



災難復原 NetApp virtualization solutions

NetApp
July 21, 2026

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

目錄

災難復原	1
Trident Protect/AppMirror 適用於 OpenShift 虛擬化災難復原的先決條件	1
先決條件	1
安裝 NetApp Trident Protect for OpenShift Virtualization	1
Red Hat OpenShift 虛擬化災難復原的來源叢集設定	2
為 OpenShift 虛擬化設定災難復原來源叢集	2
使用 ONTAP S3 建立 AppVault	2
為來源虛擬機器建立 Trident Protect 應用程式	4
使用 Trident Protect 建立虛擬機器快照	4
使用 Trident Protect 建立虛擬機器的排程快照	5
Red Hat OpenShift 虛擬化災難復原的目標叢集設定	5
OpenShift 虛擬化災難復原中的 VM 故障移轉	8
OpenShift 虛擬化無站台中斷的容錯移轉	8
OpenShift 虛擬化災難復原中的虛擬機器故障回復	10
OpenShift 虛擬化災難復原的容錯回復	10

災難復原

Trident Protect/AppMirror 適用於 OpenShift 虛擬化災難復原的先決條件

本節提供有關使用 NetApp Trident Protect 以及 AppMirror 對 OpenShift 虛擬化工作負載進行災難復原的先決條件的資訊。這包括必要的叢集組態、儲存需求，以及設定 Trident Protect 和 AppMirror 以有效災難復原在 OpenShift 虛擬化環境中執行的虛擬機器所需的安裝步驟。

先決條件

1. 已安裝並設定 OpenShift Virtualization 的 Red Hat OpenShift 叢集。如需安裝說明，請參閱 ["文件在此處"](#)。
2. 兩台 NetApp ONTAP 儲存系統，每台系統上都配置了一個 SVM，用於為作用中叢集和災難復原 OpenShift 叢集提供儲存。每個 SVM 必須至少配置一個管理 LIF 和一個資料 LIF，並且這些 LIF 必須能夠從對應的 OpenShift 叢集存取。
3. 在兩個 ONTAP 系統之間設定叢集對等連接和 SVM 對等連接，以允許將資料從來源叢集的 SVM 複製到目標叢集的 SVM。有關如何設定叢集對等連線和 SVM 對等連線的說明，請參閱 ["ONTAP 叢集對等互連文件在此處"](#)。
4. NetApp Trident 已安裝並設定於 OpenShift 叢集上，用於從 ONTAP SVM 佈建持續性儲存。如需安裝說明，請參閱 ["Trident 文件在此"](#)。
5. 已為 ONTAP SVM 建立 Trident 後端組態，且已在 OpenShift 叢集上設定 StorageClass 以使用該 Trident 後端作為資源配置程式。如需有關如何建立 Trident 後端組態與 StorageClass 的說明，請參閱 ["Trident 後端設定文件在此處"](#)。
6. 叢集管理員對 OpenShift 叢集的存取權限，以及對 ONTAP 儲存系統的管理員存取權限，以執行必要的組態設定。
7. 管理員工作站已安裝 `tridentctl` 和 `oc` 工具，並已新增至 `$PATH` 環境變數，以便與 OpenShift 叢集和 Trident 互動。
8. OpenShift 叢集上需要有足夠的硬體資源來支援 OpenShift Virtualization operator 和將要佈建的虛擬機器。有關資源需求的詳細資訊，請參閱 ["文件在此處"](#)。
9. （選用）配置 OpenShift 虛擬化節點放置規則，以指定叢集節點的子集來託管 OpenShift 虛擬化操作員、控制器和虛擬機器。有關如何配置節點放置規則的說明，請參閱 ["文件在此處"](#)。
10. 對於支援 OpenShift 虛擬化的儲存後端，建議使用專用的 StorageClass，從特定的 Trident 後端請求儲存，而該後端又由專用的 SVM 提供支援。這樣可以確保 OpenShift 叢集上基於虛擬機器的工作負載所服務的資料維持一定程度的多租用戶特性。
11. OpenShift Virtualization 中必須有一個可用的 VM。有關部署新 VM 或將現有 VM 遷移到 OpenShift Virtualization 的詳細信息，請參閱文件中的相應部分。

