Red Hat OpenShift Service on AWS 4

备份和恢复应用程序

备份和恢复应用程序数据

Last Updated: 2024-06-28

Red Hat OpenShift Service on AWS 4 备份和恢复应用程序

备份和恢复应用程序数据

法律通告

摘要

本文档提供有关备份应用程序的信息。

目录

第 1 章 备份应用程序

您可以将 OpenShift API 用于 Red Hat OpenShift Service on AWS (ROSA)集群的数据保护(OADP)来备份和恢复应用程序数据。在安装 OADP 前，您必须为 OADP 设置角色和策略凭证，以便可以使用 AWS API。

这是一个包括两个阶段的过程：

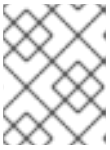
1. 准备 AWS 凭证。
2. 安装 OADP Operator，并将其提供给 IAM 角色。

1.1. 准备 AWS 凭证

AWS 帐户必须准备好接受 OADP 安装。

流程

1. 运行以下命令来创建以下环境变量：



注意

更改集群名称来匹配您的 ROSA 集群，并确保以管理员身份登录到集群。在继续操作前，确保所有字段被正常输出。

```
$ export CLUSTER_NAME=my-cluster (1)
export ROSA_CLUSTER_ID=$(rosa describe cluster -c ${CLUSTER_NAME} --output json | jq -r .id)
export REGION=$(rosa describe cluster -c ${CLUSTER_NAME} --output json | jq -r .region.id)
export OIDC_ENDPOINT=$(oc get authentication.config.openshift.io cluster -o jsonpath='{.spec.serviceAccountIssuer}' | sed 's|^https://||')
export AWS_ACCOUNT_ID=$(aws sts get-caller-identity --query Account --output text)
export CLUSTER_VERSION=$(rosa describe cluster -c ${CLUSTER_NAME} -o json | jq -r .version.raw_id | cut -f -2 -d '.')
export ROLE_NAME="${CLUSTER_NAME}-openshift-oadp-aws-cloud-credentials"
export SCRATCH="/tmp/${CLUSTER_NAME}/oadp"
mkdir -p ${SCRATCH}
echo "Cluster ID: ${ROSA_CLUSTER_ID}, Region: ${REGION}, OIDC Endpoint: ${OIDC_ENDPOINT}, AWS Account ID: ${AWS_ACCOUNT_ID}"
```

(1) 将 **my-cluster** 替换为您的 ROSA 集群名称。

2. 在 AWS 帐户上，创建一个 IAM 策略以允许访问 S3。
   a. 运行以下命令，检查策略是否存在：

```
$ POLICY_ARN=$(aws iam list-policies --query "Policies[?PolicyName=='RosaOadpVer1'].{ARN:Arn}" --output text) (1)
```

(1) 将 **RosaOadp** 替换为您的策略名称。

b. 使用以下命令来创建策略 JSON 文件，然后在 ROSA 中创建策略。

注意

如果没有找到策略 ARN，该命令将创建策略。如果策略 ARN 已存在，则 **if** 语句将跳过策略创建。

```
$ if [[ -z "${POLICY_ARN}" ]]; then
cat << EOF > ${SCRATCH}/policy.json (1)
{
"Version": "2012-10-17",
"Statement": [
 {
   "Effect": "Allow",
   "Action": [
     "s3:CreateBucket",
     "s3:DeleteBucket",
     "s3:PutBucketTagging",
     "s3:GetBucketTagging",
     "s3:PutEncryptionConfiguration",
     "s3:GetEncryptionConfiguration",
     "s3:PutLifecycleConfiguration",
     "s3:GetLifecycleConfiguration",
     "s3:GetBucketLocation",
     "s3:ListBucket",
     "s3:GetObject",
     "s3:PutObject",
     "s3:DeleteObject",
     "s3:ListBucketMultipartUploads",
     "s3:AbortMultipartUpload",
     "s3:ListMultipartUploadParts",
     "ec2:DescribeSnapshots",
     "ec2:DescribeVolumes",
     "ec2:DescribeVolumeAttribute",
     "ec2:DescribeVolumesModifications",
     "ec2:DescribeVolumeStatus",
     "ec2:CreateTags",
     "ec2:CreateVolume",
     "ec2:CreateSnapshot",
     "ec2:DeleteSnapshot"
   ],
   "Resource": "*"
 }
]}
EOF

POLICY_ARN=$(aws iam create-policy --policy-name "RosaOadpVer1" \
--policy-document file:///${SCRATCH}/policy.json --query Policy.Arn \
--tags Key=rosa_openshift_version,Value=${CLUSTER_VERSION}
Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-oadp Key=operator_name,Value=openshift-
oadp \
--output text)
fi
```

