



Recuperação de desastres

NetApp virtualization solutions

NetApp
July 14, 2026

Índice

Recuperação de desastres	1
Pré-requisitos do Trident Protect/AppMirror para recuperação de desastres em OpenShift Virtualization ...	1
Pré-requisitos	1
Instale NetApp Trident Protect para OpenShift Virtualização	2
Configuração do cluster de origem para recuperação de desastres do Red Hat OpenShift Virtualization ...	2
Configurar cluster de origem de recuperação de desastres para OpenShift Virtualization	2
Criar AppVault usando ONTAP S3	3
Crie um aplicativo Trident Protect para a VM de origem	5
Crie um Snapshot da VM usando Trident Protect	5
Crie um snapshot agendado da VM usando Trident Protect	6
Configuração de cluster de destino para Red Hat OpenShift Virtualization recuperação de desastres	7
Failover de uma máquina virtual em OpenShift Virtualization Disaster Recovery	9
Failover sem falha no local para OpenShift Virtualization	10
Failback de uma máquina virtual em OpenShift Virtualization Disaster Recovery	12
Failback para recuperação de desastres de virtualização do OpenShift	12

Recuperação de desastres

Pré-requisitos do Trident Protect/AppMirror para recuperação de desastres em OpenShift Virtualization

Esta seção fornece informações sobre os pré-requisitos para usar NetApp Trident Protect e AppMirror para a recuperação de desastres de cargas de trabalho de virtualização do OpenShift. Isso inclui as configurações de cluster necessárias, os requisitos de storage e as etapas de instalação para configurar o Trident Protect e o AppMirror para uma recuperação eficaz de desastres de máquinas virtuais em execução na virtualização do OpenShift.

Pré-requisitos

1. Um cluster Red Hat OpenShift com OpenShift Virtualization instalado e configurado. Para obter instruções de instalação, consulte o ["documentação aqui"](#).
2. Dois sistemas de storage NetApp ONTAP com um SVM configurado em cada um, para fornecer storage para os clusters OpenShift ativo e de recuperação de desastres. Cada SVM deve ter pelo menos uma LIF de gerenciamento e uma LIF de dados configuradas e acessíveis a partir do cluster OpenShift correspondente.
3. O emparelhamento de clusters e o emparelhamento de SVMs configurados entre os dois sistemas ONTAP para permitir a replicação de dados do SVM do cluster de origem para o SVM do cluster de destino. Para obter instruções sobre como configurar o emparelhamento de clusters e o emparelhamento de SVMs, consulte o ["Documentação sobre peering de clusters ONTAP aqui"](#).
4. NetApp Trident instalado e configurado no cluster OpenShift para provisionar storage persistente a partir do ONTAP SVM. Para instruções de instalação, consulte o ["Documentação do Trident aqui"](#).
5. Configuração de backend Trident criada para a ONTAP SVM e uma StorageClass configurada no cluster OpenShift para usar esse backend Trident como provisionador. Para instruções sobre como criar uma configuração de backend Trident e StorageClass, consulte o ["Documentação de configuração do backend Trident aqui"](#).
6. Acesso de administrador do cluster ao cluster OpenShift e acesso de administrador ao sistema de storage ONTAP para realizar as configurações necessárias.
7. Uma estação de trabalho administrativa com `tridentctl` e `oc` ferramentas instaladas e adicionadas à variável de ambiente `$PATH` para interagir com o cluster OpenShift e Trident.
8. Recursos de hardware adequados no cluster OpenShift para suportar o operador OpenShift Virtualization e as VMs que serão provisionadas. Para obter mais detalhes sobre os requisitos de recursos, consulte a ["documentação aqui"](#).
9. Opcionalmente, configure regras de posicionamento de nós para OpenShift Virtualization para especificar um subconjunto de nós do cluster para hospedar os operadores, controladores e máquinas virtuais do OpenShift Virtualization. Para obter instruções sobre como configurar regras de posicionamento de nós, consulte o ["documentação aqui"](#).
10. Para o storage que dá suporte à OpenShift Virtualization, é recomendado ter uma StorageClass dedicada que solicite storage de um backend Trident específico, que por sua vez é suportado por uma SVM dedicada. Isso mantém um nível de multitenancy em relação aos dados fornecidos para cargas de trabalho baseadas em máquinas virtuais no cluster OpenShift.
11. Uma VM deve estar disponível no OpenShift Virtualization. Para obter detalhes sobre como implantar uma

nova VM ou migrar uma VM existente para o OpenShift Virtualization, consulte a seção apropriada na documentação.

