재해 복구

NetApp virtualization solutions

NetApp
July 21, 2026

목차

재해 복구

Trident Protect/AppMirror OpenShift 가상화 재해 복구를 위한 필수 조건

이 섹션에서는 OpenShift Virtualization 워크로드의 재해 복구를 위해 NetApp Trident Protect 및 AppMirror를 사용하기 위한 전제 조건에 대한 정보를 제공합니다. 여기에는 OpenShift Virtualization에서 실행되는 VM의 효과적인 재해 복구를 위해 Trident Protect 및 AppMirror를 설정하는 데 필요한 클러스터 구성, 스토리지 요구사항 및 설치 단계가 포함됩니다.

필수 조건

1. Red Hat OpenShift Virtualization이 설치 및 구성된 OpenShift 클러스터입니다. 설치 지침은 "여기에 문서가 있습니다."을 참조하십시오.
2. 액티브 및 재해 복구 OpenShift 클러스터에 스토리지를 제공하기 위해 각각 SVM이 구성된 두 개의 NetApp ONTAP 스토리지 시스템. 각 SVM에는 해당 OpenShift 클러스터에서 액세스할 수 있도록 구성된 관리 LIF와 데이터 LIF가 각각 최소 하나 이상 있어야 합니다.
3. 두 ONTAP 시스템 간에 클러스터 피어링 및 SVM 피어링을 구성하여 소스 클러스터의 SVM에서 타겟 클러스터의 SVM으로 데이터를 복제할 수 있도록 합니다. 클러스터 피어링 및 SVM 피어링 설정 방법에 대한 자세한 내용은 "ONTAP 클러스터 피어링 관련 문서는 여기에서 확인할 수 있습니다."을 참조하십시오.
4. NetApp Trident가 OpenShift 클러스터에 설치 및 구성되어 ONTAP SVM에서 영구 스토리지를 프로비저닝합니다. 설치 지침은 "Trident 관련 문서는 여기에서 확인할 수 있습니다."을 참조하십시오.
5. ONTAP SVM용으로 생성된 Trident 백엔드 구성 및 해당 Trident 백엔드를 프로비저너로 사용하도록 OpenShift 클러스터에 구성된 StorageClass입니다. Trident 백엔드 구성 및 StorageClass를 생성하는 방법에 대한 자세한 내용은 "Trident 백엔드 구성 문서는 여기에서 확인할 수 있습니다."을 참조하십시오.
6. OpenShift 클러스터에 대한 클러스터 관리자 액세스 권한과 필요한 구성을 수행하기 위한 ONTAP 스토리지 시스템에 대한 관리자 액세스 권한이 필요합니다.
7. `tridentctl` 및 `oc` 도구가 설치되어 $PATH 환경 변수에 추가된 관리자 워크스테이션으로 OpenShift 클러스터 및 Trident와 상호 작용합니다.
8. 프로비저닝될 VM과 OpenShift Virtualization 운영자를 지원하기 위해 OpenShift 클러스터에 충분한 하드웨어 리소스가 필요합니다. 리소스 요구 사항에 대한 자세한 내용은 "여기에 문서가 있습니다."을 참조하십시오.
9. 선택적으로 OpenShift Virtualization의 노드 배치 규칙을 구성하여 OpenShift Virtualization 운영자, 컨트롤러 및 VM을 호스팅할 클러스터 노드 하위 집합을 지정할 수 있습니다. 노드 배치 규칙 구성 방법에 대한 지침은 "여기에 문서가 있습니다."을 참조하십시오.
10. OpenShift 가상화를 지원하는 스토리지의 경우, 특정 Trident 백엔드에서 스토리지를 요청하는 전용 StorageClass를 사용하는 것이 좋습니다. 이 백엔드는 전용 SVM에 의해 지원됩니다. 이를 통해 OpenShift 클러스터에서 VM 기반 워크로드에 제공되는 데이터에 대한 멀티테넌시를 유지할 수 있습니다.
11. OpenShift Virtualization에서 VM을 사용할 수 있어야 합니다. 새 VM을 배포하거나 기존 VM을 OpenShift Virtualization으로 마이그레이션하는 방법에 대한 자세한 내용은 설명서의 해당 섹션을 참조하세요.

