



Using Veeam Replication and FSx for ONTAP for Disaster recovery to VMware Cloud on AWS

NetApp Solutions

NetApp
October 20, 2023

Table of Contents

| | |
|--|----|
| Using Veeam Replication and FSx for ONTAP for Disaster recovery to VMware Cloud on AWS | 1 |
| Overview | 1 |
| Problem Statement | 1 |
| Solution Deployment | 2 |
| Conclusion | 15 |

Using Veeam Replication and FSx for ONTAP for Disaster recovery to VMware Cloud on AWS

Author: Niyaz Mohamed - NetApp Solutions Engineering

Overview

Amazon FSx for NetApp ONTAP integration with VMware Cloud on AWS is an AWS-managed external NFS datastore built on NetApp's ONTAP file system that can be attached to a cluster in the SDDC. It provides customers with flexible, high-performance virtualized storage infrastructure that scales independently of compute resources.

For those customers looking to use VMware Cloud on AWS SDDC as the disaster recovery target, FSx for ONTAP datastores can be used to replicate data from on-premises using any validated third-party solution that provides VM replication capability. By adding FSx for ONTAP datastore, it will enable cost optimised deployment than building VMware cloud on AWS SDDC with enormous amount of ESXi hosts just to accommodate the storage.

This approach also helps customers to use pilot light cluster in VMC along with FSx for ONTAP datastores to host the VM replicas. The same process can also be extended as a migration option to VMware Cloud on AWS by gracefully failing over the replication plan.

Problem Statement

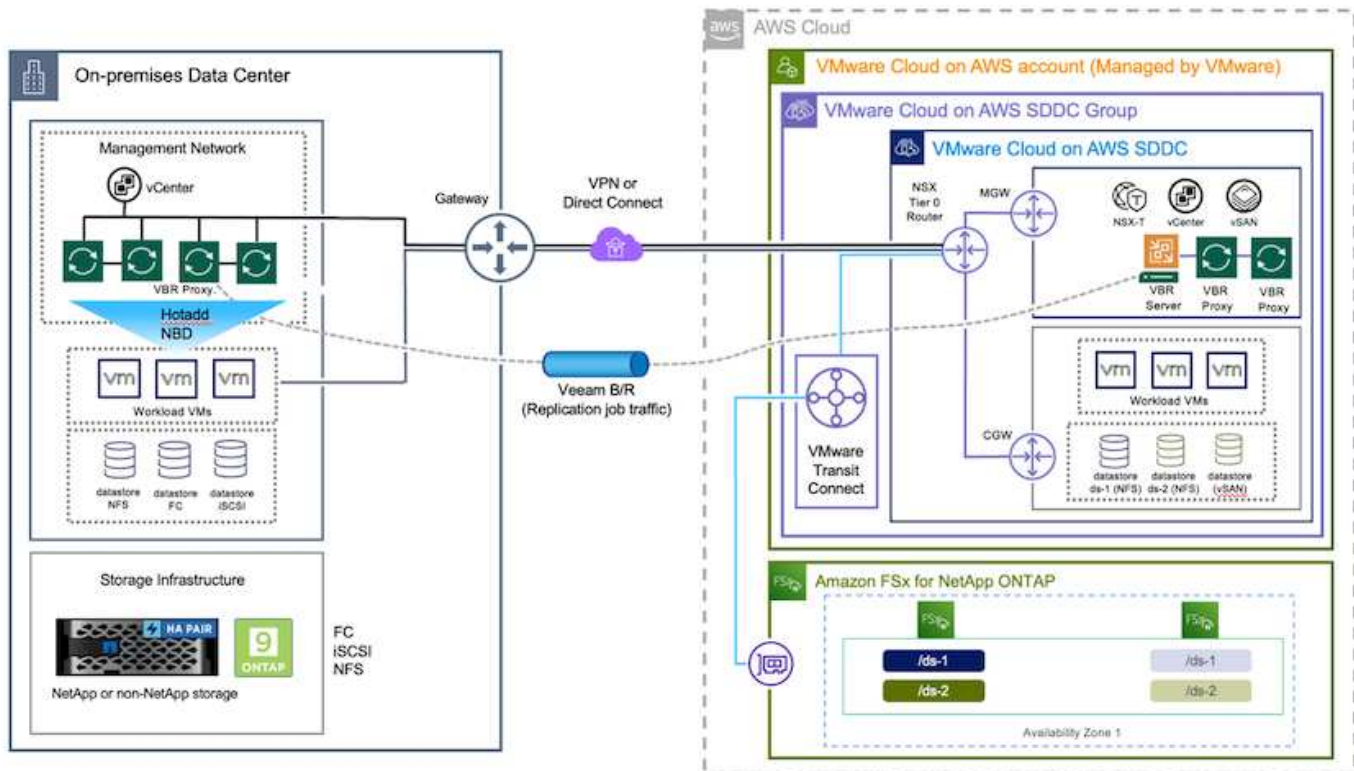
This document describes how to use FSx for ONTAP datastore and Veeam Backup and replication to set up disaster recovery for on-premises VMware VMs to VMware Cloud on AWS using the VM replication functionality.

Veeam Backup & Replication allows onsite and remote replication for disaster recovery (DR). When virtual machines are replicated, Veeam Backup & Replication creates an exact copy of the VMs in the native VMware vSphere format on the target VMware Cloud on AWS SDDC cluster and keeps the copy synchronized with the original VM.

Replication provides the best recovery time objective (RTO) values as there is a copy of a VM in the ready-to-start state. This replication mechanism ensures that the workloads can quickly start in VMware Cloud on AWS SDDC in case of a disaster event. The Veeam Backup & Replication software also optimizes traffic transmission for replication over WAN and slow connections. In addition, it also filters out duplicate data blocks, zero data blocks, swap files and excluded VM guest OS files, and compresses the replica traffic.

To prevent replication jobs from consuming the entire network bandwidth, WAN accelerators and network throttling rules can be put in place. The replication process in Veeam Backup & Replication is job driven which means replication is performed by configuring replication jobs. In case of a disaster event, failover can be triggered to recover the VMs by failing over to its replica copy.

When failover is performed, a replicated VM takes over the role of the original VM. Fail over can be performed to the latest state of a replica or to any of its good known restore points. This enables ransomware recovery or isolated testing as needed. In Veeam Backup & Replication, failover and failback are temporary intermediate step that should be further finalized. Veeam Backup & Replication offers multiple options to handle different disaster recovery scenarios.



