Table of Contents

Deploy Cloud Data Sense ................................................................. 1
  Deploy Cloud Data Sense in the cloud .......................................... 1
  Deploy Cloud Data Sense on your premises ..................................... 5
Deploy Cloud Data Sense

Deploy Cloud Data Sense in the cloud

Complete a few steps to deploy Cloud Data Sense in the cloud.

Note that you can also deploy Data Sense on your premises. The on-prem installation may be a good option if you prefer to scan on-premises ONTAP systems using a Data Sense instance that's also located on premises— but this is not a requirement. The software functions exactly the same way regardless of which installation method you choose.

Quick start

Get started quickly by following these steps, or scroll down to the remaining sections for full details.

1. Create a Connector

If you don’t already have a Connector, create a Connector in AWS, Azure, or GCP. See creating a Connector in AWS, creating a Connector in Azure, or creating a Connector in GCP.

You can also deploy the Connector on-premises on a Linux host in your network or in the cloud.

2. Review prerequisites

Ensure that your environment can meet the prerequisites. This includes outbound internet access for the instance, connectivity between the Connector and Cloud Data Sense over port 80, and more. See the complete list.

The default configuration requires 16 vCPUs for the Cloud Data Sense instance. See more details about the instance type.

3. Deploy Cloud Data Sense

Launch the installation wizard to deploy the Cloud Data Sense instance in the cloud.

4. Subscribe to the Cloud Data Sense service

The first 1 TB of data that Cloud Data Sense scans in Cloud Manager is free. A subscription to the AWS or Azure Marketplace, or a BYOL license from NetApp, is required to continue scanning data after that point.

Create a Connector

If you don’t already have a Connector, create a Connector in AWS, Azure, or GCP. See creating a Connector in AWS or creating a Connector in Azure, or creating a Connector in GCP. In most cases you will probably have a Connector set up before you attempt to activate Cloud Data Sense because most Cloud Manager features require a Connector, but there are cases where you’ll you need to set one up now.

There are some scenarios where you have to use a Connector that's deployed in a specific cloud provider:
When scanning data in Cloud Volumes ONTAP in AWS, Amazon FSx for ONTAP, or in AWS S3 buckets, you use a connector in AWS.

When scanning data in Cloud Volumes ONTAP in Azure or in Azure NetApp Files, you use a connector in Azure.

When scanning data in Cloud Volumes ONTAP in GCP, you use a Connector in GCP.

On-prem ONTAP systems, non-NetApp file shares, generic S3 Object storage, databases, and OneDrive folders can be scanned using any of these cloud Connectors.

Note that you can also deploy the Connector on-premises on a Linux host in your network or in the cloud. Some users planning to install Data Sense on-prem may also choose to install the Connector on-prem.

As you can see, there may be some situations where you need to use multiple Connectors.

If you’re planning on scanning Azure NetApp Files volumes, you need to make sure you’re deploying in the same region as the volumes you wish to scan.

Review prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you deploy Cloud Data Sense in the cloud.

Enable outbound internet access from Cloud Data Sense

Cloud Data Sense requires outbound internet access. If your virtual or physical network uses a proxy server for internet access, ensure that the Data Sense instance has outbound internet access to contact the following endpoints. When you deploy Data Sense in the cloud, it's located in the same subnet as the Connector.

Review the appropriate table below depending on whether you are deploying Cloud Data Sense in AWS, Azure, or GCP.

Required endpoints for AWS deployments:

<table>
<thead>
<tr>
<th>Endpoints</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a></td>
<td>Communication with the Cloud Manager service, which includes Cloud Central accounts.</td>
</tr>
<tr>
<td><a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a></td>
<td>Communication with NetApp Cloud Central for centralized user authentication.</td>
</tr>
<tr>
<td><a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a></td>
<td>Enables NetApp to stream data from audit records.</td>
</tr>
</tbody>
</table>
## Endpoints and Purpose