NetApp Trident Protect를 OpenShift 가상화 환경에 설치합니다

NetApp Trident Protect를 사용하여 OpenShift Virtualization 워크로드에 대한 재해 복구 기능을 활성화하려면 OpenShift 클러스터에 Trident Protect가 설치 및 구성되어 있어야 합니다. Trident Protect는 Helm 차트를 사용하여

설치할 수 있습니다.

Trident Protect 설치는 Trident 설치 후에 수행해야 합니다.

자세한 설치 지침은 "Trident Protect 관련 문서는 여기에서 확인할 수 있습니다."을 참조하십시오.

예를 보여주세요

Red Hat OpenShift 가상화 재해 복구를 위한 소스 클러스터 설정

이 섹션에서는 NetApp Trident Protect 및 AppMirror를 사용하여 OpenShift Virtualization 워크로드의 재해 복구를 위한 소스 클러스터를 설정하는 방법에 대한 정보를 제공합니다. 여기에는 ONTAP S3를 사용하여 AppVault를 생성하고, 소스 VM을 위한 Trident Protect 애플리케이션을 생성하며, Trident Protect를 사용하여 VM의 온디맨드 및 예약된 스냅샷을 생성하는 작업이 포함됩니다. 이러한 단계는 소스 클러스터가 재해 복구 타겟 클러스터로 데이터를 복제하고 재해 발생 시 VM 복구를 지원하도록 올바르게 구성되었는지 확인하는 데 필수적입니다.

OpenShift 가상화를 위한 재해 복구 소스 클러스터 설정

다음의 모든 단계는 소스 클러스터, 즉 보호 대상 VM이 현재 실행 중인 클러스터에서 수행됩니다.

ONTAP S3를 사용하여 AppVault 생성

이 섹션에서는 ONTAP S3 객체 스토리지를 사용하여 Trident Protect에서 AppVault 객체를 설정하는 방법을 보여줍니다. 이 단계에서 생성된 AppVault는 소스 클러스터의 복제된 데이터를 저장하는 데 사용되며, 해당 데이터는 재해 복구 타겟 클러스터에서 복구에 사용됩니다.

아래에 표시된 oc 명령어와 yaml 파일을 사용하여 ONTAP s3용 시크릿과 AppVault 사용자 지정 리소스를 생성하세요. 반드시 trident-protect 네임스페이스에 생성해야 합니다.

예를 보여주세요

```
apiVersion: v1
# You can provide the keys either as stringData or base 64 encoded data
stringData:
  accessKeyID: "<access key id as obtained from ONTAP>"
  secretAccessKey: "<secret access key as obtained from ONTAP>"
#data:
  #accessKeyID: <base 64 encoded value of access key>
  #secretAccessKey: <base 64 encoded value of secret access key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque
```

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    s3:
      bucketName: oc-dr
      endpoint: <data lif to use to access S3>
      secure: "false" # Setting this to "false" will disable TLS, which
is not recommended for production environments.
      skipCertValidation: "true" # When TLS is enabled, setting
skipCertValidation to "true" will skip TLS certificate validation,
which is not recommended for production environments.
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3
```

ONTAP S3 볼트가 생성되었고 사용 가능 상태인지 확인하십시오.

```
oc create -f app-vault-secret.yaml -n trident-protect
oc create -f app-vault.yaml -n trident-protect
```

```
[root@00-50-56-b5-2b-9b dr]# oc get appvault -n trident-protect
NAME                STATE       ERROR   MESSAGE   AGE
ontap-s3-appvault   Available                     2d23h
```

소스 VM용 Trident Protect 앱 생성

소스 VM이 위치한 네임스페이스에 애플리케이션 사용자 지정 리소스를 생성합니다.

예를 보여주세요

```
# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: test-source-app
  namespace: test-dr-ns
spec:
  includedNamespaces:
  - namespace: test-dr-ns
```

```
tridentctl-protect create app <source-vm> -n <source-ns> --namespaces
<source-ns>
```

```
[root@00-50-56-b5-2b-9b dr]# oc get applications.protect.trident.netapp.io -n test-dr-ns
NAME              PROTECTION STATE   AGE
test-source-app   Partial            25h
```

앱 사용자 지정 리소스에 포함된 네임스페이스의 VM 및 해당 PVC는 아래와 같습니다.