Solution Deployment

High level steps

1. Veeam Backup and Replication software is running in on-premises environment with appropriate network connectivity.
2. Configure VMware Cloud on AWS, see the VMware Cloud Tech Zone article [VMware Cloud on AWS integration with Amazon FSx for NetApp ONTAP Deployment Guide](#) to deploy, configure VMware Cloud on AWS SDDC and FSx for ONTAP as NFS datastore. (A pilot-light environment set up with a minimal configuration can be used for DR purposes. VMs will fail over to this cluster in the event of an incident, and additional nodes can be added).
3. Set up replication jobs to create VM replicas using Veeam Backup and Replication.
4. Create failover plan and perform failover.
5. Switch back to production VMs once the disaster event is complete and primary site is Up.

Pre-requisites for Veeam VM Replication to VMC and FSx for ONTAP datastores

1. Ensure Veeam Backup & Replication backup VM is connected to the source vCenter as well as the target VMware cloud on AWS SDDC clusters.
2. The backup server must be able to resolve short names and connect to source and target vCenters.
3. The target FSx for ONTAP datastore must have enough free space to store VMDKs of replicated VMs

For additional information, refer to "Considerations and Limitations" covered [here](#).

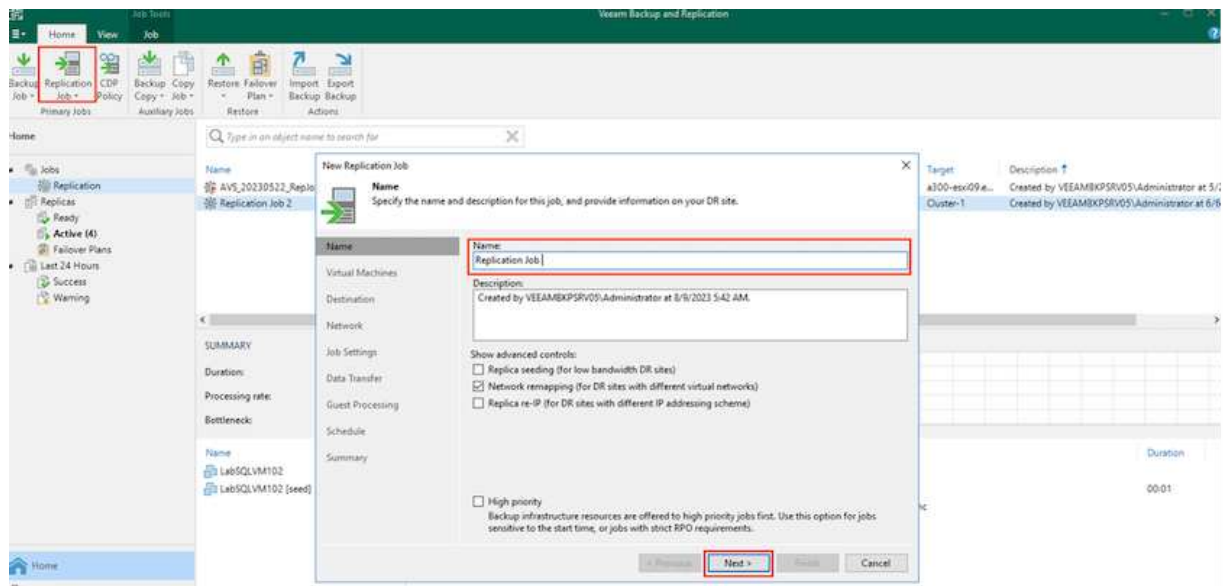
Deployment Details

Step 1: Replicate VMs

Veeam Backup & Replication leverages VMware vSphere snapshot capabilities and during replication, Veeam Backup & Replication requests VMware vSphere to create a VM snapshot. The VM snapshot is the point-in-time copy of a VM that includes virtual disks, system state, configuration and so on. Veeam Backup & Replication uses the snapshot as a source of data for replication.

To replicate VMs, follow the below steps:

1. Open the Veeam Backup & Replication Console.
2. On the Home view, select Replication Job > Virtual machine > VMware vSphere.
3. Specify a job name and select the appropriate advanced control checkbox. Click Next.
 - Select the Replica seeding check box if connectivity between on-premises and AWS has restricted bandwidth.
 - Select the Network remapping (for AWS VMC sites with different networks) check box if segments on VMware Cloud on AWS SDDC do not match that of on-premises site networks.
 - If the IP addressing scheme in on-premises production site differs from the scheme in the AWS VMC site, select the Replica re-IP (for DR sites with different IP addressing scheme) check box.



4. Select the VMs that needs to be replicated to FSx for ONTAP datastore attached to VMware Cloud on AWS SDDC in the **Virtual Machines** step. The Virtual machines can be placed on vSAN to fill the available vSAN datastore capacity. In a pilot light cluster, the usable capacity of a 3-node cluster will be limited. The rest of the data can be replicated to FSx for ONTAP datastores. Click **Add**, then in the **Add Object** window select the necessary VMs or VM containers and click **Add**. Click **Next**.

Virtual Machines
Select one or more VMs to replicate. Use exclusion settings to exclude specific VMs and virtual disks from replication.

Virtual machines to replicate:

| Name | Type | Size |
|-------------|-----------------|---------|
| TestVeeam21 | Virtual Machine | 873 MB |
| TestVeeam22 | Virtual Machine | 890 MB |
| TestVeeam23 | Virtual Machine | 883 MB |
| TestVeeam24 | Virtual Machine | 879 MB |
| TestVeeam25 | Virtual Machine | 885 MB |
| TestVeeam26 | Virtual Machine | 883 MB |
| TestVeeam27 | Virtual Machine | 879 MB |
| TestVeeam28 | Virtual Machine | 880 MB |
| TestVeeam29 | Virtual Machine | 878 MB |
| TestVeeam30 | Virtual Machine | 876 MB |
| TestVeeam31 | Virtual Machine | 888 MB |
| TestVeeam32 | Virtual Machine | 881 MB |
| TestVeeam33 | Virtual Machine | 877 MB |
| TestVeeam34 | Virtual Machine | 875 MB |
| TestVeeam35 | Virtual Machine | 882 MB |
| WinSQL401 | Virtual Machine | 20.3 GB |
| WinSQL405 | Virtual Machine | 24.2 GB |

Buttons: Add..., Remove, Exclusions..., Source..., Up, Down, Recalculate, Total size: 120 GB

Navigation: < Previous, **Next >**, Finish, Cancel

- After that, select the destination as VMware Cloud on AWS SDDC cluster / host and the appropriate resource pool, VM folder and FSx for ONTAP datastore for VM replicas. Then Click **Next**.

Destination
Specify where replicas should be created in the DR site.

