<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1 VMware Getting Started - Deploying SoftNAS Cloud Virtual Machines</td>
<td>5</td>
</tr>
<tr>
<td>0.2 VMware Getting Started - Adding Storage</td>
<td>28</td>
</tr>
<tr>
<td>0.3 VMware Getting Started - Configuring High Availability</td>
<td>46</td>
</tr>
<tr>
<td>0.4 VMware Getting Started - Project Planning</td>
<td>56</td>
</tr>
<tr>
<td>0.5 VMware Getting Started: Choosing Your HA Solution</td>
<td>60</td>
</tr>
</tbody>
</table>
VMware: Getting Started with SoftNAS Cloud®

Overview

As a first-time user, the primary goals are simply to see the product in action, to determine its capabilities, and then to determine the requirements. This document will focus on providing you a functional pair of instances, both on VMware, sharing a CIFS volume, and configured for high availability. This basic setup will allow you to test the key features of SoftNAS, while providing a baseline for your production requirements.

Note: The guidance in the following document applies equally to all editions of SoftNAS Cloud® (Enterprise and Essentials), however, bear in mind the limitations of Essentials, notably that Essentials is object storage only, and currently does not provide high availability. However, the process of creating your instance, configuring disks, pools and volumes are the same.

Planning Your Instance

There are numerous considerations when creating any storage solution, and SoftNAS Cloud® is no exception. Dependent on the use case, the expected performance levels, the platform you select, and much more, one configuration of SoftNAS Cloud® will look much different from the rest. For the purposes of a basic proof of concept deployment (or POC), many of these elements might seem irrelevant, but they are not. For a POC to be of value, it must provide insight into not only the product but also what you intend to use it for. If your POC is not designed to provide you a baseline of the functionality you expect in a production environment, then it may be a wasted exercise.

To ensure your instance meets your needs, the following considerations are key:

- **Instance Size** – What performance characteristics do you require? A great deal of RAM to handle large-scale data storage? Processing power (vCPU) to handle encryption or compression?
- **Storage** – What performance characteristics do you require from your storage? Is it an infrequently accessed archive? Is it a database serving a demanding application?
- **Network/Throughput** – do you require a great deal of throughput? Does your use case require constant and immediate access to the data in question?
- **Security** – Should data be encrypted? Do you wish to restrict access to a specific IP or IP range? What traffic do you wish to allow?
- **Type of High Availability** - Will you be leveraging SoftNAS’ standard SNAP HA functionality, or is this an object storage configuration for which Dual Controller HA is the best option? See AWS Getting Started: Choosing your HA Solution for more information.

In order to assist you during the creation of the POC, we will be providing information on the key considerations listed above as they arise in the creation process.

VMware HA Considerations

As we are creating a highly available deployment on VMware, there are a few requirements specific to setting up high availability through SoftNAS. SnapReplicate™ can be performed as described in SnapReplicate™, and requires only two nodes.

Setting up SNAP HA™ in any VMWare virtualized environment requires the following:

- Two SoftNAS Cloud® controller nodes for replication and their corresponding IP addresses (DNS names) and networking credentials.
- A virtual IP within the storage VLAN subnet (see HA Design Principles for more information).
- An additional SoftNAS controller node is required, to act as an HA Controller. This SoftNAS SNAP HA™ Controller node is necessary, as it acts as a 3rd party witness and controller to all SNAP HA™ failover and takeover operations.
- Replication must be set up between the two SoftNAS Cloud® controller nodes.

Of the above considerations, the primary difference between VMware instances and Cloud based instances is the requirement of a third SoftNAS VM as HA controller.
- VMware Getting Started - Deploying SoftNAS Cloud Virtual Machines
- VMware Getting Started - Adding Storage
- VMware Getting Started - Configuring High Availability
- VMware Getting Started - Project Planning
- VMware Getting Started: Choosing Your HA Solution
Deploying Your First SoftNAS Instance in VMware vSphere

Deploying your SoftNAS instance through VMware is a simple process. After obtaining the SoftNAS OVF file from our site (via purchase or trial, see Launching SoftNAS Cloud® Platforms), note the storage location, and make sure it is accessible from the machine hosting your vSphere Client.

1. Log into your vSphere client with the appropriate credentials.
2. Select the ESXi host upon which you will be placing the virtual machine (if there is more than one to choose from).
3. Click File, and Deploy OVF Template.

4. Click Browse to go to the location of your OVF file, and select it.
5. Click **Next**, then **Next** again on **OVF Template Details**.
   Type a name, select a location, and click **Next**.
6. Select the Host or Cluster you wish to deploy on, and click **Next**.
7. Select a Resource Pool. Click **Next**.
8. Select your destination storage. Click **Next**.
9. Select a Disk Format, depending on your requirements. For example if running your VM in an environment with space constraints, select thin provisioning. Look to VMware help for more information. Click Next.
10. Select a network for your VM. If creating an HA environment, be sure to select the same network as other instances.
Note: If creating an HA environment, you will require at least three VMs, two to act as paired nodes, and one to act as HA Controller. Plan accordingly.