安裝 NetApp Trident Protect for OpenShift Virtualization

若要使用 NetApp Trident Protect 啟用 OpenShift Virtualization 工作負載的災難復原功能，您必須在 OpenShift 叢集上安裝並設定 Trident Protect。Trident Protect 可以使用 Helm chart 進行安裝。



Trident Protect 的安裝必須在 Trident 安裝之後進行。

有關完整的安裝說明，請參閱["Trident Protect 文件在此處"](#)。

顯示範例

```
[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 虛擬化災難復原的來源叢集設定

本節提供關於使用 NetApp Trident Protect 和 AppMirror 設定來源叢集，以進行 OpenShift Virtualization 工作負載災難復原的資訊。這包括使用 ONTAP S3 建立 AppVault、為來源 VM 建立 Trident Protect 應用程式，以及使用 Trident Protect 建立 VM 的隨選和排程快照。這些步驟對於確保正確設定來源叢集以將資料複寫到災難復原目標叢集，並在發生災難時啟用 VM 復原至關重要。

為 OpenShift 虛擬化設定災難復原來源叢集

以下所有步驟均在來源叢集上執行，即受保護的虛擬機器目前運作所在的叢集。

使用 ONTAP S3 建立 AppVault

本節說明如何使用 ONTAP S3 物件儲存在 Trident Protect 中設定 AppVault 物件。此步驟建立的 AppVault 將用於儲存來自來源叢集的複寫資料，這些資料將用於災難復原目標叢集中的復原。

使用 oc 命令和下面顯示的 yaml 檔案，為 ONTAP s3 建立金鑰和 AppVault 自訂資源。確保在 trident-protect 命名空間中建立它們。

```

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

```

確保已建立 ONTAP S3 儲存庫並處於可用狀態

```
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
```

為來源虛擬機器建立 Trident Protect 應用程式

在來源虛擬機器所在的命名空間中建立應用程式自訂資源。

顯示範例

```
# 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
```

下面顯示了應用程式自訂資源中包含的命名空間中的虛擬機器及其 PVC。

```
[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 建立虛擬機器快照

您可以使用 Trident Protect CLI 或 API 按需建立虛擬機器快照。此快照將儲存在上一個步驟建立的 AppVault 中，並可用於災難復原目標叢集中的復原。

顯示範例

```
# 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 建立虛擬機器的排程快照

您也可以透過在與 Application 自訂資源相同的命名空間中建立 Schedule 自訂資源來建立排程快照。該排程將按照指定的排程自動建立虛擬機器的快照，並將其儲存在 AppVault 中。

顯示範例

```
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 虛擬化災難復原的目標叢集設定

本節提供關於使用 NetApp Trident Protect 和 AppMirror 設定用於 OpenShift Virtualization

工作負載災難復原之目標叢集的資訊。這包括使用 ONTAP S3 建立 AppVault，以及為目的地 VM 建立新的命名空間。這些步驟對於確保正確設定目的地叢集以接收來自來源叢集的複寫資料，並在發生災難時啟用 VM 復原至關重要。

1. 在目標叢集中建立 AppVault 物件。此物件應指向與來源叢集相同的 S3，以便從來源叢集存放快照的 S3 中取得快照。


```

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. 在目標叢集上建立一個新的命名空間，用於託管故障轉移的虛擬機器。在目標叢集中建立一個應用程式，該應用程式引用步驟 1 中建立的 AppVault 和新命名空間。此應用程式將用於建立來源叢集和目標叢集之間的 AppMirror 關係，並管理從來源叢集到目標叢集的資料複製。

顯示範例

