Deploying VMware High Availability & Fault Tolerance cluster on HA3969U (NFS)

Application Note
# Table of Contents

- Products covered by this document ................................................................. 3
- About VMware Virtualization ............................................................................ 4
- VMware High Availability and Fault Tolerance ............................................... 6
  - High Availability .................................................................................................. 6
  - Fault Tolerance .................................................................................................... 7
- Setting up VMware vSphere HA with HA3969U ........................................... 8
  - Step 1: Prepare the environment ......................................................................... 8
  - Step 2: Enable 2 shared folders on HA3969U to become VMware datastores .... 9
  - Step 3: Create HA protected VMware Cluster .................................................. 10
  - Step 4: Add hosts to the cluster .......................................................................... 11
  - Step 5: Set up Fault Tolerance for a Virtual Machine ......................................... 12
- Simulating VMware High Availability Failover .............................................. 16
- Testing VMware Fault Tolerance Failover ..................................................... 18
- Frequently Asked Questions ............................................................................... 20
Products covered by this document

This document applies to the following product models:

- HA3969U Single Controller 12 Bay
- HA3969U Single Controller 16 Bay
- HA3969U Dual Controller 12 Bay
- HA3969U Dual Controller 16 Bay
About VMware Virtualization

The concept of virtualization originated in the 1960s but was not applied to x86 architecture until the 1990s. However, since the 1980s, x86 servers have been widely adopted in IT environments because they are much cheaper than mainframe computers. The distributed system of computing allows for reduced total cost of ownership but may create other challenges, such as low infrastructure utilization, increased physical infrastructure requirements and higher IT management costs, plus insufficient failover and disaster protection. Virtualization is an effective way to deal with these challenges.

In VMware virtualization technology, ESX Server has been the foundation of virtualized environments.

![Figure 1: VMware ESX server](image)

Installed on an x86 or x64-based server, VMware ESX Server provides a virtualization layer on the host OS to consolidate all hardware resources, including processors, memory, storage, and networking. It applies them to virtual machines (i.e. virtual servers) running on the physical server. Each virtual machine can have its own OS and applications. By sharing hardware resources across multiple virtual machines, users can improve resource utilization and in turn greatly reduce costs involved in building physical data center infrastructure.
Besides optimized resource utilization, VMware virtualization also reduces deployment efforts and simplifies management tasks. Free from physical considerations and requirements, deploying virtual machines can be done in as little as just a few minutes. After deployment, managers can easily monitor the entire virtual data center through a unified management pane. When any of the physical devices fail, the high availability features of VMware ensure continuous system operation.
VMware High Availability and Fault Tolerance

No matter how big your company is and how many business critical servers are running in your infrastructure, you always expect your data to be safe and continuously available. Any unplanned downtime in data and IT resources availability will cause losses in time and money. This is why your virtual infrastructure should be robust and highly-available enough to guarantee uninterrupted access to your company’s resources and continuity of business operations.

VMware provides two solutions that aim at providing access to your virtual machines at nearly 100% uptime. The first one is High Availability (HA) that can automatically migrate and restart VMs on a secondary ESXi server in case of any failures occurred on the primary one. Although being fully automatic, VMware HA cannot completely meet the needs of business-critical operations that require 100% uptime, and that is where Fault Tolerance (FT) comes in. FT keeps a shadow up-to-date copy of the original VM on the second ESXi server, which can fully eliminate service downtime during the switch between the original and secondary VMs. Both solutions are illustrated and described below.

High Availability

![VMware HA architecture](image)

As you can see from the picture above, VMware gathers all virtual machines into a shared resource pool or "cluster". After HA is enabled for a cluster, it starts to monitor ESXi servers’ availability. If one of the servers fails, its VMs will be migrated and restarted on other servers.
Fault Tolerance

Fault Tolerance (FT) provides continuous availability for VMs in case of ESXi server failure. FT leverages existing vSphere HA clusters, and utilizes the vLockstep technology to protect specific business-critical VMs by keeping their identical VMs (or "shadow VMs") on secondary ESX /ESXi servers. When the primary server fails, the shadow VMs could be restarted instantly, thus guaranteeing zero downtime and no data, transaction, or connection loss.

