



Recuperación ante desastres

NetApp virtualization solutions

NetApp
July 21, 2026

This PDF was generated from <https://docs.netapp.com/es-es/netapp-solutions-virtualization/openshift/osv-disaster-recovery-requirements.html> on July 21, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Recuperación ante desastres. 1
 - Requisitos previos de Trident Protect/AppMirror para la recuperación ante desastres de OpenShift
 - Virtualization. 1
 - Prerrequisitos. 1
 - Instala Trident Protect de NetApp para la virtualización de OpenShift 2
 - Configuración del clúster de origen para la recuperación ante desastres de Red Hat OpenShift
 - Virtualization. 2
 - Configura el clúster de origen para la recuperación ante desastres en la virtualización de OpenShift. 2
 - Crea AppVault usando ONTAP S3. 3
 - Crear una aplicación Trident Protect para la máquina virtual de origen 5
 - Crea una instantánea de la máquina virtual con Trident Protect 6
 - Crea una instantánea programada de la máquina virtual con Trident Protect. 6
 - Configuración del clúster de destino para la recuperación ante desastres de Red Hat OpenShift
 - Virtualization. 7
 - Conmutación por error de una máquina virtual en OpenShift Virtualization Disaster Recovery 9
 - Conmutación por error sin fallo energético en el sitio para OpenShift Virtualization. 10
 - Reversión de una máquina virtual en la recuperación ante desastres de OpenShift Virtualization. 12
 - Recuperación tras un fallo para OpenShift Virtualization Disaster Recovery 12

Recuperación ante desastres

Requisitos previos de Trident Protect/AppMirror para la recuperación ante desastres de OpenShift Virtualization

En esta sección se ofrece información sobre los requisitos previos para utilizar NetApp Trident Protect y AppMirror para la recuperación ante desastres de cargas de trabajo de OpenShift Virtualization. Esto incluye las configuraciones de clúster necesarias, los requisitos de almacenamiento y los pasos de instalación para configurar Trident Protect y AppMirror para una recuperación ante desastres eficaz de las máquinas virtuales que se ejecutan en OpenShift Virtualization.

Prerrequisitos

1. Un clúster de Red Hat OpenShift con OpenShift Virtualization instalado y configurado. Para obtener instrucciones de instalación, consulta el ["documentación aquí"](#).
2. Dos sistemas de almacenamiento NetApp ONTAP con un SVM configurado en cada uno, para proporcionar almacenamiento a los clústeres activo y de recuperación ante desastres OpenShift. Cada SVM debe tener al menos un LIF de gestión y un LIF de datos configurados y accesibles desde el clúster correspondiente OpenShift.
3. Se han configurado el emparejamiento de clústeres y el emparejamiento de SVM entre los dos sistemas ONTAP para permitir la replicación de datos desde el SVM del clúster de origen al SVM del clúster de destino. Para obtener instrucciones sobre cómo configurar el emparejamiento de clústeres y el emparejamiento de SVM, consulta el ["Documentación sobre la conexión entre clústeres de ONTAP aquí"](#).
4. NetApp Trident se ha instalado y configurado en el clúster OpenShift para proporcionar almacenamiento persistente desde el SVM de ONTAP. Para obtener instrucciones de instalación, consulta ["Documentación de Trident aquí"](#).
5. Se ha creado una configuración de backend de Trident para el SVM de ONTAP y se ha configurado un StorageClass en el clúster OpenShift para usar ese backend de Trident como el aprovisionador. Para instrucciones sobre cómo crear una configuración de backend de Trident y StorageClass, consulta la ["Documentación sobre la configuración del backend de Trident aquí"](#).
6. Acceso de administrador del clúster al clúster OpenShift y acceso de administrador al sistema de almacenamiento ONTAP para realizar las configuraciones necesarias.
7. Una estación de trabajo de administración con `tridentctl` y `oc` herramientas instaladas e incluidas en la variable de entorno `$PATH` para interactuar con el clúster OpenShift y Trident.
8. Recursos de hardware adecuados en el clúster OpenShift para dar soporte al operador OpenShift Virtualization y a las máquinas virtuales que se van a aprovisionar. Para obtener más detalles sobre los requisitos de recursos, consulta el ["documentación aquí"](#).
9. Opcionalmente, configura las reglas de ubicación de nodos para OpenShift Virtualization para especificar un subconjunto de nodos del clúster que alojarán los operadores, controladores y máquinas virtuales de OpenShift Virtualization. Para ver las instrucciones sobre cómo configurar las reglas de ubicación de nodos, consulta el ["documentación aquí"](#).
10. Para el almacenamiento que respalda OpenShift Virtualization, se recomienda tener un StorageClass dedicado que solicite almacenamiento de un backend de Trident en particular, que a su vez esté respaldado por un SVM dedicado. Esto mantiene un nivel de multitenencia con respecto a los datos que se sirven para las cargas de trabajo basadas en máquinas virtuales en el clúster de OpenShift.