1 **SCRATCH** 是为环境变量创建的临时目录的名称。

c. 运行以下命令来查看策略 ARN：

```
$ echo ${POLICY_ARN}
```

3. 为集群创建 IAM 角色信任策略：

a. 运行以下命令来创建信任策略文件：

```
$ cat <<EOF > ${SCRATCH}/trust-policy.json
{
    "Version": "2012-10-17",
    "Statement": [{
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::${AWS_ACCOUNT_ID}:oidc-
provider/${OIDC_ENDPOINT}"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "${OIDC_ENDPOINT}:sub": [
            "system:serviceaccount:openshift-adp:openshift-adp-controller-manager",
            "system:serviceaccount:openshift-adp:velero"]
        }
      }
    }]
}
EOF
```

b. 运行以下命令来创建角色：

```
$ ROLE_ARN=$(aws iam create-role --role-name \
  "${ROLE_NAME}" \
  --assume-role-policy-document file://${SCRATCH}/trust-policy.json \
  --tags Key=rosa_cluster_id,Value=${ROSA_CLUSTER_ID}
Key=rosa_openshift_version,Value=${CLUSTER_VERSION}
Key=rosa_role_prefix,Value=ManagedOpenShift
Key=operator_namespace,Value=openshift-adp
Key=operator_name,Value=openshift-oadp \
    --query Role.Arn --output text)
```

c. 运行以下命令来查看角色 ARN：

```
$ echo ${ROLE_ARN}
```

4. 运行以下命令，将 IAM 策略附加到 IAM 角色：

```
$ aws iam attach-role-policy --role-name "${ROLE_NAME}" \
  --policy-arn ${POLICY_ARN}
```

后续步骤

- 继续*安装 OADP Operator 并提供 IAM 角色*。

1.2. 安装 OADP OPERATOR 并提供 IAM 角色

AWS 安全令牌服务 (AWS STS) 是一个全局 Web 服务，它为 IAM 或联邦用户提供简短凭证。使用 STS 的 Red Hat OpenShift Service on AWS (ROSA) 是 ROSA 集群的建议凭证模式。本文档论述了如何使用 AWS STS 为 Data Protection (OADP) on (ROSA) with AWS STS 安装 OpenShift API for Data Protection (OADP)。

重要

使用 AWS STS 环境的 ROSA 上的 OADP 不支持 Restic 和 Kopia。确保禁用 Restic/Kopia 节点代理。对于备份卷，使用 AWS STS 的 ROSA 上 OADP 只支持原生快照和 CSI 快照。如需更多信息，请参阅 *已知问题*。

重要

在使用 STS 验证的 Amazon ROSA 集群中，不支持在不同的 AWS 区域中恢复备份的数据。

目前，ROSA 集群不支持 Data Mover 功能。您可以使用原生 AWS S3 工具移动数据。

先决条件

- 具有所需访问权限和令牌的集群。具体步骤请参阅"准备 AWS 凭证"。如果您计划使用两个不同的集群来备份和恢复，您需要为每个集群准备 AWS 凭证，包括 **ROLE_ARN**。

流程

1. 输入以下命令，从 AWS 令牌文件创建 OpenShift secret。

   a. 创建凭证文件：

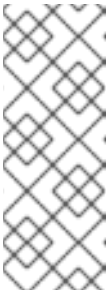
   ```
   $ cat <<EOF > ${SCRATCH}/credentials
   [default]
   role_arn = ${ROLE_ARN}
   web_identity_token_file = /var/run/secrets/openshift/serviceaccount/token
   EOF
   ```

   b. 为 OADP 创建命名空间：

   ```
   $ oc create namespace openshift-adp
   ```

   c. 创建 OpenShift secret：

   ```
   $ oc -n openshift-adp create secret generic cloud-credentials \
     --from-file=${SCRATCH}/credentials
   ```



