



# **Configure backup for multi-account access in AWS**

## **Cloud Manager**

Tom Onacki  
June 15, 2021

This PDF was generated from [https://docs.netapp.com/us-en/occm/reference\\_backup\\_multi\\_account\\_aws.html](https://docs.netapp.com/us-en/occm/reference_backup_multi_account_aws.html) on September 09, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- Configure backup for multi-account access in AWS..... 1
  - Set up VPC peering between accounts ..... 1
  - Add a route to the route tables in both accounts ..... 3
  - Add the second AWS account credentials in Cloud Manager ..... 4
  - Enable backup in the other AWS account ..... 6

# Configure backup for multi-account access in AWS

Cloud Backup enables you to create backup files in an AWS account that is different than where your source volumes reside. And both of those accounts can be different than the account where the Cloud Manager Connector resides.

Just follow the steps below to set up your configuration in this manner.

## Set up VPC peering between accounts

1. Log in to second account and Create Peering Connection:
  - a. Select a local VPC: Select the VPC of the second account.
  - b. Select another VPC: Enter the account ID of the first account.
  - c. Select the Region where the Cloud Manager Connector is running. In this test setup both accounts are running in same region.
  - d. VPC ID: Log into first account and enter the acceptor VPC ID. This is the VPC ID of the Cloud Manager Connector.

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 (Acceptor)\*

A Success dialog displays.



### 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	-

The status of the peering connection shows as Pending Acceptance.

Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
cbs-multi-ac...	pcx-049758069d9...	Pending Acceptance	vpc-82f55afa   VP...	vpc-116d9174	10.0.0.0/16	-	733004784675	464262061435
cbs-multi-peer	pcx-05f2d310cb7f...	Deleted	vpc-82f55afa   VP...	vpc-116d9174	-	-	733004784675	464262061435
New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4   V...	vpc-fc2aa39a   De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

2. Log into the first account and accept the peering request:

Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
cbs-multi-ac...	pcx-049758069d9...	Pending Acceptance	vpc-82f55afa   VP...	vpc-116d9174	10.0.0.0/16	-	733004784675	464262061435
cbs-multi-peer	pcx-05f2d310cb7f...	Deleted	vpc-82f55afa   VP...	vpc-116d9174	-	-	733004784675	464262061435
New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4   V...	vpc-fc2aa39a   De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

### Accept VPC Peering Connection Request

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

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

Cancel

Yes, Accept

a. Click **Yes**.

### 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

The connection now shows as Active. We have also added a Name tag to identify the peering connection called **cbs-multi-account**.

<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"/>	hili-vpc-peer-chen	pcx-0d0e5c7fc4360254d	Active	vpc-0d12df59528f...	vpc-824dc0e4   nf...	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435

b. Refresh the peering connection in the second account and notice that the status changes to 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

## Add a route to the route tables in both accounts

1. Go to VPC > Subnet > Route table.

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. Click on the Routes tab.

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. Click **Edit routes**.

### 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. Click **Add route**, and from the Target drop-down list select **Peering Connection**, and then select the peering connection that you created.
  - a. In the Destination, enter the other account's subnet 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

Cancel **Save routes**

pcx-05f2d310cb7f49843

pcx-004715531514cb0d8

**pcx-049758069d9b7c140** cbs-multi-account

pcx-094f9fdb10a2045ea hill-peer-vadim-vpc

pcx-0791b47f6f9a27d65

pcx-0305041f9cc2dfbdb estycvoconnect

- b. Click **Save routes** and a Success dialog displays.

[Route Tables](#) > Edit routes

### Edit routes

✓ **Routes successfully edited**

**Close**

## Add the second AWS account credentials in Cloud Manager

1. Add the second AWS account, for example, *Saran-XCP-Dev*.

Credentials

+ Add Credentials

3 Credentials

aws Instance Profile

Credential Type: AWS Keys

464262061435

AWS Account ID

CBS-SR-OCCMOCCM1620912870830...

