Manage AWS credentials

Setup and administration

NetApp
June 30, 2023

This PDF was generated from https://docs.netapp.com/us-en/bluexp-setup-admin/concept-accounts-aws.html on June 30, 2023. Always check docs.netapp.com for the latest.

Table of Contents

Manage AWS credentials 1
AWS credentials and permissions 1
Manage AWS credentials and subscriptions for BlueXP 3

Manage AWS credentials

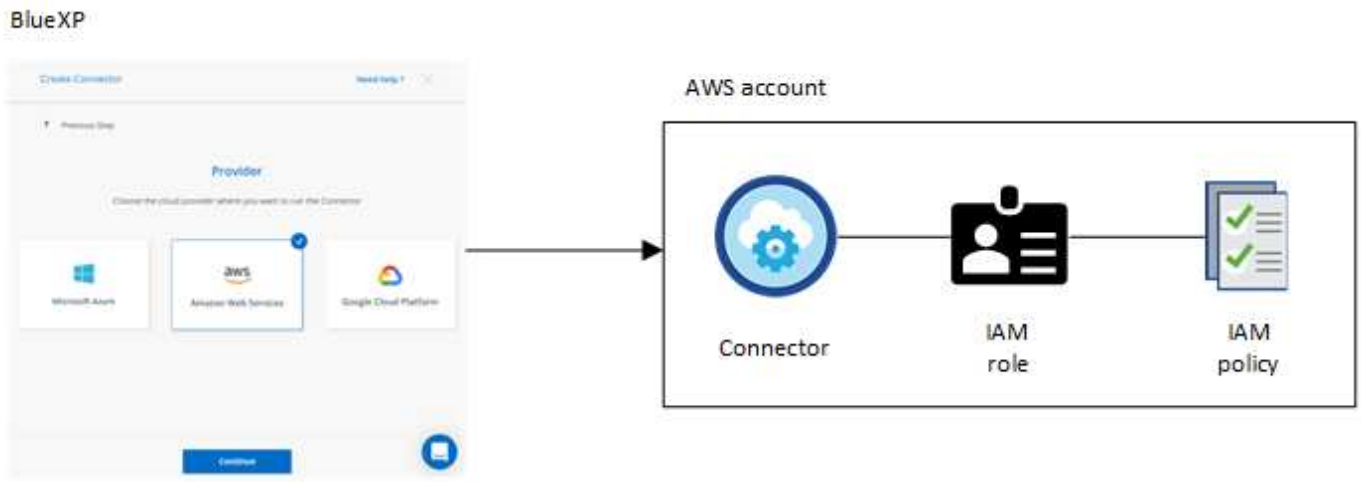
AWS credentials and permissions

Learn how BlueXP uses AWS credentials and permissions to perform actions on your behalf. Understanding these details can be helpful as you manage the credentials for one or more AWS accounts in BlueXP. For example, you might want to learn about when to add additional AWS credentials to BlueXP.

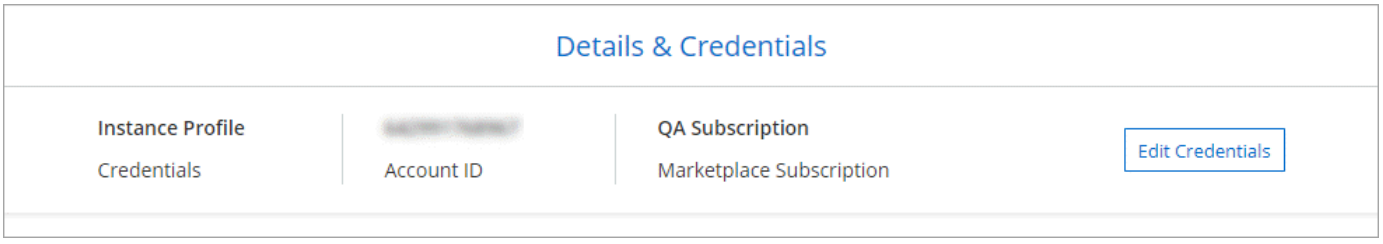
Initial AWS credentials

When you deploy a Connector from BlueXP, you need to provide the ARN of an IAM role or access keys for an IAM user. The authentication method that you use must have the required permissions to deploy the Connector instance in AWS. The required permissions are listed in the Connector deployment policy for AWS.

