Abstract
This document describes the required steps to implement a site disaster recovery plan to Amazon AWS with NetApp® and ONTAP® Cloud. The example in the document demonstrates how to recover an Atlassian Jira application. This example can also be utilized on other enterprise applications.
TABLE OF CONTENTS

1 Introduction ........................................................................................................................................... 3
  1.1 Purpose ............................................................................................................................................ 3
  1.2 Environment .................................................................................................................................... 3

2 Prerequisites ......................................................................................................................................... 3

3 Installation on Production Site ............................................................................................................. 3

4 Installation on AWS Account ................................................................................................................. 4
  4.1 General ........................................................................................................................................... 4
  4.2 ONTAP Cloud Setup on OCCM ...................................................................................................... 4
  4.3 ONTAP Cloud Volume Creation .................................................................................................... 6
  4.4 Volume Replication Creation .......................................................................................................... 7

5 Executing Recovery Plan ...................................................................................................................... 9
  5.1 Break Replication ............................................................................................................................ 9
  5.2 Install Jira in AWS Account ........................................................................................................... 9

6 Resync After Recovery .......................................................................................................................... 10
1 Introduction

1.1 Purpose

This document describes the required steps to implement a site disaster recovery plan to Amazon AWS with NetApp and ONTAP Cloud. The example in the document demonstrates how to recover an Atlassian Jira application. This example can also be utilized on other enterprise applications, such as Stash, TeamCity, and so on, when the organization wants to separate the data from the application and perform disaster recovery at the data level only.

1.2 Environment

- A DataCenter, which serves as the production site, including applications running on physical servers or VMWare with Netapp as shared storage.
- VPN connection between the production site and the DR site in AWS.
- The necessary ports (For SnapMirror and for the applications) must be opened in the production site Firewall.
- NetApp OnCommand® Cloud Manager (OCCM) for ONTAP Cloud in an AWS account. Here, a new ONTAP Cloud will be created with dedicated volumes for the replication from the production site.

Figure 1) Disaster Recovery Diagram

2 Prerequisites

The prerequisites for implementing a site disaster recovery plan include:

- Amazon AWS account
- VPN connection between AWS account and production site
- NetApp FAS/V-Series storage system in the production site

3 Installation on Production Site

For installation, follow these steps:
**Note:** The volume name is AppData, and the mount point is /dada. It can be changed to any other name.

1. Install Linux server.

2. Create a dedicated volume in the NetApp storage system:
   a. Note: The following example creates a new volume named AppData on a Vserver named vs0 and a storage aggregate named aggr1. Upon its creation, the volume is placed in the online state. It uses the export policy named default_exportpolicy.
   
   ```
   node::> volume create -vserver vs0 -volume AppData -aggregate aggr1 -state online -policy default_exportpolicy -junction-path /AppData -size 150g -space-guarantee volume -percent-snapshot-space 20 -foreground false
   ```
   
   b. `node::> volume create -vserver vs0 -volume AppData -aggregate aggr1 -state online -policy default_exportpolicy -junction-path /AppData -size 150g -space-guarantee volume -percent-snapshot-space 20 -foreground false`

3. On the Linux server, create a mount point to the volume. Edit /etc/fstab and add a line with the NFS mount so that it mounts automatically after reboot:
   a. 10.1.1.1:/AppData /data nfs  rsize=65536,wsize=65536,timeo=600
   b. Type mount -a, then type df -h /data. Here is an example of the command output:
      ```
      • 10.1.1.1:/AppData 150G 92G 59G 62% /data
      ```

4. Install MySQL and configure the datadir in my.cnf to be the mount point created in the previous step:
   ```
   • atadir=/data/Jira/mysql
   ```

5. Install the Jira application. During the installation, configure the JIRA_HOME folder to be the mount point created in step 3. In this example it is /data/Jira/Jira_Data.

6. Start Jira and perform tests to verify that Jira is working correctly.

### 4 Installation on AWS Account

**Note:** At this stage a VPN connection between production site and AWS account must be established.

#### 4.1 General

In this section we perform the following:

- Install NetApp OnCommand® Cloud Manager (OCCM) for ONTAP Cloud in an AWS account
- Discover production NetApp storage (on the premises) in the OCCM
- Create ONTAP Cloud working environment, which is used to store the replicated volume
- Create a replication between the volume in NetApp production storage and the new volume in the AWS working environment

#### 4.2 ONTAP Cloud Setup on OCCM

To set up ONTAP Cloud on OCCM, follow these steps:

1. Log in to AWS with your credentials.

2. Install OnCommand Cloud Manager for ONTAP Cloud (OCCM). The AMI can be found in the AWS marketplace here:
   ```
   ```

3. Open a web browser and browse to the OCCM public IP.

4. Instigate and run the setup wizard.

5. Discover on-premises NetApp storage located in your production site:
a. Click Add Environment.

b. Click Data ONTAP (the left cloud).

c. Type your production NetApp IP, user name, and password and click Continue.
d. The OCCM connects to the production NetApp storage and displays it in the gallery page.