IAM Role

aws-sub-a2

Subscription

2

Working Environments

aws Saran-XCP-Dev

Credential Type: AWS Keys

733004784675

AWS Account ID

AKIA2VKTSMQRZRAWW3HI

AWS Access Key

aws-sub-a2

Subscription

0

Working Environments

- In the Discover Cloud Volumes ONTAP page, select the newly added credentials.

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

- Select the Cloud Volumes ONTAP system you want to discover from second account. You can also deploy a new Cloud Volumes ONTAP system in the second account.

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

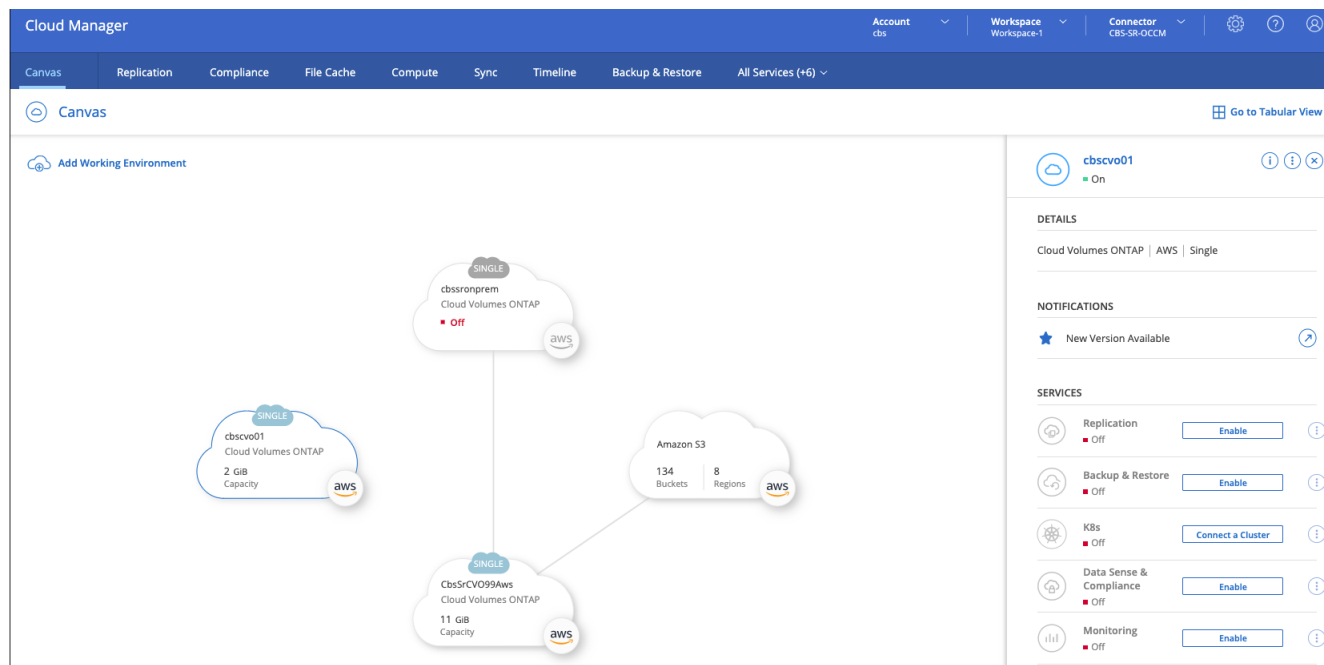
US East | N. Virginia

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
idanAwsHa991001	VPC for VSA	us-east-1a	subnet-c1d99699	idanAwsHa991001	172.31.5.234,172.31.5.110	HA Cloud Volumes ONTAP