11. Click Finish.

Your SoftNAS VirtualMachine will deploy after a short interval.

Customizing the System Using the SoftNAS Console

SoftNAS appliances provide a Console for managing key settings in VMware vSphere.

1. Log into vSphere Client.
2. On the Home Page, double click the Host and Clusters option under the Inventory section.
All **Hosts and Clusters** will be displayed.

3. Right click on the **SoftNAS VM** and select **Open Console** option.
4. The console of the selected VM will be displayed.

**Note:** Check the status of VM on the console. If it is off, power it on. Right click on the **SoftNAS VM** and select the **Power On** option.
The **Console** with the new configuration screen will be displayed.
The Console has 3 options:

- **Customize System** - To Customize the system, press the F2 function key on the keyboard.
- **Run Desktop** - To run the desktop, press the F8 function key on the keyboard.
- **Shutdown/R Restart** - To shutdown or restart the system, press the F12 key on the keyboard.

5. To configure our SoftNAS Instance, we will select F2 to customize our system.

6. Enter an authorized login name and password for the logged in VM. If the defaults have not been changed, use the login id as ‘root’ in the Login text entry box. Enter the root password as **Pass4W0rd** in the Password text entry box (change the root password using the console). Press the **Enter** key on the keyboard to log in.

7. The **System Customization** screen will be displayed. The **System Customization** screen allows configuration of all the core components of the network (VMware vSphere platforms only).

The screen has the following options:

- Configure Password
- Configure Management Network
- Restart Management Network
- Test Management Network
- Network Restore Options
- Configure Date and Time
8. Use the Up/Down arrows on your keyboard to navigate between the options.

Changing the Password

1. In the System Customization Console, navigate to the Configure Password option.

2. Press Enter.
   The Configure Root and SoftNAS Password screen will be displayed.
   Setting the password for the "root" and "softnas" login names will prevent unauthorized access to this host.
3. Enter the old (or default) password in the **Old Password** field.

4. Enter the new password in the **New Password** field.

5. Confirm the password by re-entering it in the **Confirm Password** field.

6. Press **Enter**.

The password will be reset.

**Configuring the Management Network**

1. On the **System Customization Console**, navigate to the **Configure Management Network** option.

2. Press **Enter**.
   The **Configure Management Network** screen will be displayed.
From here, we can configure the following options:

- Network Adapters
- IP Configuration
- DNS Configuration
- Custom DNS Suffixes

**Note:** To view or modify this host’s management network settings in detail, select the required option and press the Enter key on the keyboard. Configure the selected adapter’s IP Address and DNS settings.

3. On the **Network Adapters** option, press the **Enter** key on the keyboard.
   The network adapter screen will be displayed with the available interfaces.

4. Check the **Mac Address** and **Status** of the device.
   Press the **Esc** key on the keyboard.
   The **Configure Management Network** screen will be displayed.
5. Navigate to the **IP Configuration** option. Press **Enter**.
The IP Configuration dialog will be displayed.

6. Select the network adapter for configuration. Press **Enter** key on the keyboard.
The configuration options for the selected adapter will be displayed.
This adapter can obtain network settings automatically on a network including a DHCP server. If it does not, configure the right options.

7. Scroll down to static IP address and network configuration.
To select it, press the **Spacebar** key on the keyboard.

8. Set the static IP address. For simplicity's sake you can lock in the DHCP assigned IP address.

9. Configure the subnet mask address.

10. Enter the default gateway.
Press the **Enter** key on the keyboard to accept the changes.

11. Back on the **Configure Management Network** screen, note the DNS Configuration option.
12. Press **Enter**.

**Note:** This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically. As we set our instance to a static IP in the previous step(as per best practice), we will need to supply the appropriate DNS information.
13. Configure the required settings.


When using short, unqualified names, DNS queries will attempt to locate the specified host by appending the suffixes listed here in the order shown until a match is found or the list is exhausted.

If no suffixes are specified here, a default suffix list is derived from the local domain name.

DNS queries will attempt to locate hosts by appending the suffixes specified here to short, unqualified names.

15. Enter the proper suffix in the Suffixes field. Use spaces or commas to separate multiple entries. Press Enter.

**Restarting the Management Network**

After making changes to your Management Network, it is always best practice to restart the network. This step is often required to restore networking or renew a DHCP lease.

1. To restart the management network, on the System Configuration screen, select the Restart Management Network option.
2. Press Enter on your keyboard.

**Note:** Restarting the management network will result in a brief network outage that may temporarily affect running virtual machines.

**Testing the Management Network**

1. On the System Configuration screen, select the Test Management Network option.

2. To perform a brief network test, press the Enter key on the keyboard.

By default, this test will attempt to ping the configured default gateway, ping the configured primary and alternate DNS servers, and resolve the configured hostname.
Updating VMware Tools

As with any VM, it is important to ensure VMware Tools are current and operating correctly. SoftNAS ships with the latest version of VMware Tools already installed, but it is a recommended best practice to ensure the VMware Tools are installed and compatible.