<table>
<thead>
<tr>
<th>Endpoints</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a></td>
<td>Enables Cloud Data Sense to access and download manifests and templates, and to send logs and metrics.</td>
</tr>
<tr>
<td><a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://user-feedback-store-prod.s3.us-west-2.amazonaws.com">https://user-feedback-store-prod.s3.us-west-2.amazonaws.com</a></td>
<td></td>
</tr>
</tbody>
</table>

### Required endpoints for Azure and GCP deployments:

<table>
<thead>
<tr>
<th>Endpoints</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a></td>
<td>Communication with the Cloud Manager service, which includes Cloud Central accounts.</td>
</tr>
<tr>
<td><a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> / auth0.com</td>
<td>Communication with NetApp Cloud Central for centralized user authentication.</td>
</tr>
<tr>
<td><a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a></td>
<td>Provides access to software images, manifests, templates, and to send logs and metrics.</td>
</tr>
<tr>
<td><a href="https://hub.docker.com">https://hub.docker.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://auth.docker.io">https://auth.docker.io</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://registry-1.docker.io">https://registry-1.docker.io</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://index.docker.io">https://index.docker.io</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://dseasb33srnrn.cloudfront.net/">https://dseasb33srnrn.cloudfront.net/</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> / auth0.com</td>
<td>Enables NetApp to stream data from audit records.</td>
</tr>
</tbody>
</table>

### Ensure that Cloud Manager has the required permissions

Ensure that Cloud Manager has permissions to deploy resources and create security groups for the Cloud Data Sense instance. You can find the latest Cloud Manager permissions in the policies provided by NetApp.

**Note:** If you created the Connector in GCP using Cloud Manager 3.9.10 or greater, then you’re all set. If you created the Connector using an earlier version, then you’ll need to add the following permissions to the GCP service account associated with the Connector to deploy Cloud Data Sense to GCP.

```markdown
compute.instances.addAccessConfig
compute.subnetworks.use
compute.subnetworks.useExternalIp
```

### Check your vCPU limits

Ensure that your cloud provider’s vCPU limit allows for the deployment of an instance with 16 cores. You’ll need to verify the vCPU limit for the relevant instance family in the region where Cloud Manager is running. See the required instance types.

See the following links for more details on vCPU limits:
Ensure that the Cloud Manager Connector can access Cloud Data Sense

Ensure connectivity between the Connector and the Cloud Data Sense instance. The security group for the Connector must allow inbound and outbound traffic over port 80 to and from the Data Sense instance.

This connection enables deployment of the Data Sense instance and enables you to view information in the Compliance and Governance tabs.

Ensure that you can keep Cloud Data Sense running

The Cloud Data Sense instance needs to stay on to continuously scan your data.

Ensure web browser connectivity to Cloud Data Sense

After Cloud Data Sense is enabled, ensure that users access the Cloud Manager interface from a host that has a connection to the Data Sense instance.

The Data Sense instance uses a private IP address to ensure that the indexed data isn’t accessible to the internet. As a result, the web browser that you use to access Cloud Manager must have a connection to that private IP address. That connection can come from a direct connection to your cloud provider (for example, a VPN), or from a host that's inside the same network as the Data Sense instance.

Deploy Data Sense in the cloud

Follow these steps to deploy an instance of Cloud Data Sense in the cloud.

Steps

1. In Cloud Manager, click Data Sense.
2. Click Activate Data Sense.
3. Click **Activate Data Sense** to start the cloud deployment wizard.

![Select where to deploy Data Sense](image)

4. The wizard displays progress as it goes through the deployment steps. It will stop and ask for input if it runs into any issues.

![Deploying Cloud Data Sense](image)

5. When the instance is deployed, click **Continue to configuration** to go to the **Configuration** page.

**Result**
Cloud Manager deploys the Cloud Data Sense instance in your cloud provider.

**What's Next**
From the Configuration page you can select the data sources that you want to scan.

You can also set up licensing for Cloud Data Sense at this time. You will not be charged until the amount of data exceeds 1 TB.

**Deploy Cloud Data Sense on your premises**
Complete a few steps to deploy Cloud Data Sense on a host in an on-premises site that has internet access.