Host or cluster:

Resource pool:

Resources

Pick resource pool for selected replicas

VM folder:

vm

Pick VM folder for selected replicas

Datastore:

_Veeam [5.6 TB free]

Pick datastore for selected virtual disks

Navigation: < Previous, Next >, Finish, Cancel

6. In the next step, create the mapping between source and destination virtual network as needed.

Network

Select how virtual networks map to each other between production and DR sites.

| Name |
|------------------|
| Virtual Machines |
| Destination |
| Network |
| Job Settings |
| Data Transfer |
| Guest Processing |
| Schedule |
| Summary |

Network mapping:

| Source network | Target network |
|-----------------------|----------------|
| VM_3508 (vDS-Switch0) | SepSeg |
| VM_3510 (vDS-Switch0) | SegmentTemp |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Add...
Edit...
Remove

< Previous
Next >
Finish
Cancel

7. In the **Job Settings** step, specify the backup repository that will store metadata for VM replicas, retention policy and so on.
8. Update the **Source** and **Target** proxy servers in the **Data Transfer** step and leave **Automatic** selection (default) and keep **Direct** option selected and click **Next**.
9. At the **Guest Processing** step, select **Enable application-aware processing** option as needed. Click **Next**.

Guest Processing
Choose guest OS processing options available for running VMs.

Name

Virtual Machines

Destination

Network

Job Settings

Data Transfer

Guest Processing

Schedule

Summary

☐ **Enable application-aware processing**
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications **Applications...**

Guest interaction proxy:
Automatic selection **Choose...**

Guest OS credentials:
Add...

Manage accounts

Customize guest OS credentials for individual machines and operating systems **Credentials...**

Verify network connectivity and credentials for each machine included in the job **Test Now**

< Previous **Next >** **Finish** **Cancel**

10. Choose the replication schedule to run the replication job to run on a regular basis.

11. At the **Summary** step of the wizard, review details of the replication job. To start the job right after the wizard is closed, select the **Run the job when I click Finish** check box, otherwise leave the check box unselected. Then click **Finish** to close the wizard.

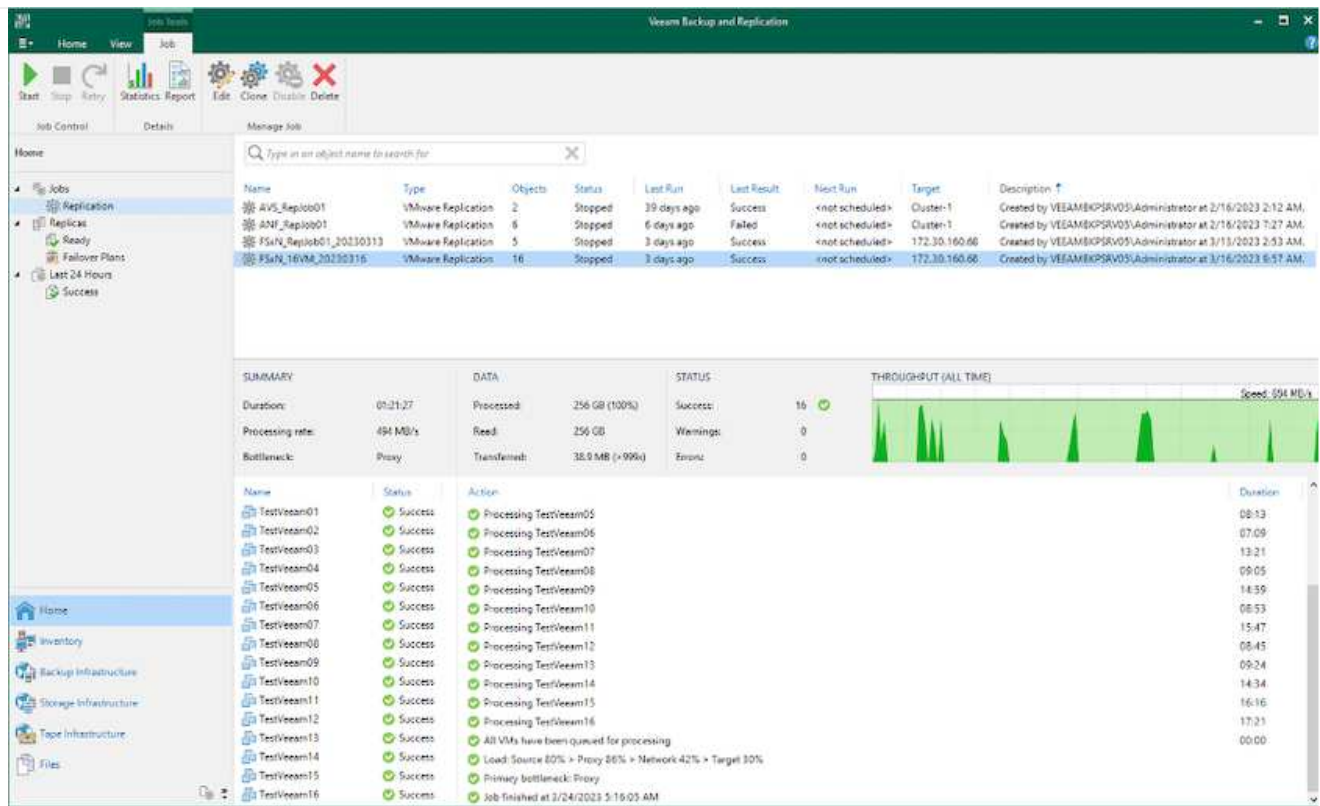
Home

Q Type in an object name to search for

T All jobs

| Name | Type | Objects | Status | Last Run | Last Result | Next Run | Target | Description |
|--------------------------|--------------------|---------|---------|-------------|-------------|---------------|---------------|---|
| ANP_Replicat01 | VMware Replication | 6 | Stopped | 2 days ago | Failed | not scheduled | Cluster-1 | Created by VESAMBRSPR03\Administrator at 2/16/2022... |
| ANP_Replicat04 | VMware Replication | 2 | Stopped | 11 days ago | Success | not scheduled | Cluster-1 | Created by VESAMBRSPR03\Administrator at 2/18/2022... |
| FSch_Replicat01_20220318 | VMware Replication | 18 | Stopped | 2 days ago | Success | not scheduled | 172.30.160-88 | Created by VESAMBRSPR03\Administrator at 3/18/2022... |
| FSch_Replicat01_20220318 | VMware Replication | 5 | Stopped | 8 days ago | Success | not scheduled | 172.30.160-88 | Created by VESAMBRSPR03\Administrator at 3/18/2022... |

Once the replication job starts, the VMs with the suffix specified will be populated on the destination VMC SDDC cluster / host.