![OCCI connection to NetApp storage](image)

e. Double-click the environment (in this example, TLV-Cluster). All volumes should appear, including the AppData volume created earlier.

![OCCI gallery page with volumes](image)

### 4.3 ONTAP Cloud Volume Creation

**Note:** In this section we create ONTAP Cloud and put a volume in it.

1. From the OCCM gallery page, click Add Environment.
2. Choose Create and click ONTAP Cloud.
3. Type the working environment name (that is, ClusterDR), then continue.
4. Choose None or AWS Encryption for data security.
5. Choose your region, VPC, and subnet, then continue.
6. Choose license type, then continue.
7. Enter NetApp Support site credentials (optional).
8. Type the ONTAP Cloud password, choose the AWS disk, then continue.
9. In the volume creation page, click Skip. Then continue.
10. In the Review page, verify that all parameters are correct, approve terms and conditions, and click Go.
11. ONTAP Cloud creation starts. It takes ~25 minutes.
12. After ONTAP Cloud creation finishes, the new environment appears in the Gallery page.

### 4.4 Volume Replication Creation

**Note:** In this section we create a replication between AppData volume in a production site to the new ONTAP Cloud storage in AWS.

1. In the gallery page where both (On-Premises and ClusterDR appear, click the On-Premises cloud over the ClusterDR cloud.

2. The Replication Setup wizard starts.
3. Choose the AppData volume and click Continue.

4. Type in the destination volume name. By default, it is AppData_copy, but it can be changed to any other name. Click Advanced Options and choose the destination aggregate.

6. Choose the schedule for the replication.
7. In the Review page, make sure everything (source destination and all other parameters) is as it should be.
8. Click More Information to verify if additional AWS HW needs to be purchased.
9. Approve terms and conditions and click Go.
10. The replication process starts. Now the data transfer from the AppData volume in the production site to AWS AppData_copy starts.
11. To verify the status of the replication, click Replication Status.
5 Executing Recovery Plan

5.1 Break Replication

Note: In this stage we assume the production site is down, and we need to continue working on Jira in AWS.

1. Break the replication. Go to the Replication Status page, click the icon, and click Break.

2. Click the AppData_copy volume and choose Edit.

3. Change the access control to Custom Export Policy. Fill in the correct subnet.

4. The replication breaks, and now the AppData_copy volume changes from DP to RW, meaning it is possible to mount to it.

5.2 Install Jira in AWS Account

To install Jira in an AWS account, follow these steps:

1. Deploy a new Linux instance in the AWS account.

2. Log in to the Linux server, install MySQL, and configure the data folder to be /data/Jira/mysql.

3. Note: /data should be for now the local folder in the Linux server and not a mount point.

4. Install the same version of the Jira application that is installed on the production site. During the installation, configure the JIRA_HOME folder to be /data/Jira/Jira_Data.

5. After the installation is finished, stop Jira and MySQL.

6. Create NFS mount to the AppData_copy volume in the ClusterDR environment. Use the ClusterDR NFS data IP (in the following example it's 10.10.10.1) 10.10.10.1:/AppData_copy /data nfs rsize=65536,wsize=65536,timeo=600.
7. Browse to the mount point created and verify that you can see the content of the volume.
8. Start MySQL and Jira.
9. Log in to the Jira webpage and verify that everything is working correctly.

6  Resync After Recovery

At this stage we assume the disaster has been overcome. It is usually necessary to return operations back to the production site.

The assumption here is that after recovery, the production site has the same configuration as it had before the disaster: NetApp with the volume AppData and Jira installed as it was installed in section 3.

1. Log in to the OCCM public IP.

2. Go to the Replication Status page, click the icon, and click Reverse Resync.

3. A new popup window appears. Verify that AppData_copy volume is the source and AppData volume is the destination, then click Approve.

4. Click the protection → Operations → Reverse Resync.

5. The reverse resync starts. Here is an example of the replication that should appear:

6. Now the replication is reversed from the AppData_copy in AWS to the AppData in the production site.

7. After the resync is finished, break the replication so that the AppData volume is RW.

8. Mount to the AppData volume from Jira installed on the production site.

9. Start up MySQL and Jira.
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 © 1994–2016 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, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, ONTAP Cloud, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Fitness, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, SnapCopy, Snap Creator, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, StorageGRID, Tech OnTap, Unbound Cloud, vFiler, WAFL, and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx TR-4554-0916