When BlueXP launches the Connector instance in AWS, it creates an IAM role and an instance profile for the instance. It also attaches a policy that provides the Connector with permissions to manage resources and processes within that AWS account. Review how BlueXP uses the permissions.



BlueXP selects these AWS credentials by default when you create a new working environment for Cloud Volumes ONTAP:



You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

Additional AWS credentials

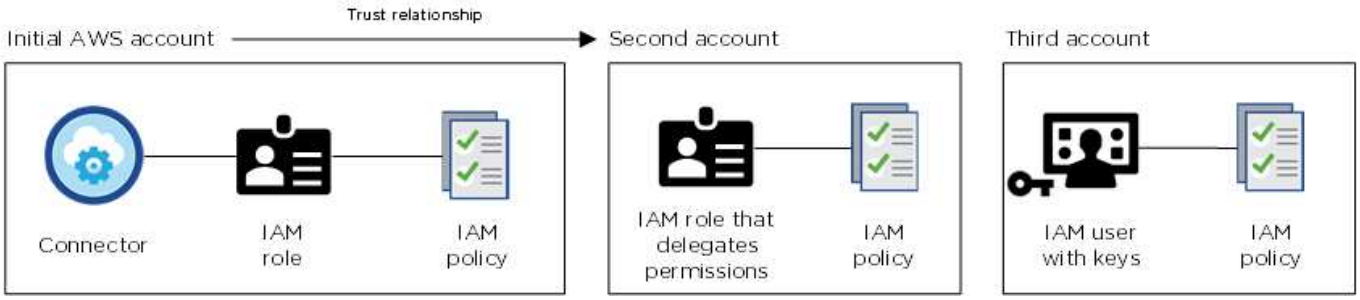
There are two ways to add additional AWS credentials:

- You can add AWS credentials to an existing Connector
- You can add AWS credentials directly to BlueXP

Review the sections below for more details.

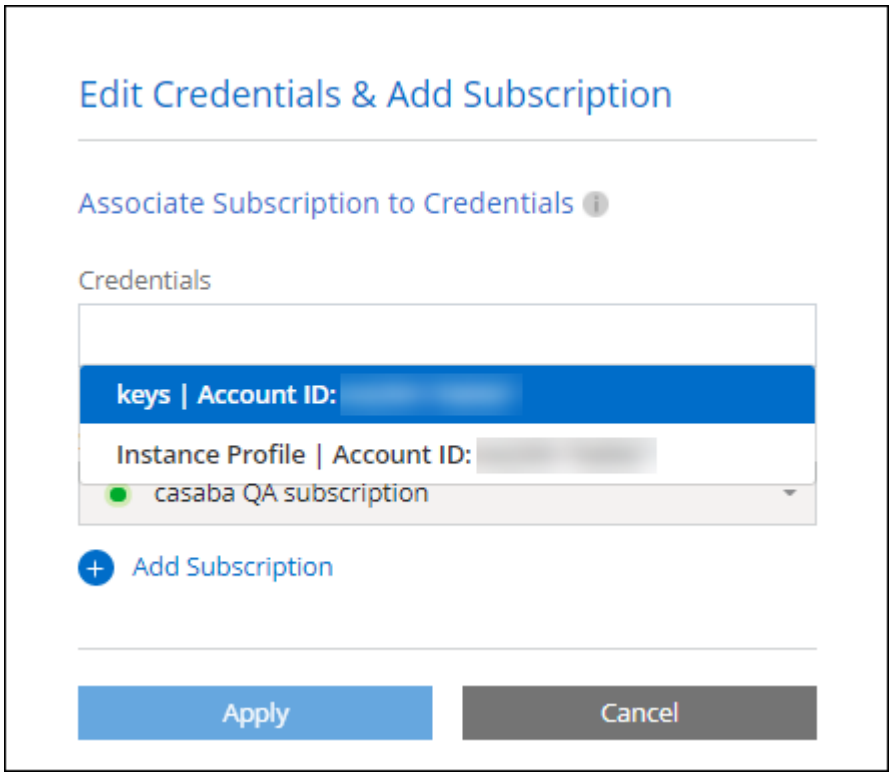
Add AWS credentials to an existing Connector

If you want to launch Cloud Volumes ONTAP in different AWS accounts, then you can either provide AWS keys for an IAM user or the ARN of a role in a trusted account. The following image shows two additional accounts, one providing permissions through an IAM role in a trusted account and another through the AWS keys of an IAM user:



You would then add the account credentials to BlueXP by specifying the Amazon Resource Name (ARN) of the IAM role, or the AWS keys for the IAM user.