Note that you can also deploy Data Sense in the cloud.

The on-prem installation may be a good option if you prefer to scan on-premises ONTAP systems using a Data Sense instance that's also located on premises — but this is not a requirement. The software functions exactly
the same way regardless of which installation method you choose.

**Quick start**

Get started quickly by following these steps, or scroll down to the remaining sections for full details.

[Number 1] Create a Connector

If you don’t already have a Connector, create a Connector in AWS, Azure or GCP. See creating a Connector in AWS, creating a Connector in Azure, or creating a Connector in GCP.

You can also deploy the Connector on-premises on a Linux host in your network or in the cloud.

[Number 2] Review prerequisites

Ensure that your environment can meet the prerequisites. This includes outbound internet access for the instance, connectivity between the Connector and Cloud Data Sense over port 80, and more. See the complete list.

You also need a Linux system that meets the following requirements.

[Number 3] Deploy Cloud Data Sense

Download the Cloud Data Sense software from the NetApp Support Site and copy the installer file to the Linux host you plan to use. Then launch the installation wizard and follow the prompts to deploy the Cloud Data Sense instance.

[Number 4] Subscribe to the Cloud Data Sense service

The first 1 TB of data that Cloud Data Sense scans in Cloud Manager is free. A subscription to the AWS or Azure Marketplace, or a BYOL license from NetApp, is required to continue scanning data after that point.

**Create a Connector**

If you don’t already have a Connector, create a Connector in AWS, Azure, or GCP. See creating a Connector in AWS or creating a Connector in Azure, or creating a Connector in GCP. In most cases you will probably have a Connector set up before you attempt to activate Cloud Data Sense because most Cloud Manager features require a Connector, but there are cases where you'll you need to set one up now.

There are some scenarios where you have to use a Connector that’s deployed in a specific cloud provider:

- When scanning data in Cloud Volumes ONTAP in AWS, Amazon FSx for ONTAP, or in AWS S3 buckets, you use a connector in AWS.
- When scanning data in Cloud Volumes ONTAP in Azure or in Azure NetApp Files, you use a connector in Azure.
- When scanning data in Cloud Volumes ONTAP in GCP, you use a connector in GCP.

On-prem ONTAP systems, non-NetApp file shares, generic S3 Object storage, databases, and OneDrive folders can be scanned using any of these cloud Connectors.

Note that you can also deploy the Connector on-premises on a Linux host in your network or in the cloud. Some users planning to install Data Sense on-prem may also choose to install the Connector on-prem.

As you can see, there may be some situations where you need to use multiple Connectors.
If you’re planning on scanning Azure NetApp Files volumes, you need to make sure you’re deploying in the same region as the volumes you wish to scan.

Review prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you deploy Cloud Data Sense on a Linux system.

Enable outbound internet access from Cloud Data Sense

Cloud Data Sense requires outbound internet access. If your virtual or physical network uses a proxy server for internet access, ensure that the Data Sense instance has outbound internet access to contact the following endpoints.

<table>
<thead>
<tr>
<th>Endpoints</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a></td>
<td>Communication with the Cloud Manager service, which includes Cloud Central accounts.</td>
</tr>
<tr>
<td><a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a></td>
<td>Communication with NetApp Cloud Central for centralized user authentication.</td>
</tr>
<tr>
<td><a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a></td>
<td>Provides access to software images, manifests, templates, and to send logs and metrics.</td>
</tr>
<tr>
<td><a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a></td>
<td>Enables NetApp to stream data from audit records.</td>
</tr>
</tbody>
</table>

Ensure that Cloud Manager has the required permissions

Ensure that Cloud Manager has permissions to deploy resources and create security groups for the Cloud Data Sense instance. You can find the latest Cloud Manager permissions in the policies provided by NetApp.

Note: If you created the Connector in GCP using Cloud Manager 3.9.10 or greater, then you’re all set. If you created the Connector using an earlier version, then you’ll need to add the following permissions to the GCP service account associated with the Connector to deploy Cloud Data Sense to GCP.
Ensure that the Cloud Manager Connector can access Cloud Data Sense

Ensure connectivity between the Connector and the Cloud Data Sense instance. The security group for the Connector must allow inbound and outbound traffic over port 80 to and from the Data Sense instance.