SoftNAS makes use of the vmxnet 3 network driver to support 10 GbE virtual NICs, support which is provided by drivers that come with VMware Tools. These drivers are compatible across all ESXi 5.x versions.

To update VMware Tools on Linux, follow VMware's instructions here. Log in as root (use the default password “Pass4W0rd” if the administrator has not yet changed the root password). To log in, open up a console window on VMware and press F8 in the SoftNAS Console, log in with the root password, then log into the SoftNAS Desktop and launch a command shell, then follow the VMware Tools installation and update instructions.

As shown below, after pressing F8, enter the root password.

![SoftNAS Console with root login interface]

We recommend automatic kernel rebuilds (the last question during VMware Tools installs), so that VMware Tools remains compatible with future kernel updates.

Configuring Your Instance via SoftNAS StorageCenter™

Once connected to your instance, there are several common configuration steps which may or may not be required, depending on your use case. Some of the below configurations should already be configured from the VMware console (notably password and network settings), however, you should at least be familiar with how to make changes in SoftNAS StorageCenter itself, should changes be required later. The Getting Started Checklist provides a guide to these tasks.
1. The first of these tasks is Network Settings. For your VMware instance, network settings are taken care of during setup in the System Customization Console. However, if adding additional network interfaces, or changing IP addresses, routing and gateways, hostnames or host addresses, this can be done via **Network Configuration**, in the **Storage Administration** pane under **Settings**.

2. Your default password should have been changed via the VMware console as described in the previous section. However, any required password changes can also be performed from within the SoftNAS StorageCenter™ interface.

   a. Changing your password is simple. From the **Storage Administration** pane, under **Settings**, select **Change Passwords**.

   ![Change Password](image)

   b. Select the account(s) you wish to change. SoftNAS recommends changing the default password for both the **softnas** and **root** user(s) at a minimum.
c. Once the account you wish to change is selected, provide the new password. If handing the instance to a new administrator, check the box to **Force user to change password at next login**. This will allow the new softnas admin to select his own password. Click **Change**.

3. The third step is to ensure your instance is up to date. To update your SoftNAS Cloud Instance, expand **Settings** in the **Storage Administration** pane, and select **Software Updates**. If an update is available, the latest version will be listed, and you will see an option to **Apply Update Now**.

   Click **Apply Update Now** to begin the update. To ensure customers are aware that downtime may occur, a confirmation prompt will appear. Click **Yes** to begin the upgrade. Be sure not to shut down the Virtual Machine or interrupt the upgrade process. Click **Finish** when prompted. This will trigger a reboot, requiring you to log back into your instance.

   **Note:** SoftNAS recommends reading the linked Release Notes. The Release Notes may contain information not only about the features and fixes, but also about whether the update will require downtime, allowing you to plan accordingly. This is not particularly relevant for a POC deployment, but important in a production scenario.

   **Note:** Updating your software to obtain the latest features, security improvements and bug fixes is always recommended. SoftNAS takes this recommendation a step further, and has tied the latest updates to their **No Downtime Guarantee**. This ensures our clients are receiving the best version of our product.
and support to match. To be eligible for the No Downtime Guarantee, the following minimum requirements must be met:

- Software version must be 3.4.9.7 or above.
- Software updates must be applied within 30 days of availability.

4. Next comes licensing your instance. If you do need to apply a license (you can obtain a free trial license by registering here) simply go to the Storage Administration pane, and select Licensing, under Settings.

Provide the license in the field provided, as well as organizational information. Your license will be sent to your registration email, and can also be found by logging into the SoftNAS portal.

5. To ensure that SoftNAS support, and you as an administrator for your SoftNAS Cloud instance, have adequate information to troubleshoot your instance, it is important to provide a means of communication. For this reason, an email address must be supplied to which support reports and logs can be sent at scheduled intervals, or if there is a specific problem.

To establish a notification email, expand Settings in the Storage Administration pane, and select Administrator. Go to the Monitoring tab, and enter the email address you wish reports and logs to be sent to.

Note: Providing a notification email is a requirement. If you do not provide one during instance configuration, you will be required to provide one prior to configuring SnapReplicate™.

Note: Support Reports and notifications will be sent to SoftNAS support automatically. The notification email is to ensure the administrator for the instance is kept apprised.

Deploying Your 2nd SoftNAS Instance on VMware vSphere

1. Log into your vSphere client with the appropriate credentials.

2. Select the same ESXi host upon which you deployed the first virtual machine (if there is more than one to choose from).

3. Click File, and Deploy OVF Template.

4. Click Browse to go to the location of your OVF file, and select it.

5. Click Next, then Next again on OVF Template Details.

6. Type a name, select the same location as your previous VM, and click Next.

7. Select the Host or Cluster you deployed on previously, and click Next.

8. Select the same Resource Pool. Click Next.
9. Select your destination storage. Click Next.

10. Select a Disk Format, mirroring the first VM. Click Next.

11. Select a network for your VM. If creating an HA environment, be sure to select the same network as other instances.

12. Click Finish.

Your 2nd SoftNAS instance will deploy after a short interval.