After you add another set of credentials, you can switch to them when creating a new working environment:



Learn how to add AWS credentials to an existing Connector.

Add AWS credentials directly to BlueXP

Adding new AWS credentials to BlueXP provides the permissions needed to create and manage an FSx for ONTAP working environment or to create a Connector.

- Learn how to add AWS credentials to BlueXP for Amazon FSx for ONTAP
- Learn how to add AWS credentials to BlueXP for creating a Connector

What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from BlueXP. You can also deploy a Connector in AWS from the AWS Marketplace and you can manually install the Connector software on your own Linux host.

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the IAM role, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up an IAM role for the BlueXP system, but you can provide permissions using AWS access keys.

To learn how to set up permissions, refer to the following pages:

- Standard mode
  - Set up AWS permissions
  - Set up cloud permissions for on-prem deployments
- Set up cloud permissions for restricted mode
- Set up cloud permissions for private mode

How can I securely rotate my AWS credentials?

As described above, BlueXP enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys.

With the first two options, BlueXP uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice—it's automatic and it's secure.

If you provide BlueXP with AWS access keys, you should rotate the keys by updating them in BlueXP at a regular interval. This is a completely manual process.

Manage AWS credentials and subscriptions for BlueXP

Add and manage AWS credentials so that BlueXP has the permissions that it needs to deploy and manage cloud resources in your AWS accounts. If you manage multiple AWS Marketplace subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

Overview

You can add AWS credentials to an existing Connector or directly to BlueXP:

- Add additional AWS credentials to an existing Connector

  Adding AWS credentials to an existing Connector provides the permissions needed to manage resources and processes within your public cloud environment. Learn how to add AWS credentials to a Connector.

- Add AWS credentials to BlueXP for creating a Connector

  Adding new AWS credentials to BlueXP gives BlueXP the permissions needed to create a Connector. Learn how to add AWS credentials to BlueXP.

- Add AWS credentials to BlueXP for FSx for ONTAP

  Adding new AWS credentials to BlueXP gives BlueXP the permissions needed to create and manage FSx for ONTAP. Learn how to set up permissions for FSx for ONTAP

How to rotate credentials

BlueXP enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys. Learn more about AWS credentials and permissions.

With the first two options, BlueXP uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice because it's automatic and it's secure.

If you provide BlueXP with AWS access keys, you should rotate the keys by updating them in BlueXP at a regular interval. This is a completely manual process.

Add additional credentials to a Connector

Add additional AWS credentials to a Connector so that it has the permissions needed to manage resources and processes within your public cloud environment. You can either provide the ARN of an IAM role in another account or provide AWS access keys.

If you're just getting started with BlueXP, Learn how BlueXP uses AWS credentials and permissions.

Grant permissions

Before you add AWS credentials to a Connector, you need to provide the required permissions. The permissions enable BlueXP to manage resources and processes within that AWS account. How you provide the permissions depends on whether you want to provide BlueXP with the ARN of a role in a trusted account or AWS keys.

If you deployed a Connector from BlueXP, BlueXP automatically added AWS credentials for the account in which you deployed the Connector. This initial account is not added if you deployed the Connector from the AWS Marketplace or if you manually installed the Connector software on an existing system. Learn about AWS credentials and permissions.

Choices

- Grant permissions by assuming an IAM role in another account
- Grant permissions by providing AWS keys

Grant permissions by assuming an IAM role in another account

You can set up a trust relationship between the source AWS account in which you deployed the Connector instance and other AWS accounts by using IAM roles. You would then provide BlueXP with the ARN of the IAM roles from the trusted accounts.

If the Connector is installed on premises, you can't use this authentication method. You must use AWS keys.

Steps

1. Go to the IAM console in the target account in which you want to provide the Connector with permissions.
2. Under Access Management, select **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the ID of the account where the Connector instance resides.
   - Create the required policies by copying and pasting the contents of the IAM policies for the Connector.
3. Copy the Role ARN of the IAM role so that you can paste it in BlueXP later on.

Result

The account now has the required permissions. You can now add the credentials to a Connector.