Figure 3: VMware FT architecture
Setting up VMware vSphere HA with HA3969U

Storageflex HA3969U models are fully compatible with vSphere High Availability features and together can help small business minimize unexpected downtime and guarantee business continuity.

**Figure 4: Basic topology for testing environment**

**Step 1: Prepare the environment**

To prepare the test environment for this application note, the following minimum hardware is required:

- At least two VMware compatible hardware servers running ESXi server
- At least one Storageflex HA3969U storage system
- At least one LAN switch/router

To create a HA cluster, the following requirements have to be met:

- One HA cluster must have at least 2 ESXi hosts
- All hosts in a HA cluster must be licensed for vSphere HA
- All hosts should have access to the same VM networks and datastores
- All hosts in the HA cluster should have static IP addresses or keep the same dynamic IP address after reboots

Detailed information about HA cluster requirements can be found in VMware vSphere 5.5 Documentation Center:


In order to protect business critical VMs with FT, the following additional requirements should be met:
- There should be at least two hosts running the same FT version/host build number
- Protected VMs must be stored in virtual RDM or virtual machine disk (VMDK) files that are thick provisioned

Full list of FT requirements can be found in VMware vSphere 5.5 Documentation Center:


**Step 2: Enable 2 shared folders on HA3969U to become VMware datastores**

In order to create a HA protected cluster, both ESXi hosts should have at least two shared datastores (as per VMware requirements).

After the two datastores (e.g. "nfs_db" and "nfs_db2") are successfully added to both of the ESXi hosts, you can open vSphere Client and check their information in the Status column of the Storage panel.

<table>
<thead>
<tr>
<th>View:</th>
<th>Datastores</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Datastores</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification</td>
<td>Status</td>
<td>Device</td>
</tr>
<tr>
<td>nfs_db</td>
<td>Normal</td>
<td>172.24.110.40;P...</td>
</tr>
<tr>
<td>nfs_db2</td>
<td>Normal</td>
<td>172.24.110.40;P...</td>
</tr>
</tbody>
</table>

Keep in mind that vSphere HA (vSphere 5) requires at least two shared datastores to be shared between all hosts in a cluster to guarantee proper datastore heartbeat detection to function. If you use only one datastore, you may see the following notification on the ESXi 5.x hosts:

- The number of heartbeat datastores for host is 1, which is less than required: 2
- The number of heartbeat datastores for host is 0, which is less than required: 2

If you still want to use just one shared datastore without seeing the above message, you will need to add the "das.ignoreInsufficientHbDatastore" entry in the cluster settings. Refer to VMware knowledge base article for further information:

Step 3: Create HA protected VMware Cluster

Open vSphere Web Client or vSphere Client, navigate to the datacenter where you want to create the cluster, and then click **New Cluster**.

Follow the wizard to complete the setup.

Keep in mind that if you enable HA before ESXi hosts are added to the cluster, the cluster will not be fully functional until hosts join it.

Also note that you can decide whether you want to enable vSphere DRS (Distributed Resource Scheduler which is responsible for automated load balancing), which is compatible with vSphere HA, and is therefore enabled in our example. For more information about vSphere DRS, refer to VMware vSphere features overview web page: [http://www.vmware.com/products/vsphere/features/drs-dpm.html](http://www.vmware.com/products/vsphere/features/drs-dpm.html)
**Step 4: Add hosts to the cluster**

In vSphere Web Client or vSphere Client, navigate to the cluster you just created, and select **Add Host**. You will need to provide host name, username, and password for the hosts.

If you decide to enable vSphere HA after adding hosts to the cluster, from the details panel you will see the status of HA agent installation for the newly added hosts.

In our example (shown below), you can see the process of configuring vSphere HA after two ESXi hosts are added to the cluster.

vSphere HA is now successfully configured for cluster1, which has two ESXi hosts (172.24.110.35 and 172.24.110.53)
For each host added to a vSphere HA cluster, an HA agent is installed to communicate with other agents in the cluster. Every host in the cluster serves either as a master host or a slave host (shown below).

**Step 5: Set up Fault Tolerance for a Virtual Machine**

After a HA protected cluster is successfully created, you can take VMware High Availability features to the next level by protecting business critical VMs with vSphere Fault Tolerance.