Instale NetApp Trident Protect para OpenShift Virtualização

Para habilitar os recursos de recuperação de desastres para cargas de trabalho de virtualização do OpenShift usando o NetApp Trident Protect, você precisa ter o Trident Protect instalado e configurado no cluster OpenShift. O Trident Protect pode ser instalado usando um Helm chart.



A instalação do Trident Protect deve ser feita após a instalação do Trident.

Para obter instruções completas de instalação, consulte o "[Documentação do Trident Protect aqui](#)".

Mostrar exemplo

```
[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]#
```

Configuração do cluster de origem para recuperação de desastres do Red Hat OpenShift Virtualization

Esta seção fornece informações sobre como configurar o cluster de origem para recuperação de desastres de cargas de trabalho de virtualização do OpenShift usando NetApp Trident Protect e AppMirror. Isso inclui criar um AppVault usando ONTAP S3, criar um aplicativo Trident Protect para a VM de origem e criar snapshots sob demanda e agendados da VM usando Trident Protect. Essas etapas são essenciais para garantir que o cluster de origem esteja configurado corretamente para replicar dados para o cluster de destino de recuperação de desastres e permitir a recuperação de VMs em caso de desastre.

Configurar cluster de origem de recuperação de desastres para OpenShift Virtualization

Todas as etapas a seguir são executadas no cluster de origem, que é o cluster onde a VM protegida está em execução no momento.

Criar AppVault usando ONTAP S3

Esta seção mostra como configurar um objeto AppVault no Trident Protect usando o storage de objetos ONTAP S3. O AppVault criado nesta etapa será usado para armazenar dados replicados do cluster de origem, e esses dados serão usados para recuperação no cluster de destino de recuperação de desastres.

Utilize os comandos oc e os arquivos yaml mostrados abaixo para criar um segredo e o recurso personalizado AppVault para ONTAP s3. Certifique-se de criá-los no namespace trident-protect.

Mostrar exemplo

```
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
```

Certifique-se de que o cofre S3 do ONTAP foi criado e está no estado Disponível

```
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
```

Crie um aplicativo Trident Protect para a VM de origem

Crie um recurso personalizado de Application no namespace onde a VM de origem está localizada.

Mostrar exemplo

```
# 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 VM e seu PVC no namespace incluído no recurso personalizado do App são mostrados abaixo.

```
[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  34144990000  RWX          sc-nas        <unset>                 25h
```

Crie um Snapshot da VM usando Trident Protect

Você pode criar um snapshot sob demanda da VM usando o Trident Protect CLI ou API. Esse snapshot será armazenado no AppVault criado na etapa anterior e poderá ser usado para recuperação no cluster de destino de recuperação de desastres.

Mostrar exemplo

```
# 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

Crie um snapshot agendado da VM usando Trident Protect

Você também pode criar um snapshot agendado criando um recurso personalizado de Agendamento no mesmo namespace do recurso personalizado de Aplicativo. O agendamento criará automaticamente snapshots da máquina virtual no cronograma especificado e os armazenará no AppVault.

Mostrar exemplo

```
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"
```


Configuração de cluster de destino para Red Hat OpenShift Virtualization recuperação de desastres

Esta seção fornece informações sobre como configurar o cluster de destino para recuperação de desastres de cargas de trabalho de virtualização do OpenShift usando NetApp Trident Protect e AppMirror. Isso inclui a criação de um AppVault usando ONTAP S3 e a criação de um novo namespace para a máquina virtual de destino. Essas etapas são essenciais para garantir que o cluster de destino esteja configurado corretamente para receber dados replicados do cluster de origem e permitir a recuperação das máquinas virtuais em caso de desastre.

1. Crie um objeto AppVault no cluster de destino. Este objeto deve apontar para o mesmo S3 que o cluster de origem, para que possa obter o Snapshot do S3 onde o cluster de origem o armazenou.

Mostrar exemplo

```
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. Crie um novo namespace no cluster de destino para hospedar a máquina virtual que foi transferida após a falha. Crie um App no cluster de destino que faça referência ao AppVault criado na etapa 1 e ao novo namespace. Esse App será usado para estabelecer o relacionamento AppMirror entre o cluster de origem e o cluster de destino, e para gerenciar a replicação de dados do cluster de origem para o cluster de destino.

Mostrar exemplo