```
[root@00-50-56-b5-2b-9b dr]# oc get vm,pods,pvc -n test-dr-ns
NAME                                        AGE   STATUS    READY
virtualmachine.kubevirt.io/test-dr-vm1   25h   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-test-dr-vm1-ns9qq   1/1     Running   0          25h

NAME                                  STATUS   VOLUME                                     CAPACITY     ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/test-dr-vm1   Bound    pvc-43b51d12-ce76-4063-bd59-6e74588ee266   34144990004   RWX            sc-nas         <unset>                 25h
```

Trident Protect를 사용하여 VM의 스냅샷을 생성합니다.

Trident Protect CLI 또는 API를 사용하여 필요에 따라 VM의 스냅샷을 생성할 수 있습니다. 이 스냅샷은 이전 단계에서 생성한 AppVault에 저장되며 재해 복구 타겟 클러스터에서 복구에 사용할 수 있습니다.

예를 보여주세요

```
# snapshot.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  name: test-source-dr-init-snapshot
  namespace: test-dr-ns
spec:
  applicationRef: test-source-app
  appVaultRef: ontap-s3-appvault
  reclaimPolicy: Delete
```

```
[root@00-50-56-b5-2b-9b dr]# oc get snapshot -n test-dr-ns
NAME                          APP              RECLAIM POLICY   STATE       ERROR   AGE
test-source-dr-init-snapshot  test-source-app   Delete           Completed           25h
```

Trident Protect를 사용하여 VM의 예약된 스냅샷 생성

애플리케이션 사용자 지정 리소스와 동일한 네임스페이스에 스케줄 사용자 지정 리소스를 생성하여 예약된 스냅샷을 만들 수도 있습니다. 이 스케줄은 지정된 일정에 따라 VM의 스냅샷을 자동으로 생성하고 AppVault에 저장합니다.

예를 보여주세요

```
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  name: appmirror-sched1
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: test-source-app
  backupRetention: "0"
  enabled: true
  granularity: Custom
  recurrenceRule: |-
    DTSTART:20240901T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  snapshotRetention: "2"
```

Red Hat OpenShift 가상화 재해 복구를 위한 타겟 클러스터 설정

이 섹션에서는 NetApp Trident Protect 및 AppMirror를 사용하여 OpenShift Virtualization

워크로드의 재해 복구를 위한 타겟 클러스터를 설정하는 방법에 대한 정보를 제공합니다. 여기에는 ONTAP S3를 사용하여 AppVault를 생성하고 타겟 VM을 위한 새 네임스페이스를 생성하는 작업이 포함됩니다. 이러한 단계는 타겟 클러스터가 소스 클러스터로부터 복제된 데이터를 수신하도록 올바르게 구성되고 재해 발생 시 VM 복구를 가능하게 하는 데 필수적입니다.

1. 타겟 클러스터에 AppVault 객체를 생성합니다. 이 객체는 소스 클러스터와 동일한 S3를 가리켜야 소스 클러스터가 저장한 S3에서 스냅샷을 가져올 수 있습니다.

예를 보여주세요

