



# **Integrate Protection into CI/CD Pipelines with NetApp Astra Control**

NetApp Solutions

NetApp  
October 20, 2023

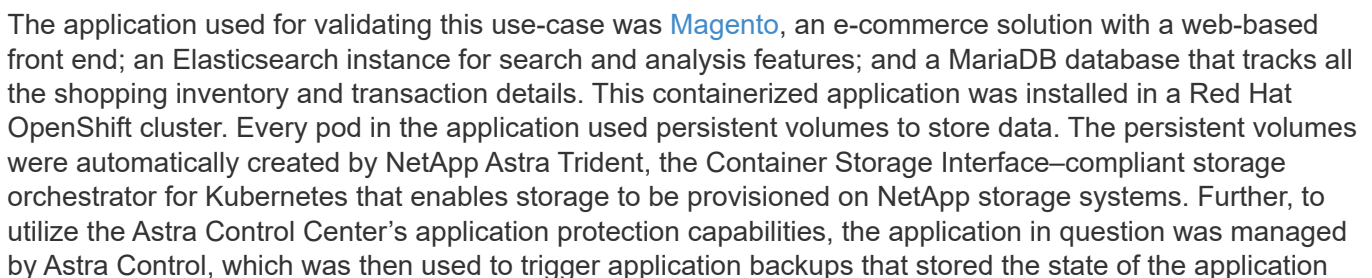
This PDF was generated from [https://docs.netapp.com/us-en/netapp-solutions/containers/devops\\_with\\_netapp/dwn\\_use\\_case\\_integrated\\_data\\_protection.html](https://docs.netapp.com/us-en/netapp-solutions/containers/devops_with_netapp/dwn_use_case_integrated_data_protection.html) on October 20, 2023. Always check docs.netapp.com for the latest.

# Table of Contents

- Integrate Protection into CI/CD Pipelines with NetApp Astra Control ..... 1
  - Overview ..... 1
  - Use-case validation prerequisites ..... 2
  - Installing the application ..... 2
  - Manage the Magento application in Astra Control Center ..... 3
  - CI/CD pipeline with integrated protection ..... 3

# Overview

In this use case, we take a closer look at a promotion-to-production pipeline that deploys a new version of an application: first into a staging environment and then into a production environment. This example applies equally to the major public clouds and also to an on-premises environment. Although we show the deployment of one version of the app, the pipeline can also be used with other strategies, such as blue/green or canary deployment. As part of the CI/CD pipeline, we're going to protect the application by creating a complete application backup. An application-aware backup of the in-production application and its data, state, and configuration can be useful for numerous DevOps workflows.



along with the data held in persistent volumes. We used the [NetApp Astra Control Python SDK](#) to automate the process of triggering application backups, which was then introduced into a CI/CD pipeline. This pipeline was created and executed using a popular CI/CD tool called [[Jenkins](#)] to automate the flow to build, protect, and deploy the application.

Let us run through the prerequisites and procedure to introduce protection in a CI/CD pipeline.

## Use-case validation prerequisites

The following tools or platforms were deployed and configured as prerequisites:

1. Red Hat OpenShift Container Platform
2. NetApp Astra Trident installed on OpenShift with a backend to NetApp ONTAP system configured
3. A default storageclass configured, pointing to a NetApp ONTAP backend
4. NetApp Astra Control Center installed on an OpenShift cluster
5. OpenShift cluster added as a managed cluster to Astra Control Center
6. Jenkins installed on an OpenShift cluster and configured with an agent node with a Docker engine installed on it

## Installing the application

Let's start with the initial installation of the application in the staging and production environments. For the purpose of this use case, this step is a prerequisite, so it is performed manually. The CI/CD pipeline is used for subsequent build and deploy workflows as a result of new version releases of the application.

The production environment in this use case is a namespace called `magento-prod`, and the corresponding staging environment is a namespace called `magento-staging` configured on the Red Hat OpenShift cluster. To install the application, complete the following steps:

1. Install the Magento application using bitnami helm chart on the production environment. We use RWX PVs for Magento and Mariadb pods.

```
[netapp-user@rhel7 na_astra_control_suite]$ helm install --version 14
magento bitnami/magento -n magento-prod --create-namespace --set
image.tag=2.4.1-debian-10-
r11,magentoHost=10.63.172.243,persistence.magento.accessMode=ReadWriteMa
ny,persistence.apache.accessMode=ReadWriteMany,mariadb.master.persistenc
e.accessModes[0]=ReadWriteMany
```



Magento bitnami helm chart requires a LoadBalancer service to expose the Magento GUI service. We used [MetalLB](#) for providing an on-prem load balancer service in this example.