```
# 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>
```

Failover de uma máquina virtual em OpenShift Virtualization Disaster Recovery

Esta seção descreve como realizar um failover de uma máquina virtual (VM) de um cluster de origem para um cluster de destino de recuperação de desastres usando NetApp Trident Protect e AppMirror. Isso é útil para testar o processo de failover e para realizar manutenção planejada no cluster de origem. Seguindo estas etapas, você garante que sua VM estará em execução no cluster de destino de recuperação de desastres com todas as alterações intactas após um evento de recuperação de desastres.

Failover sem falha no local para OpenShift Virtualization

Esta seção descreve como realizar um failover de uma VM de um cluster de origem sem falha no local. Isso é útil para testar o processo de failover e para realizar manutenção planejada no cluster de origem. +

Para realizar um failover sem falha no local, primeiro certifique-se de que os clusters de origem e destino estejam configurados para recuperação de desastres, conforme descrito nas seções anteriores. Em seguida, execute as seguintes etapas:

1. Estabeleça a relação AppMirror entre o cluster de origem e o cluster de destino. Quando a relação AppMirror é estabelecida, o snapshot mais recente é transferido para o namespace de destino. O PVC é criado para a VM no namespace de destino, porém, o pod da VM ainda não é criado nesse namespace de destino.

Mostrar exemplo

```
# 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



O AppMirror relacionamento deve ser criado a partir da cli do cluster de destino. Ele deve ser criado com o estado desejado como Established. Isso garantirá que os dados do snapshot mais recente sejam replicados para o cluster de destino.

2. Promova o relacionamento AppMirror. Altere o estado desejado do relacionamento para "Promoted" para criar a máquina virtual no namespace de destino. A máquina virtual continua em execução no namespace de origem. Os dados do snapshot mais recente são replicados para o cluster de destino e a máquina virtual é iniciada no cluster de destino. Esse método permite que você teste o failover e mantenha a disponibilidade da máquina virtual sem precisar interromper todo o cluster de origem.

Mostrar exemplo

```
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
```

Failback de uma máquina virtual em OpenShift Virtualization Disaster Recovery

Esta seção fornece informações sobre o processo de failback para uma VM em OpenShift Virtualization recuperação de desastres usando NetApp Trident Protect e AppMirror. Após uma operação de failover para alternar para um cluster de destino de recuperação de desastres, você pode usar o processo de failback para reverter a direção da replicação e restaurar o cluster de origem como o cluster primário da VM. Isso envolve ressincronizar quaisquer alterações feitas na VM durante o período de failover de volta para o cluster de origem e, em seguida, promover o relacionamento de replicação na direção inversa. Seguindo essas etapas, você pode garantir que sua VM esteja em execução no cluster de origem com todas as alterações intactas após um evento de recuperação de desastres.

Failback para recuperação de desastres de virtualização do OpenShift

Com Trident Protect, você pode realizar o "fail back" após uma operação de failover seguindo a seguinte sequência de operações. Nesse fluxo de trabalho para restaurar a direção de replicação original, Trident Protect replica (ressincroniza) quaisquer alterações do aplicativo de volta para o aplicativo de origem original antes de reverter a direção da replicação.

Esse processo começa a partir de uma relação que concluiu um failover para um destino e envolve as seguintes etapas:

1. Comece com um estado de failover.
2. Reverter a resincronização do relacionamento de replicação

Ao reverter a resincronização de uma relação de replicação com falha, o aplicativo de destino torna-se o aplicativo de origem e a origem torna-se o destino. As alterações feitas no aplicativo de destino durante a falha são mantidas.

- a. No cluster de destino original, exclua o CR AppMirrorRelationship. Isso faz com que o destino se torne o cluster de origem. Se houver algum agendamento de proteção restante no novo cluster de destino, remova-os.

Mostrar exemplo

```
[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. Crie um Snapshot no novo cluster de origem (destino original) para capturar quaisquer alterações feitas durante o período de failover. Isso garante que todas as alterações sejam replicadas de volta para o cluster de origem durante o processo de ressincronização.

Mostrar exemplo

```
# 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. Configure uma relação de replicação do novo cluster de origem (antigo destino) para o cluster de origem original, configurando os valores para a direção inversa.

Mostrar exemplo

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. Promova a relação de replicação do novo cluster de origem (antigo destino) para o cluster de origem original, atualizando o campo desiredState no CR AppMirrorRelationship para "Promoted".

Mostrar exemplo

```
[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
```

Agora você verá a VM em execução no cluster de origem. O processo de failback está concluído. Agora você pode liberar os recursos no cluster de destino. Você também pode configurar um novo relacionamento de replicação se quiser manter a capacidade de recuperação de desastres após o processo de failback.



Não execute uma operação de ressincronização normal, pois isso descartará dados gravados no cluster de destino durante o procedimento de fail over.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.