13. Configure your instance with a static IP address and change your password via the SoftNAS console as described above.

14. Upgrade your instance if necessary, license your instance, and make any other changes required to mirror the first SoftNAS VM within SoftNAS StorageCenter as described in Configuring Your Instance via SoftNAS StorageCenter™.

Deploying Your HA Controller VM

1. Log into your vSphere client with the appropriate credentials.

2. Select the same ESXi host upon which you deployed the first two virtual machines (if there is more than one to choose from).

3. Click File, and Deploy OVF Template.

4. Click Browse to go to the location of your OVF file, and select it.

5. Click Next, then Next again on OVF Template Details.

6. Type a name, select the same location as your previous VM, and click Next.

7. Select the Host or Cluster you deployed on previously, and click Next.

8. Select the same Resource Pool. Click Next.

9. Select your destination storage. Click Next.

10. Select a Disk Format, mirroring the first VM. Click Next.

11. Select a network for your VM. If creating an HA environment, be sure to select the same network as other instances.

12. Click Finish.

Your HA controller SoftNAS instance will deploy after a short interval.

13. Configure your instance with a static IP address and change your password via the SoftNAS console as described above.

Be sure to record the IP address of the HA controller in order to have it handy when setting up SNAP HA™.
VMware Getting Started - Adding Storage

Adding Storage to your Source and Target SoftNAS Cloud Virtual Machine

You will not be adding storage to the third virtual machine created, as it acts as a 3rd party witness and controller to all SNAP HA™ failover and takeover operations. The following steps will be performed on the two virtual machines designated as source and target for HA and replication.

1. Log into your vSphere client and find the first of the newly created VMs. In this example, the VM is named SofTNAS_Kai_1. Right-click the virtual machine and select **Edit Settings**.

*Note:* Adding hard disks can be done regardless of whether the virtual machine powered up, or offline. If changing the available RAM, the VM must be powered off.
2. In Virtual Machine Properties for your selected machine, click **Add**.

3. Select **Hard Disk** from the available options, and click **Next**.
4. Select **Create a New Virtual Disk**, and click **Next**.
5. Select **Disk capacity**, and **Disk Provisioning**. If space is at a premium in your environment, we recommend thin-provisioning. Thick-provisioning VMware datastores provides increased write performance, and should be preferred over thin-provisioning of VMDKs when optimal performance is required.

Here you can also decide where you wish to draw this additional storage capacity from. By default, **Store with the virtual machine** will be selected, which simply means that the VMDK will be stored in the same datastore used by the virtual machine itself. Alternatively, you can select a different datastore, by clicking the radio button labelled **Specify a datastore or datastore cluster**. One reason to do this might be that one datastore offers better performance than another – for example, one might be comprised of SSD storage, while the other consists of magnetic drives. For this POC example, we will stick with the default.
6. Next, you will be provided with advanced options. As it states, these will rarely need to be changed. The effects of each change are explained alongside each option. For this POC, the default settings will be kept. Click Next.
7. Next, a summary of your selections will be presented. Verify the selections and click Finish if all is as expected.
8. The VMDK (hard disk) will be created and added to your virtual machine after a few moments. Wait for the disk to be added.

9. If using SoftNAS’ Software RAID, you will need to add a number of disks commensurate with the RAID level selected. Repeat the above process as necessary to provide the number of disks required for your desired RAID level (for example, RAID 1 will require two VMDKs of the same size and configuration).

In order to show a basic software RAID configuration in upcoming steps, two hard disks will be created, and configured with RAID 1 in the upcoming Creating a Pool and Volume section.

Preparing the Target Node

Repeat the process above, and add the same number and configuration of disks to your target virtual machine. Your second virtual machine should mirror the first virtual machine in every aspect, up until this point.

Remember, no additional disks need to be added to the HA controller node. This will remain a default SoftNAS Cloud virtual machine, with no additional configuration changes.

Creating a CIFS enabled Volume in your Source Virtual Machine
As mentioned at the beginning of this document, we are guiding you towards the creation of a CIFS enabled volume on a highly available pairing of SoftNAS virtual machines. With VMware, the underlying storage available will have a great deal to do with performance – if your underlying disks are SSD, performance will be better than with magnetic drives. This is perhaps self-evident, but must be mentioned as you will want to ensure your POC mirrors your intended use case as closely as possible.

With VMware, the underlying storage is not added via the SoftNAS® StorageCenter™ interface, but from within VMware itself, as described in Adding Storage. However, it is possible to leverage AWS or Azure storage as described in SoftNAS’ documentation.

For more information about adding disk devices from cloud services, see the following:

- Adding Amazon EBS Disks
- Adding Cloud Disk Extenders
- Adding Azure Block Storage from the SoftNAS UI
- Adding Object Storage from the SoftNAS UI

However, for the purposes of this document, we will be using the disks created in the previous section. They will, however, need to be partitioned.