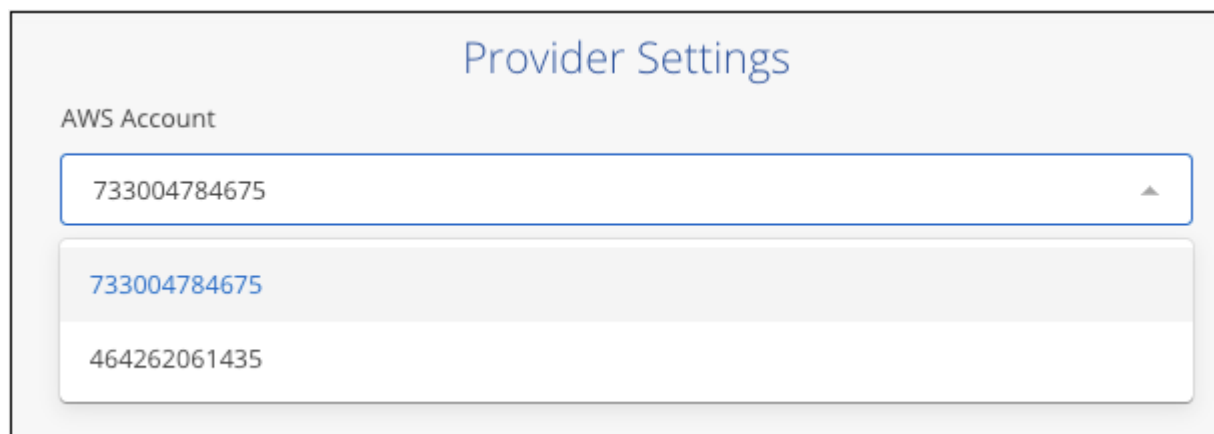
Continue

The Cloud Volumes ONTAP system from the second account is now added to Cloud Manager which is running in a different account.



## Enable backup in the other AWS account

1. In Cloud Manager, enable backup for the Cloud Volumes ONTAP system running in the first account, but select the second account as the location for creating the backup files.

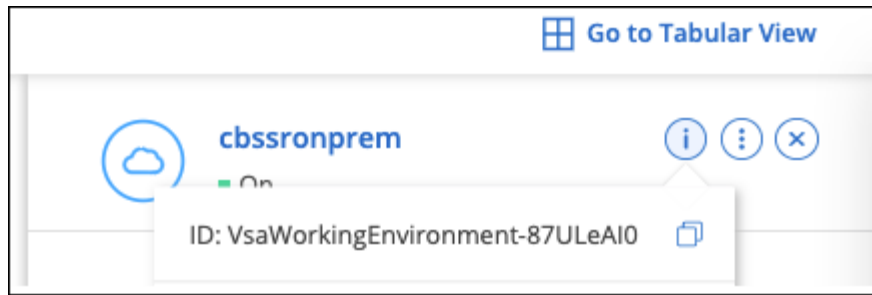


2. Then select a backup policy and the volumes you want to back up, and Cloud Backup attempts to create a new bucket in the selected account.

However, adding the bucket to the Cloud Volumes ONTAP system will fail because Cloud Backup uses the instance profile to add the bucket and the Cloud Manager instance profile doesn't have access to the resources in the second account.

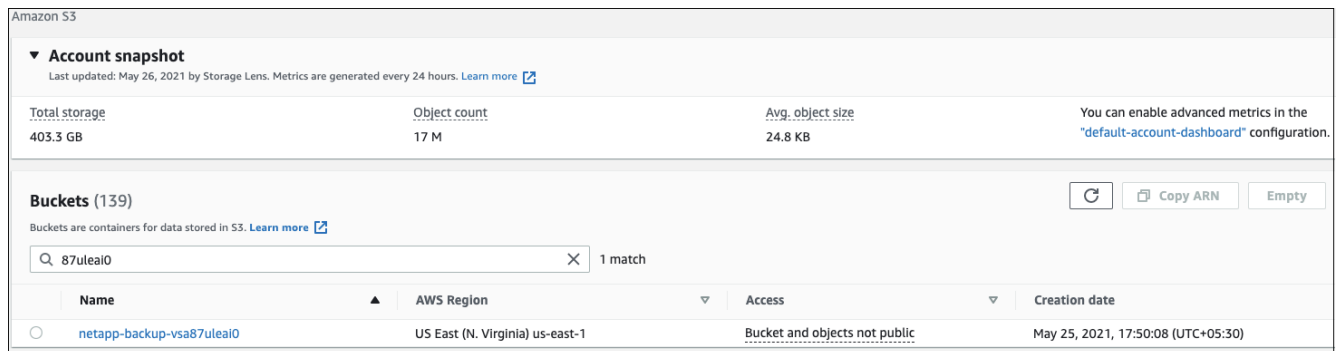
3. Get the working environment ID for the Cloud Volumes ONTAP system.