```
apiVersion: v1
# You can provide the keys either as stringData or base 64 encoded
data
stringData:
  accessKeyID: "<access key id as obtained from ONTAP>"
  secretAccessKey: "<secret access key as obtained from ONTAP>"
#data:
  #accessKeyID: <base 64 encoded value of access key>
  #secretAccessKey: <base 64 encoded value of secret access key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque
```

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    s3:
      bucketName: oc-dr
      endpoint: <data lif to use to access S3>
      secure: "false" # Setting this to "false" will disable TLS,
which is not recommended for production
      skipCertValidation: "true" # When TLS is enabled, setting
skipCertValidation to "true" will skip TLS certificate validation,
which is not recommended for production environments.
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3
```

```
oc create -f app-vault-secret.yaml -n trident-protect
oc create -f app-vault.yaml -n trident-protect
```

```
[root@00-50-56-b5-01-5b dr]# oc get appvault -A
NAMESPACE          NAME                                STATE       ERROR   MESSAGE   AGE
trident-protect    ontap-s3-appvault                   Available                     29h
```

2. 장애 조치된 VM을 호스팅할 새 네임스페이스를 타겟 클러스터에 생성합니다. 1단계에서 생성한 AppVault와 새 네임스페이스를 참조하는 앱을 타겟 클러스터에 생성합니다. 이 앱은 소스 클러스터와 타겟 클러스터 간의 AppMirror 관계를 설정하고 소스 클러스터에서 타겟 클러스터로의 데이터 복제를 관리하는 데 사용됩니다.

   예를 보여주세요

```
# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: test-dest-app
  namespace: test-dr-ns-dest
spec:
  includedNamespaces:
  - namespace: test-dr-ns-dest
```

```
tridentctl-protect create app <dest-app-name> -n <dest-ns>
--namespaces <dest-ns>
```

OpenShift 가상화 재해 복구에서 VM의 페일오버

이 섹션에서는 NetApp Trident Protect 및 AppMirror를 사용하여 소스 클러스터에서 재해 복구 타겟 클러스터로 VM을 페일오버하는 방법을 설명합니다. 이는 페일오버 프로세스를 테스트하고 소스 클러스터에서 계획된 유지 관리를 수행하는 데 유용합니다. 이러한 단계를 따르면 재해 복구 이벤트 후에도 모든 변경 사항이 그대로 유지된 상태로 재해 복구 타겟 클러스터에서 VM이 실행되도록 할 수 있습니다.

OpenShift Virtualization에서 사이트 중단 없이 장애 조치

이 섹션에서는 사이트 중단 없이 소스 클러스터에서 VM의 페일오버를 수행하는 방법을 설명합니다. 이는 페일오버 프로세스를 테스트하고 소스 클러스터에서 계획된 유지 관리를 수행하는 데 유용합니다. +

사이트 중단 없이 페일오버를 수행하려면 먼저 이전 섹션에서 설명한 대로 소스 및 타겟 클러스터가 재해 복구를 위해

설정되어 있는지 확인하십시오. 그런 다음 다음 단계를 수행하십시오.

1. 소스 클러스터와 타겟 클러스터 간에 AppMirror 관계를 설정합니다. AppMirror 관계가 설정되면 최신 스냅샷이 대상 네임스페이스로 전송됩니다. 대상 네임스페이스에 VM용 PVC가 생성되지만, VM Pod는 아직 생성되지 않습니다.

   예를 보여주세요

   ```
   # application-mirror-relationship.yaml
   apiVersion: protect.trident.netapp.io/v1
   kind: AppMirrorRelationship
   metadata:
     name: amr1
   spec:
     desiredState: Established
     destinationAppVaultRef: ontap-s3-appvault
     destinationApplicationRef: test-dest-app
     namespaceMapping:
     - destination: test-dr-ns-dest
       source: test-dr-ns
     recurrenceRule: |-
       DTSTART:20240901T000200Z
       RRULE:FREQ=MINUTELY;INTERVAL=5
     sourceAppVaultRef: ontap-s3-appvault
     sourceApplicationName: test-source-app
     sourceApplicationUID: "<application-uid-of-the-source-app>"
     storageClassName: "sc-nas"
   ```

   ```
   [root@00-50-56-b5-2b-9b dr]# oc get amr -n test-dr-ns
   NAME   DESIRED STATE   STATE          ERROR   AGE
   amr1   Established     Establishing           115s
   ```

   ```
   [root@00-50-56-b5-2b-9b dr]# oc get amr -A
   NAMESPACE     NAME   DESIRED STATE   STATE         ERROR   AGE
   test-dr-ns    amr1   Established     Established           94s
   ```

   AppMirror 관계는 타겟 클러스터의 CLI에서 생성해야 합니다. 생성 시 원하는 상태는 'Established'로 설정해야 합니다. 이렇게 하면 최신 스냅샷 데이터가 타겟 클러스터에 복제됩니다.

2. AppMirror 관계를 승격합니다. 관계의 원하는 상태를 "승격됨"으로 변경하여 대상 네임스페이스에 VM을 생성합니다. VM은 소스 네임스페이스에서 계속 실행됩니다. 최신 스냅샷 데이터가 타겟 클러스터에 복제되고 VM이 타겟 클러스터에서 시작됩니다. 이 방법을 사용하면 전체 소스 클러스터를 중단하지 않고도 페일오버를 테스트하고 VM 가용성을 유지할 수 있습니다.

예를 보여주세요

```
oc patch amr amr1 -n test-dr-ns-dest --type=merge -p
'{"spec":{"desiredState":"Promoted"}}'
```

```
[root@00-50-56-b5-01-5b dr]# oc get amr -n test-dr-ns-dest
NAME   DESIRED STATE   STATE      ERROR   AGE
amr2   Promoted        Promoted           25h
```

```
oc get pod, pvc,vm -n test-dr-ns-dest
oc get pod, pvc,vm -n test-dr-ns
```

OpenShift 가상화 재해 복구에서 VM의 페일백

이 섹션에서는 NetApp Trident Protect 및 AppMirror를 사용하는 OpenShift Virtualization 재해 복구에서 VM의 페일백 프로세스에 대한 정보를 제공합니다. 재해 복구 타겟 클러스터로 전환하기 위해 페일오버 작업을 수행한 후, 페일백 프로세스를 사용하여 복제 방향을 역전시키고 원래 소스 클러스터를 VM의 기본 클러스터로 복원할 수 있습니다. 여기에는 페일오버 기간 동안 VM에 발생한 모든 변경 사항을 원래 소스 클러스터로 다시 동기화한 다음 복제 관계를 역방향으로 승격하는 작업이 포함됩니다. 다음 단계를 수행하면 재해 복구 이벤트가 발생한 후 모든 변경 사항이 그대로 유지된 상태로 원래 소스 클러스터에서 VM이 실행되도록 할 수 있습니다.

OpenShift 가상화 재해 복구를 위한 페일백

Trident Protect를 사용하면 다음 일련의 작업을 통해 페일오버 작업 후 "페일 백"을 구현할 수 있습니다. 원래 복제 방향을 복원하는 이 워크플로에서 Trident Protect는 복제 방향을 반전하기 전에 모든 애플리케이션 변경 사항을 원래 소스 애플리케이션으로 복제(재동기화)합니다.

이 프로세스는 타겟으로 페일오버가 완료된 관계에서 시작되며 다음 단계를 포함합니다.

1. 장애 조치 상태로 시작합니다.
2. 복제 관계를 역방향으로 다시 동기화

   장애 조치 복제 관계를 역동기화하면 타겟 애플리케이션이 소스 애플리케이션이 되고 소스가 타겟이 됩니다. 장애 조치 중에 타겟 애플리케이션에 변경된 내용은 유지됩니다.

   a. 원래 타겟 클러스터에서 AppMirrorRelationship CR을 삭제합니다. 이렇게 하면 타겟이 소스가 됩니다. 새 타겟 클러스터에 보호 스케줄이 남아 있는 경우 이를 제거합니다.

예를 보여주세요

```
[root@00-50-56-b5-01-5b dr]# oc delete -f app-mirror-relationship.yaml -n test-dr-ns-dest
appmirrorrelationship.protect.trident.netapp.io "amr2" deleted from test-dr-ns-dest namespace
```

b. 장애 조치 기간 동안 발생한 변경 사항을 캡처하기 위해 새 소스 클러스터(원래 타겟)에 스냅샷을 생성합니다. 이렇게 하면 재동기화 프로세스 중에 모든 변경 사항이 원래 소스 클러스터로 복제됩니다.