### Partitioning Disks

1. Log into your ‘source’ SoftNAS virtual machine via your web browser, and the IP address assigned to your virtual machine.

   **Note:** In order to access your virtual machine, you must be logged into the same network your virtual machines are hosted on.

2. In the Storage Administration Pane, select the Disk Devices option under the Storage section. The Disk Devices panel will be displayed.

   ![Disk Devices panel](image)

3. Disk devices must be partitioned prior to use. The available devices are listed in the Available Devices grid, as shown above.

   The Device Usage column indicates the current status of the device, which can be:

   - **Device needs partition** - the initial state for a new device that has no partition
- **Available to assign** - the device is partitioned and ready for use in a storage pool
- **Used in pool <poolname>** - the device is in use by the indicated storage pool name

4. Use the buttons on the toolbar to partition the devices for initial use.
   a. Use **Partition All** to partition all disk devices.

   ![Partition All Button](image)

   b. Alternatively, select each disk device, then use **Create Partition** to partition each device individually.

   ![Create Partition Button](image)

   c. Remove Partition can be used to remove an existing partition that is no longer needed.

**Create the Storage Pool**

1. Click the **Storage Pools** option under the Storage section in the Storage Administration Panel (on the left).
2. The Storage Pools panel will be displayed with the list of all the existing storage pools that are already allocated. To create a new storage pool, click Create.
3. The Add Storage Pool dialog will be displayed.

![Add Storage Pool dialog]

a. Here you will determine whether you wish to create a ‘Standard’ storage pool with block storage, such as EBS volumes or Azure Standard or Premium disks, or if you wish to create a single pool of shared storage by leveraging object storage from the platform of your choice (Azure Hot or Cool Blob or Amazon S3 object storage). If deploying a highly available configuration, the selection made here will determine how SNAP HA will be implemented.

- **Standard** - If Standard is selected, our patented original SNAP HA™ methodology will be implemented, replicating your block storage across two nodes, with minute by minute updates to ensure parity.
- **Shared Storage** - If Shared Storage is selected, SNAP HA will initiate a Dual Controller HA™ configuration, which will instead propagate the configuration files of your storage pool to both nodes (each acting as a controller in this scenario) in the HA pairing, allowing the shared storage pool to be nearly immediately imported in the event of primary node failure.

Click **Next** to begin creating your pool via the Create a New Storage Pool dialog box.

**Note:** Regardless of the option selected here, the process for configuring High Availability with SNAP HA™ remains unchanged. Dual Controller HA™ is a simple add-on to SNAP HA™. SNAP HA™ will recognize automatically which method to use based on the selection made above, and will configure high availability according to the storage pool settings. Each instance can support both standard SNAP HA™ and Dual Controller HA™ configurations in a mixed environment.

4. Upon clicking **Next**, the Create a New Storage Pool wizard will open. Fill in the required information based on the directions to follow:

a. Enter the name for the storage pool to be created in the **Pool Name** text entry box.
Some example storage pool naming schemes might include:

- **Generic naming**: naspool1, naspool2, ...
- **Disk-type naming**: SAS1, SAS2, SATA1, SATA2
- **Use-case naming**: OS1, OS2, Exchange1, SQLData1, UserData1, Geology, Accounting, IT, R&D, QA, Corp01, etc.

b. Select the redundancy level from the RAID Level drop down list.

**Note:** If using hardware RAID at the disk controller level and have a single data disk presented to SoftNAS Cloud® for a storage pool, then software RAID may not be required; in such case, select No RAID/JBOD, as the RAID is implemented at a lower level and no Software RAID will be necessary.

c. Select the disks to be allocated to this storage pool.

**Note:** Each of the devices show the Disk Availability status as Available for Use. This implies that these disks are already partitioned. New disk devices must be partitioned before use. Remember to select the appropriate number of disks for your Software RAID selection.

d. In the **Choose Pool Options** step, check the box in the Forced Creation field to overwrite any older pools on the disks selected.

**Note:** If any of the disk devices chosen have been used as a part of another storage pool in the past (e.g., one that was deleted), use the Forced Creation option to overwrite the previous data in
e. Decide whether you wish to add LUKS Encryption (optional).

**Note:** LUKS encryption allows you to add a layer of security to your SoftNAS volumes and pools, and if implemented along with Data-In-Flight encryption via SMB3 for CIFS, or by tunneling through SSH for NFS, can protect your data both at rest and in-flight.

- To add LUKS encryption check the box.
- In the Type dropdown, select Password.
- Provide a password and confirm.

f. Choose the required Sync Mode:

**standard:**

This is the default option. Synchronous file system transactions (fsync, O_DSYNC, O_SYNC, etc) are written out (to the intent log) and then secondly all devices written are flushed to ensure the data is stable (not cached by device controllers).

**always:**

For the ultra-cautious, every file system transaction is written and flushed to stable storage by a system call return. This obviously has a big performance penalty.