11. Una VM debe estar disponible en OpenShift Virtualization. Para obtener detalles sobre cómo implementar una nueva VM o migrar una VM existente a OpenShift Virtualization, consulte la sección correspondiente en la documentación.

Instala Trident Protect de NetApp para la virtualización de OpenShift

Para habilitar las funciones de recuperación ante desastres para las cargas de trabajo de virtualización de OpenShift usando NetApp Trident Protect, debes tener Trident Protect instalado y configurado en el clúster de OpenShift. Trident Protect se puede instalar usando un Helm chart.



La instalación de Trident Protect debe realizarse después de instalar Trident.

Para obtener instrucciones completas de instalación, consulta el ["Documentación de Trident Protect aquí"](#).

Mostrar ejemplo

```
[root@00-50-56-b5-2b-9b ~]# helm repo add netapp-trident-protect https://netapp.github.io/trident-protect-helm-chart
```

```
[root@00-50-56-b5-2b-9b ~]# helm repo update
```

```
[root@00-50-56-b5-2b-9b ~]# helm install trident-protect-crds netapp-trident-protect/trident-protect-crds --version 100.2602.0 --create-namespace --namespace trident-protect
```

```
[root@00-50-56-b5-2b-9b ~]# helm install trident-protect netapp-trident-protect/trident-protect --set clusterName=ubr-plugin-dr --version 100.2602.0 --create-namespace --namespace trident-protect
```

```
[root@localhost SnapMirror]#  
[root@localhost SnapMirror]# oc get pods -n trident-protect  
NAME                                     READY   STATUS    RESTARTS   AGE  
autosupportbundle-e9252a48-34a9-4b40-99c2-c00876d962ee-bk2vx  1/1     Running   0          16h  
trident-protect-controller-manager-7b76c8b59f-2rmh2          2/2     Running   0          22h  
[root@localhost SnapMirror]#
```

Configuración del clúster de origen para la recuperación ante desastres de Red Hat OpenShift Virtualization

En esta sección se ofrece información sobre cómo configurar el clúster de origen para la recuperación ante desastres de cargas de trabajo de virtualización de OpenShift utilizando NetApp Trident Protect y AppMirror. Esto incluye la creación de un AppVault utilizando ONTAP S3, la creación de una aplicación de Trident Protect para la VM de origen y la creación de instantáneas bajo demanda y programadas de la VM mediante Trident Protect. Estos pasos son esenciales para garantizar que el clúster de origen esté correctamente configurado para replicar los datos al clúster de destino de recuperación ante desastres y permitir la recuperación de las VMs en caso de desastre.

Configura el clúster de origen para la recuperación ante desastres en la virtualización de OpenShift

Todos los pasos siguientes se llevan a cabo en el clúster de origen, que es el clúster donde la máquina virtual protegida se está ejecutando actualmente.

Crea AppVault usando ONTAP S3

Esta sección muestra cómo configurar un objeto AppVault en Trident Protect usando almacenamiento de objetos ONTAP S3. El AppVault creado en este paso se usará para almacenar los datos replicados desde el clúster de origen, y esos datos se usarán para la recuperación en el clúster de destino de recuperación ante desastres.