Grant permissions by providing AWS keys

If you want to provide BlueXP with AWS keys for an IAM user, then you need to grant the required permissions to that user. The BlueXP IAM policy defines the AWS actions and resources that BlueXP is allowed to use.

You must use this authentication method if the Connector is installed on premises. You can't use an IAM role.

Steps

1. From the IAM console, create policies by copying and pasting the contents of the IAM policies for the Connector.

   AWS Documentation: Creating IAM Policies

2. Attach the policies to an IAM role or an IAM user.
   - AWS Documentation: Creating IAM Roles
   - AWS Documentation: Adding and Removing IAM Policies

Result

The account now has the required permissions. You can now add the credentials to a Connector.

Add the credentials

After you provide an AWS account with the required permissions, you can add the credentials for that account to an existing Connector. This enables you to launch Cloud Volumes ONTAP systems in that account using the same Connector.

Before you get started

If you just created these credentials in your cloud provider, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

Steps

1. Ensure that the correct Connector is currently selected in BlueXP.
2. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.

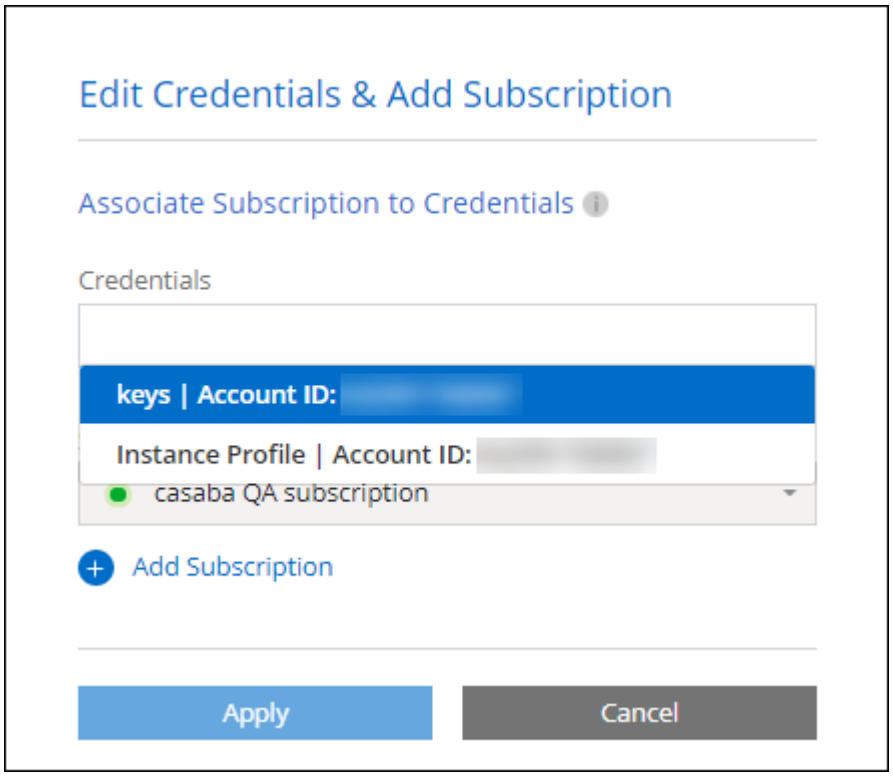
3. On the **Account credentials** page, select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Amazon Web Services > Connector**.
   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of a trusted IAM role, or enter an AWS access key and secret key.
   c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

      To pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or with an annual contract, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

   d. **Review**: Confirm the details about the new credentials and select **Add**.

Result

You can now switch to a different set of credentials from the Details and Credentials page when creating a new working environment:



Add credentials to BlueXP for creating a Connector

Add AWS credentials to BlueXP by providing the ARN of an IAM role that gives BlueXP the permissions needed to create a Connector. You can choose these credentials when creating a new Connector.

Set up the IAM role

Set up an IAM role that enables the BlueXP SaaS layer to assume the role.

Steps

1. Go to the IAM console in the target account.
2. Under Access Management, select **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the ID of the BlueXP SaaS: 952013314444
   - Create a policy that includes the permissions required to create a Connector.
     - View the permissions needed for FSx for ONTAP
     - View the Connector deployment policy
3. Copy the Role ARN of the IAM role so that you can paste it in BlueXP in the next step.

Result

The IAM role now has the required permissions. You can now add it to BlueXP.

