



Release notes

Set up and administration

NetApp

November 01, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-setup-admin/whats-new.html> on November 01, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Release notes	1
What's new	1
Known limitations	10

Release notes

What's new

Learn what's new with BlueXP (formerly Cloud Manager) administration features: NetApp accounts, Connectors, cloud provider credentials, and more.

1 November 2022

Cloud Manager now prompts you to update the credentials associated with your NetApp Support Site accounts when the refresh token associated with your account expires after 3 months. [Learn how to manage NSS accounts](#)

18 September 2022

Connector 3.9.22

- We enhanced the Connector deployment wizard by adding an *in-product guide* that provides steps to meet the minimum requirements for Connector installation: permissions, authentication, and networking.
- You can now create a NetApp support case directly from Cloud Manager in the **Support Dashboard**.

[Learn how to create a case.](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

31 July 2022

Connector 3.9.21

- We've introduced a new way to discover the existing cloud resources that you're not yet managing in Cloud Manager.

On the Canvas, the **My Opportunities** tab provides a centralized location to discover existing resources that you can add to Cloud Manager for consistent data services and operations across your hybrid multicloud.

In this initial release, My Opportunities enables you to discover existing FSx for ONTAP file systems in your AWS account.

[Learn how to discover FSx for ONTAP using My Opportunities](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

15 July 2022

Policy changes

We updated the documentation by adding the Cloud Manager policies directly inside the docs. This means you can now view the required permissions for the Connector and Cloud Volumes ONTAP right alongside the steps that describe how to set them up. These policies were previously accessible from a page on the NetApp Support Site.

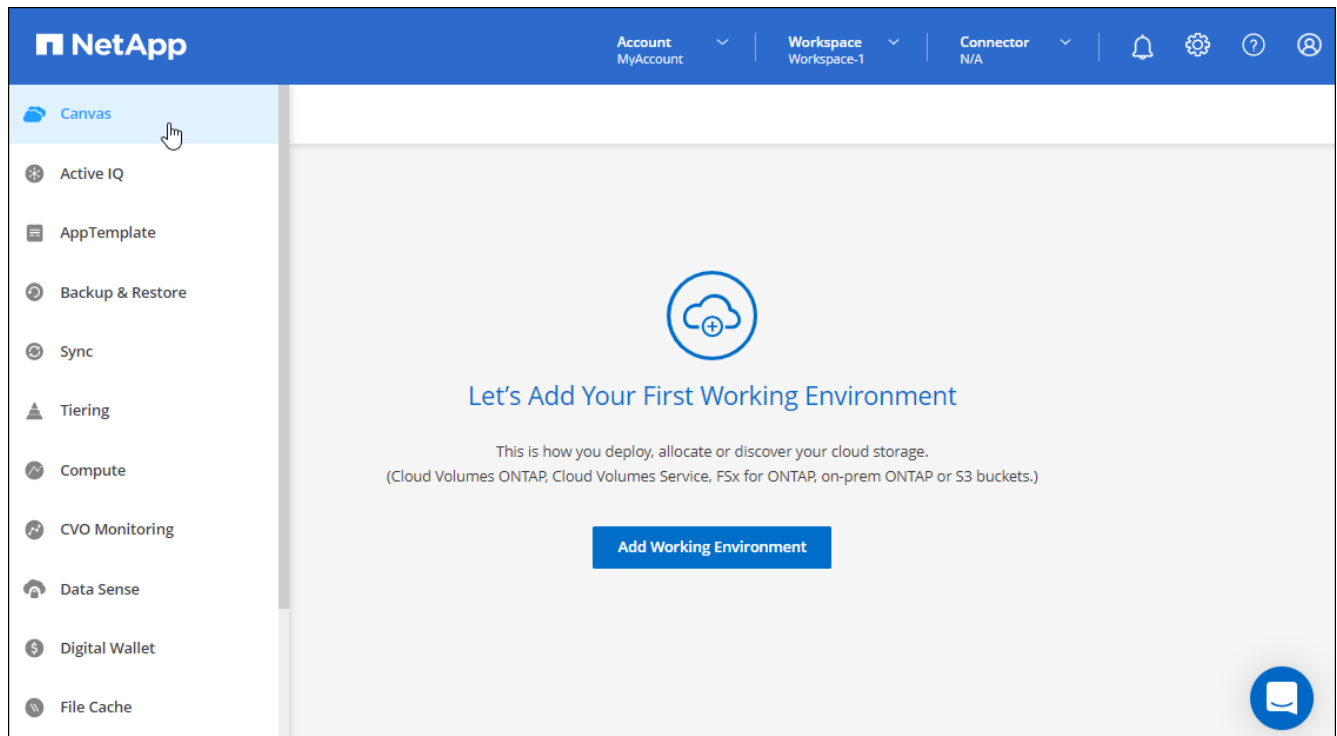
[Here's an example that shows the AWS IAM role permissions used to create a Connector.](#)

We also created a page that provides links to each of the policies. [View the permissions summary for Cloud Manager.](#)

3 July 2022

Connector 3.9.20

- We've introduced a new way to navigate to the growing list of features in the Cloud Manager interface. All the familiar Cloud Manager capabilities can now be easily found by hovering over the left panel.