Utiliza los comandos oc y los archivos yaml que se muestran a continuación para crear un secreto y el recurso personalizado AppVault para ONTAP s3. Asegúrate de crearlos en el espacio de nombres trident-protect.

Mostrar ejemplo

```
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
```

Asegúrate de que el almacén S3 de ONTAP está creado y en estado Disponible

```
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
```

Crear una aplicación Trident Protect para la máquina virtual de origen

Crea un recurso personalizado de tipo Application en el espacio de nombres donde se encuentra la máquina virtual de origen.

Mostrar ejemplo

```
# 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
```

A continuación se muestra la máquina virtual y su PVC en el espacio de nombres incluido en el recurso personalizado de la App.

```
[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  3414499000  RWX           sc-nas        <unset>                 25h
```

Crea una instantánea de la máquina virtual con Trident Protect

Puedes crear una instantánea bajo demanda de la máquina virtual usando la CLI o la API de Trident Protect. Esta instantánea se almacenará en el AppVault creado en el paso anterior y puede usarse para la recuperación en el clúster de destino de recuperación ante desastres.

Mostrar ejemplo

```
# 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

Crea una instantánea programada de la máquina virtual con Trident Protect

También puedes crear una instantánea programada creando un recurso personalizado Schedule en el mismo espacio de nombres que el recurso personalizado Application. La programación creará automáticamente instantáneas de la máquina virtual según la programación especificada y las almacenará en el AppVault.

Mostrar ejemplo

```
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"
```

Configuración del clúster de destino para la recuperación ante desastres de Red Hat OpenShift Virtualization

En esta sección se ofrece información sobre cómo configurar el clúster de destino para la recuperación ante desastres de cargas de trabajo de virtualización de OpenShift utilizando NetApp Trident Protect y AppMirror. Esto incluye la creación de un AppVault mediante ONTAP S3 y la creación de un nuevo espacio de nombres para la máquina virtual de destino. Estos pasos son esenciales para garantizar que el clúster de destino esté correctamente configurado para recibir los datos replicados desde el clúster de origen y permitir la recuperación de las máquinas virtuales en caso de desastre.

1. Crea un objeto AppVault en el clúster de destino. Este debe apuntar al mismo S3 que el clúster de origen, para que pueda obtener la instantánea del S3 donde el clúster de origen la colocó.

Mostrar ejemplo

```
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. Crea un nuevo espacio de nombres en el clúster de destino para alojar la máquina virtual con conmutación por error. Crea una App en el clúster de destino que haga referencia al AppVault creado en el paso 1 y al nuevo espacio de nombres. Esta App se usará para establecer la relación AppMirror entre el clúster de origen y el clúster de destino, y para gestionar la replicación de datos desde el clúster de origen al clúster de destino.

Mostrar ejemplo

```
# 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>
```

Conmutación por error de una máquina virtual en OpenShift Virtualization Disaster Recovery

En esta sección se describe cómo realizar una conmutación por error de una máquina virtual desde un clúster de origen a un clúster de destino de recuperación ante desastres usando NetApp Trident Protect y AppMirror. Esto es útil para probar el proceso de conmutación por error y para realizar mantenimiento planificado en el clúster de origen. Si sigues estos pasos, puedes asegurarte de que tu máquina virtual esté funcionando en el clúster de destino de recuperación ante desastres con todos los cambios intactos después de un evento de recuperación ante desastres.

Conmutación por error sin fallo energético en el sitio para OpenShift Virtualization

En esta sección se describe cómo realizar una conmutación por error de una máquina virtual desde un clúster de origen sin que se produzca un fallo energético en el sitio. Esto resulta útil para probar el proceso de conmutación por error y para llevar a cabo tareas de mantenimiento planificadas en el clúster de origen. +

Para realizar una conmutación por error sin que se produzca un fallo energético en el sitio, primero asegúrate de que el clúster de origen y el clúster de destino estén configurados para la recuperación ante desastres como se describe en las secciones anteriores. Luego, realiza los siguientes pasos:

1. Establece la relación AppMirror entre el clúster de origen y el clúster de destino. Cuando se establece la relación AppMirror, la instantánea más reciente se transfiere al espacio de nombres de destino. El PVC se crea para la VM en el espacio de nombres de destino, pero el pod de la VM aún no se ha creado en el espacio de nombres de destino.

