Red Hat OpenShift Service on AWS 4

アプリケーションのバックアップおよび復元

アプリケーションデータのバックアップおよび復元

Last Updated: 2024-04-13

Red Hat OpenShift Service on AWS 4 アプリケーションのバックアップおよび復元

アプリケーションデータのバックアップおよび復元

法律上の通知

概要

本書では、アプリケーションのバックアップに関する情報を提供します。

目次

第1章 アプリケーションのバックアップ

Red Hat OpenShift Service on AWS (ROSA) クラスターで OpenShift API for Data Protection (OADP) を使用して、アプリケーションデータをバックアップおよび復元できます。OADP をインストールする前に、OADP が AWS API を使用できるように、OADP のロールとポリシーの認証情報を設定する必要があります。

これは 2 段階のプロセスです。

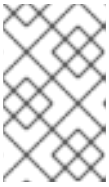
1. AWS 認証情報を準備します。
2. OADP Operator をインストールし、IAM ロールを指定します。

1.1. AWS 認証情報の準備

AWS アカウントは、OADP インストールを受け入れる準備ができている必要があります。

手順

1. 次のコマンドを実行して、以下の環境変数を作成します。



注記

ROSA クラスターに一致するようにクラスター名を変更し、管理者としてクラスターにログインしていることを確認します。続行する前に、すべてのフィールドが正しく出力されていることを確認します。

```
$ 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) **my-cluster** は、ROSA クラスター名に置き換えます。

2. AWS アカウントで、S3 へのアクセスを許可する IAM ポリシーを作成します。
   a. 以下のコマンドを実行して、ポリシーが存在するかどうかを確認します。

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

1 **RosaOadp** は、実際のポリシー名に置き換えます。

b. 以下のコマンドを使用してポリシー JSON ファイルを作成し、ROSA でポリシーを作成します。

注記

ポリシー ARN が見つからない場合は、このコマンドではポリシーが作成されます。ポリシー ARN がすでに存在する場合、**if** ステートメントはポリシーの作成を意図的にスキップします。

```
$ 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** は、環境変数用に作成された一時ディレクトリーの名前です。

c. 以下のコマンドを実行してポリシー ARN を表示します。

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

3. クラスターの IAM ロール信頼ポリシーを作成します。

a. 次のコマンドを実行して、信頼ポリシーファイルを作成します。

```
$ 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. 以下のコマンドを実行してロールを作成します。

```
$ 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. 次のコマンドを実行して、ロール ARN を表示します。

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

4. 次のコマンドを実行して、IAM ポリシーを IAM ロールにアタッチします。

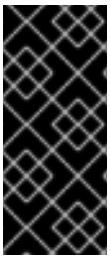
```
$ aws iam attach-role-policy --role-name "${ROLE_NAME}" \
  --policy-arn ${POLICY_ARN}
```

次のステップ

- **OADP Operator のインストールと IAM ロールの指定**に進みます。

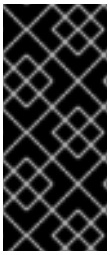
1.2. OADP OPERATOR のインストールおよび IAM ロールの指定

AWS Security Token Service (AWS STS) は、IAM またはフェデレーションされたユーザーの短期認証情報を提供するグローバル Web サービスです。STS を使用した Red Hat OpenShift Service on AWS (ROSA) は、ROSA クラスターに推奨される認証情報モードです。このドキュメントでは、AWS STS を使用して (ROSA) に OpenShift API for Data Protection (OADP) をインストールする方法を説明します。



重要

Restic と Kopia は、AWS STS を使用する ROSA 環境の OADP ではサポートされていません。必ず Restic/Kopia ノードエージェントを無効にしてください。ボリュームのバックアップに関しては、AWS STS を使用する ROSA の OADP は、ネイティブスナップショットと CSI スナップショットのみをサポートします。詳細は、**既知の問題** を参照してください。



重要

STS 認証を使用する Amazon ROSA クラスターでは、別の AWS リージョンでのバックアップデータの復元はサポートされていません。

Data Mover 機能は現在、ROSA クラスターではサポートされていません。データの移動にはネイティブ AWS S3 ツールを使用できます。

前提条件

- 必要なアクセス権とトークンを備えたクラスター。詳細は、「AWS 認証情報の準備」の手順を参照してください。バックアップと復元に 2 つの異なるクラスターを使用する予定の場合は、**ROLE_ARN** を含む AWS 認証情報をクラスターごとに準備する必要があります。

手順

1. 次のコマンドを入力して、AWS トークンファイルから OpenShift シークレットを作成します。

   a. 認証情報ファイルを作成します。

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

   b. OADP の namespace を作成します。

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

c. OpenShift シークレットを作成します。

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

注記

Red Hat OpenShift Service on AWS バージョン 4.15 以降、Operator Lifecycle Manager (OLM) および Cloud Credentials Operator (CCO) により、OADP Operator で標準化された新しい STS ワークフローがサポートされるようになりました。このワークフローでは、上記のシークレットを作成する必要はありません。OLM 管理の Operator のインストール中に Red Hat OpenShift Service on AWS Web コンソール でロール ARN を指定するだけで済みます。上記のシークレットは、CCO によって自動的に作成されます。

2. OADP Operator をインストールします。

   a. Red Hat OpenShift Service on AWS Web コンソールで、Operators → OperatorHub に移動します。

   b. OADP Operator を検索し、**インストール** をクリックします。

3. AWS 認証情報を使用して AWS クラウドストレージを作成します。

```
$ 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. **DataProtectionApplication** リソースを作成します。これは、バックアップとボリュームスナップショットが保存されるストレージへの接続を設定するために使用されます。

```
$ 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 以下の最初の注記を参照してください。

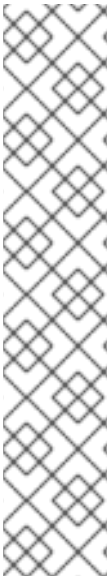
2 **credentialsFile** フィールドは、Pod のバケット認証情報のマウント先です。

3 **enableSharedConfig** フィールドを使用すると、**snapshotLocations** がバケットに定義された認証情報を共有または再利用できます。

4 AWS 認証情報ファイルに設定されているプロファイル名を使用します。

5 **region** は、お使いの AWS リージョンに指定します。これはクラスターリージョンと同じである必要があります。

OADP ドキュメント に記載されているように、OpenShift アプリケーションをバックアップおよび復元する準備が整いました。



注記

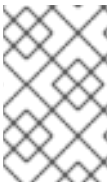
OADP は ROSA 環境で Restic をサポートしていないため、**restic** の **enable** パラメーターは **false** に設定されています。

OADP 1.2 を使用している場合は、次の設定を置き換えます。

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

次の設定に置き換えます。

```
restic:
  enable: false
```



注記

バックアップと復元に 2 つの異なるクラスターを使用する場合、cloudstorage CR と OADP **DataProtectionApplication** 設定の両方で、2 つのクラスターの AWS S3 ストレージ名が同一である必要があります。

関連情報

- AWS 認証情報の準備

1.3. 既知の問題

Restic、Kopia、DataMover はサポートまたは推奨されていない

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

1.4. 関連情報

- STS での ROSA について
- ROSA STS の使用
- STS を使用した ROSA クラスターの作成
- OADP のインストールについて
- CSI ボリュームの設定
- ROSA ストレージオプション