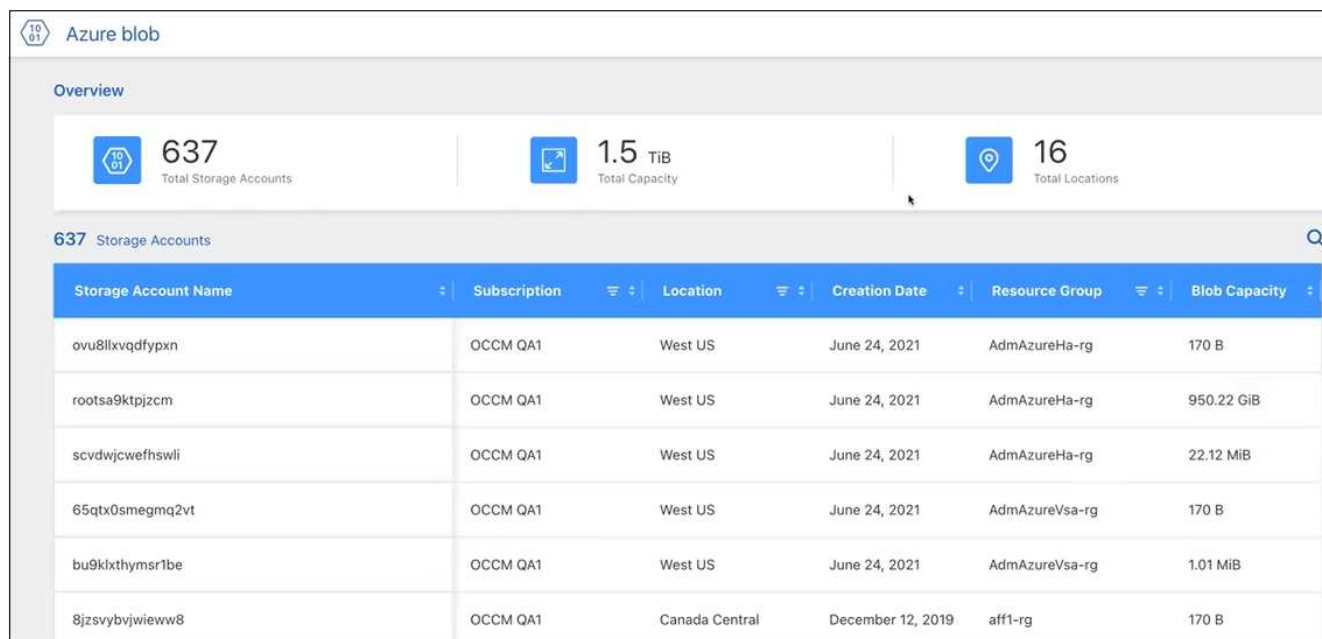
- You can now configure Cloud Manager to send notifications by email so you can be informed of important system activity even when you're not logged into the system.

[Learn more about monitoring operations in your account.](#)

- Cloud Manager now supports Azure Blob storage and Google Cloud Storage as working environments, similar to Amazon S3 support.

After you install a Connector in Azure or Google Cloud, Cloud Manager now automatically discovers information about Azure Blob storage in your Azure subscription or the Google Cloud Storage in the project where the Connector is installed. Cloud Manager displays the object storage as a working environment that you can open to view more detailed information.

Here's an example of an Azure Blob working environment:



Storage Account Name	Subscription	Location	Creation Date	Resource Group	Blob Capacity
ovu8lilxvqdfypxn	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	170 B
rootsa9ktpjzcm	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	950.22 GiB
scvdwjcwehfswli	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	22.12 MiB
65qtx0smegmq2vt	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	170 B
bu9klxthymr1be	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	1.01 MiB
8jzsvybvjiwieww8	OCCM QA1	Canada Central	December 12, 2019	aff1-rg	170 B

- We redesigned the resources page for an Amazon S3 working environment by providing more detailed information about S3 buckets, such as capacity, encryption details, and more.
- The Connector is now supported in the following Google Cloud regions:
 - Madrid (europe-southwest1)
 - Paris (europe-west9)
 - Warsaw (europe-central2)
- The Connector is now supported in the Azure West US 3 region.

