



灾难恢复

NetApp virtualization solutions

NetApp
July 21, 2026

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

目录

灾难恢复	1
Trident Protect/AppMirror 针对 OpenShift 虚拟化灾难恢复的先决条件	1
前提条件	1
安装 NetApp Trident Protect 以用于 OpenShift 虚拟化	1
Red Hat OpenShift 虚拟化灾难恢复的源集群设置	2
设置 OpenShift Virtualization 的灾难恢复源集群	2
使用 ONTAP S3 创建 AppVault	2
为源虚拟机创建 Trident Protect 应用程序	4
使用 Trident Protect 创建虚拟机快照	4
使用 Trident Protect 创建虚拟机的计划快照	5
Red Hat OpenShift 虚拟化灾难恢复的目标集群设置	5
OpenShift 虚拟化灾难恢复中虚拟机的故障转移	8
OpenShift 虚拟化的无站点中断故障切换	8
OpenShift 虚拟化灾难恢复中虚拟机的故障恢复	10
OpenShift 虚拟化灾难恢复的故障恢复	10

灾难恢复

Trident Protect/AppMirror 针对 OpenShift 虚拟化灾难恢复的先决条件

本节提供有关使用 NetApp Trident Protect 和 AppMirror 对 OpenShift 虚拟化工作负载进行灾难恢复的先决条件的信息。这包括设置 Trident Protect 和 AppMirror 以对在 OpenShift 虚拟化上运行的虚拟机进行有效灾难恢复所需的集群配置、存储要求和安装步骤。

前提条件

1. 已安装并配置 OpenShift Virtualization 的 Red Hat OpenShift 集群。有关安装说明，请参见 ["此处文档"](#)。
2. 两个各自配置了 SVM 的 NetApp ONTAP 存储系统，为活动和灾难恢复 OpenShift 集群提供存储。每个 SVM 必须至少配置一个管理 LIF 和一个数据 LIF，并可从相应的 OpenShift 集群访问。
3. 在两个 ONTAP 系统之间配置集群对等和 SVM 对等，以允许将数据从源集群的 SVM 复制到目标集群的 SVM。有关如何设置集群对等和 SVM 对等的说明，请参见["此处为 ONTAP 集群对等关系文档"](#)。
4. NetApp Trident 已在 OpenShift 集群上安装并配置，以从 ONTAP SVM 提供永久性存储。有关安装说明，请参见 ["Trident 文档"](#)。
5. 为 ONTAP SVM 创建了 Trident 后端配置，并在 OpenShift 集群上配置了 StorageClass，以将该 Trident 后端用作置备程序。有关如何创建 Trident 后端配置和 StorageClass 的说明，请参见 ["此处为 Trident 后端配置文档"](#)。
6. 对 OpenShift 集群的 Cluster-admin 访问权限和对 ONTAP 存储系统的管理员访问权限，以执行必要的配置。
7. 已安装 `tridentctl` 和 `oc` 工具并将其添加到 `$PATH` 环境变量中的管理工作站，用于与 OpenShift 集群和 Trident 交互。
8. OpenShift 集群上有足够的硬件资源来支持 OpenShift Virtualization operator 和将要预配的虚拟机。有关资源要求的详细信息，请参见 ["此处文档"](#)。
9. （可选）为 OpenShift 虚拟化配置节点放置规则，以指定集群节点的子集来托管 OpenShift 虚拟化操作员、控制器和虚拟机。有关如何配置节点放置规则的说明，请参见 ["此处文档"](#)。
10. 对于支持 OpenShift 虚拟化的存储，建议使用专用的 StorageClass，从特定 Trident 后端请求存储，而该后端又由专用 SVM 提供支持。这在 OpenShift 集群上为基于虚拟机的工作负载提供数据方面保持了一定程度的多租户隔离。
11. OpenShift Virtualization 中必须有一个可用的 VM。有关部署新 VM 或将现有 VM 迁移到 OpenShift Virtualization 的详细信息，请参阅文档中的相应部分。

安装 NetApp Trident Protect 以用于 OpenShift 虚拟化

要使用 NetApp Trident Protect 为 OpenShift Virtualization 工作负载启用灾难恢复功能，您必须在 OpenShift 集群上安装并配置 Trident Protect。可以使用 Helm chart 安装 Trident Protect。



Trident Protect 的安装必须在安装 Trident 之后完成。

有关完整的安装说明，请参见 ["Trident Protect 文档位于此处"](#)。

```
[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]#
```

Red Hat OpenShift 虚拟化灾难恢复的源集群设置

本节提供有关使用 NetApp Trident Protect 和 AppMirror 设置源集群以对 OpenShift Virtualization 工作负载进行灾难恢复的信息。这包括使用 ONTAP S3 创建 AppVault，为源虚拟机创建 Trident Protect 应用程序，以及使用 Trident Protect 创建该虚拟机的按需和计划快照。这些步骤对于确保正确配置源集群以将数据复制到灾难恢复目标集群并在发生灾难时恢复虚拟机至关重要。

设置 OpenShift Virtualization 的灾难恢复源集群

以下所有步骤均在源集群上执行，该集群是受保护虚拟机当前正在运行的集群。

使用 ONTAP S3 创建 AppVault

本节展示如何使用 ONTAP S3 对象存储在 Trident Protect 中设置 AppVault 对象。在此步骤中创建的 AppVault 将用于存储来自源集群的复制数据，该数据将用于在灾难恢复目标集群中进行恢复。

使用 oc 命令和下面显示的 yaml 文件为 ONTAP s3 创建密钥和 AppVault 自定义资源。请确保在 trident-protect 命名空间中创建它们。