This connection enables deployment of the Data Sense instance and enables you to view information in the Compliance and Governance tabs.

Ensure that you can keep Cloud Data Sense running

The Cloud Data Sense instance needs to stay on to continuously scan your data.

Ensure web browser connectivity to Cloud Data Sense

After Cloud Data Sense is enabled, ensure that users access the Cloud Manager interface from a host that has a connection to the Data Sense instance.

The Data Sense instance uses a private IP address to ensure that the indexed data isn’t accessible to the internet. As a result, the web browser that you use to access Cloud Manager must have a connection to that private IP address. That connection can come from a direct connection to your cloud provider (for example, a VPN), or from a host that’s inside the same network as the Data Sense instance.

Deploy Data Sense on premises

For typical configurations you’ll install the software on a single host system. For very large configurations where you’ll be scanning petabytes of data, you can include additional hosts as scanner nodes to provide additional processing power.

Upgrades to Data Sense software is automated as long as the instance has internet connectivity.

Cloud Data Sense is currently unable to scan S3 buckets, Azure NetApp Files, or FSx for ONTAP when the software is installed on premises. In these cases you’ll need to deploy a separate Connector and instance of Data Sense in the cloud and switch between Connectors for your different data sources.

Host requirements

- Operating system: Red Hat Enterprise Linux or CentOS version 8.0 or 8.1
  - Version 7.8 can be used, but the Linux kernel version must be 4.14 or greater
  - The OS must be capable of installing the docker engine (for example, disable the firewalld service if needed)
- RAM: 64 GB (swap memory must be disabled on the host)
- CPU: 16 cores
- Disk: 500 GB SSD

Note that you can deploy Data Sense on a system with fewer CPUs and less RAM, but there are limitations when using these systems. See Using a smaller instance type for details.
• A Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it’s not registered, the system can’t access repositories to update required 3rd party software during installation.
• Make sure port 8080 is open so you can see the installation progress in Cloud Manager.
• Root privileges are required to install Cloud Data Sense.

See Reviewing prerequisites for the full list of requirements and endpoints that Cloud Data Sense must be able to reach over the internet.

Single-host installation for typical configurations

Follow these steps when installing Data Sense software on a single on-premises host.

Steps
1. Download the Cloud Data Sense software from the NetApp Support Site.
2. Copy the installer file to the Linux host you plan to use (using `scp` or some other method).
3. In Cloud Manager, click Data Sense.
4. Click Activate Data Sense.
5. Click Activate Data Sense to start the on-prem deployment wizard.
6. In the *Deploy Data Sense On Premises* dialog, copy the provided command and paste it in a text file so you can use it later, and click **Close**. For example:

```
sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq
```

7. Unzip the installer file on the host machine:

```
tar -xzf cc_onprem_installer.tar.gz
```

8. When prompted by the installer, you can enter the required values in a series of prompts, or you can enter the complete command in the first prompt:

<table>
<thead>
<tr>
<th>Enter parameters as prompted:</th>
<th>Enter the full command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Paste the information you copied from step 6:</td>
<td>Alternatively, you can create the whole command in advance and enter it in the first prompt:</td>
</tr>
<tr>
<td>sudo ./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt;</td>
<td>sudo ./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt; --host &lt;ds_host&gt; --cm-host &lt;cm_host&gt; --proxy-host &lt;proxy_host&gt; --proxy-port &lt;proxy_port&gt; --proxy-scheme &lt;proxy_scheme&gt; --proxy-user &lt;proxy_user&gt; --proxy-password &lt;proxy_password&gt;</td>
</tr>
<tr>
<td>2. Enter the IP address or host name of the Data Sense host machine so it can be accessed by the Connector instance.</td>
<td></td>
</tr>
<tr>
<td>3. Enter the IP address or host name of the Cloud Manager Connector host machine so it can be accessed by the Data Sense instance.</td>
<td></td>
</tr>
<tr>
<td>4. Enter proxy details as prompted. If your Cloud Manager already uses a proxy, there is no need to enter this information again here since Data Sense will automatically use the proxy used by Cloud Manager.</td>
<td></td>
</tr>
</tbody>
</table>

Variable values:

- **account_id** = NetApp Account ID
- **agent_id** = Connector ID
- **token** = jwt user token
- **ds_host** = IP address or host name of the Data Sense Linux system.
- **cm_host** = IP address or host name of the Cloud Manager Connector system.
- **proxy_host** = IP or host name of the proxy server if the host is behind a proxy server.
- **proxy_port** = Port to connect to the proxy server (default 80).
- **proxy_scheme** = Connection scheme: https or http (default http).
- **proxy_user** = Authenticated user to connect to the proxy server, if basic authentication is required.
- **proxy_password** = Password for the user name that you specified.

**Result**

The Cloud Data Sense installer installs packages, installs docker, registers the installation, and installs Data Sense. Installation can take 10 to 20 minutes.

If there is connectivity over port 8080 between the host machine and the Connector instance, you will see the installation progress in the Data Sense tab in Cloud Manager.
What's Next
From the Configuration page you can select the data sources that you want to scan.

You can also set up licensing for Cloud Data Sense at this time. You will not be charged until the amount of data exceeds 1 TB.

Multi-host installation for large configurations
Follow these steps when installing Data Sense software on multiple on-premises hosts.

When using multiple host systems, the primary system is called the Manager node and the additional systems that provide extra processing power are called Scanner nodes.

Requirements
• See Reviewing prerequisites for the full list of requirements and endpoints that Cloud Data Sense must be able to reach over the internet.
• The host requirements are the same for Scanner nodes as they are for Manager nodes. See Host requirements for details.
• You must have the IP addresses of the scanner node hosts that you plan to use.
• The following ports and protocols must be enabled on all hosts:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2377</td>
<td>TCP</td>
<td>Cluster management communications</td>
</tr>
<tr>
<td>7946</td>
<td>TCP, UDP</td>
<td>Inter-node communication</td>
</tr>
<tr>
<td>4789</td>
<td>UDP</td>
<td>Overlay network traffic</td>
</tr>
<tr>
<td>50</td>
<td>ESP</td>
<td>Encrypted IPsec overlay network (ESP) traffic</td>
</tr>
<tr>
<td>111</td>
<td>TCP, UDP</td>
<td>NFS Server for sharing files between the hosts (needed from each scanner node to manager node)</td>
</tr>
<tr>
<td>2049</td>
<td>TCP, UDP</td>
<td>NFS Server for sharing files between the hosts (needed from each scanner node to manager node)</td>
</tr>
</tbody>
</table>

Steps
1. Follow steps 1 through 7 from the Single-host installation on the manager node.
2. As shown in step 8, when prompted by the installer, you can enter the required values in a series of prompts, or you can enter the complete command in the first prompt.

In addition to the variables available for a single-host installation, a new option -n <node_ip> is used to specify the IP addresses of the scanner nodes. Multiple scanner node IPs are separated by a comma.

For example, this command adds 3 scanner nodes:
sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --cm-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password>

3. Before the manager node installation completes, a dialog displays the installation command needed for the scanner nodes. Copy the command and save it in a text file. For example:
sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212

4. On each scanner node host:
   a. Copy the Data Sense installer file (cc_onprem_installer.tar.gz) to the host machine (using `scp` or some other method).
   b. Unzip the installer file.
   c. Paste and execute the command that you copied in step 3.

   When the installation finishes on all scanner nodes and they have been joined to the manager node, the manager node installation finishes as well.

**Result**
The Cloud Data Sense installer finishes installing packages, docker, and registers the installation. Installation can take 10 to 20 minutes.

**What’s Next**
From the Configuration page you can select the data sources that you want to scan.

You can also set up licensing for Cloud Data Sense at this time. You will not be charged until the amount of data exceeds 1 TB.
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.