**disabled:**

Synchronous requests are disabled. File system transactions only commit to stable storage on the next DMU transaction group commit which can be many seconds. This option gives the highest performance, but may result in out-of-spec behavior, application data loss and increased vulnerability to replay attacks, as ZFS is ignoring the synchronous transaction demands of applications such as databases or NFS. This option does *NOT* affect ZFS on-disk consistency. Administrators should only use this when these risks are understood.

5. Click **Create**.

The new storage pool is created and is ready for use.

**Create the Volume**

1. Click the **Volumes and LUNS** option under the Storage section in the Storage Administration Panel (on the left).
2. Click **Create** in the toolbar.

3. The **Create Volume** dialog will be displayed.
3.
   a. Enter the name of the volume in the Volume Name text entry box.
   b. To select the storage pool where the storage space for the volume has to be reserved. Type the name of the storage pool, or click the Storage Pool button.

   The Choose a Storage Pool dialog will be displayed. Select the desired pool from the listed options, and click Select Pool.
Select the required storage pool from the list of available storage pools. Click Select Pool. Back in the Create Volume dialog, the name of the selected storage pool will be displayed in the Storage Pool field.

c. Select the type of the volume from the Volume Type section. The available volume types are File System (NFS, CIFS, AFP) and Block Device (iSCSI LUN).
d. For this POC, we are creating a CIFS volume. Click Share via CIFS.

e. Select the type of the storage provisioning option. The available options include:
   Thin Provision - Dynamically allocate space as it is needed.
   Thick Provision - Preallocate space from storage pool now.

   If Thick Provision is selected, you will have to specify the size of the volume in the Volume Size field and select the size unit. Once a Storage Pool has been selected for a thick-provisioned volume, the amount of available space to allocate is displayed below the Volume Size field.

   The Volume Size value can be any valid numeric value; e.g., 10, 12.5, 100.0, 1.25, provided it does not exceed available storage of the
f. Select the required option for storage optimization in the Storage Optimization Options section. The available options are Compression and Deduplication. The Compression type saves disk space, but requires more of CPU space. The Deduplication type eliminates duplicates, but consumes more memory space.

Note: When compressing a significant amount of data, be sure to observe the amount of actual CPU consumed during a typical day, and if necessary, add more CPU capacity to the SoftNAS Cloud® VM as required to ensure compression is fast and efficient. If data is not highly compressible, then disabling compression provides a better performance tradeoff.

Note: It is recommended to avoid using deduplication unless the data is highly-duplicative, because of the memory impact of deduplication. It is estimated that for every terabyte of deduplicated data managed, one gigabyte of memory is required for the deduplication lookup tables. These tables compete with cache memory, which can reduce the overall performance of SoftNAS Cloud®.

g. Sync mode can be determined at the volume level as well as at pool level.

standard:

This is the default option. Synchronous file system transactions (fsync, O_DSYNC, O_SYNC, etc) are written out (to the intent log) and then secondly all devices written are flushed to ensure the data is stable (not cached by device controllers).

always:

For the ultra-cautious, every file system transaction is written and flushed to stable storage by a system call return. This obviously has a big performance penalty.

disabled:

Synchronous requests are disabled. File system transactions only commit to stable storage on the next DMU transaction group commit which can be many seconds. This option gives the highest performance, but may result in out-of-spec behavior, application data loss and increased vulnerability to replay attacks, as ZFS is ignoring the synchronous transaction demands of applications such as databases or NFS. This option does *NOT* affect ZFS on-disk consistency. Administrators should only use this when these risks are understood.

4. Click Create.

Preparing the 2\textsuperscript{nd} Virtual Machine for HA

The second SoftNAS instance must mirror the first in almost every respect. This means adequate storage space must be provided, as well as a storage pool ready to receive the volume in a failover situation.

1. Log onto the 2\textsuperscript{nd} instance using its public IP address, the softnas username, and the default password (the instance ID, unless changed).
2. If you have not yet done so, add two hard disks by following the instructions provided earlier in Adding Storage to your Source and Target SoftNAS Cloud Virtual Machine. Provide the same type and amount of storage and the same number of disks as for your first virtual machine.
3. Create a storage pool by following the instructions provided above in Create the Storage Pool. The pool MUST have the same name as the pool in the first SoftNAS instance.

You will NOT create a volume on the second instance. The storage pool on the 2\textsuperscript{nd} instance will serve as a
landing strip for the volume (and any data contained within) in a failover situation once SnapReplicate™ and SNAP HA™ have been configured.
What is Dual Controller HA?

Dual Controller HA™ is an extension to our existing SoftNAS Cloud® high availability solution, SNAP HA™. It is designed to provide high availability for a shared pool of object storage only.