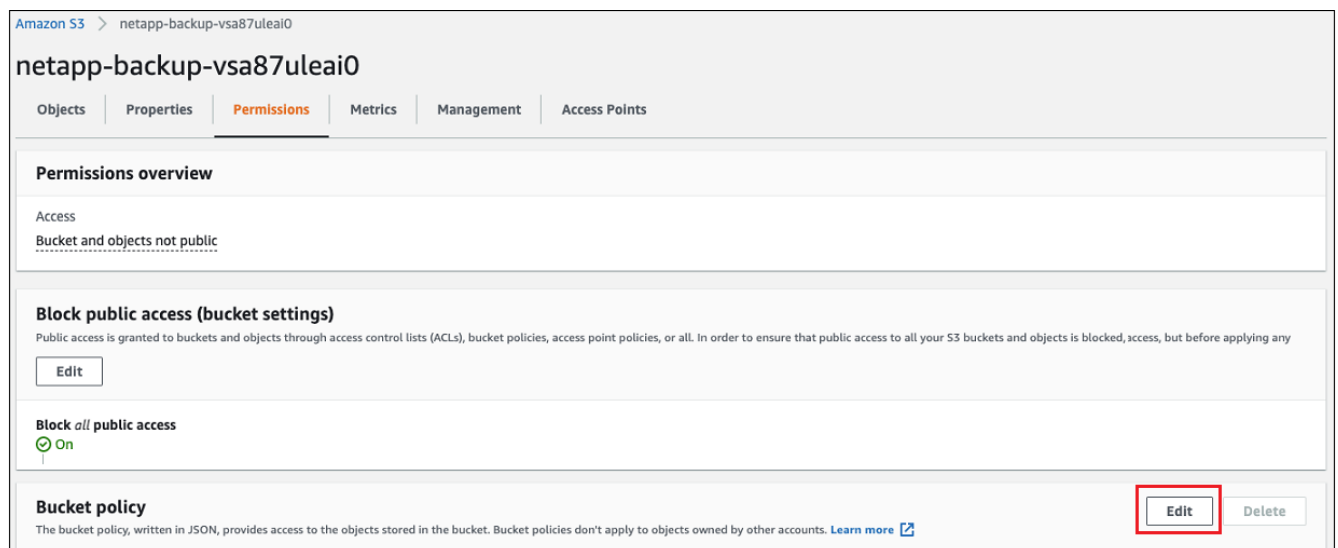


Cloud Backup creates every bucket with the prefix **Netapp-backup-** and will include the working environment ID; for example: **87ULeAI0**

- In the EC2 portal, go to S3 and search for the bucket with name ending with **87uLeAI0** and you'll see the bucket name displayed as **Netapp-backup-vsa87uLeAI0**.



- Click on the bucket, then click the Permissions tab, and then click **Edit** in the Bucket policy section.



- Add a bucket policy for the newly created bucket to provide access to the Cloud Manager's AWS account, and then Save the changes.

```

{
  "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/*"
      ]
    }
  ]
}

```

Note that "AWS": "arn:aws:iam::464262061435:root" gives complete access this bucket for all resources in account 464262061435. If you want to reduce it to specific role, level, you can update the policy with specific role(s). If you are adding individual roles, ensure that occm role also added, otherwise backups will not get updated in the Cloud Backup UI.

For example: "AWS": "arn:aws:iam::464262061435:role/cvo-instance-profile-version10-d8e-lamInstanceRole-IKJPJ1HC2E7R"

7. Retry enabling Cloud Backup on the Cloud Volumes ONTAP system and this time it should be successful.

## Copyright Information

Copyright © 2021 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.