For additional information for Veeam replication, refer to [How Replication Works](#).

Step 2: Create a failover plan

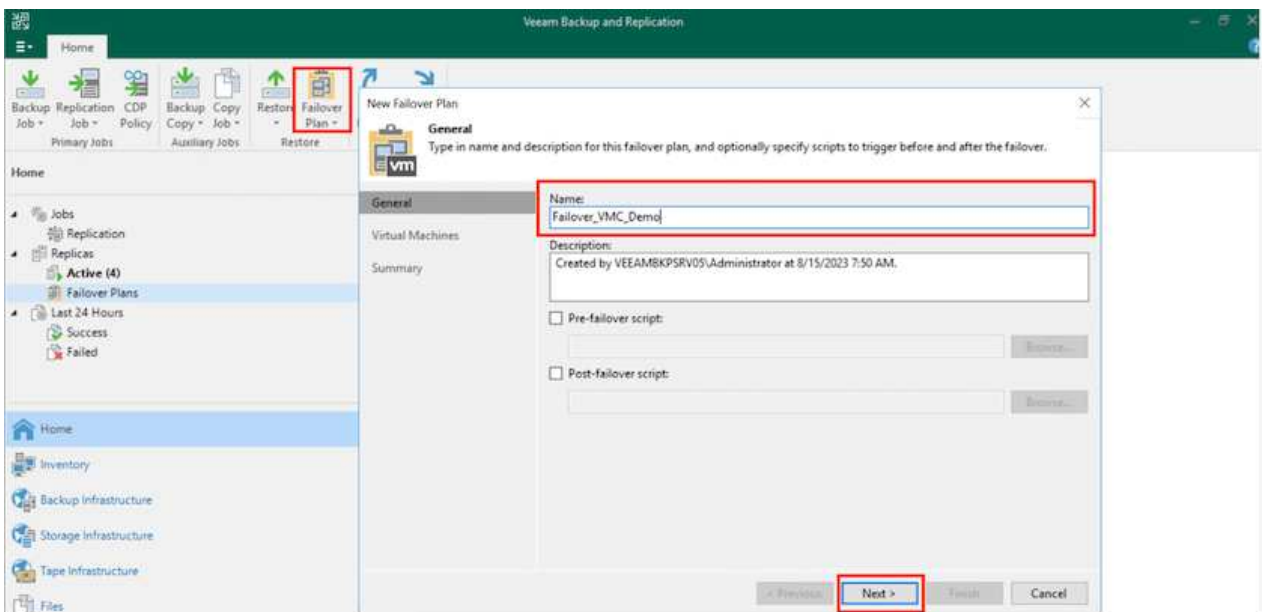
When the initial replication or seeding is complete, create the failover plan. Failover plan helps in performing failover for dependent VMs one by one or as a group automatically. Failover plan is the blueprint for the order in which the VMs are processed including the boot delays. The failover plan also helps to ensure that critical dependant VMs are already running.

To create the plan, navigate to the new sub section called Replicas and select Failover Plan. Choose the appropriate VMs. Veeam Backup & Replication will look for the closest restore points to this point in time and use them to start VM replicas.

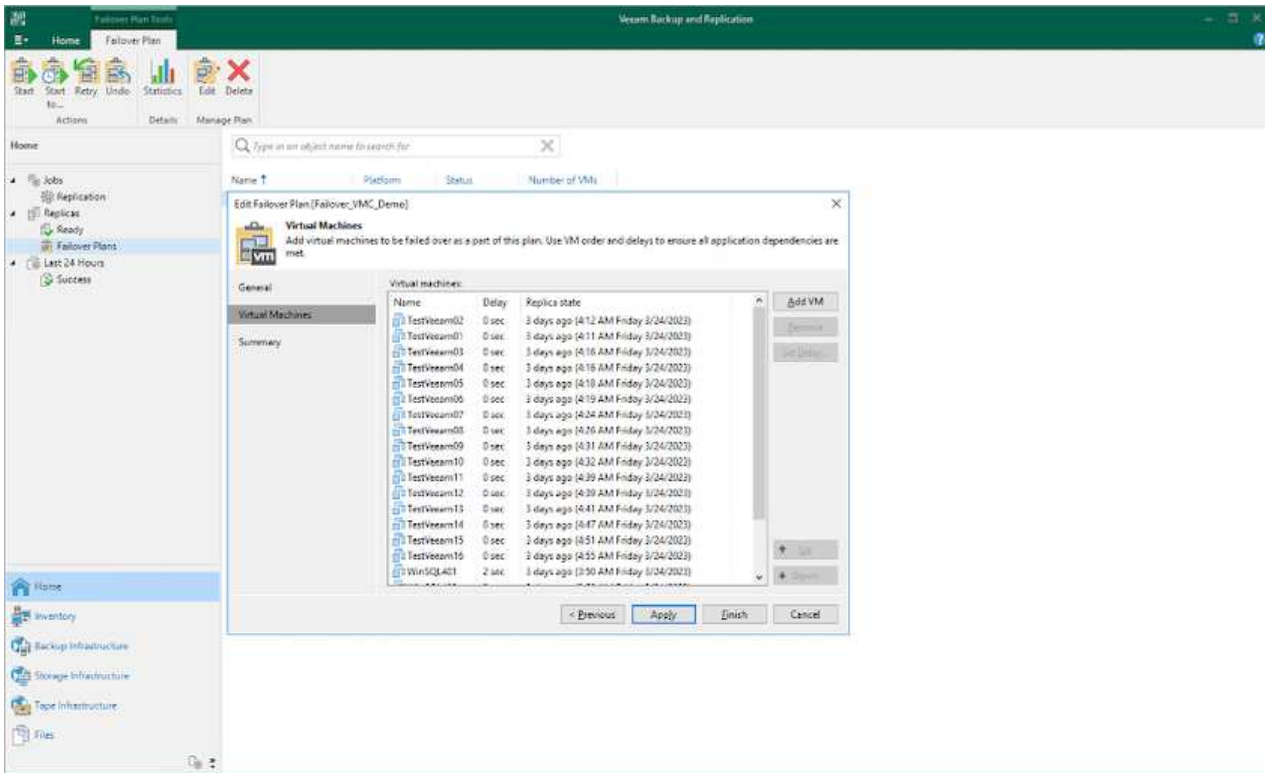
-  The failover plan can only be added once the initial replication is complete and the VM replicas are in Ready state.
-  The maximum number of VMs that can be started simultaneously when running a failover plan is 10.
-  During the failover process, the source VMs will not be powered off.