Adding a device to a dedicated storage pool results in the pool being replicated in the usual way, via SyncImage and asynchronous SnapReplicate ZFS send/receive once per minute, ensuring a copy of the pool’s data is maintained on the target node. HA failover operates as always, with dedicated storage devices and pools on each node having their own distinct, non-shared data that requires replication for use in HA (original design of SNAP HA). SoftNAS SNAP HA™ provides NFS, CIFS and iSCSI services via redundant storage controllers. One controller is active, while another is a standby controller. As only one controller is active at a time, this can be considered single-controller HA.

Dual Controller HA™ on the other hand, only applies if a shared pool of object storage, such as AWS S3, or Azure Hot or Cool blob storage, is specified at storage pool creation. After adding object storage ‘disks’ via Disk Devices, and selecting Create in Storage Pools, the following dialog will appear. If Shared Storage is selected, Dual Controller HA™ will automatically be applied to the shared pool after SNAP HA™ is configured.

Shared pools operate very differently from dedicated pools from an HA perspective. First, underlying storage devices are shared across nodes. Such shared devices (e.g., S3 cloud disks, Azure Hot and Cool Blob storage) include their own data redundancy, and are typically accessed over a network connection, enabling it to be shared across two or more nodes (only two nodes are currently supported).

A second major difference is the take-over process for shared pools. Volume configuration files are replicated between both the primary and secondary controller (hence Dual Controller). Failover is initiated at the point the primary controller fails to reply to an IO request within the expected time frame.

During a take-over event, first the devices associated with a shared pool must be mounted by the target node (and sometimes disconnected or unmounted from the original node, if required by the device type). Next, the shared pool is imported using the ZFS import command (and verified the pool was imported successfully and is not degraded or faulted). The appropriate level of both debug_TRACE and info/error logging is provided in existing HA log files, to ensure it’s possible to troubleshoot and provide support in the field if errors or issues arise.

With this method of failover:

- Very little data needs to be transferred for fail-over to occur.
- There is no need to create duplicate pools of already resilient object storage.
- No potential loss of transactional data occurs due to standard SNAP HA asynchronous replication delays.

To determine if Dual Controller HA is right for your deployment, see VMware Getting Started: Choosing your HA Solution.

No change to Dedicated Pools

As stated above, Dual Controller HA does not change the way SNAP HA is configured, nor does it change how it operates for dedicated pools. SoftNAS has worked very hard to ensure that this feature is a seamless addition, with little to no change to existing functionality, or configuration.

Regardless of whether it is a shared pool or dedicated, the customer must first define a SnapReplicate™ relationship between the primary and secondary node, then add the SNAP HA relationship. In other words, there is no change to the SnapReplicate/SNAP HA process shown below.
Adding a device to a shared storage pool results in the pool being excluded (skipped) by SnapReplicate; i.e., the data on the underlying device is already shared across nodes, so there is no need to replicate shared storage pools. This involves a change in SnapReplicate’s “pool discovery” logic, forcing it to first read the sharedpools.xml file to get the list of shared pool names, then exclude those pools from the list of pools to be replicated (similar to how pool names not found on the target node get excluded).

This allows SnapReplicate and SNAP HA to function across both types of pools, and to differentiate between them. Existing SNAP HA customer installations continue to operate uninterrupted, and new SoftNAS instances can be paired with both Dual Controller HA shared storage pools and dedicated pools asynchronously replicating via “standard” SNAP HA simultaneously. This also ensures that regardless of which type of pool selected, the customer can confidently set up SNAP HA with the same documentation.

**Configuring SnapReplicate™**

Having prepared the environment on both SoftNAS Cloud AWS instances, we can now set up high availability. The first step towards high availability in SoftNAS is to establish replication. SnapReplicate™ makes this as simple as completing a quick wizard.

To establish the secure SnapReplicate relationship between two SoftNAS Cloud® nodes, simply follow the steps given below:

1. Log into the source controller’s (the first instance within which you created the CIFS enabled volume) SoftNAS StorageCenter administrator interface using a web browser.

2. In the Left Navigation Pane, select the **SnapReplicate™/SNAP HA™** option.

   ![SnapReplicate/SNAP HA page](image)

   The **SnapReplicate/SNAP HA** page will be displayed.

3. Click the **Add Replication** button in the **Replication Control Panel**.
The **Add Replication** wizard will be displayed. Read the instructions on the screen and then click the **Next** button.

4. In the next step, enter the IP address or DNS name of the remote, target SoftNAS Cloud® controller node in the Hostname or IP Address text entry box. Note that by specifying the replication target's IP address, you are specifying the network path the SnapReplicate™ traffic will take.
5. The source node must be able to connect via HTTPS to the target node (similar to how the browser user logs into StorageCenter using HTTPS). HTTPS is used to create the initial SnapReplicate configuration. Next, several SSH sessions are established to ensure two-way communications between the nodes is possible. Ensure that any firewall that may interfere in the connectivity between your two nodes are configured to allow SSH and HTTPS traffic from the IP addresses of the nodes.

Provide the username (softnas) and the password (if default, this is the instance id) of the target instance. Type the password again to verify, then click Next.