注意

在 Red Hat OpenShift Service on AWS 版本 4.15 及更新的版本中，OADP Operator 通过 Operator Lifecycle Manager (OLM)和 Cloud Credentials Operator (CCO)支持新的标准化 STS 工作流。在此工作流中，您不需要创建上述 secret，您只需要在 通过 Red Hat OpenShift Service on AWS Web 控制台安装 OLM 管理的 Operator 期间提供角色 ARN。以上 secret 通过 CCO 自动创建。

2. 安装 OADP Operator。

   a. 在 Red Hat OpenShift Service on AWS web 控制台中进入 Operators → OperatorHub。

   b. 搜索 OADP Operator，然后点 **Install**。

3. 使用 AWS 凭证创建 AWS 云存储：

```
$ cat << EOF | oc create -f -
apiVersion: oadp.openshift.io/v1alpha1
kind: CloudStorage
metadata:
  name: ${CLUSTER_NAME}-oadp
  namespace: openshift-adp
spec:
  creationSecret:
    key: credentials
    name: cloud-credentials
  enableSharedConfig: true
  name: ${CLUSTER_NAME}-oadp
  provider: aws
  region: $REGION
EOF
```

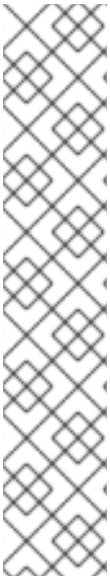
4. 创建 **DataProtectionApplication** 资源，用于配置与存储备份和卷快照的存储的连接：

```
$ cat << EOF | oc create -f -
apiVersion: oadp.openshift.io/v1alpha1
kind: DataProtectionApplication
metadata:
  name: ${CLUSTER_NAME}-dpa
  namespace: openshift-adp
spec:
  backupLocations:
  - bucket:
      cloudStorageRef:
        name: ${CLUSTER_NAME}-oadp
      credential:
        key: credentials
        name: cloud-credentials
      prefix: velero
      default: true
      config:
        region: ${REGION}
  configuration:
    velero:
      defaultPlugins:
```

```
      - openshift
      - aws
    nodeAgent: 1
      enable: false
      uploaderType: restic
  snapshotLocations:
    - velero:
        config:
          credentialsFile: /tmp/credentials/openshift-adp/cloud-credentials-credentials 2
          enableSharedConfig: "true" 3
          profile: default 4
          region: ${REGION} 5
        provider: aws
EOF
```

1. 请参见以下的第一备注。
2. **credentialsFile** 字段是 pod 上存储桶凭证的挂载位置。
3. **enableSharedConfig** 字段允许 **snapshotLocations** 共享或重复使用为存储桶定义的凭证。
4. 使用 AWS 凭证文件中设置的配置集名称。
5. 将 **region** 指定为您的 AWS 区域。这必须与集群区域相同。

现在，您可以备份和恢复 OpenShift 应用程序，如 OADP 文档所述。



注意

此配置中的 **restic** 的 **enable** 参数设置为 **false**，因为 OADP 不支持 ROSA 环境中的 Restic。

如果使用 OADP 1.2，请替换此配置：

```
nodeAgent:
  enable: false
  uploaderType: restic
```

使用以下命令：

```
restic:
  enable: false
```

注意

如果要使用两个不同的集群来备份和恢复，则两个集群在 cloudstorage CR 和 OADP **DataProtectionApplication** 配置中必须具有相同的 AWS S3 存储名称。

其他资源

- 准备 AWS 凭证

1.3. 已知问题

不支持或推荐使用 Restic、Kopia 和 DataMover

- CloudStorage: openshift-adp-controller-manager crashloop seg fault with Restic enabled
- （只有 OADP 1.1.x_ 受影响）： CloudStorage: bucket is removed on CS CR delete, although it doesn't have "oadp.openshift.io/cloudstorage-delete": "true"

1.4. 其他资源

- Understanding ROSA with STS
- ROSA STS 入门
- 创建带有 STS 的 ROSA 集群
- 关于安装 OADP
- 配置 CSI 卷
- ROSA 存储选项