



# **Verify Azure platform image**

## **Cloud Volumes ONTAP**

NetApp

January 13, 2026

This PDF was generated from <https://docs.netapp.com/us-en/storage-management-cloud-volumes-ontap/concept-azure-image-verification.html> on January 13, 2026. Always check docs.netapp.com for the latest.

# Table of Contents

- Verify Azure platform image ..... 1
  - Azure marketplace image verification for Cloud Volumes ONTAP ..... 1
    - Azure’s alteration of published VHD files ..... 1
  - Download the Azure image file for Cloud Volumes ONTAP ..... 1
  - Export VHD images for Cloud Volumes ONTAP from the Azure marketplace ..... 2
    - Export VHD file using the Azure Cloud Shell on Linux ..... 4
    - Export VHD file using the Azure CLI on Linux ..... 6
  - Verify file signature ..... 8
    - Azure marketplace image signature verification for Cloud Volumes ONTAP ..... 8
    - Verify Azure marketplace image signature for Cloud Volumes ONTAP on Linux ..... 9
    - Verify Azure marketplace image signature for Cloud Volumes ONTAP on macOS ..... 10

# Verify Azure platform image

## Azure marketplace image verification for Cloud Volumes ONTAP

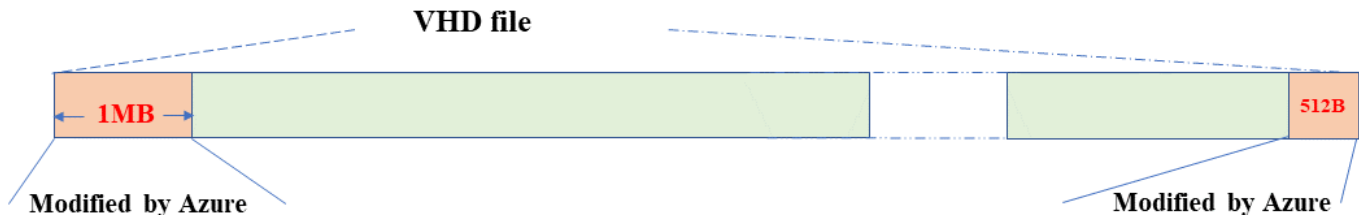
Azure image verification complies with enhanced NetApp security requirements. Verifying an image file is a straightforward process. However, the Azure image signature verification requires specific considerations for the Azure VHD image file because it is altered in the Azure marketplace.



Azure image verification is supported on Cloud Volumes ONTAP 9.15.0 and later.

### Azure's alteration of published VHD files

The 1 MB (1048576 bytes) at the beginning and 512 bytes at the end of the VHD file is modified by Azure. NetApp signs the remaining VHD file.



In the example, the VHD file is of 10GB. The portion that NetApp signed is marked in green (10 GB - 1 MB - 512 bytes).

### Related links

- [Page Fault Blog: How to sign and verify using OpenSSL](#)
- [Use Azure Marketplace image to create VM image for your Azure Stack Edge Pro GPU | Microsoft Learn](#)
- [Export/Copy a managed disk to a storage account using the Azure CLI | Microsoft Learn](#)
- [Azure Cloud Shell Quickstart - Bash | Microsoft Learn](#)
- [How to install the Azure CLI | Microsoft Learn](#)
- [az storage blob copy | Microsoft Learn](#)
- [Sign in with Azure CLI — Login and Authentication | Microsoft Learn](#)

## Download the Azure image file for Cloud Volumes ONTAP

You can download the Azure image file from the [NetApp Support Site](#).

The *tar.gz* file contains the files required for image signature verification. Along with the *tar.gz* file, you should also download the *checksum* file for the image. The checksum file contains the md5 and sha256 checksums of the *tar.gz* file.

### Steps

1. Go to the [Cloud Volumes ONTAP product page on the NetApp Support Site](#) and download the required

software version from the **Downloads** section.

2. On the Cloud Volumes ONTAP download page, click the downloadable file for the Azure image and download the *tar.gz* file.

## Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

[DOWNLOAD 9150P1\\_V\\_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9150P1\\_V\\_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9150P1\\_V\\_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

[DOWNLOAD 9150P1\\_V\\_NODAR\\_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9150P1\\_V\\_NODAR\\_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9150P1\\_V\\_NODAR\\_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP

[DOWNLOAD GCP-9-15-0P1\\_PKG.TAR.GZ \[7.49 KB\]](#)

[View and download checksums](#)

[DOWNLOAD AZURE-9-15-0P1\\_PKG.TAR.GZ \[7.64 KB\]](#)

[View and download checksums](#)

3. On Linux, run `md5sum AZURE-<version>_PKG.TAR.GZ`.

On macOS, run `sha256sum AZURE-<version>_PKG.TAR.GZ`.

4. Verify that the `md5sum` and `sha256sum` values match those in the downloaded Azure image.
5. On Linux and macOS, extract the *tar.gz* file using the `tar -xzf` command.