Navigate to the virtual machine you want to protect with Fault Tolerance (e.g. "linux_vm"), right-click on it, and then select either of the following:

- For vSphere Web Client: All vCenter Actions > Fault Tolerance > Turn On Fault Tolerance.
- For vSphere Client: Fault Tolerance > Turn On Fault Tolerance

Click Yes when the confirmation message appears.

After the task is complete and FT is successfully enabled for the VM, you can see the status of the task becoming green.
FT information for a host can be seen in the Summary tab. In our example, the ESXi host inside cluster1 is the master host configured for HA and FT, and hosts one primary VM.

As to the slave host of cluster1, it is also HA protected and configured for FT, but the VM it hosts is a secondary VM (populated from the primary one).
At this point, if you check the VMs for cluster1 (shown below), you will notice a second instance of the FT protected VM appeared in the list. Original FT protected VM ("linux_vm") is running on ESXi host 172.24.110.53, and the secondary VM (or "shadow copy") of the original VM is running on ESXi host 172.24.110.42.

You can also check vSphere map to see the primary and secondary VMs.

After the entire configuration is done, we can start testing the efficiency of the solution. In order to do this, we will simulate vSphere High Availability Failover and then vSphere Fault Tolerance failover.
Simulating VMware High Availability Failover

There are four methods of testing VMware HA described in VMware Knowledge Base:

In this example (172.24.110.42 as the primary server; 172.24.110.53 as the secondary one), we are going to simulate a power-outage situation by right-clicking on the primary host and selecting Shut Down, and then observe the duration of VM unavailability on the secondary host.

Keep in mind that the VM in this example (called "ubuntu") is not FT protected.

Now, right-click on the primary host and choose Shut Down. In a few seconds you will see the host become unavailable.
The HA protected VM on the server becomes unavailable, too, but it is being migrated to the secondary host. As soon as the migration is finished, the protected VM is restarted on the secondary host.

Downtime for this VM is a little bit longer that 1 minute, which under most circumstances is NOT acceptable for many mission critical applications.
Testing VMware Fault Tolerance Failover

There are several scenarios when FT is triggered:

- The primary ESX host fails
- The primary VM becomes non-responsive
- FT test is initiated from vCenter Server

Among all the above scenarios, we are going to use vCenter Server to test the FT capability by right-clicking on a FT protected VM and selecting Fault Tolerance > Test Failover.

Observing the status in the Recent Tasks panel of vSphere Web Client or vSphere Client, you can see the process being finished in just a few seconds.
Protected VM will remain available during this test without any interruption, while there might be a slight delay depending on the network latency. According to VMware Fault Tolerance FAQ, this delay is usually less than 1 millisecond (ms). Refer to VMware Fault Tolerance FAQ for additional information:
Frequently Asked Questions

**Q: What is VMware Cluster?**

**A:** VMware Cluster allows aggregating and managing multiple hosts resources as a single collection. Please refer to VMware vSphere Client Cluster Introduction for more details:

**What is a cluster?**

A cluster is a group of hosts that share resources and a management interface. When you add a host to a cluster, the host's resources become part of the cluster's resources. The cluster manages the resources of all hosts within it.

Clusters enable the vSphere Distributed Resource Scheduler (DRS) and vSphere High Availability (HA) solutions. vSphere DRS continuously balances virtual machine workloads across your ESXi hosts. vSphere HA allows the virtual machines running on ESXi hosts to automatically recover from host failures.

**Q: Do vSphere HA and FT leverage storage array replication techniques?**

**A:** No. These two features are Application and OS agnostic.

**Q: How can I disable vSphere FT?**

**A:** There are 2 ways to deactivate FT: a) by disabling FT, and b) by turning off FT. If you disable FT, the secondary VM will be powered off. On the other hand, if you turn off FT, the secondary VM will be completely removed.

- To disable TF, right-click on the FT protected virtual machine, and select Fault Tolerance > Disable Fault Tolerance.
- To turn off FT, right-click on the FT protected virtual machine, and select Fault Tolerance > Turn Off Fault Tolerance.

**Q: Where can I obtain more information on vSphere High Availability?**

**A:** Refer to VSphere Availability guide: