



Solution Brief

PostgreSQL Database as a Service (DBaaS) with Astra Control

Simplified day 2 operations

January 2022

TABLE OF CONTENTS

Introduction	3
NetApp Astra Control overview	4
Managing PostgreSQL with Astra	4
Migrating PostgreSQL application to another cloud provider	8
Summary	10
Where can I learn more?	10
About NetApp.....	10
Legal Notice	11

Introduction

Kubernetes has become the standard IT infrastructure for businesses of all sizes. Production applications are being deployed on or migrated to Kubernetes.

Running a stateful application like PostgreSQL requires lots of planning, understanding the challenges, and identifying the right solutions. Do-it-yourself will result you to take the entire responsibility for building the database, setting up the backup and disaster recovery strategies. More Importantly to identify the way to do entire application portability.

The journey of implementing DBaaS for PostgreSQL requires the following actions on day 1, whether it's

a managed Kubernetes service or vanilla Kubernetes:

1. Identify or build your own registry.
2. Identify the right storage and the Container Storage Interface (CSI) provisioner.
3. Find the performance requirements and define appropriate storage classes.
4. Create your own manifest or identify a helm chart that meets your requirements.

Deploy the PostgreSQL application

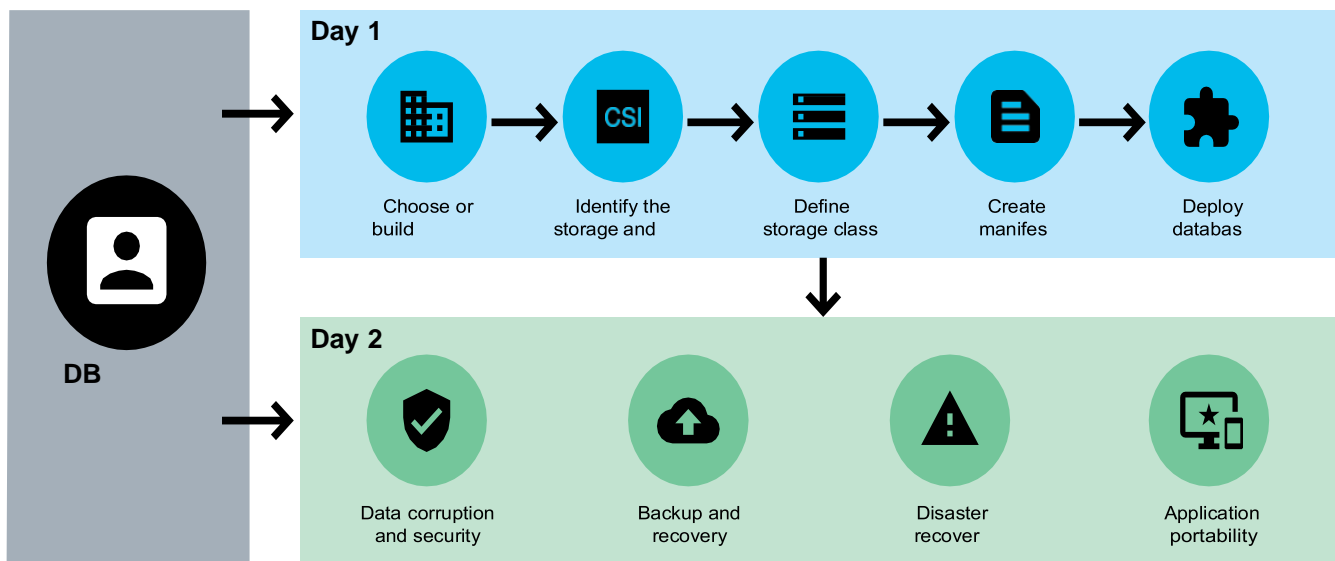


Figure 1) Build your own DBaaS.

Kubernetes offers solutions for all day 1 requirements. When it comes to day 2 operations, you need a strategy and solution for:

1. Data corruption and security
2. Backup and recovery
3. Disaster recovery

4. Application portability

Kubernetes natively doesn't have any solutions to address the day 2 challenges.

