Red Hat OpenShift Service on AWS 4

애플리케이션 백업 및 복원

애플리케이션 데이터 백업 및 복원

Last Updated: 2024-11-03

Red Hat OpenShift Service on AWS 4 애플리케이션 백업 및 복원

애플리케이션 데이터 백업 및 복원

법적 공지

초록

이 문서에서는 애플리케이션 백업에 대한 정보를 제공합니다.

차례

1장. 애플리케이션 백업 **3**
1.1. AWS 인증 정보 준비 3
1.2. OADP OPERATOR 설치 및 IAM 역할 제공 6
1.3. ROSA STS를 사용하여 OADP에서 워크로드 백업 10
1.4. 확인된 문제 14
1.5. 추가 리소스 14

1장. 애플리케이션 백업

ROSA(Red Hat OpenShift Service) 클러스터와 함께 OADP(OpenShift API for Data Protection)를 사용하여 애플리케이션 데이터를 백업하고 복원할 수 있습니다. OADP를 설치하기 전에 AWS API를 사용할 수 있도록 OADP의 역할 및 정책 자격 증명을 설정해야 합니다.

이는 두 단계의 프로세스입니다.

1. AWS 인증 정보를 준비합니다.
2. OADP Operator를 설치하고 IAM 역할을 제공합니다.

1.1. AWS 인증 정보 준비

AWS 계정은 OADP 설치를 수락할 준비가 되어 있어야 합니다.

절차

1. 다음 명령을 실행하여 다음 환경 변수를 생성합니다.

참고

ROSA 클러스터와 일치하도록 클러스터 이름을 변경하고 관리자로 클러스터에 로그인했는지 확인합니다. 계속하기 전에 모든 필드가 올바르게 출력되었는지 확인합니다.

```
$ 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** 를 ROSA 클러스터 이름으로 교체합니다.

2. AWS 계정에서 S3에 대한 액세스를 허용하는 IAM 정책을 생성합니다.
   a. 다음 명령을 실행하여 정책이 존재하는지 확인합니다.

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

(1) **RosaOadp** 를 정책 이름으로 교체합니다.

b. 다음 명령을 사용하여 정책 JSON 파일을 생성한 다음 ROSA에서 정책을 생성합니다.

참고

정책 ARN을 찾을 수 없는 경우 명령에서 정책을 생성합니다. 정책 ARN이 이미 존재하는 경우 **if** 문이 의도적으로 정책 생성을 건너뜁니다.

```
$ 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** 는 환경 변수에 대해 생성된 임시 디렉터리의 이름입니다.

c. 다음 명령을 실행하여 정책 ARN을 확인합니다.

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

3. 클러스터에 대한 IAM 역할 신뢰 정책을 생성합니다.

a. 다음 명령을 실행하여 신뢰 정책 파일을 생성합니다.

```
$ 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. 다음 명령을 실행하여 역할을 생성합니다.

```
$ 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. 다음 명령을 실행하여 역할 ARN을 확인합니다.

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

4. 다음 명령을 실행하여 IAM 역할에 IAM 정책을 연결합니다.

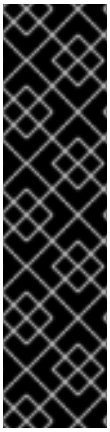
```
$ aws iam attach-role-policy --role-name "${ROLE_NAME}" \
  --policy-arn ${POLICY_ARN}
```

다음 단계

- *OADP Operator 설치를 계속하고 IAM 역할을 제공합니다 .*

1.2. OADP OPERATOR 설치 및 IAM 역할 제공

AWS STS(AWS Security Token Service)는 IAM 또는 페더레이션 사용자를 위한 단기 인증 정보를 제공하는 글로벌 웹 서비스입니다. STS를 사용하는 ROSA(Red Hat OpenShift Service on AWS)는 ROSA 클러스터에 권장되는 인증 정보 모드입니다. 이 문서에서는 AWS STS를 사용하여 ROSA에 OADP(OpenShift API for Data Protection)를 설치하는 방법을 설명합니다.



중요

Restic 및 Kopia는 AWS STS 환경의 ROSA의 OADP에서 지원되지 않습니다. Restic 및 Kopia 노드 에이전트가 비활성화되어 있는지 확인합니다. 볼륨 백업의 경우 AWS STS를 사용하여 ROSA의 OADP는 기본 스냅샷 및 CSI(Container Storage Interface) 스냅샷만 지원합니다.

STS 인증을 사용하는 Amazon ROSA 클러스터에서는 다른 AWS 리전에서 백업 데이터를 복원할 수 없습니다.

Data Mover 기능은 현재 ROSA 클러스터에서 지원되지 않습니다. 데이터 이동을 위해 기본 AWS S3 툴을 사용할 수 있습니다.