[View the full list of supported regions](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

28 June 2022

Log in with NetApp credentials

When new users sign up to Cloud Central, they can now select the **Log in with NetApp** option to log in with their NetApp Support Site credentials. This is an alternative to entering an email address and password.



Existing logins that use an email address and password need to keep using that login method. The Log in with NetApp option is available for new users who sign up.

7 June 2022

Connector 3.9.19

- The Connector is now supported in the AWS Jakarta region (ap-southeast-3).

- The Connector is now supported in the Azure Brazil Southeast region.

[View the full list of supported regions](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements and on-prem ONTAP cluster enhancements.
 - [Learn about Cloud Volumes ONTAP enhancements](#)
 - [Learn about ONTAP on-prem cluster enhancements](#)

12 May 2022

Connector 3.9.18 patch

We updated the Connector to introduce bug fixes. The most notable fix is to an issue that affects Cloud Volumes ONTAP deployment in Google Cloud when the Connector is in a shared VPC.

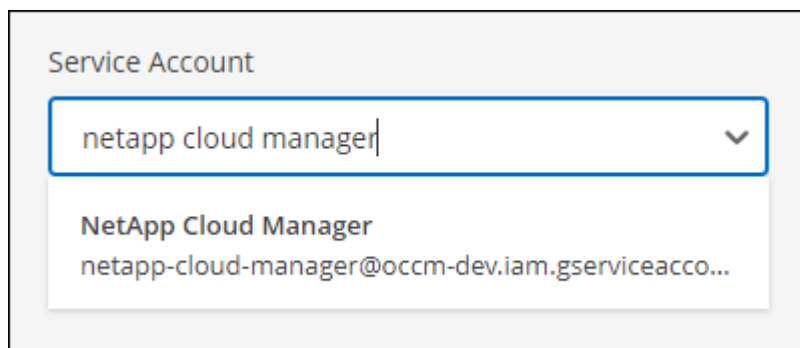
2 May 2022

Connector 3.9.18

- The Connector is now supported in the following Google Cloud regions:
 - Delhi (asia-south2)
 - Melbourne (australia-southeast2)
 - Milan (europe-west8)
 - Santiago (southamerica-west1)

[View the full list of supported regions](#)

- When you select the Google Cloud service account to use with the Connector, Cloud Manager now displays the email address that's associated with each service account. Viewing the email address can make it easier to distinguish between service accounts that share the same name.



- We have certified the Connector in Google Cloud on a VM instance with an OS that supports [Shielded VM features](#)
- This release of the Connector also includes Cloud Volumes ONTAP enhancements. [Learn about those enhancements](#)
- New AWS permissions are required for the Connector to deploy Cloud Volumes ONTAP.

The following permissions are now required to create an AWS spread placement group when deploying an

HA pair in a single Availability Zone (AZ):