Astra Control simplifies and automates the day 1 operations by simply registering the Kubernetes cluster. The day 1 operations are simplified to

1. Identify or build your own registry.
2. Create your own manifest or identify a helm chart that meets your requirements.
3. Register the Kubernetes cluster with Astra.
4. Deploy the PostgreSQL application

Astra Control managing your application addresses the following day 2 challenges

1. Data corruption and security
2. Backup and recovery
3. Disaster recovery
4. Application portability

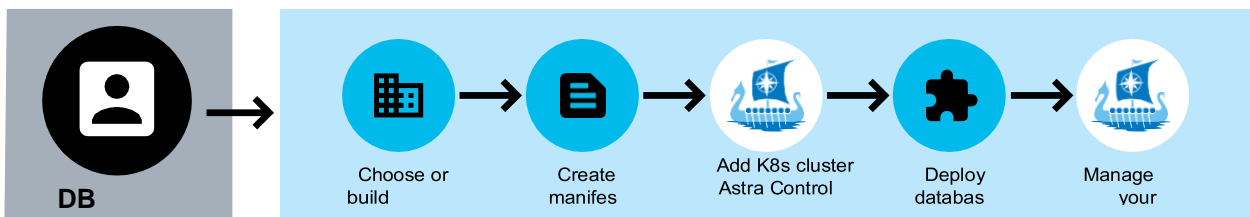


Figure 2) Day 1 operations with Astra.

NetApp Astra Control overview

NetApp Astra Control is an application-aware data management solution that manages, protects, and moves data-rich Kubernetes workloads in both public clouds and on-premises. Astra Control enables data protection, disaster recovery, and migration for your Kubernetes workloads leveraging NetApp's industry-leading data management technology for snapshots, backups, replication, and cloning. NetApp Astra Control is available in two deployment models:

- NetApp Astra Control Service: A NetApp-managed service that provides application-aware data management of Kubernetes clusters in Google Kubernetes Engine (GKE) and Azure Kubernetes Service (AKS).
- NetApp Astra Control Center: Self-managed software that provides application-aware data management of Kubernetes clusters running in your on-premises environment.

Managing PostgreSQL with Astra

Astra Control Service (ACS) provides management, protection, and cloning for Google Kubernetes Engine (GKE) or Azure Kubernetes Service (AKS) clusters located in the public cloud. Astra Control

Center (ACC) provides the same experience and functionality for RedHat Openshift Container Platform (OCP), Rancher or Upstream Kubernetes clusters located on-premises.

Upon adding a cluster, ACS:

- Installs NetApp® Trident, NetApp's open-source Kubernetes storage orchestrator.
- Creates a bucket on the cloud object store for saving application backups.
- Creates a service account on your cluster for itself.

ACC on premises (supported with Redhat OpenShift Container Platform, Rancher and Upstream Kubernetes) uses your current Trident installation, Trident based Storage classes for ONTAP backend and allows you to add your own object storage bucket for backups.

The following example shows two Kubernetes clusters, one AKS (Azure Kubernetes Service) cluster located in Azure East US (Virginia) region and another GKE (Google Kubernetes Engine) cluster located in the GCP europe-west2 region.

Name	Ready	Type	Version	Location	Actions
longboat-cluster-1	✓	Azure Kubernetes Service	v1.21.7	eastus	Running
longboat-cluster-2	✓	Google Kubernetes Engine	v1.21.5-gke.1302	europe-west2-a	Running

Figure 3) Registered kubernetes clusters.

After your Kubernetes cluster is registered, install PostgreSQL on cluster longboat-cluster-2 using the current Bitnami Helm chart or a custom manifest. Trident automatically provisions the Kubernetes Persistent Volume Claims from Cloud Volume Services GCP for PostgreSQL. Astra Control discovers the applications on your registered clusters, and you can easily manage either just the application, all the resources in the entire namespace as one unit or a custom group based on kubernetes labels.

Name	Ready	Cluster	Group	Discovered	Actions
ns-postgres	✓	longboat-cluster-2	ns-postgres	2022/01/20 22:13 UTC	Unmanaged
app-postgres-postgresql	✓	longboat-cluster-2	ns-postgres # app.kubernetes.io/name: postgresql	2022/01/20 22:13 UTC	Manage Ignore

Figure 4) Managing the PostgreSQL application.

After managing the application, Astra Control can take snapshots, backups, and clones of that application, its Kubernetes resources, and its associated Persistent Volumes.

ns-postgres Running

APPLICATION STATUS: Healthy

APPLICATION PROTECTION STATUS: Unprotected

Images: docker.io/bitnami/postgresql:11.11.0-debian-10-r62

Protection schedule: Disabled

Group: ns-postgres

Cluster: longboat-cluster-2

Kubernetes Objects

Overview Data protection Storage **Resources** Execution hooks Activity

All types 1-10 of 10 entries

Resource	Type	UID	Created
kube-root-ca.crt	ConfigMap	e93b0dde-6b32-4c74-91ef-943bccef2aee	2022/01/20 22:12 UTC
data-app-postgres-postgresql-0 # app.kubernetes.io/instance: app-postgres +2	PersistentVolumeClaim	70050f30-fe48-44b5-84ed-c93fd13d0870	2022/01/20 22:12 UTC
app-postgres-postgresql-0 # controller-revision-hash: app-postgres-postgresql-859dd5d6c +7	Pod	087c01bc-c843-4128-9de9-c1a9ed54b4b3	2022/01/20 22:12 UTC
default-token-m4zrw	Secret	c5ab10bd-9cba-4c68-a18d-65d7fe4830ac	2022/01/20 22:12 UTC
app-postgres-postgresql # app.kubernetes.io/instance: app-postgres +3	Secret	db39a09d-1bcd-4a97-8345-8640e13fa635	2022/01/20 22:12 UTC
sh.helm.release.v1.app-postgres.v1 # version: 1 +4	Secret	ead48c6f-ab65-436a-8fc5-d64313eca563	2022/01/20 22:12 UTC
app-postgres-postgresql-headless # app.kubernetes.io/instance: app-postgres +4	Service	7364f36e-3543-430c-b9ce-59ca44e17948	2022/01/20 22:12 UTC

Figure 6) Kubernetes objects of managed PostgreSQL application.

All the data generated by PostgreSQL database clients can be automatically protected by using snapshots and backups. Astra Control snapshots and backups preserve the application state, its Kubernetes resources, and its volumes in one easily manageable unit. PostgreSQL and other stateful applications benefit from application consistent snapshots and backups. In built Pre and Post execution hooks in Astra Control provide the ability to perform application aware backups for PostgreSQL.

NetApp Astra Control supports both on-demand and scheduled snapshots and backups. When using execution hooks, the pre-snapshot script will run first before taking any snapshot or backup. When taking on-demand backups, you have the option to choose any existing snapshot. Otherwise, the backup will be created from the application's current state (from a new snapshot). Astra Control application backups are always saved in an external object store. You can choose a different object store when Astra Control has more than one object store configured.

ns-postgres Running

APPLICATION STATUS: Healthy

APPLICATION PROTECTION STATUS: Unprotected

Images: docker.io/bitnami/postgresql:11.11.0-debian-10-r62

Protection schedule: Disabled

Group: ns-postgres

Cluster: longboat-cluster-2

Astra Control inbuilt execution hook scripts for PostgreSQL

Overview Data protection Storage Resources **Execution hooks** Activity

Actions + Add new hook 1-2 of 2 entries

Hook name	Script name	Container image matches	Source	Type	Created	Script file checksum	Actions
NetApp-PostgreSQL-post-snapshot	NetApp-PostgreSQL.sh	docker.io/bitnami/postgresql:11.11.0-debian-10-r62	NetApp	Post-snapshot	2021/12/14 19:34 UTC	89bfca8522e9301d709cdc5f90c8a1f0	Enabled
NetApp-PostgreSQL-pre-snapshot	NetApp-PostgreSQL.sh	docker.io/bitnami/postgresql:11.11.0-debian-10-r62	NetApp	Pre-snapshot	2021/12/14 19:34 UTC	89bfca8522e9301d709cdc5f90c8a1f0	Enabled

Figure 7) Astra Control inbuilt pre and post snapshot execution hooks for PostgreSQL

Snapshot application STEP 1/2: DETAILS

SNAPSHOT DETAILS

Name
ns-postgres-snapshot-20220120222431

Can also provide custom snapshot name

CREATING APPLICATION SNAPSHOTS

Astra Control can take a quick snapshot of your application configuration and persistent storage. Enter a snapshot name to get started.

Read more in [Protect apps](#)

Application
ns-postgres

Namespace
ns-postgres

Cluster
longboat-cluster-2

Cancel Next

Figure 8) On-demand application snapshot.

Activity

Export to CSV

All managed applications All severity All users Time range

1-25 of 490 entries

Activity

Execution hook scripts are executed before and after a snapshot

Activity	Severity	Source	User	Occurred
Post-snapshot execution hook 'NetApp-PostgreSQL-post-snapshot' succeeded	Informational	nautilus	Jaimeon George	2022/01/20 22:26 UTC
Post-snapshot execution hook 'NetApp-PostgreSQL-post-snapshot' started	Informational	nautilus	Jaimeon George	2022/01/20 22:26 UTC
Pre-snapshot execution hook 'NetApp-PostgreSQL-pre-snapshot' succeeded	Informational	nautilus	Jaimeon George	2022/01/20 22:26 UTC
Pre-snapshot execution hook 'NetApp-PostgreSQL-pre-snapshot' started	Informational	nautilus	Jaimeon George	2022/01/20 22:25 UTC

Figure 9) Running Pre and Post Execution hooks

Backup application STEP 1/2: DETAILS

BACKUP DETAILS

Name
ns-postgres-backup-20220120222939

To select existing snapshots

Backup from an existing snapshot

BACKUP DESTINATION

Bucket
astra-6cb378a8-d3ab-4b9d-a140-a01ee3d9e0a1-backup - astra-6cb378a8-d3ab-4b9d-a140-a01ee3d9e0a1-backup Available Default

Optionally choose another object store

CREATING APPLICATION BACKUPS

Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

Read more in [Application backups](#)

Application
ns-postgres

Namespace
ns-postgres

Cluster
longboat-cluster-2

Cancel Next

Figure 9) On-demand application backup.

Set up a snapshot and backup schedule and retention policy for the snapshots and backups.

Configure protection policy STEP 1/2: DETAILS

PROTECTION SCHEDULE

Hourly: Every hour on the 30th minute, keep the last 4 snapshots, keep the last backup

Daily: Daily at 04:00 (UTC), keep the last snapshot, keep the last backup

Weekly: Weekly on Mondays at 04:00 (UTC), keep the last snapshot, keep the last backup

Monthly: Every 1st of the month at 04:00 (UTC), keep the last snapshot, keep the last backup

● Hourly ● Daily ● Weekly ● **Monthly**

Days(s) of Month (optional): 1 x

Time (UTC) (optional): 04:00

Snapshots to keep: 1

Backups to keep: 1

BACKUP DESTINATION

Bucket: astra-6cb378a8-d3ab-4b9d-a140-a01ee3d9e0a1-backup - astra-6cb378a8-d3ab-4b9d-a140-a01ee3d9e0a1-backup Available Default

Optionally you can choose alternate backup location

CONFIGURING PROTECTION POLICIES

Define a policy to continuously protect your application on a schedule and configure a retention count to get started.

For select stateful applications, expect I/O to pause for a short time during a backup or snapshot operation.

Read more in [Protection policies](#)

Application: ns-postgres

Namespace: ns-postgres

Cluster: longboat-cluster-2

Cancel Next →

Figure 10) Configure protection policy.

After reviewing the information, set the protection policy. Astra Control automatically takes snapshots and backups based on the schedule and follows the retention policy defined.

Migrating PostgreSQL application to another cloud provider

After a successful backup, the PostgreSQL application is protected against disasters like losing the Kubernetes cluster or a human error like deleting the namespace. You can use the Clone option to redeploy PostgreSQL to a new namespace within the cluster or to the new cluster. When choosing the option, you can also select an existing snapshot or backup to go back to a point in time copy of the PostgreSQL application.

```
postgres=#
postgres=#
postgres=# \l

```

Name	Owner	Encoding	Collate	Ctype	Access privileges
locations	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	
postgres	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	
template0	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	=c/postgres postgres=CTc/postgres +
template1	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	=c/postgres postgres=CTc/postgres +

```

(4 rows)

postgres=# \c locations;
You are now connected to database "locations" as user "postgres".
locations=#
locations=# \d

```

Schema	Name	Type	Owner
public	attractions	table	postgres

```

(1 row)

locations=#
locations=# select * from attractions;

```

city	attractions	country
Amsterdam	canals	Netherlands

```

(1 row)

locations=#

```

Figure 11) Test database in PostgreSQL application

Clone PostgreSQL to longboat-cluster-1, in Azure region, east-us using its current state. You could also clone from an existing backup or snapshot. When cloning from the current state, Astra Control first creates a backup and then uses that backup for migrating to the destination cluster. This brings up a new instance of PostgreSQL, running at the same state as in the source kubernetes cluster.

For example, suppose that you have a new team in a different location that is going to take over the responsibility of managing the PostgreSQL database. But they are using Azure Subscription to run the application. You want to migrate the PostgreSQL applications to an AKS cluster that's using the new team. PostgreSQL is currently running on the longboat-cluster-2 (GKE) cluster located in the EU-WEST-2 (London) region.

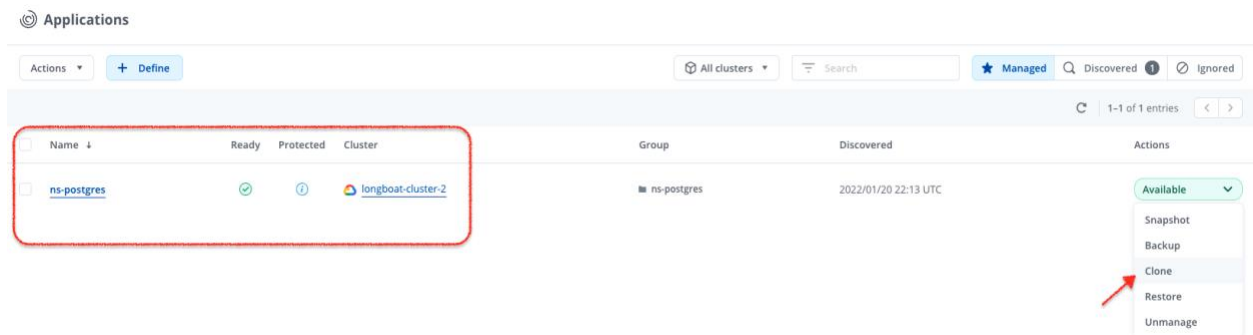


Figure 12a) Migrating PostgreSQL from the current state.

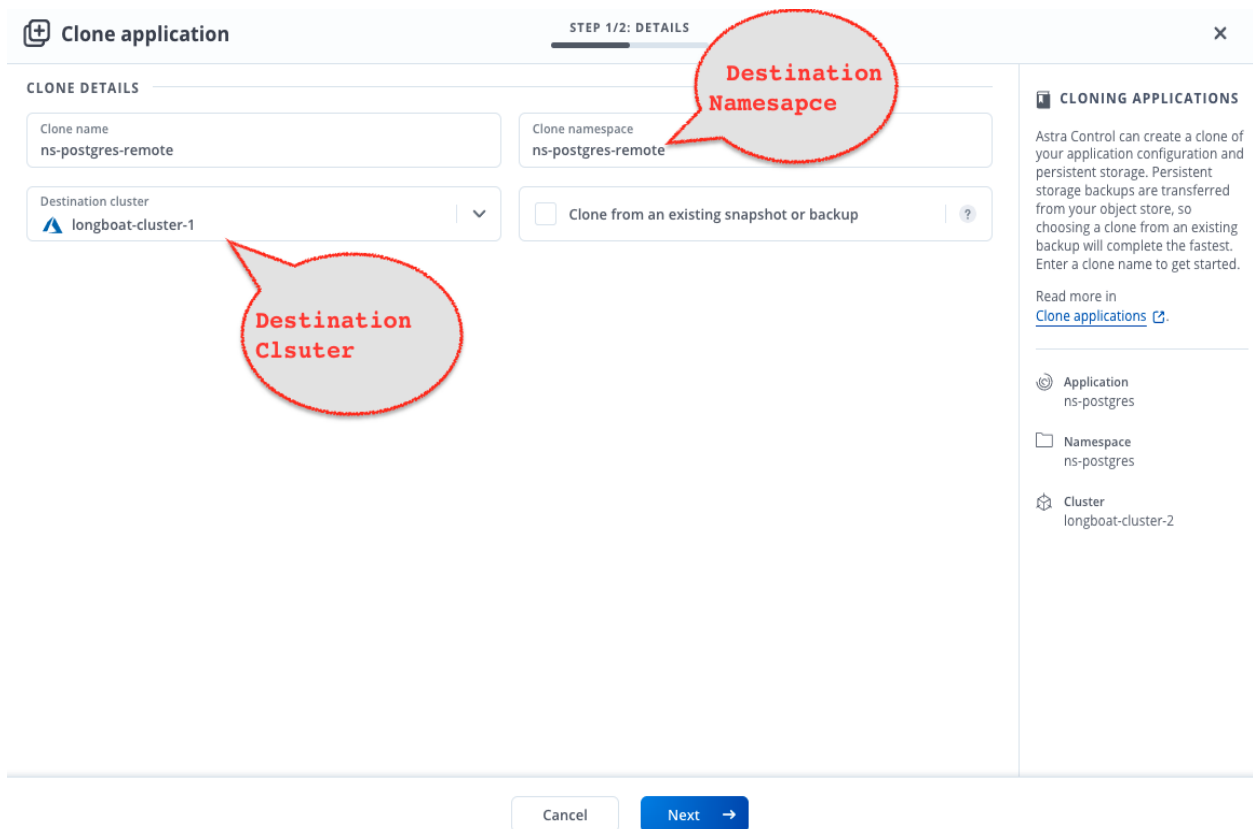


Figure 11b) Migrating PostgreSQL from the current state.

A new PostgreSQL clone is provisioned in the destination AKS cluster, and the application is automatically managed by Astra Control.

Name	Ready	Protected	Cluster	Group	Discovered	Actions
ns-postgres	✓	ⓘ	longboat-cluster-2	ns-postgres	2022/01/20 22:13 UTC	Available
ns-postgres-remote	✓	⚠	longboat-cluster-1	ns-postgres-remote	2022/01/20 23:08 UTC	Available

Figure 13) PostgreSQL migrated to the destination cluster.

After the migration, the PostgreSQL application has the same Kubernetes resources and data as in the source cluster.

Summary

This solution guide provided a step-by-step guide for validating the following key benefits NetApp Astra Control provides to PostgreSQL:

- Automatic storage provisioning and Storage Class setup
- Rich set of application-aware data management functionality (snapshot revert, backup and restore, activity log, and active cloning) for data protection, disaster recovery, data audit, and migration use-cases.
- Consistent data management UI.
- Clear visualization of data protection status.
- Simple data protection management.
- Seamless portability and migration.

Start your free trial of NetApp Astra Control today by registering at <https://cloud.netapp.com/astra-register>.

Where can I learn more?

To learn more, visit the NetApp Astra [website](#) and the [documentation](#).

About NetApp

In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of the cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify, and connect your cloud, and securely deliver the right data, services, and applications to the right people — anytime, anywhere.

Legal Notice

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).

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.