To create the **Failover Plan**, do the following:

1. On the Home view, select **Failover Plan > VMware vSphere**.
2. Next, provide a name and a description to the plan. Pre and Post-failover script can be added as required. For instance, run a script to shutdown VMs before starting the replicated VMs.



3. Add the VMs to the plan and modify the VM boot order and boot delays to meet the application dependencies.



For additional information for creating replication jobs, refer [Creating Replication Jobs](#).

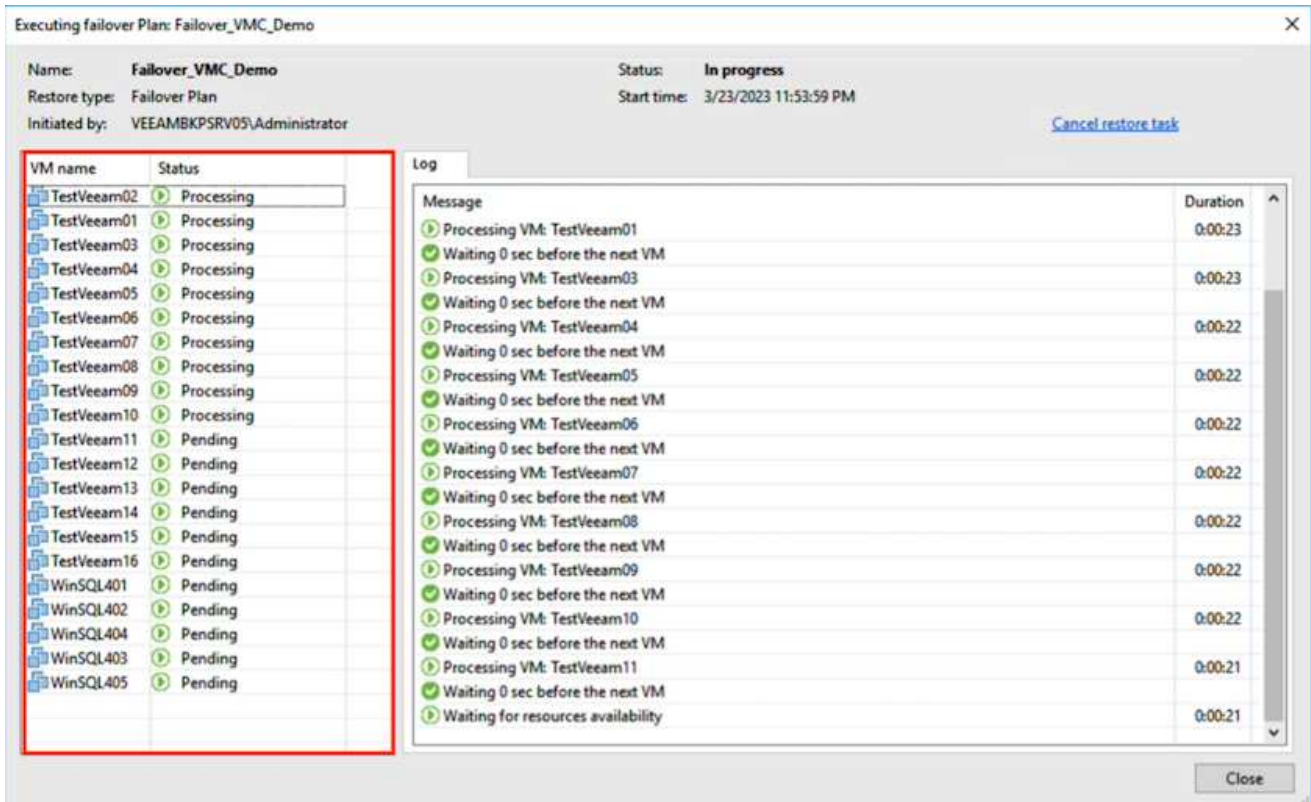
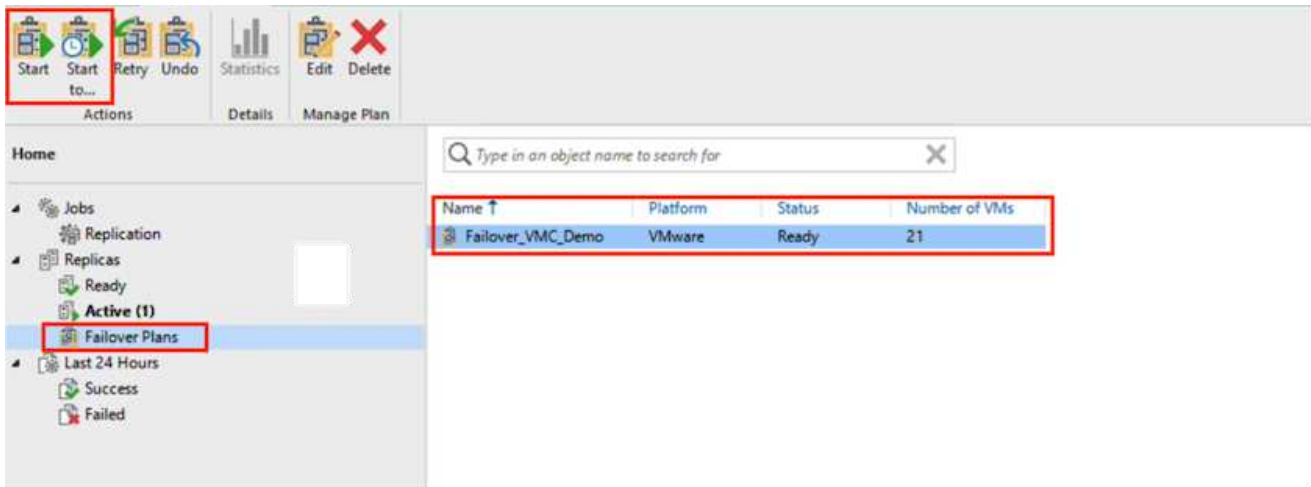
Step 3: Run the failover plan

During failover, the source VM in the production site is switched over to its replica at the disaster recovery site. As part of the failover process, Veeam Backup & Replication restores the VM replica to the required restore point and moves all I/O activities from the source VM to its replica. Replicas can be used not only in case of a disaster, but also to simulate DR drills. During failover simulation, the source VM remains running. Once all the necessary tests have been conducted, you can undo the failover and return to normal operations.