```
# 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 虛擬化災難復原中的 VM 故障移轉

本節介紹如何使用 NetApp Trident Protect 和 AppMirror 將虛擬機器從來源叢集故障轉移到災難復原目標叢集。這有助於測試故障轉移程序，以及對來源叢集執行計劃性維護。按照這些步驟操作，您可以確保在災難復原事件發生後，虛擬機器在災難復原目標叢集上正常運行，並且所有變更都完好無損。

OpenShift 虛擬化無站台中斷的容錯移轉

本節介紹如何在不中斷網站服務的情況下，將虛擬機器從來源叢集進行故障轉移。這對於測試故障轉移程序以及對來源叢集執行計劃內維護非常有用。+

若要在不中斷站台服務的情況下執行容錯移轉，首先要確保來源叢集和目標叢集已依照前幾節所述設定災難恢復。然後，執行以下步驟：

1. 建立來源叢集與目標叢集之間的 AppMirror 關係。AppMirror 關係建立後，最新快照將傳輸至目標命名空間。目標命名空間中的 VM 已建立 PVC，但 VM Pod 尚未在目標命名空間中建立。

顯示範例

```
# 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
```



應從目標叢集的 CLI 建立 AppMirror 關係。應以「已建立」作為所需狀態來建立此關係。這將確保最新的快照資料複製到目標叢集。

2. 提升 AppMirror 關係。將關係的期望狀態變更為「已提升」，即可在目標命名空間中建立虛擬機器。虛擬機器仍在來源命名空間中運作。最新的快照資料將複製到目標叢集，虛擬機器將在目標叢集上啟動。此方法可讓您測試容錯移轉並保持虛擬機器可用性，而無需關閉整個來源叢集。

顯示範例

```
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 虛擬化災難復原中的虛擬機器故障回復

本節提供有關使用 NetApp Trident Protect 和 AppMirror 在 OpenShift Virtualization 災害復原中進行 VM 容錯回復程序的資訊。在執行容錯移轉作業以切換至災害復原目標叢集之後，您可以使用容錯回復程序來反轉複寫方向，並將原始來源叢集還原為 VM 的主要叢集。這包括將容錯移轉期間對 VM 所做的任何變更重新同步回原始來源叢集，然後反向提升複寫關係。透過遵循這些步驟，您可以確保在發生災害復原事件之後，您的 VM 能夠在原始來源叢集上執行，且所有變更均保持完整。

OpenShift 虛擬化災難復原的容錯回復

使用 Trident Protect，您可以透過以下步驟在故障轉移作業後實現「故障復原」。在此工作流程中，為了恢復原始複寫方向，Trident Protect 會在反轉複寫方向之前，將所有應用程式變更複寫（重新同步）回原始來源應用程式。

此程序從已完成容錯移轉至目的地的關係開始，並涉及下列步驟：

1. 從故障轉移狀態開始。
2. 反向重新同步複製關係

當您對故障轉移的複製關係進行反向同步時，目標應用程式將變為來源應用程式，而來源應用程式將變為目標應用程式。故障轉移期間對目標應用程式所做的變更將被保留。

- a. 在原始目標叢集上，刪除 AppMirrorRelationship CR。這將使目標叢集變為來源叢集。如果新目標叢集上仍有任何保護排程，請將其刪除。

顯示範例

```
[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. 在新來源叢集（原目標叢集）上建立快照，以擷取故障轉移期間所做的任何變更。這可確保在重新同步過程中，所有變更都會複製回原始來源叢集。

顯示範例

```
# 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. 從新來源叢集（原始目標）到原始來源叢集建立複寫關係，並設定反向的值。

```
# 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. 透過將 AppMirrorRelationship CR 中的 desiredState 欄位更新為 "Promoted"，將複寫關係從新來源叢集（原始目的地）提升至原始來源叢集。

顯示範例

```
[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
```

現在您將看到虛擬機器在原始來源叢集中運作。故障回復程序現已完成。您現在可以清理原始目標叢集中的資源。如果您希望在故障回復程序後保持災難復原能力，也可以設定新的複寫關係。



不要執行正常的重新同步作業，因為這會捨棄在容錯移轉程序期間寫入目的地叢集的資料。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。