



跨帐户和跨区域配置 Cloud Backup

NetApp
April 12, 2022

目录

- 跨帐户和跨区域配置 1
 - 在 AWS 中为多帐户访问配置备份 1
 - 在 Azure 中配置用于多帐户访问的备份 9

跨帐户和跨区域配置

这些主题介绍如何在使用不同的云提供商时为跨帐户配置配置 Cloud Backup 。

- ["在 AWS 中配置 Cloud Backup 以实现多帐户访问"](#)
- ["在 Azure 中配置 Cloud Backup 以实现多帐户访问"](#)

在 **AWS** 中为多帐户访问配置备份

通过 Cloud Backup ，您可以在与源 Cloud Volumes ONTAP 卷所在位置不同的 AWS 帐户中创建备份文件。这两个帐户都可以与 Cloud Manager Connector 所在的帐户不同。

只有在您使用时，才需要执行这些步骤 ["将 Cloud Volumes ONTAP 数据备份到 Amazon S3"](#)。

按照以下步骤以这种方式设置您的配置。

在帐户之间设置 **VPC** 对等关系

1. 登录到第二个帐户并创建对等连接：
 - a. 选择本地 VPC ：选择第二个帐户的 VPC 。
 - b. 选择其他 VPC ：输入第一个帐户的帐户 ID 。
 - c. 选择运行 Cloud Manager Connector 的区域。在此测试设置中，两个帐户都在同一区域运行。
 - d. VPC ID ：登录到第一个帐户并输入接收者 VPC ID 。这是 Cloud Manager Connector 的 VPC ID 。

aws Services ▾

Peering Connections > Create Peering Connection

Create Peering Connection

Peering connection name tag ⓘ

Select a local VPC to peer with

VPC (Requester)* ↕ ↻

CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	● associated	

Select another VPC to peer with

Account ☐ My account ☒ Another account

Account ID*

Region ☒ This region (us-east-1) ☐ Another Region

VPC ID (Accepter)*

此时将显示成功对话框。

Success

A VPC peering connection (pcx-049758069d9b7c140) has been requested.
The owner of **vpc-116d9174** must accept the peering connection.

Requester VPC owner	733004784675 (This account)	Accepter VPC owner	464262061435
Requester VPC ID	vpc-82f55afa	Accepter VPC ID	vpc-116d9174
Requester VPC Region	us-east-1	Accepter VPC Region	us-east-1
Requester VPC CIDRs	10.0.0.0/16	Accepter VPC CIDRs	-

对等连接的状态显示为待接受。

	Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
<input checked="" type="checkbox"/>	cbs-multi-ac...	pcx-049758069d9b7c140	● Pending Acceptance	vpc-82f55afa VP...	vpc-116d9174	10.0.0.0/16	-	733004784675	464262061435
<input type="checkbox"/>	cbs-multi-peer	pcx-05f2d310cb7f...	● Deleted	vpc-82f55afa VP...	vpc-116d9174	-	-	733004784675	464262061435
<input type="checkbox"/>	New_Peering	pcx-6d55ca04	● Active	vpc-b16c90d4 V...	vpc-fc2aa39a De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

2. 登录到第一个帐户并接受对等请求：

Create Peering Connection		Actions							

Accept VPC Peering Connection Request

×

Are you sure you want to accept this VPC peering connection request (pcx-049758069d9b7c140)?

Requester Account ID

733004784675

Requester VPC ID

vpc-82f55afa

Requester VPC Region

us-east-1

Requester VPC CIDR

10.0.0.0/16

Accepter Account ID

464262061435 (This account)

Accepter VPC ID

vpc-116d9174

Accepter VPC Region

us-east-1

Accepter VPC CIDR

-

Cancel

Yes, Accept

a. 单击 * 是 *。

Accept VPC Peering Connection Request

×

Your VPC Peering Connection has been established.