Add the credentials

After you provide the IAM role with the required permissions, add the role ARN to BlueXP.

Before you get started

If you just created the IAM role, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.

2. On the **Account credentials** page, select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Amazon Web Services > BlueXP**.
   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of the IAM role.
   c. **Review**: Confirm the details about the new credentials and select **Add**.

Result

You can now use the credentials when creating a new Connector.

Add credentials to BlueXP for Amazon FSx for ONTAP

For details, refer to the BlueXP documentation for Amazon FSx for ONTAP

Associate an AWS subscription

After you add your AWS credentials to BlueXP, you can associate an AWS Marketplace subscription with those credentials. The subscription enables you to pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or using an annual contract, and to use other BlueXP services.

There are two scenarios in which you might associate an AWS Marketplace subscription after you've already added the credentials to BlueXP:

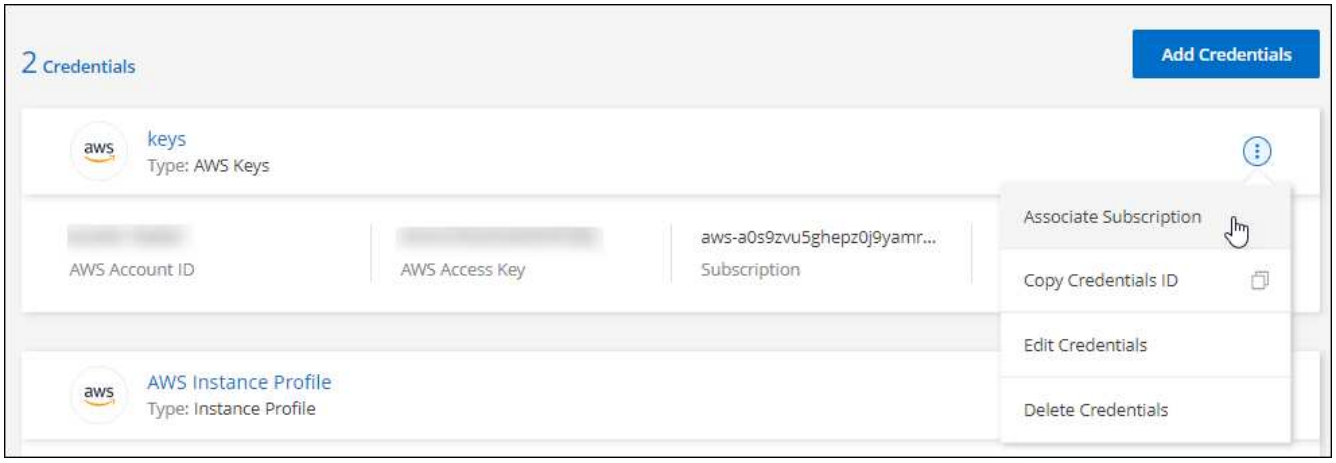
- You didn't associate a subscription when you initially added the credentials to BlueXP.
- You want to replace an existing AWS Marketplace subscription with a new subscription.

What you'll need

You need to create a Connector before you can change BlueXP settings. Learn how to create a Connector.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select the action menu for a set of credentials and then select **Associate Subscription**.



3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Associate**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
   a. Select **View purchase options**.
   b. Select **Subscribe**.
   c. Select **Set up your account**.

      You'll be redirected to the BlueXP website.

   d. From the **Subscription Assignment** page:
      - Select the BlueXP accounts that you'd like to associate this subscription with.

- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one account with this new subscription.

  BlueXP replaces the existing subscription for all credentials in the account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

  For all other accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

  The following video shows the steps to subscribe from the Google Cloud Marketplace:

  ► https://docs.netapp.com/us-en/bluexp-setup-admin//media/video_subscribing_aws.mp4 *(video)*

Edit credentials

Edit your AWS credentials in BlueXP by changing the account type (AWS keys or assume role), by editing the name, or by updating the credentials themselves (the keys or the role ARN).

You can't edit the credentials for an instance profile that is associated with a Connector instance.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then select **Apply**.

Delete credentials

If you no longer need a set of credentials, you can delete them from BlueXP. You can only delete credentials that aren't associated with a working environment.

You can't delete the credentials for an instance profile that is associated with a Connector instance.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
3. Select **Delete** to confirm.

Copyright information

Copyright © 2023 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.