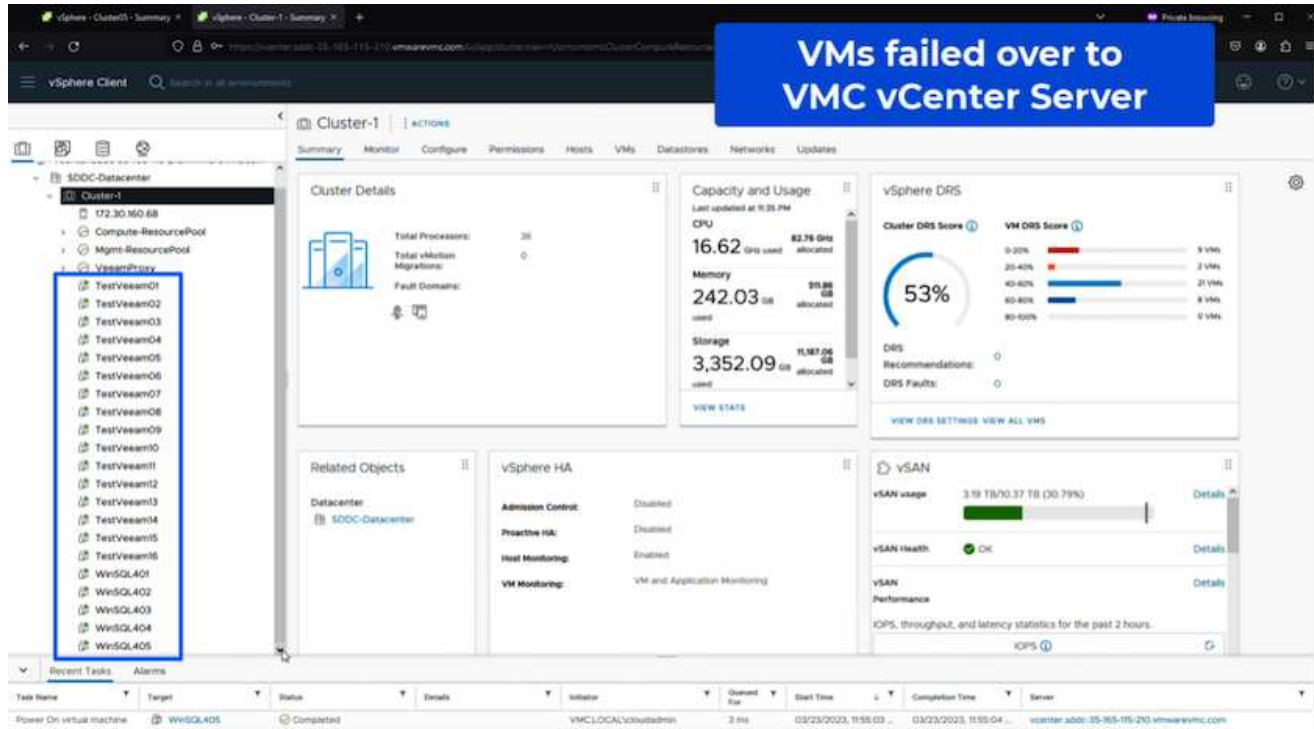


Make sure network segmentation is in place to avoid IP conflicts during DR drills.

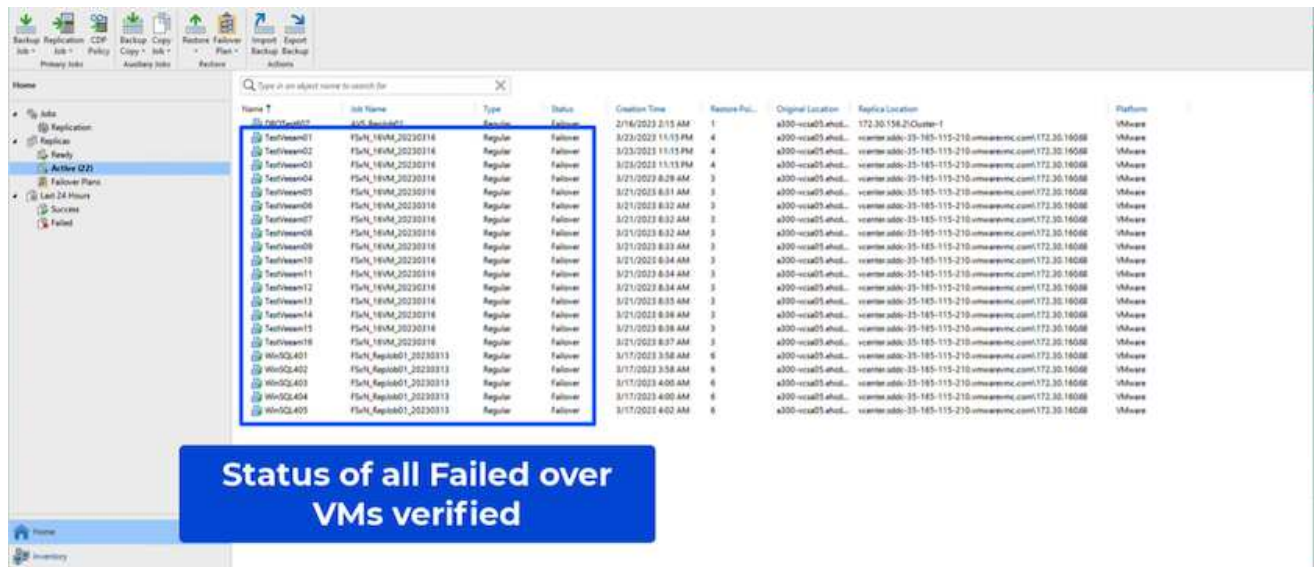
To start the failover plan, simply click in **Failover Plans** tab and right click on the failover plan. Select **Start**. This will failover using the latest restore points of VM replicas. To fail over to specific restore points of VM replicas, select **Start to**.



The state of the VM replica changes from Ready to Failover and VMs will start on the destination VMware Cloud on AWS SDDC cluster / host.



Once the failover is complete, the status of the VMs will change to “Failover”.



Veeam Backup & Replication stops all replication activities for the source VM until its replica is returned to the Ready state.

For detailed information about failover plans, refer to [Failover Plans](#).