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy",
```

These permissions are now required to optimize how Cloud Manager creates the placement group.

Be sure to provide these permissions to each set of AWS credentials that you've added to Cloud Manager.

[View the latest IAM policy for the Connector.](#)

3 April 2022

Connector 3.9.17

- You can now create a Connector by letting Cloud Manager assume an IAM role that you set up in your environment. This authentication method is more secure than sharing an AWS access key and secret key.

[Learn how to create a Connector using an IAM role.](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements. [Learn about those enhancements](#)

27 February 2022

Connector 3.9.16

- When you create a new Connector in Google Cloud, Cloud Manager will now display all of your existing firewall policies. Previously, Cloud Manager wouldn't display any policies that didn't have a target tag.
- This release of the Connector also includes Cloud Volumes ONTAP enhancements. [Learn about those enhancements](#)

30 January 2022

Connector 3.9.15

This release of the Connector includes Cloud Volumes ONTAP enhancements. [Learn about those enhancements](#)

2 January 2022

Reduced endpoints for the Connector

We reduced the number of endpoints that a Connector needs to contact in order to manage resources and processes within your public cloud environment.

[View the list of required endpoints](#)

EBS disk encryption for the Connector

When you deploy a new Connector in AWS from Cloud Manager, you can now choose to encrypt the Connector's EBS disks using the default master key or a managed key.

✓ Get Ready

✓ AWS Credentials

3 Details

4 Network

5 Security Group

6 Review

Details

Connector Instance Name

Connector1

Connector Role

☒ Create Role ☐ Select an existing Role

Role Name

Cloud-Manager-Operator-9yils3K

+ Add Tags to Connector Instance

☒ AWS Managed Encryption

Master Key: aws/ebs (default) [Change Key](#)

Email address for NSS accounts

Cloud Manager can now display the email address that's associated with a NetApp Support Site account.



28 November 2021

Update required for NetApp Support Site accounts

Starting in December 2021, NetApp now uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing. As a result of this update, Cloud Manager will prompt you to update the credentials for any existing NetApp Support Site accounts that you previously added.

If you haven't yet migrated your NSS account to IDaaS, you first need to migrate the account and then update your credentials in Cloud Manager.

- [Learn how to update an NSS account to the new authentication method.](#)
- [Learn more about NetApp's use of Microsoft Azure AD for identity management](#)

Change NSS accounts for Cloud Volumes ONTAP

If your organization has multiple NetApp Support Site accounts, you can now change which account is associated with a Cloud Volumes ONTAP system.

[Learn how to attach a working environment to a different NSS account.](#)

4 November 2021

SOC 2 Type 2 certification

An independent certified public accountant firm and services auditor examined Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense, and Cloud Backup (Cloud Manager platform), and affirmed that they have achieved SOC 2 Type 2 reports based on the applicable Trust Services criteria.

[View NetApp's SOC 2 reports.](#)

Connector no longer supported as a proxy

You can no longer use the Cloud Manager Connector as a proxy server to send AutoSupport messages from Cloud Volumes ONTAP. This functionality has been removed and is no longer supported. You will need to provide AutoSupport connectivity through a NAT instance or your environment's proxy services.

[Learn more about verifying AutoSupport with Cloud Volumes ONTAP](#)

31 October 2021

Authentication with service principal

When you create a new Connector in Microsoft Azure, you can now authenticate with an Azure service principal, rather than with Azure account credentials.

[Learn how to authenticate with an Azure service principal.](#)

Credentials enhancement

We redesigned the Credentials page for ease of use and to match the current look and feel of the Cloud Manager interface.

2 September 2021

A new Notification Service has been added

The Notification service has been introduced so you can view the status of Cloud Manager operations that you have initiated during your current login session. You can verify whether the operation was successful, or if it failed. [See how to monitor operations in your account.](#)

1 August 2021

RHEL 7.9 support with the Connector

The Connector is now supported on a host that's running Red Hat Enterprise Linux 7.9.

[View system requirements for the Connector.](#)

7 July 2021

Enhancements to Add Connector wizard

We redesigned the **Add Connector** wizard to add new options and to make it easier to use. You can now add

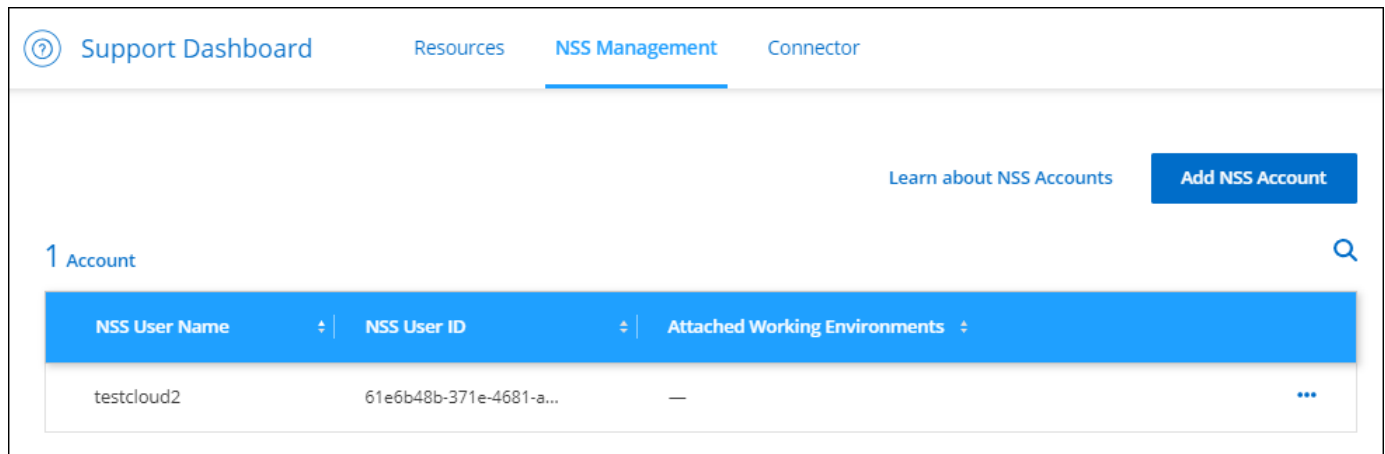
tags, specify a role (for AWS or Azure), upload a root certificate for a proxy server, view code for Terraform automation, view progress details, and more.

- [Create a Connector in AWS](#)
- [Create a Connector in Azure](#)
- [Create a Connector in GCP](#)

NSS account management from Support Dashboard

NetApp Support Site (NSS) accounts are now managed from the Support Dashboard, rather than from the Settings menu. This change makes it easier to find and manage all support-related information from a single location.

[Learn how to manage NSS accounts.](#)



5 May 2021

Accounts in the Timeline

The Timeline in Cloud Manager now shows actions and events related to account management. The actions include things like associating users, creating workspaces, and creating Connectors. Checking the Timeline can be helpful if you need to identify who performed a specific action, or if you need to identify the status of an action.

[Learn how to filter the Timeline to the Tenancy service.](#)

11 April 2021

API calls directly to Cloud Manager

If you configured a proxy server, you can now enable an option to send API calls directly to Cloud Manager without going through the proxy. This option is supported with Connectors that are running in AWS or in Google Cloud.

[Learn more about this setting.](#)

Service account users

You can now create a service account user.

A service account acts as a "user" that can make authorized API calls to Cloud Manager for automation purposes. This makes it easier to manage automation because you don't need to build automation scripts based on a real person's user account who can leave the company at any time. And if you're using federation, you can create a token without generating a refresh token from the cloud.

[Learn more about using service accounts.](#)

Private previews

You can now allow private previews in your account to get access to new NetApp cloud services as they are made available as a preview in Cloud Manager.

[Learn more about this option.](#)

Third-party services

You can also allow third-party services in your account to get access to third-party services that are available in Cloud Manager.

[Learn more about this option.](#)

9 February 2021

Support Dashboard improvements

We've updated the Support Dashboard by enabling you to add your NetApp Support Site credentials, which registers you for support. You can also initiate a NetApp Support case directly from the dashboard. Just click the Help icon and then **Support**.

Known limitations

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

These limitations are specific to BlueXP set up and administration: the Connector, the SaaS platform, and more.

Connector limitations

Possible conflict with IP addresses in the 172 range

BlueXP deploys the Connector with two interfaces that have IP addresses in the 172.17.0.0/16 and 172.18.0.0/16 ranges.

If your network has a subnet configured with either of these ranges, then you might experience connectivity failures from BlueXP. For example, discovering on-prem ONTAP clusters in BlueXP might fail.

See Knowledge Base article [BlueXP Connector IP conflict with existing network](#) for instructions on how to change the IP address of the Connector's interfaces.

Only an HTTP proxy server is supported

If your corporate policies require you to use a proxy server for all HTTP communication to the internet, then you must configure your Connectors to use that HTTP proxy server. The proxy server can be in the cloud or in your network.

BlueXP doesn't support using an HTTPS proxy with the Connector.

SSL decryption isn't supported

BlueXP doesn't support firewall configurations that have SSL decryption enabled. If SSL decryption is enabled, error messages appear in BlueXP and the Connector instance displays as inactive.

For enhanced security, you have the option to [install an HTTPS certificate signed by a certificate authority \(CA\)](#).

Blank page when loading the local UI

If you load the local user interface for a Connector, the UI might fail to display sometimes, and you just get a blank page.

This issue is related to a caching problem. The workaround is to use an incognito or private web browser session.

Shared Linux hosts are not supported

The Connector isn't supported on a VM that is shared with other applications. The VM must be dedicated to the Connector software.

3rd-party agents and extensions

3rd-party agents or VM extensions are not supported on the Connector VM.

SaaS limitations

SaaS platform is disabled for Government regions

If you deploy a Connector in an AWS GovCloud region, an Azure Gov region, or an Azure DoD region, access to BlueXP is available only through a Connector's host IP address. Access to the SaaS platform is disabled for the entire account.

This means that only privileged users who can access the end-user internal VPC/VNet can use BlueXP's UI or API.

Note that the only services supported in these regions are Cloud Volumes ONTAP, Cloud Backup, Cloud Data Sense, and Replication. No other NetApp services are supported in Government regions.

[Learn how to access the local UI on the Connector.](#)

Marketplace limitations

Pay-as-you-go not available for Azure and Google Cloud partners

If you are a Microsoft Cloud Solution Provider (CSP) partner or a Google Cloud partner, NetApp pay-as-you-go

subscriptions are not available. You must purchase a license and deploy NetApp cloud solutions with a BYOL license.

Pay-as-you-go subscriptions are not available for the following NetApp cloud services:

- Cloud Volumes ONTAP
- Cloud Tiering
- Cloud Backup
- Cloud Data Sense

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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.