Mostrar ejemplo

```
# 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



La relación AppMirror debe crearse desde la cli del clúster de destino. Debe crearse con el estado deseado como Established. Esto asegurará que los datos de la instantánea más reciente se reproduzcan en el clúster de destino.

2. Promociona la relación AppMirror. Cambia el estado deseado de la relación a "Promocionada" para crear la máquina virtual en el espacio de nombres de destino. La máquina virtual sigue ejecutándose en el espacio de nombres de origen. Los datos de la instantánea más reciente se replican al clúster de destino y la máquina virtual se inicia en el clúster de destino. Este método te permite probar la conmutación por error y mantener la disponibilidad de la máquina virtual sin tener que detener todo el clúster de origen.

Mostrar ejemplo

```
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
```

Reversión de una máquina virtual en la recuperación ante desastres de OpenShift Virtualization

Esta sección ofrece información sobre el proceso de reversión (failback) de una VM en OpenShift Virtualization disaster recovery usando NetApp Trident Protect y AppMirror. Después de realizar una operación de conmutación por error para cambiar a un clúster de destino de recuperación ante desastres, puedes usar el proceso de reversión para invertir la dirección de la replicación y restaurar el clúster de origen original como el clúster principal para la VM. Esto implica resincronizar cualquier cambio hecho en la VM durante el periodo de conmutación por error de vuelta al clúster de origen original y luego promover la relación de replicación en la dirección inversa. Siguiendo estos pasos, puedes asegurarte de que tu VM esté ejecutándose en el clúster de origen original con todos los cambios intactos después de un evento de recuperación ante desastres.

Recuperación tras un fallo para OpenShift Virtualization Disaster Recovery

Con Trident Protect, puedes lograr la "recuperación" después de una operación de conmutación por error usando la siguiente secuencia de operaciones. En este flujo de trabajo para restaurar la dirección de replicación original, Trident Protect replica (resincroniza) cualquier cambio de la aplicación de vuelta a la aplicación de origen original antes de invertir la dirección de replicación.

Este proceso parte de una relación que ha completado una conmutación por error a un destino e implica los siguientes pasos:

1. Empieza con un estado conmutado por error.
2. Volver a sincronizar la relación de replicación

Cuando haces una resincronización inversa de una relación de replicación fallida, la aplicación de destino se convierte en la aplicación de origen y la de origen en la de destino. Los cambios hechos en la aplicación de destino durante el failover se mantienen.

- a. En el clúster de destino original, elimina el CR AppMirrorRelationship. Esto hace que el destino se convierta en el origen. Si quedan programas de protección en el nuevo clúster de destino, elimínalos.

Mostrar ejemplo

```
[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. Crea una instantánea en el nuevo clúster de origen (destino original) para capturar cualquier cambio realizado durante el periodo de conmutación por error. Esto garantiza que todos los cambios se reproduzcan de nuevo en el clúster de origen original durante el proceso de resincronización.

Mostrar ejemplo

```
# 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. Configura una relación de replicación desde el nuevo clúster de origen (destino original) hacia el clúster de origen original, configurando los valores para la dirección inversa.

Mostrar ejemplo

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. Promociona la relación de replicación desde el nuevo clúster de origen (clúster de destino original) al clúster de origen original actualizando el campo desiredState en el CR de AppMirrorRelationship a "Promoted".

Mostrar ejemplo

```
[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
```

Ahora verás la máquina virtual en ejecución en el clúster de origen original. El proceso de recuperación tras fallo ya ha finalizado. Ahora puedes limpiar los recursos en el clúster de destino original. También puedes configurar una nueva relación de replicación si quieres mantener las capacidades de recuperación ante desastres después del proceso de recuperación tras fallo.



No realices una operación de resincronización normal, ya que esto descartará los datos escritos en el clúster de destino durante el procedimiento de conmutación por error.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.