To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. [Learn more](#)

[Modify my route tables now](#)

Close

此时，此连接将显示为 "Active"。我们还添加了一个名称标记来标识名为 CBS-Multi-account 的对等连接。

<input type="checkbox"/>	Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
<input type="checkbox"/>		pcx-004715531514cb0d8	Active	vpc-0647747d M...	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435
<input type="checkbox"/>	estycvoconnect	pcx-0305041f9cc2dfbdb	Active	vpc-116d9174	vpc-445d4f21	172.31.0.0/16	10.129.0.0/20	464262061435	759995470648
<input checked="" type="checkbox"/>	cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
<input type="checkbox"/>	hill-vpc-peer-chen	pcx-0d0e5c7fc4360254d	Active	vpc-0d12df59528f...	vpc-824dc0e4 nf...	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435

a. 刷新第二个帐户中的对等连接，并注意状态将更改为 "Active"。

<input type="checkbox"/>	Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
<input checked="" type="checkbox"/>	cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa VP...	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
<input type="checkbox"/>	New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4 V...	vpc-fc2aa39a De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

向两个帐户中的路由表添加路由

1. 转至 VPC > 子网 > 路由表。

VPC > Subnets > subnet-4d315328

subnet-4d315328 / The Subnet created

Details

Subnet ID subnet-4d315328	State Available	VPC vpc-116d9174	IPv4 CIDR 172.31.64.0/20
Available IPv4 addresses 3587	IPv6 CIDR -	Availability Zone us-east-1a	Availability Zone ID use1-az1
Network border group us-east-1	Route table rtb-4da55528	Network ACL acl-c37384a6	Default subnet Yes
Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	Owner 464262061435	Subnet ARN arn:aws:ec2:us-east-1:464262061435:subnet/subnet-4d315328	

[Flow logs](#)
[Route table](#)
[Network ACL](#)
[Sharing](#)
[Tags](#)

2. 单击路由选项卡。

Route Table ID : rtb-4da55528 Add filter

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
rtb-4da55528	subnet-4d315328	-		Yes	vpc-116d9174	464262061435

Route Table: rtb-4da55528

[Summary](#)
[Routes](#)
[Subnet Associations](#)
[Edge Associations](#)
[Route Propagation](#)
[Tags](#)

[Edit routes](#)

View All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
pl-63a5400a	vpce-098587ed33c36408c	active	No

3. 单击 * 编辑路由 *。

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
10.20.30.0/24	pcx-0791b47f6f9a27d65	active	No
10.129.0.0/20	pcx-0305041f9cc2dfbdb	active	No

[Add route](#)

* Required

[Cancel](#)
[Save routes](#)

4. 单击 * 添加路由 *，然后从目标下拉列表中选择 * 对等连接 *，然后选择您创建的对等连接。

a. 在目标中，输入另一帐户的子网 CIDR。

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
10.20.30.0/24	pcx-0791b47f6f9a27d65	active	No
10.129.0.0/20	pcx-0305041f9cc2dfbdb	active	No
10.0.0.0/24	pcx-		No

Add route

* Required

pcx-05f2d310cb7f49843

pcx-004715531514cb0d8

pcx-049758069d9b7c140 cbs-multi-account

pcx-094f9fdb10a2045ea hill-peer-vadim-vpc

pcx-0791b47f6f9a27d65

pcx-0305041f9cc2dfbdb estycvoconnect

Cancel Save routes

b. 单击 * 保存路由 * ，此时将显示一个成功对话框。

Route Tables > Edit routes

Edit routes

✓ Routes successfully edited

Close

在 Cloud Manager 中添加第二个 AWS 帐户凭据

1. 添加第二个 AWS 帐户，例如 *Saran-XCP-Dev* 。

Credentials + Add Credentials

3 Credentials

aws Instance Profile	Credential Type: AWS Keys	aws Saran-XCP-Dev	Credential Type: AWS Keys
464262061435 AWS Account ID	CBS-5R-OCCMOCCM1620912870830... IAM Role	733004784675 AWS Account ID	AKIA2VKT5MQRZRAWW3HI AWS Access Key
aws-sub-a2 Subscription	2 Working Environments	aws-sub-a2 Subscription	0 Working Environments

2. 在发现 Cloud Volumes ONTAP 页面中，选择新添加的凭据。

Choose an AWS region and then select the working environment that you want to discover.

AWS Region

US East | N. Virginia

aws AWS Credentials

Credential Name

Saran-XCP-Dev | Account ID: 733004784675

Instance Profile | Account ID: 464262061435

To add new AWS credentials, go to the [Credentials settings](#).

Apply Cancel

- 选择要从第二个帐户发现的 Cloud Volumes ONTAP 系统。您也可以在第二个帐户中部署新的 Cloud Volumes ONTAP 系统。

Add an Existing Cloud Volumes ONTAP Region

↑ Previous Step This working environment will be created in Cloud Provider Account: **Saran-XCP-Dev** | Account ID: 733004784675 | [Switch Account](#)

Choose an AWS region and then select the working environment that you want to discover.

AWS Region

US East | N. Virginia

Cloud Volumes ONTAP instances found

Name	VPC Name	Availability Zone	Subnet Id	Cloud Formation Name	Cluster Address	Type
cbscv001	VPC-NAT	us-east-1f	subnet-68e8d464	cbscv001	10.0.0.80	Cloud Volumes ONTAP
testbyolliraz	VPC for VSA	us-east-1a	subnet-c1d99699	testbyolliraz	172.31.5.142	Cloud Volumes ONTAP
ldanAwsHa991001	VPC for VSA	us-east-1a	subnet-c1d99699	ldanAwsHa991001	172.31.5.234,172.31.5.110	HA Cloud Volumes ONTAP

Continue

现在，第二个帐户中的 Cloud Volumes ONTAP 系统将添加到在其他帐户中运行的 Cloud Manager 中。



在其他 **AWS** 帐户中启用备份

1. 在 Cloud Manager 中，为第一个帐户中运行的 Cloud Volumes ONTAP 系统启用备份，但选择第二个帐户作为创建备份文件的位置。



2. 然后，选择一个备份策略以及要备份的卷， Cloud Backup 将尝试在选定帐户中创建一个新存储分段。

但是，将存储分段添加到 Cloud Volumes ONTAP 系统将失败，因为 Cloud Backup 使用实例配置文件添加存储分段，而 Cloud Manager 实例配置文件无法访问第二个帐户中的资源。

3. 获取 Cloud Volumes ONTAP 系统的工作环境 ID 。



Cloud Backup 会创建前缀为 `netapp-backup-` 的每个存储分段，并包含工作环境 ID；例如：87ULeAI0

- 在 EC2 门户中，转到 S3 并搜索名称以 87uLeAI0 结尾的分段，此时您将看到分段名称显示为 `NetApp-backup-vsa87uLeAI0`。



- 单击存储分段，然后单击权限选项卡，然后单击存储分段策略部分中的 * 编辑 *。



- 为新创建的存储分段添加存储分段策略，以访问 Cloud Manager 的 AWS 帐户，然后保存更改。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::464262061435:root"
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::netapp-backup-vsa87uleai0",
        "arn:aws:s3:::netapp-backup-vsa87uleai0/*"
      ]
    }
  ]
}
```

请注意，"AWS"："ARN：AWS：iam：：464262061435：root" 为帐户 464262061435 中的所有资源提供了此存储分段的完全访问权限。如果要策略缩减为特定角色，级别，则可以使用特定角色更新策略。如果要添加单个角色，请确保同时添加了 `occa` 角色，否则备份将不会在 Cloud Backup UI 中更新。

例如："AWS"："ARN：AWS：iam：：464262061435：role/cvo-instance-profile-version10-d8e-lamInstanceRole-ikjpJ1HC2E7R"

7. 请重试在 Cloud Volumes ONTAP 系统上启用云备份，此时应成功启用。

在 Azure 中配置用于多帐户访问的备份

通过 Cloud Backup，您可以在与源 Cloud Volumes ONTAP 卷所在位置不同的 Azure 帐户中创建备份文件。这两个帐户都可以与 Cloud Manager Connector 所在的帐户不同。

只有在您使用时，才需要执行这些步骤 ["将 Cloud Volumes ONTAP 数据备份到 Azure Blob 存储"](#)。

只需按照以下步骤以这种方式设置您的配置即可。

在帐户之间设置 vNet 对等关系

请注意，如果您希望 Cloud Manager 在其他帐户 / 区域管理您的 Cloud Volumes ONTAP 系统，则需要设置 vNet 对等关系。存储帐户连接不需要建立 vNet 对等关系。

1. 登录到 Azure 门户，然后从主页选择 Virtual Networks。
2. 选择要用作订阅 1 的订阅，然后单击要设置对等关系的 vNet。



3. 选择 * cbsnetwork*，然后从左侧面板中单击 * 产品*，然后单击 * 添加*。

Subscription * ⓘ
OCCM Automation

Virtual network *
cbse2evnet

Traffic to remote virtual network ⓘ
☒ Allow (default)
☐ Block all traffic to the remote virtual network

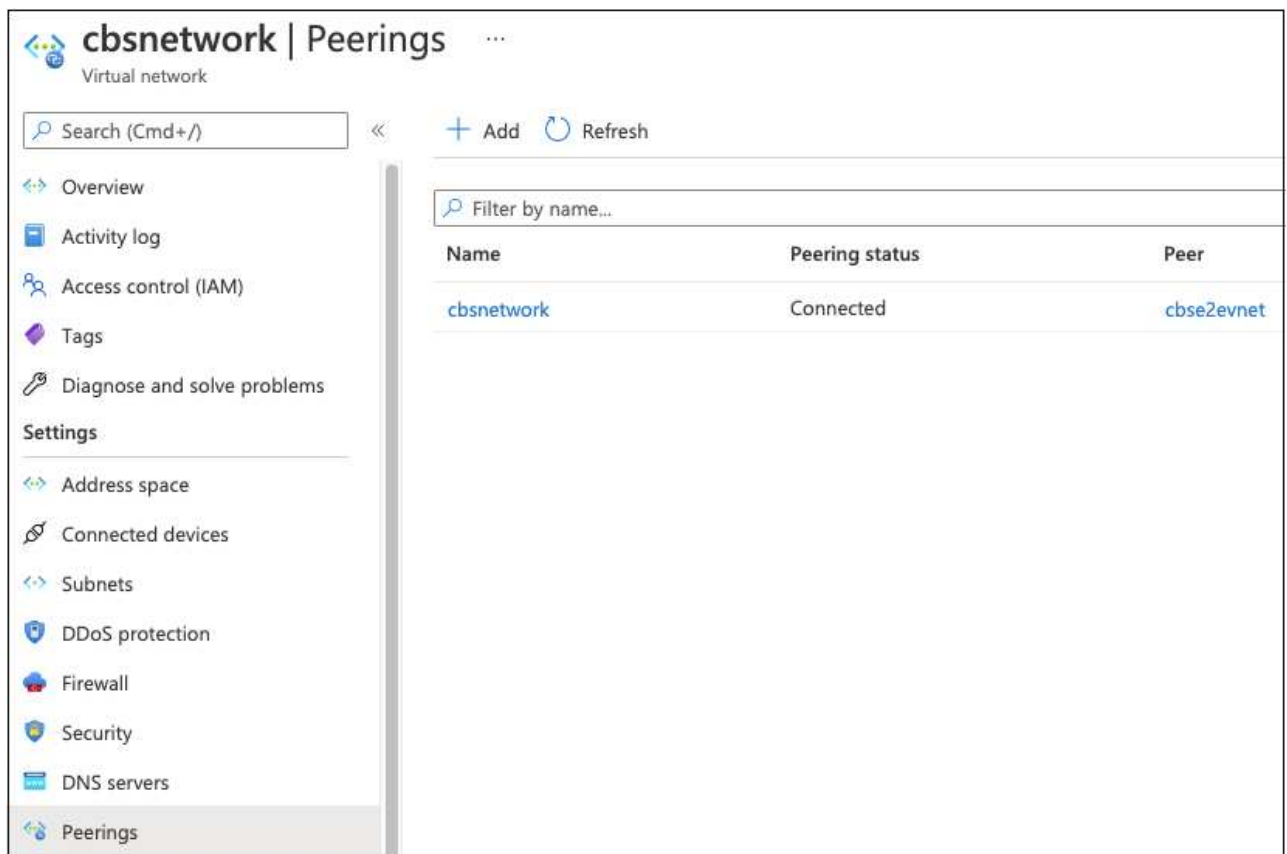
Traffic forwarded from remote virtual network ⓘ
☒ Allow (default)
☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ
☐ Use this virtual network's gateway or Route Server
☐ Use the remote virtual network's gateway or Route Server
☒ None (default)

Add

4. 在对等页面上输入以下信息，然后单击 * 添加*。
 - 此网络的对等链路名称：您可以提供任何名称来标识对等连接。
 - 远程虚拟网络对等链路名称：输入一个名称以标识远程 vNet。
 - 将所有选择保留为默认值。

- 在订阅下，选择订阅 2.
- 虚拟网络，请在订阅 2 中选择要设置对等关系的虚拟网络。



5. 在 subscription 2 vNet 中执行相同的步骤，并指定 subscription 1 的订阅和远程 vNet 详细信息。

Subscription * ⓘ

OCCM Dev

Virtual network *

cbsnetwork

Traffic to remote virtual network ⓘ

☒ Allow (default)
☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)
☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server
☐ Use the remote virtual network's gateway or Route Server
☒ None (default)

Add

此时将添加对等设置。

cbse2evnet | Peerings

Virtual network

Search (Cmd+ /)

<<

+ Add

Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

Filter by name...

Name	Peering status	Peer
cbsnetworkpeer	Connected	cbsnetwork

为存储帐户创建私有端点

现在，您需要为此存储帐户创建一个专用端点。在此示例中，存储帐户在订阅 1 中创建， Cloud Volumes ONTAP 系统在订阅 2 中运行。



要执行以下操作，您需要网络贡献者权限。

```

{
  "id": "/subscriptions/d333af45-0d07-4154-943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}

```

1. 转到存储帐户 > 网络 > 专用端点连接，然后单击 * + 专用端点 *。



2. 在 Private Endpoint _Basics 页面中:

- 选择订阅 2 （部署 Cloud Manager Connector 和 Cloud Volumes ONTAP 系统的位置）和资源组。
- 输入端点名称。
- 选择区域。

Create a private endpoint

1 Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * ① OCCM Dev

Resource group * ① cbsoccmdevcvo-rg [Create new](#)

Instance details

Name * cbse2e ✓

Region * (Asia Pacific) East Asia

3. 在 Resources 页面中，选择目标子资源为 * BLOB *。

Create a private endpoint ...

✓ Basics **2 Resource** 3 Configuration 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription OCCM Dev (d333af45-0d07-4154-943d-c25fbbce1b18)

Resource type Microsoft.Storage/storageAccounts

Resource test150521

Target sub-resource * ⓘ blob

4. 在配置页面中：

- 选择虚拟网络和子网。
- 单击 * 是 * 单选按钮以 " 与专用 DNS 区域集成 "。

Create a private endpoint ...

✓ Basics ✓ Resource **3 Configuration** 4 Tags 5 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network * ⓘ cbsnetwork

Subnet * ⓘ default (10.2.0.0/24)

i If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net

Review + create < Previous Next : Tags >

5. 在专用 DNS 区域列表中，确保从正确的区域中选择了专用区域，然后单击 * 查看 + 创建 *。

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net
		<div>Filter private DNS zones</div> <div> <div>occm_group_centralus</div> <div>privatelink.blob.core.windows.net</div> </div> <div> <div>occm_group_eastus</div> <div>privatelink.blob.core.windows.net</div> </div> <div> <div>occm_group_eastus2</div> <div>privatelink.blob.core.windows.net</div> </div>

现在，存储帐户（在订阅 1 中）可以访问在订阅 2 中运行的 Cloud Volumes ONTAP 系统。

- 请重试在 Cloud Volumes ONTAP 系统上启用云备份，此时应成功启用。

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.