Step 4: Failback to the Production site

When the failover plan is running, it is considered as an intermediate step and needs to be finalized based on the requirement. The options include the following:

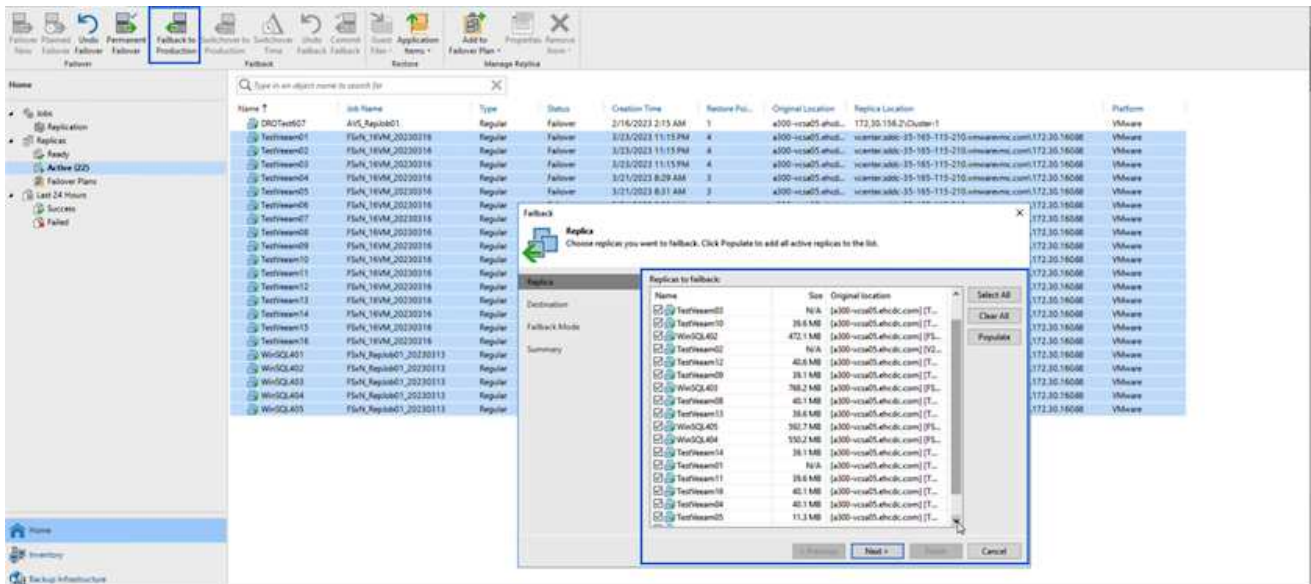
- **Failback to production** - switch back to the original VM and transfer all changes that took place while the VM replica was running to the original VM.

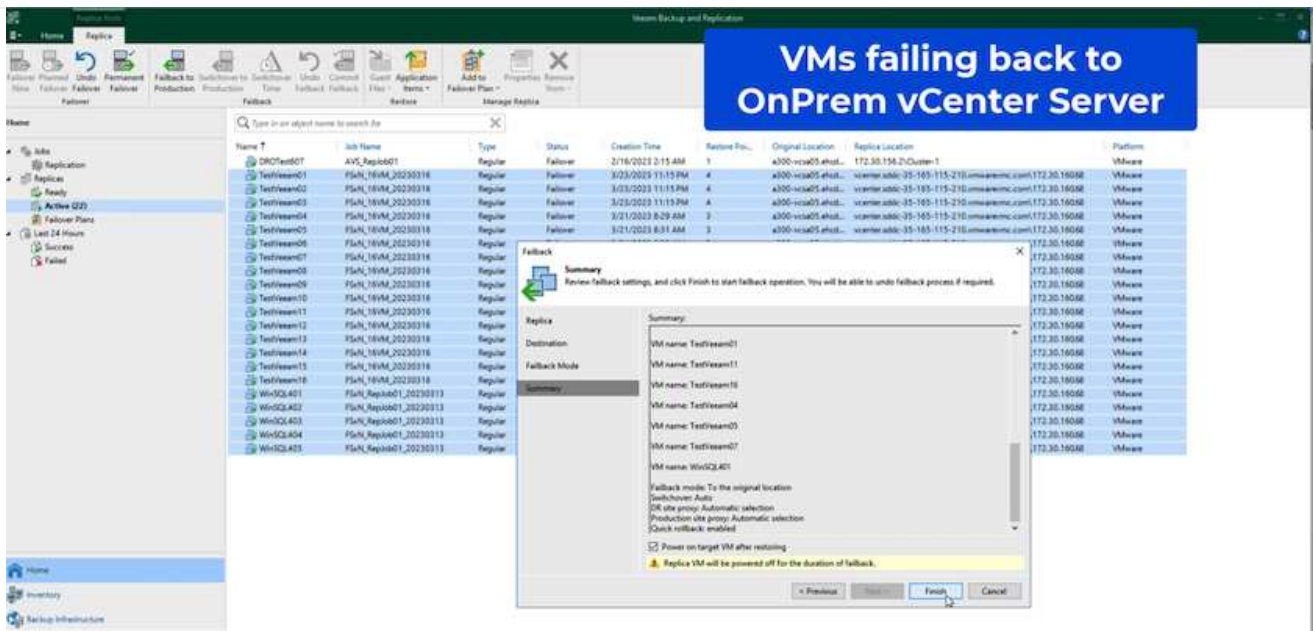


When you perform failback, changes are only transferred but not published. Choose **Commit failback** (once the original VM is confirmed to work as expected) or **Undo failback** to get back to the VM replica If the original VM is not working as expected.

- **Undo failover** - switch back to the original VM and discard all changes made to the VM replica while it was running.
- **Permanent Failover** - permanently switch from the original VM to a VM replica and use this replica as the original VM.

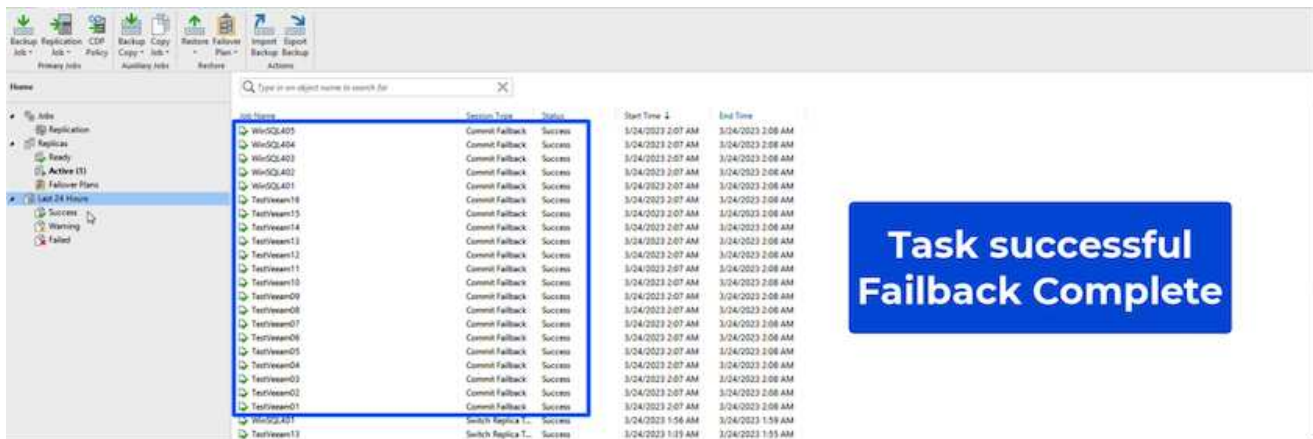
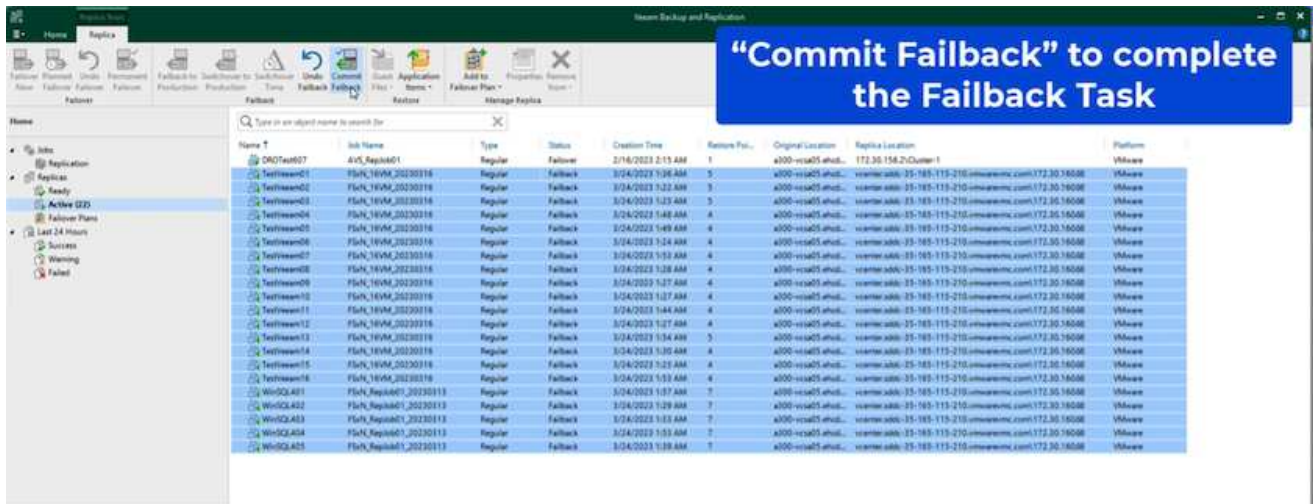
In this demo, Failback to production was chosen. Failback to the original VM was selected during the Destination step of the wizard and “Power on VM after restoring” check box was enabled.



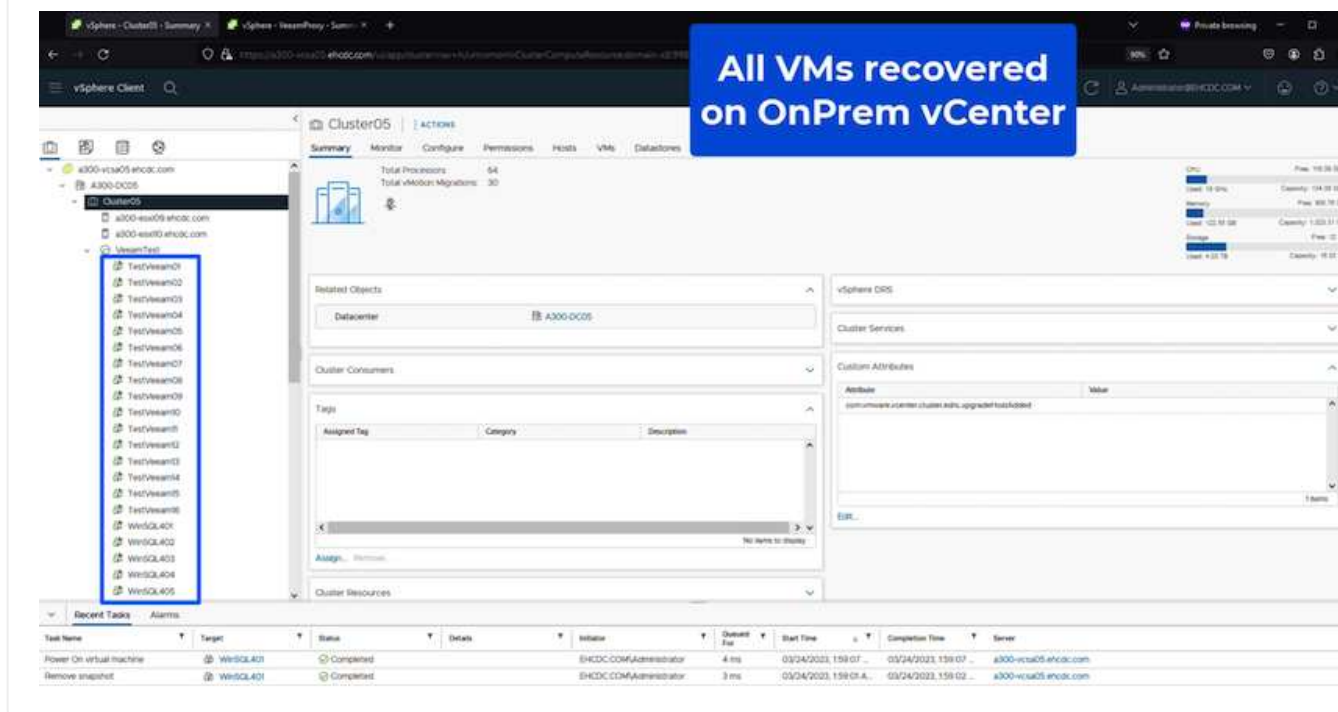


Failback commit is one of the ways to finalize failback operation. When failback is committed, it confirms that the changes sent to the VM which is failed back (the production VM) are working as expected. After the commit operation, Veeam Backup & Replication resumes replication activities for the production VM.

For detailed information about the failback process, refer Veeam documentation for [Failover and Failback for replication](#).



After failback to production is successful, the VMs are all restored back to the original production site.



Conclusion

FSx for ONTAP datastore capability enables Veeam or any validated third-party tool to provide low-cost DR solution using Pilot light cluster and without standing up large number of hosts in the cluster just to accommodate the VM replica copy. This provides a powerful solution to handle a tailored, customized disaster recovery plan and also allows to reuse existing backup products in house to meet the DR needs, thus enabling cloud-based disaster recovery by exiting DR datacentres on-premises. Failover can be done as planned failover or failover with a click of a button when disaster occurs, and decision is made to activate the DR site.

To learn more about this process, feel free to follow the detailed walkthrough video.

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a>

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.