2. After a few minutes, verify that all pods and services are running.


```
[netapp-user@rhel7 na_astra_control_suite]$ oc get pods -n magento-prod
```


NAME	READY	STATUS
magento-9d658fd96-grxmt	1/1	Running
magento-elasticsearch-coordinating-only-69869cc5-768rm	1/1	Running
magento-elasticsearch-data-0	1/1	Running
magento-elasticsearch-master-0	1/1	Running
magento-mariadb-0	1/1	Running


3. Repeat the same procedure for the staging environment.


## Manage the Magento application in Astra Control Center


1. Navigate to Applications and select the Discovered applications tab.
2. Click the ellipsis against the Magento application in the production environment (magento-prod), and click Manage.
3. The Magento application is now managed by the Astra Control Center. All operations supported by Astra Control can be performed on the application. Note the version of the application as well.

 **magento-prod**
Available

 App status
 

 Healthy


 App protection status
 

 Partially Protected

**Images**  
 docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16  
 docker.io/bitnami/magento:2.4.1-debian-10-r11  
 docker.io/bitnami/mariadb:10.3.23-debian-10-r38

**Protection schedule**  
 Disabled

**Group**  
 ■ magento-prod

**Cluster**  
 ocp-vmw

4. Repeat the steps for managing the Magento application in the staging environment (magento-staging).

## CI/CD pipeline with integrated protection

When we work with new versions of applications, we use a CI/CD pipeline to build the container image, take backups of both the staging and production environments, deploy the new version of the application to the staging environment, wait for approval to promotion to production, and then deploy the new version of the application to the production environment. To use a CI/CD pipeline, complete the following steps:

1. Log into Jenkins, and create the required credentials: one for Magento creds, one for Mariadb admin creds, and the third for Mariadb root creds.
2. Navigate to Manage Jenkins > Manage Credentials and click the appropriate domain.

3. Click Add Credentials, and set the kind to Username with password and scope set to Global. Enter the username, password, and an ID for the credentials and click OK.

Dashboard > Credentials > System > Global credentials (unrestricted)

Back to credential domains

Add Credentials

Kind  
Username with password

Scope  
Global (Jenkins, nodes, items, all child items, etc)

Username  
admin

☐ Treat username as secret

Password  
.....

ID  
magento-cred

Description

OK


4. Repeat the same procedure for the other two credentials.
5. Go back to the Dashboard, create a pipeline by clicking New Item, and then click Pipeline.
6. Copy the pipeline from the Jenkinsfile [here](#).
7. Paste the pipeline into the Jenkins pipeline section and then click Save.
8. Fill the parameters of the Jenkins pipeline with the respective details including the helm chart version, the Magento application version to be upgraded to, the Astra toolkit version, the Astra Control Center FQDN, the API token, and its instance ID. Specify the docker registry, namespace, and Magento IP of both production and staging environments, and also specify the credential IDs of the credentials created.


```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
CHART_VERSION = '14'
RELEASE_TYPE = 'MINOR'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
DOCKER_REGISTRY = 'docker.io/netapp-solutions-cicd'
PROD_NAMESPACE = 'magento-prod'
PROD_MAGENTO_IP = 'x.x.x.x'
STAGING_NAMESPACE = 'magento-staging'
STAGING_MAGENTO_IP = 'x.x.x.x'
MAGENTO_CREDS = credentials('magento-cred')
MAGENTO_MARIADB_CREDS = credentials('magento-mariadb-cred')
MAGENTO_MARIADB_ROOT_CREDS = credentials('magento-mariadb-root-cred')
```


9. Click Build Now. The pipeline starts executing and progresses through the steps. The application image is first built and uploaded to the container registry.

