。
   默认情况下，它被设置为 **managed-csi**。

   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。
   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。

   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**。

v. 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。

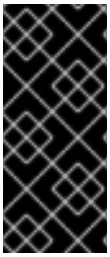
- 要验证 OpenShift 数据基础的所有组件是否已成功安装，请参阅验证您的 OpenShift Data Foundation 部署。

其他资源

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

第 3 章 在 AZURE RED HAT OPENSHIFT 上部署 OPENSHIFT DATA FOUNDATION

Azure Red Hat OpenShift 服务可让您部署完全托管的 OpenShift 集群。Red Hat OpenShift Data Foundation 可以部署在 Azure Red Hat OpenShift 服务中。



重要

Azure Red Hat OpenShift 上的 OpenShift Data Foundation 不是一个托管服务产品。需要 Red Hat OpenShift Data Foundation 订阅才能获得红帽支持团队支持的安装。您如果需要与 Red Hat OpenShift Data Foundation on Azure Red Hat OpenShift 相关的帮助，请向红帽支持团队（而不是 Microsoft）创建支持问题单，选择 **Red Hat OpenShift Data Foundation** 作为产品。

要在 Azure Red Hat OpenShift 上安装 OpenShift Data Foundation，请遵循以下部分：

1. 获取红帽 pull secret 以便部署 Azure Red Hat OpenShift 。
2. 为现有 Azure Red Hat OpenShift 集群准备红帽 pull secret 。
3. 将 pull secret 添加到集群中。
4. 验证您的红帽 pull secret 是否正在工作。
5. 安装 Red Hat OpenShift Data Foundation Operator 。
6. 创建 OpenShift Data Foundation 集群服务。

3.1. 为新部署 AZURE RED HAT OPENSHIFT 获取 RED HAT PULL SECRET

红帽 pull secret 可让集群访问红帽容器 registry 以及其他内容。

先决条件

- 红帽门户帐户。
- OpenShift Data Foundation 订阅。

流程

要获取用于新部署 Azure Red Hat OpenShift 的红帽 pull secret，请遵循官方 Microsoft Azure 文档中的获取 Red Hat pull secret 部分的步骤。

请注意，在创建 Azure Red Hat OpenShift 集群 时，您可能需要更大的 worker 节点，由 *--worker-vm-size* 或多个 worker 节点控制，由 *--worker-count* 控制。推荐的 *worker-vm-size* 是 **Standard_D16s_v3**。您也可以将专用 worker 节点用于 Red Hat OpenShift Data Foundation，请参阅 *管理和分配存储资源指南*中的专用 worker 节点部分。

3.2. 为现有 AZURE RED HAT OPENSHIFT 集群准备 RED HAT PULL SECRET

当您在没有添加 Red Hat pull secret 的情况下创建 Azure Red Hat OpenShift 集群时，仍会自动创建 pull secret。但是，这个 pull secret 不会完全填充。

使用本节来使用红帽 pull secret 中的附加值更新自动创建的 pull secret。

先决条件

- 现存的没有红帽 pull secret 的 Azure Red Hat OpenShift 集群。

流程

要为现有 Azure Red Hat OpenShift 集群准备 Red Hat pull secret，请按照官方 Mircosoft Azure 文档中的准备 pull secret 部分的步骤进行操作。

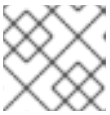
3.3. 在集群中添加 PULL SECRET

先决条件

- 红帽 pull secret。

流程

- 运行以下命令以更新 pull secret。



注意

运行此命令会导致集群节点在更新时逐一重启它们。

```
oc set data secret/pull-secret -n openshift-config --from-file=.dockerconfigjson=./pull-secret.json
```

设置 secret 后，您可以启用 Red Hat 认证的 Operator。

3.3.1. 修改配置文件以启用 Red Hat operators

要修改配置文件以启用 Red Hat operators，请按照官方 Microsoft Azure 文档中的修改配置文件的步骤进行操作。

3.4. 验证您的红帽 PULL SECRET 是否正常工作

添加 pull secret 并修改配置文件后，集群可能需要几分钟才能更新。

要检查集群是否已更新，请运行以下命令以显示经认证的 **Operator** 和 **Red Hat Operator** 源可用：

```
$ oc get catalogsource -A
NAMESPACE              NAME                DISPLAY
openshift-marketplace  redhat-operators    Red Hat Operators

 TYPE   PUBLISHER   AGE
 grpc   Red Hat     11s
```

如果没有看到 Red Hat Operator，请等待几分钟再试一次。

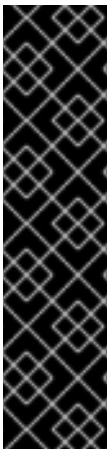
为确保您的 pull secret 已更新并正常工作，请打开 **Operator Hub** 并检查任何已验证的 Operator。例如，检查 OpenShift Data Foundation Operator 是否可用，并查看您是否有安装它的权限。

3.5. 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。
- 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。

3.6. 创建 OPENSHIFT DATA FOUNDATION 集群

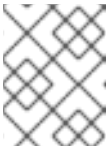
安装 OpenShift Data Foundation 操作器（operator）后，创建 OpenShift Data Foundation。

先决条件

- OpenShift Data Foundation 操作器必须从 Operator Hub 安装。如需更多信息，请参阅使用 Operator Hub 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**。
   默认情况下，它被设置为 **managed-csi**。
   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。
   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。

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**。

v. 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。

- 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。

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）

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）
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**

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。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：

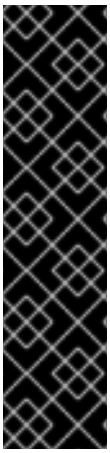
- 安装 Red Hat OpenShift Data Foundation Operator
- 创建独立多云对象网关

5.1. 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。
- 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. 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）
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。