显示示例

```
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
```

确保 ONTAP S3 保管库已创建且处于"可用"状态

```
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
```

为源虚拟机创建 **Trident Protect** 应用程序

在源 VM 所在的命名空间中创建应用程序自定义资源。

显示示例

```
# 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
```

App自定义资源中包含的命名空间中的VM及其PVC如下所示。

```
[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
```

使用 **Trident Protect** 创建虚拟机快照

您可以使用 Trident Protect CLI 或 API 创建虚拟机的按需快照。此快照将存储在上一步中创建的 AppVault 中，可用于灾难恢复目标集群中的恢复。

显示示例

```
# 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

使用 Trident Protect 创建虚拟机的计划快照

您也可以通过在与 Application 自定义资源相同的命名空间中创建 Schedule 自定义资源来创建计划快照。该计划将按照指定的计划自动创建虚拟机的快照，并将其存储在 AppVault 中。

显示示例

```
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 虚拟化灾难恢复的目标集群设置

本节提供有关使用 NetApp Trident Protect 和 AppMirror 设置用于 OpenShift Virtualization

工作负载灾难恢复的目标集群的信息。这包括使用 ONTAP S3 创建 AppVault，以及为目标 VM 创建新的命名空间。这些步骤对于确保正确配置目标集群以接收来自源集群的复制数据，并在发生灾难时实现 VM 的恢复至关重要。

1. 在目标集群中创建 AppVault 对象。此对象应指向与源相同的 S3，以便从源集群存放快照的 S3 中获取快照。

显示示例

```
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. 在目标集群上创建新的命名空间以托管故障转移 VM。在目标集群中创建一个应用程序，该应用程序引用在步骤 1 中创建的 AppVault 以及新命名空间。此应用程序将用于建立源集群和目标集群之间的 AppMirror 关系，并管理从源集群到目标集群的数据复制。

显示示例

```
# 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 虚拟化灾难恢复中虚拟机的故障转移

本节介绍如何使用 NetApp Trident Protect 和 AppMirror 将虚拟机从源集群故障转移到灾难恢复目标集群。这对于测试故障转移过程以及对源集群执行计划内维护非常有用。通过执行这些步骤，您可以确保虚拟机在灾难恢复事件发生后在灾难恢复目标集群上运行，且所有更改均完好无损。

OpenShift 虚拟化的无站点中断故障切换

本节介绍如何在没有站点中断的情况下从源集群执行 VM 故障转移。这对于测试故障转移过程以及对源集群执行计划内维护非常有用。+

要执行没有站点中断的故障转移，首先确保源和目标集群已设置为灾难恢复，如前面几节所述。然后，执行以下步骤：

1. 建立源集群和目标集群之间的 AppMirror 关系。建立 AppMirror 关系后，最新的快照将传输到目标命名空间。系统会在目标命名空间中为 VM 创建 PVC，但尚未在目标命名空间中创建 VM Pod。

显示示例

```
# 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 关系应从目标集群的 cli 创建。应将其创建为所需状态“已建立”。这将确保最新的快照数据复制到目标集群。

2. 提升 AppMirror 关系。将此关系的所需状态更改为“Promoted”，以在目标命名空间中创建虚拟机。此虚拟机仍在源命名空间中运行。将最新的快照数据复制到目标集群，并在目标集群上启动虚拟机。此方法允许您测试故障转移并维护虚拟机可用性，而无需关闭整个源集群。

显示示例

```
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 虚拟化灾难恢复中虚拟机的故障恢复

本节提供有关在使用 NetApp Trident Protect 和 AppMirror 的 OpenShift Virtualization 灾难恢复中 VM 故障回切过程的信息。在执行故障转移操作以切换到灾难恢复目标集群后，您可以使用故障回切过程来反转复制方向，并将原始源集群恢复为 VM 的主集群。这涉及将故障转移期间对 VM 进行的任何更改重新同步回原始源集群，然后反向提升复制关系。通过遵循这些步骤，您可以确保在发生灾难恢复事件后，您的 VM 能够在原始源集群上运行，且所有更改均保持完好。

OpenShift 虚拟化灾难恢复的故障恢复

使用 Trident Protect，您可以使用以下操作序列在故障转移操作后实现“回切”。在此工作流程中，为了还原原始复制方向，Trident Protect 会在反转复制方向之前将任何应用程序更改复制（重新同步）回原始源应用程序。

此过程从已完成故障转移到目标的关系开始，涉及以下步骤：

1. 从故障转移状态开始。
2. 反向重新同步复制关系

当您反向重新同步故障转移复制关系时，目标应用程序将成为源应用程序，而源应用程序将成为目标。在故障转移期间对目标应用程序所做的更改将被保留。

- a. 在原始目标集群上，删除 AppMirrorRelationship CR。这会导致目标成为源。如果新目标集群上还有任何保护计划，请将其删除。

显示示例

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

- b. 在新的源集群（初始目标）上创建快照，以捕获故障转移期间所做的任何更改。这可确保在重新同步过程中将所有更改复制回初始源集群。

显示示例

```
# 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. 设置从新源集群（初始目标）到初始源集群的复制关系，为反向方向配置相应值。

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. 通过将 AppMirrorRelationship CR 中的 desiredState 字段更新为 "Promoted", 将复制关系从新源集群 (原始目标) 提升至原始源集群。

显示示例

```
[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
```

您现在将看到虚拟机在原始源集群中运行。故障恢复过程现已完成。您现在可以清理原始目标集群中的资源。如果要在故障恢复过程后保持灾难恢复功能，还可以设置新的复制关系。



请勿执行正常的重新同步操作，因为这将丢弃在故障转移过程中写入目标集群的数据。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。