Build & Publish Segment	Build Docker Image	Publish Image to Registry	Protect & Deploy Segment	Install & Configure Pre-requisites	Download & Configure Astra Toolkit	Backup Tasks	Backup of Staging Env	Backup of Production Env	Deploy to Staging environment [Minor/Patch]	Deploy to Staging environment [Major]	Promote to Production?	Deploy to Production environment [Minor/Patch]	Deploy to Production environment [Major]	Delete temporary files
4s	24s	5s	213ms	40s	2s	290ms	1min 38s	1min 2s	6min 29s	229ms	361ms	2min 57s	200ms	850ms
3s														
18min 29s														

10. The application backups are initiated via Astra Control.


**magento-prod**
Available


 App status  
Healthy

 App protection status  
Partially Protected

**Images**  
docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16  
docker.io/bitnami/magento:2.4.1-debian-10-r11  
docker.io/bitnami/mariadb:10.3.23-debian-10-r38

**Protection schedule**  
Disabled




**Group**  
magento-prod

**Cluster**  
 ocp-vmw


Overview
Data protection
Storage
Resources
Activity


Actions
Configure protection policy
Search


1-8 of 8 entries

<input type="checkbox"/>	Name	Ready	On-Schedule/On-Demand	Created ↑	Actions
<input type="checkbox"/>	upgrade-prod-2-4-1-debian-10-r20		 On-Demand	2021/10/29 14:43 UTC	Running 

11. After the backup stages have completed successful, verify the backups from the Astra Control Center.


**magento-prod**
Available



**App status**  
Healthy


**App protection status**  
Partially Protected

**Images**  
 docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16  
 docker.io/bitnami/magento:2.4.1-debian-10-r11  
 docker.io/bitnami/mariadb:10.3.23-debian-10-r38

**Protection schedule**  
 Disabled

**Group**  
 magento-prod

**Cluster**  
 ocp-vmw

Overview

**Data protection**

Storage

Resources

Activity

Actions

Configure protection policy

Search

1-8 of 8 entries

<input type="checkbox"/>	Name	Ready	On-Schedule/On-Demand	Created ↑	Actions
<input type="checkbox"/>	upgrade-prod-2-4-1-debian-10-r20	<span>✓</span>	On-Demand	2021/10/29 14:43 UTC	<span>Available</span>

12. The new version of the application is then deployed to the staging environment.

Build & Publish Segment	Build Docker Image	Publish Image to Registry	Protect & Deploy Segment	Install & Configure Pre-requisites	Download & Configure Astra Toolkit	Backup Tasks	Backup of Staging Env	Backup of Production Env	Deploy to Staging environment [Minor/Patch]	Deploy to Staging environment [Major]	Promote to Production?	Deploy to Production environment [Minor/Patch]	Deploy to Production environment [Major]	Delete temporary files
4s	47s	7s	238ms	1min 25s	2s	273ms	1min 53s	1min 18s	5min 20s	211ms	337ms	2min 39s	187ms	780ms
3s	4min 16s	30s	485ms	7s	3s	153ms	6min 9s	5min 9s						
7min 1s														

13. After this step is completed, the program waits for the user to approve deployment to production. At this stage, assume that the QA team performs some manual testing and approves production. You can then click Approve to deploy the new version of the application to the production environment.



	Deploy to Staging environment [Minor/Patch]	Deploy to Staging environment [Major]	Promote to Production?	Deploy to Production environment [Minor/Patch]	Deploy to Production environment [Major]	Delete temporary files
	3s	249ms	221ms	159ms	178ms	210ms
<div> <div>Approval for promotion to Production?</div> <div> <div>Proceed</div> <div>Abort</div> </div> </div> <div>(paused for 1min 3.5s)</div>						

14. Verify that the production application is also upgraded to the desired version.

**magento-prod**

Available

App status

Healthy

App protection status

Partially Protected

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61  
docker.io/bitnami/mariadb:10.3.24-debian-10-r49  
docker.io/niksleo415/magento:2.4.1-debian-10-r14

Protection schedule

Disabled

Group

magento-prod

Cluster

ocp-vmw

As part of the CI/CD pipeline, we demonstrated the ability to protect the application by creating a complete application-aware backup. Because the entire application has been backed up as part of the promotion-to-production pipeline, you can feel more confident about highly automated application deployments. This application-aware backup containing the data, state, and configuration of the application can be useful for numerous DevOps workflows. One important workflow would be to roll back to the previous version of the application in case of unforeseen issues.

Although we demonstrated a CI/CD workflow through with Jenkins tool, the concept can easily and efficiently be extrapolated to different tools and strategies. To see this use case in action, watch the video [here](#).

Next: [Videos and Demos - DevOps with NetApp Astra](#).

## 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.