예를 보여주세요

```yaml
# snapshot.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  name: test-source-dr-init-snapshot-failback
  namespace: test-dr-ns
spec:
  applicationRef: test-dest-app
  appVaultRef: ontap-s3-appvault
  reclaimPolicy: Delete
```

```
[root@00-50-56-b5-01-5b dr]# cat failback-snapshot.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  name: test-source-dr-init-snapshot-failback
  namespace: test-dr-ns-dest
spec:
  applicationRef: test-dest-app
  appVaultRef: ontap-s3-appvault
  reclaimPolicy: Delete
```

```
[root@00-50-56-b5-01-5b dr]# oc get snapshot -n test-dr-ns-dest
NAME                                  APP             RECLAIM POLICY   STATE     ERROR   AGE
test-source-dr-init-snapshot-failback   test-dest-app   Delete           Running           10s
```

```
[root@00-50-56-b5-01-5b dr]# oc get snapshot -n test-dr-ns-dest
NAME                                  APP             RECLAIM POLICY   STATE       ERROR   AGE
test-source-dr-init-snapshot-failback   test-dest-app   Delete           Completed           8m50s
test-source-dr-init-snapshot-failback-2   test-dest-app   Delete           Completed           32s
```

c. 새 소스 클러스터(원래 타겟)에서 원래 소스 클러스터로의 복제 관계를 설정하고, 역방향에 대한 값을 구성합니다.

예를 보여주세요

application-mirror-relationship.yaml

```
apiVersion: protect.trident.netapp.io/v1
kind: AppMirrorRelationship
metadata:
  name: amr1
spec:
  desiredState: Established
  destinationAppVaultRef: ontap-s3-appvault
  destinationApplicationRef: dr-source-vm-failback
  namespaceMapping:
  - destination: test-dr-ns
    source: test-dr-ns-dest
  recurrenceRule: |-
    DTSTART:20240901T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  sourceAppVaultRef: ontap-s3-appvault
  sourceApplicationName: test-dest-app
  sourceApplicationUID: "uid of the app in the original source
cluster"
  storageClassName: "sc-nas"
```

```
[root@00-50-56-b5-2b-9b dr]# oc get amr -n test-dr-ns
NAME   DESIRED STATE   STATE          ERROR   AGE
amr1   Established     Establishing           115s
[root@00-50-56-b5-2b-9b dr]# oc get amr -A
NAMESPACE    NAME   DESIRED STATE   STATE         ERROR   AGE
test-dr-ns   amr1   Established     Established           94s
```

d. AppMirrorRelationship CR의 desiredState 필드를 "Promoted"로 업데이트하여 새로운 소스 클러스터(원래 타겟 클러스터)에서 원래 소스 클러스터로의 복제 관계를 승격합니다.

예를 보여주세요

```
[root@00-50-56-b5-2b-9b dr]# oc get vm -n test-dr-ns
No resources found in test-dr-ns namespace.
[root@00-50-56-b5-2b-9b dr]# oc patch amr amr1 -n test-dr-ns --type=merge -p '{"spec":{"desiredState":"Promoted"}}'
appmirrorrelationship.protect.trident.netapp.io/amr1 patched
```

이제 원래 소스 클러스터에서 VM이 실행되는 것을 확인할 수 있습니다. 장애 복구 프로세스가 완료되었습니다. 이제 원래 타겟 클러스터의 리소스를 정리할 수 있습니다. 장애 복구 프로세스 후에도 재해 복구 기능을 유지하려면 새 복제 관계를 설정할 수도 있습니다.

> 일반적인 재동기화 작업을 수행하지 마십시오. 이 작업을 수행하면 장애 조치 절차 중에 타겟 클러스터에 기록된 데이터가 손실됩니다.

저작권 정보

상표 정보