The extracted *tar.gz* file contains the digest (*.sig*) file, public key certificate (*.pem*) file, and chain certificate (*.pem*) file.

**Example output after extracting the *tar.gz* file:**

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp 384 May 13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May 13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 version_readme
```

## Export VHD images for Cloud Volumes ONTAP from the Azure marketplace

Once the VHD image is published to Azure cloud, it is no longer managed by NetApp. Instead, the published image is placed on the Azure marketplace. When the image is staged and published on the Azure marketplace, Azure modifies 1 MB at the beginning and 512 bytes at the end of the VHD. To verify the signature of the VHD file, you need to

export the VHD image modified by Azure from the Azure marketplace.

### Before you begin

Ensure that the Azure CLI is installed on your system, or the Azure Cloud Shell is available through the Azure portal. For more information about how to install the Azure CLI, refer to the [Microsoft documentation: How to install the Azure CLI](#).

### Steps

1. Map the Cloud Volumes ONTAP version on your system to the Azure marketplace image version using the contents of the *version\_readme* file. The Cloud Volumes ONTAP version is represented by *buildname* and the Azure marketplace image version is represented by *version* in the version mappings.

In the following example, the Cloud Volumes ONTAP version 9.15.0P1 is mapped to the Azure marketplace image version 9150.01000024.05090105. This Azure marketplace image version is later used to set the image URN.

```
[
  "buildname": "9.15.0P1",
  "publisher": "netapp",
  "version": "9150.01000024.05090105"
]
```

2. Identify the region where you want to create the VMs. The region name is used as the value for the *locName* variable when setting the URN of the marketplace image. To list the available regions, run this command:

```
az account list-locations -o table
```

In this table, the region name appears in the *Name* field.

```
$ az account list-locations -o table
DisplayName          Name                      RegionalDisplayName
-----
East US              eastus                    (US) East US
East US 2             eastus2                   (US) East US 2
South Central US     southcentralus            (US) South Central US
...
```

3. Review the SKU names for the corresponding Cloud Volumes ONTAP versions and VM deployment types in the table below. The SKU name is used as the value for the *skuName* variable when setting the URN of the marketplace image.

For example, all single node deployments with Cloud Volumes ONTAP 9.15.0 should use *ontap\_cloud\_byol* as the SKU name.

Cloud Volumes ONTAP version	VM deployment through	SKU name
9.17.1 and later	The Azure marketplace	ontap_cloud_direct_gen2
9.17.1 and later	The NetApp Console	ontap_cloud_gen2
9.16.1	The Azure marketplace	ontap_cloud_direct
9.16.1	The Console	ontap_cloud
9.15.1	The Console	ontap_cloud
9.15.0	The Console, single node deployments	ontap_cloud_byol
9.15.0	The Console, high availability (HA) deployments	ontap_cloud_byol_ha

4. After mapping the ONTAP version and Azure marketplace image, export the VHD file from the Azure marketplace using the Azure Cloud Shell or Azure CLI.

## Export VHD file using the Azure Cloud Shell on Linux

From the Azure Cloud Shell, export the marketplace image to the VHD file (for example, *9150.01000024.05090105.vhd*), and download it to your local Linux system. Perform these steps to get the VHD image from the Azure marketplace.

### Steps

1. Set the URN and other parameters of the marketplace image. The URN format is `<publisher>:<offer>:<sku>:<version>`. Optionally, you can list NetApp marketplace images to confirm the correct image version.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Create a new managed disk from the marketplace image with the matching image version:

```

PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference $urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600 --access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas

```

3. Export the VHD file from the managed disk to Azure Storage. Create a container with the appropriate access level. In this example, we've used a container named `vm-images` with Container access level. Get the storage account access key from the Azure portal: **Storage Accounts > *examplesaname* > Access Key > *key1* > key > Show > <copy>**

```

PS /home/user1> $storageAccountName = "examplesaname"
PS /home/user1> $containerName = "vm-images"
PS /home/user1> $storageAccountKey = "<replace with the above access key>"
PS /home/user1> $destBlobName = "9150.01000024.05090105.vhd"
PS /home/user1> $destContext = New-AzureStorageContext -StorageAccountName $storageAccountName -StorageAccountKey $storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS -DestContainer $containerName -DestContext $destContext -DestBlob $destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState -Container $containerName -Context $destContext -Blob $destBlobName

```

4. Download the generated image to your Linux system. Use the `wget` command to download the VHD file:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

The URL follows a standard format. For automation, you can derive the URL string as shown below. Alternatively, you can use the Azure CLI `az` command to get the URL.

Example URL:

<https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd>

5. Clean up the managed disk

```

PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName $diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName $diskName

```

## Export VHD file using the Azure CLI on Linux

Export the marketplace image to a VHD file using the Azure CLI from a local Linux system.

### Steps

1. Log in to the Azure CLI and list marketplace images:

```
% az login --use-device-code
```

2. To sign in, use a web browser to open the page <https://microsoft.com/devicelogin> and enter the authentication code.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
  "architecture": "x64",
  "offer": "netapp-ontap-cloud",
  "publisher": "netapp",
  "sku": "ontap_cloud_byol",
  "urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
  "version": "9150.01000024.05090105"
},
...
```

3. Create a new managed disk from the marketplace image with the matching image version.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```



To automate the process, the SAS needs to be extracted from the standard output. Refer to the appropriate documents for guidance.