사전 요구 사항

- 필요한 액세스 및 토큰이 있는 AWS ROSA 클러스터의 Red Hat OpenShift Service. 자세한 내용은 *OADP에 대한AWS 인증 정보 준비* 절차를 참조하십시오. 백업 및 복원을 위해 두 개의 다른 클러스터를 사용하려면 각 클러스터에 대해 **ROLE_ARN** 을 포함한 AWS 인증 정보를 준비해야 합니다.

절차

1. 다음 명령을 입력하여 AWS 토큰 파일에서 AWS 시크릿에 Red Hat OpenShift Service를 생성합니다.

   a. 자격 증명 파일을 생성합니다.

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

   b. OADP의 네임스페이스를 생성합니다.

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

   c. AWS 시크릿에 Red Hat OpenShift Service를 생성합니다.

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

참고

AWS 버전 4.15 이상에서 OADP Operator는 OLM(Operator Lifecycle Manager) 및 CCO(Cloud Credentials Operator)를 통해 새로운 표준화된 STS 워크플로를 지원합니다. 이 워크플로우에서는 웹 콘솔을 사용하여 *OperatorHub에서 설치를 참조하십시오. 자세한 내용은 AWS 웹 콘솔에서 Red Hat OpenShift Service를 사용하여 OLM 관리 Operator 설치* 중에 위의 시크릿을 생성할 필요가 없습니다.

이전 시크릿은 CCO에 의해 자동으로 생성됩니다.

2. OADP Operator를 설치합니다.

   a. AWS 웹 콘솔의 Red Hat OpenShift Service에서 **Operator → OperatorHub** 로 이동합니다.

   b. **OADP Operator** 를 검색합니다.

   c. **role_ARN** 필드에 이전에 생성한 role_arn을 붙여넣고 **설치를** 클릭합니다.

3. 다음 명령을 입력하여 AWS 인증 정보를 사용하여 AWS 클라우드 스토리지를 생성합니다.

```
$ 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. 다음 명령을 입력하여 애플리케이션의 스토리지 기본 스토리지 클래스를 확인합니다.

```
$ oc get pvc -n <namespace>
```

출력 예

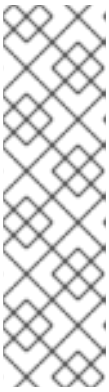
```
NAME     STATUS   VOLUME                                     CAPACITY   ACCESS MODES
STORAGECLASS   AGE
applog   Bound    pvc-351791ae-b6ab-4e8b-88a4-30f73caf5ef8   1Gi        RWO            gp3-
csi        4d19h
mysql    Bound    pvc-16b8e009-a20a-4379-accc-bc81fedd0621   1Gi        RWO            gp3-
csi        4d19h
```

5. 다음 명령을 실행하여 스토리지 클래스를 가져옵니다.

```
$ oc get storageclass
```

출력 예

```
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE
ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true
4d21h
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true
4d21h
gp3             ebs.csi.aws.com         Delete          WaitForFirstConsumer   true
4d21h
gp3-csi (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true
4d21h
```



참고

다음 스토리지 클래스가 작동합니다.

- gp3-csi
- gp2-csi
- gp3
- gp2

백업 중인 애플리케이션 또는 애플리케이션이 모두 CSI(Container Storage Interface)를 사용하는 PV(영구 볼륨)를 사용하는 경우 OADP DPA 구성에 CSI 플러그인을 포함하는 것이 좋습니다.

6. **DataProtectionApplication** 리소스를 만들어 백업 및 볼륨 스냅샷이 저장되는 스토리지에 대한 연결을 구성합니다.

   a. CSI 볼륨만 사용하는 경우 다음 명령을 입력하여 데이터 보호 애플리케이션을 배포합니다.

```
$ cat << EOF | oc create -f -
  apiVersion: oadp.openshift.io/v1alpha1
  kind: DataProtectionApplication
  metadata:
    name: ${CLUSTER_NAME}-dpa
    namespace: openshift-adp
  spec:
    backupImages: true 1
    features:
      dataMover:
        enable: false
    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
        - csi
      restic:
        enable: false
EOF
```

1 ROSA는 내부 이미지 백업을 지원합니다. 이미지 백업을 사용하지 않으려면 이 필드를 **false** 로 설정합니다.

a. CSI 또는 비 CSI 볼륨을 사용하는 경우 다음 명령을 입력하여 데이터 보호 애플리케이션을 배포합니다.

```
$ cat << EOF | oc create -f -
  apiVersion: oadp.openshift.io/v1alpha1
  kind: DataProtectionApplication
  metadata:
    name: ${CLUSTER_NAME}-dpa
    namespace: openshift-adp
  spec:
    backupImages: true 1
    features:
      dataMover:
        enable: false
    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: 2
        enable: false
        uploaderType: restic
    snapshotLocations:
      - velero:
          config:
            credentialsFile: /tmp/credentials/openshift-adp/cloud-credentials-credentials 3
            enableSharedConfig: "true" 4
            profile: default 5
```

```
        region: ${REGION} 6
      provider: aws
EOF
```

1. ROSA는 내부 이미지 백업을 지원합니다. 이미지 백업을 사용하지 않으려면 이 필드를 false로 설정합니다.
2. **nodeAgent** 속성과 관련된 중요한 노트를 참조하십시오.
3. **credentialsFile** 필드는 Pod에 버킷 인증 정보의 마운트된 위치입니다.
4. **enableSharedConfig** 필드를 사용하면 **snapshotLocations** 에서 버킷에 대해 정의된 인증 정보를 공유하거나 재사용할 수 있습니다.
5. AWS 인증 정보 파일에 설정된 프로필 이름을 사용합니다.
6. **리전을 AWS 리전** 으로 지정합니다. 이는 클러스터 리전과 동일해야 합니다.

이제 애플리케이션 백업에 설명된 대로 AWS 애플리케이션에서 Red Hat OpenShift Service를 *백업하고 복원할 수 있습니다.*

중요

OADP가 ROSA 환경에서 Restic을 지원하지 않기 때문에 **restic** 의 **enable** 매개변수는 이 구성에서 **false** 로 설정됩니다.

OADP 1.2를 사용하는 경우 이 구성을 교체합니다.

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

다음 구성에서는 다음을 수행합니다.

```
restic:
  enable: false
```

백업 및 복원을 위해 두 개의 다른 클러스터를 사용하려면 클라우드 스토리지 CR과 OADP **DataProtectionApplication** 구성 둘 다에 동일한 AWS S3 스토리지 이름이 있어야 합니다.

추가 리소스

- AWS 인증 정보 준비

1.3. ROSA STS를 사용하여 OADP에서 워크로드 백업

1.3.1. OADP 및 ROSA STS로 백업 수행

다음 예제 **hello-world** 애플리케이션에는 PV(영구 볼륨)가 연결되어 있지 않습니다. ROSA(Red Hat OpenShift Service on AWS) STS를 사용하여 OADP(OpenShift API for Data Protection)를 사용하여 백업을 수행합니다.

DPA(Data Protection Application) 구성이 작동합니다.

1. 다음 명령을 실행하여 백업할 워크로드를 생성합니다.

```
$ oc create namespace hello-world
```

```
$ oc new-app -n hello-world --image=docker.io/openshift/hello-openshift
```

2. 다음 명령을 실행하여 경로를 노출합니다.

```
$ oc expose service/hello-openshift -n hello-world
```

3. 다음 명령을 실행하여 애플리케이션이 작동하는지 확인합니다.

```
$ curl `oc get route/hello-openshift -n hello-world -o jsonpath='{.spec.host}'`
```

출력 예

```
Hello OpenShift!
```

4. 다음 명령을 실행하여 워크로드를 백업합니다.

```
$ cat << EOF | oc create -f -
  apiVersion: velero.io/v1
  kind: Backup
  metadata:
    name: hello-world
    namespace: openshift-adp
  spec:
    includedNamespaces:
    - hello-world
    storageLocation: ${CLUSTER_NAME}-dpa-1
    ttl: 720h0m0s
EOF
```

5. 백업이 완료될 때까지 기다린 후 다음 명령을 실행합니다.

```
$ watch "oc -n openshift-adp get backup hello-world -o json | jq .status"
```

출력 예

```
{
  "completionTimestamp": "2022-09-07T22:20:44Z",
  "expiration": "2022-10-07T22:20:22Z",
  "formatVersion": "1.1.0",
  "phase": "Completed",
  "progress": {
    "itemsBackedUp": 58,
    "totalItems": 58
  },
  "startTimestamp": "2022-09-07T22:20:22Z",
  "version": 1
}
```

6. 다음 명령을 실행하여 데모 워크로드를 삭제합니다.

```
$ oc delete ns hello-world
```

7. 다음 명령을 실행하여 백업에서 워크로드를 복원합니다.

```
$ cat << EOF | oc create -f -
  apiVersion: velero.io/v1
  kind: Restore
  metadata:
    name: hello-world
    namespace: openshift-adp
  spec:
    backupName: hello-world
EOF
```

8. 다음 명령을 실행하여 복원이 완료될 때까지 기다립니다.

```
$ watch "oc -n openshift-adp get restore hello-world -o json | jq .status"
```

출력 예

```
{
  "completionTimestamp": "2022-09-07T22:25:47Z",
  "phase": "Completed",
  "progress": {
    "itemsRestored": 38,
    "totalItems": 38
  },
  "startTimestamp": "2022-09-07T22:25:28Z",
  "warnings": 9
}
```

9. 다음 명령을 실행하여 워크로드가 복원되었는지 확인합니다.

```
$ oc -n hello-world get pods
```

출력 예

```
NAME                         READY   STATUS    RESTARTS   AGE
hello-openshift-9f885f7c6-kdjpj   1/1     Running   0          90s
```

10. 다음 명령을 실행하여 JSONPath를 확인합니다.

```
$ curl `oc get route/hello-openshift -n hello-world -o jsonpath='{.spec.host}'`
```

출력 예

```
Hello OpenShift!
```

참고

문제 해결 팁은 OADP 팀의 문제 해결 설명서를 참조하십시오.

1.3.2. OADP 및 ROSA STS를 사용하여 백업 후 클러스터 정리

이 예제에서 OADP(OpenShift API for Data Protection) Operator를 백업 및 S3 버킷과 함께 설치 제거해야 하는 경우 다음 지침을 따르십시오.

절차

1. 다음 명령을 실행하여 워크로드를 삭제합니다.

```
$ oc delete ns hello-world
```

2. 다음 명령을 실행하여 DPA(데이터 보호 애플리케이션)를 삭제합니다.

```
$ oc -n openshift-adp delete dpa ${CLUSTER_NAME}-dpa
```

3. 다음 명령을 실행하여 클라우드 스토리지를 삭제합니다.

```
$ oc -n openshift-adp delete cloudstorage ${CLUSTER_NAME}-oadp
```

주의

이 명령이 중단되면 다음 명령을 실행하여 종료자를 삭제해야 할 수 있습니다.

```
$ oc -n openshift-adp patch cloudstorage ${CLUSTER_NAME}-oadp -p
'{"metadata":{"finalizers":null}}' --type=merge
```

4. Operator가 더 이상 필요하지 않은 경우 다음 명령을 실행하여 Operator를 제거합니다.

```
$ oc -n openshift-adp delete subscription oadp-operator
```

5. Operator에서 네임스페이스를 제거합니다.

```
$ oc delete ns openshift-adp
```

6. 백업 및 복원 리소스가 더 이상 필요하지 않은 경우 다음 명령을 실행하여 클러스터에서 해당 리소스를 제거합니다.

```
$ oc delete backup hello-world
```

7. AWS S3에서 백업, 복원 및 원격 오브젝트를 삭제하려면 다음 명령을 실행합니다.

```
$ velero backup delete hello-world
```

8. 더 이상 CRD(Custom Resource Definitions)가 필요하지 않은 경우 다음 명령을 실행하여 클러스터에서 해당 정의를 제거하십시오.

```
$ for CRD in `oc get crds | grep velero | awk '{print $1}'`; do oc delete crd $CRD; done
```

9. 다음 명령을 실행하여 AWS S3 버킷을 삭제합니다.

```
$ aws s3 rm s3://${CLUSTER_NAME}-oadp --recursive
```

```
$ aws s3api delete-bucket --bucket ${CLUSTER_NAME}-oadp
```

10. 다음 명령을 실행하여 역할에서 정책을 분리합니다.

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

11. 다음 명령을 실행하여 역할을 삭제합니다.

```
$ aws iam delete-role --role-name "${ROLE_NAME}"
```

1.4. 확인된 문제

- Restic, Kopia, DataMover는 지원되거나 권장되지 않습니다.
- CloudStorage: Restic이 활성화된 openshift-adp-controller-manager 크래시 루프 오류가 발생합니다.
- (OADP 1.1.x_만 해당): CloudStorage: 버킷은 CS CR 삭제에서 제거되지만 "oadp.openshift.io/cloudstorage-delete": "true"가 없습니다.

1.5. 추가 리소스

- ROSA 아키텍처에 대한 자세한 내용은 ROSA 이해 를 참조하십시오.
- STS를 사용하여 ROSA를 설치하기 위한 사전 요구 사항에 대한 자세한 내용은 STS를 사용하여 ROSA에 대한 AWS 사전 요구 사항을 참조하십시오.
- 수동 모드를 사용하여 ROSA 클러스터를 배포하는 단계는 사용자 지정을 사용하여 클러스터 생성 을 참조하십시오.
- STS를 사용하여 AWS에 Red Hat OpenShift Service를 배포하는 데 필요한 AWS IAM(Identity Access Management) 리소스에 대한 자세한 내용은 STS를 사용하는 클러스터의 IAM 리소스 정보를 참조하십시오.
- OADP 설치에 대한 자세한 내용은 OADP 설치 정보를 참조하십시오.
- CSI 볼륨에 대한 자세한 내용은 CSI 볼륨 구성을 참조하십시오.
- ROSA의 저장 옵션에 대한 자세한 내용은 ROSA 스토리지 옵션을 참조하십시오.
- Red Hat 지원에 문의하려면 AWS에서 Red Hat OpenShift Service에 대한 지원 받기를 참조하십시오.