4. Export the VHD file from the managed disk.

- a. Create a container with the appropriate access level. In this example, a container named `vm-images` with Container access level is used.
- b. Get the storage account access key from the Azure portal: **Storage Accounts > *examplesaname* > Access Key > *key1* > *key* > Show > <copy>**

You can also use the `az` command for this step.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS
--destination-container $containerName --account-name
$storageAccountName --account-key $storageAccountKey --destination
-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xxxxxxxxxxxxxxxxxxxx\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Check the status of the blob copy.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
  "copy": {
    "completionTime": null,
    "destinationSnapshot": null,
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
    "incrementalCopy": null,
    "progress": "10737418752/10737418752",
    "source": "https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  },
....
```

6. Download the generated image to your Linux server.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

The URL follows a standard format. For automation, you can derive the URL string as shown below. Alternatively, you can use the Azure CLI `az` command to get the URL.

Example URL:

<https://examplesaname.bluepinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd>

7. Clean up the managed disk

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

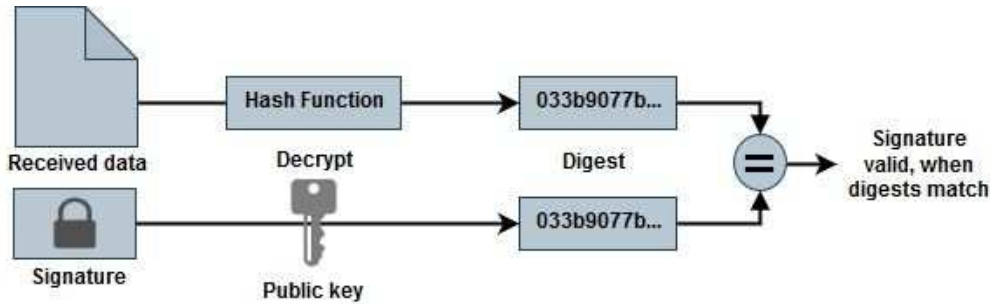
## Verify file signature

### Azure marketplace image signature verification for Cloud Volumes ONTAP

The Azure image verification process generates a digest file from the VHD file by stripping 1 MB at the beginning and 512 bytes at the end, then applying a hash function. To match the signing procedure, *sha256* is used for hashing.

## File signature verification workflow summary

The following is an overview of the file signature verification workflow process.



- Downloading the Azure image from the [NetApp Support Site](#) and extracting the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file. Refer to [Download the Azure image digest file](#) for more information.
- Verification of the chain of trust.
- Extracting the public key (.pub) from the public key certificate (.pem).
- Decrypting the digest file by using the extracted public key.
- Comparing the result against a newly generated digest of a temporary file created from the image file after removing 1 MB at the beginning and 512 bytes at the end. This step is performed by using the OpenSSL command line tool. The OpenSSL CLI tool displays appropriate messaging on success or failure in matching the files.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

## Verify Azure marketplace image signature for Cloud Volumes ONTAP on Linux

Verification of an exported VHD file signature on Linux includes validating the chain of trust, editing the file, and verifying the signature.

### Steps

1. Download the Azure image file from the [NetApp Support Site](#) and extract the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file.

Refer to [Download the Azure image digest file](#) for more information.

2. Verify the chain of trust.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remove 1 MB (1,048,576 bytes) at the beginning and 512 bytes at the end of the VHD file. When using tail, the -c +K option generates bytes from the Kth byte of the file. Therefore, it passes 1048577 to tail -c.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use OpenSSL to extract the public key from the certificate and verify the stripped file (sign.tmp) with the signature file and the public key.

The command prompt displays messages indicating success or failure based on the verification.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Clean up the workspace.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## Verify Azure marketplace image signature for Cloud Volumes ONTAP on macOS

Verification of an exported VHD file signature on Linux includes validating the chain of trust, editing the file, and verifying the signature.

### Steps

1. Download the Azure image file from the [NetApp Support Site](#) and extract the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file.

Refer to [Download the Azure image digest file](#) for more information.

2. Verify the chain of trust.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remove 1MB (1,048,576 bytes) at the beginning and 512 bytes at the end of the VHD file. When using tail, the -c +K option generates bytes from the Kth byte of the file. Therefore, it passes 1048577 to

`tail -c`. Note that on macOS, the tail command might take about ten minutes to complete.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use OpenSSL to extract the public key from the certificate and verify the stripped file (sign.tmp) with the signature file and public key. The command prompt displays messages indicating success or failure based on the verification.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0Pl_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Clean up the workspace.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## Copyright information

Copyright © 2026 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.