The IP address/DNS name and login credentials of the target node will be verified. If there is a problem, an error message will be displayed.
Click the Previous button to make the necessary corrections and then click the Next button to continue.

6. Read the final instructions and then click the Finish button.

The SnapReplicate relationship between the two SoftNAS Cloud® controller nodes will be established. The corresponding SyncImage of the SnapReplicate will be displayed.

After data from the volumes on the source node is mirrored to the target, once per minute SnapReplicate transfers keep the target node hot with data block changes from the source volumes.

The tasks and an event log will be displayed in the Replication Control Panel section. This indicates that a
SnapReplicate relationship is established and that replication should be taking place.

**Configuring SNAP HA™**

SnapReplicate™ establishes a replication relationship, one that can be manually triggered or scheduled, but is not automated. For true high availability in a failover situation, SNAP HA™ must be configured as well.

1. To configure SNAP HA™, complete the SNAP HA wizard, beginning by clicking **Add SNAP HA™**.

   ![Add SNAP HA™](image1)

   **Note:** Configuration of SnapReplicate™ is a prerequisite to setup of SNAP HA™. If SnapReplicate™ is not configured, the **Add SNAP HA™** button will be grayed out.

   If you have not yet configured a notification email, the opportunity to provide one will be presented prior to continuing SNAP HA™. Provide an email address for support reports and logs to be sent to, and click **OK**.

   ![Please enter Notification Email](image2)

2. Click **Add SNAP HA™** once more if you had not yet provided a notification email. The **Add High Availability** wizard will begin.
3. Provide a Virtual IP address, and click Next. This is a human-configured IP address (you choose the IP), and can be any IP address that falls outside the CIDR block of the IP inside of the two SoftNAS HA paired nodes.

4. Next, you will provide the IP address of the HA Controller virtual machine created earlier.
5. Click **Install** to begin the HA installation.

6. Click **Next** once installation completes.
7. Click **Finish** to complete HA setup.

At this point SoftNAS Cloud® will do all of the heavy lifting that is required to establish HA, without the need for any user intervention. The process may take several minutes.

Once complete, you should see the SNAP HA™ status shown in the SnapReplicate™/ SNAP HA™ Overview.
Overview.

VMware Getting Started - Project Planning
VMware Getting Started - Project Planning

Configuring VM Settings

Required Settings

After installing the OVF to create the **SoftNAS Virtual Storage Appliance VM**, configure the VM settings in accordance with best practices and network needs. The boot disk (Hard Disk 1) should be set to 30 GB, thin-provisioned. This is the default configuration, and should not be changed without reason.

For a quick benchmarking resource configuration, use 4 vCPUs and 4 to 8 GB of RAM. Configure storage and run benchmarking tools to observe resource utilization in the **SoftNAS StorageCenter Dashboard** charts and vSphere performance charts.

**RAM Note:** The operating system and **SoftNAS** consume up to 1 GB of RAM, using most of the remaining RAM for cache memory and metadata. The more RAM assigned to the VM, the better cache performance will be, as SoftNAS will keep as much data in RAM cache as possible. Consider this resource allocation for deduplication: at least 1 GB of RAM per terabyte of deduplicated storage, to keep the deduplication tables in memory (or supplement the RAM cache with a read cache device).

Optional Settings

**Paravirtual SCSI Disk Controller Support**

For maximum throughput and IOPS on VMware, choose the **Paravirtual SCSI Controller** for the **SoftNAS VM** instead of using the default LSI Logic Parallel SCSI controller.

**VM Snapshot Mode**

Before applying software updates to **SoftNAS** after it is in production, and to support online backups in popular backup programs, VM snapshots are useful as part of the backup and recovery process. Depending on the plan to manage backups of VM data, choose which mode snapshots will operate in.

- **Independent Mode** - to enable smaller VM snapshots, configure the boot disk, Hard Disk 1, in the “Independent” mode. This causes VM snapshots to apply only to this first hard disk by default (and not include all added data disks, which could be prohibitively large). The advantage of using independent mode is VM snapshots will be faster and smaller.
- **Dependent Mode** - by default, VM snapshots include all hard disks attached to the VM. When used with SoftNAS and a VM backup process, this setting causes all SoftNAS VM disks to be backed up together as a set. This results in much larger backup sets, but may be preferable as a means of achieving additional protection and recoverability in the event of a disaster or need to restore the entire storage system to a different computer or location. If there are only a few terabytes to back up, this may be the prudent choice.

**Network Adapter**

On a typical 1 gigabit network, the default E1000 network adapter is sufficient; however, for a 10 gigabit or higher-performance network card, the VMXNET 3 network adapter should be used for best results and higher throughput. Note that installation of the VMXNET 3 requires installation of the proper VMware Tools in the guest operating system (in this case, CentOS 64-bit Linux).

**Memory / CPU Hot Plug**

It is recommended to **allow CPU Hot Plug** and **disable Memory Hot Add**, which will make it more convenient to add CPU later to use a lot of data compression or other features that consume additional CPU. Linux seems to do fine when additional CPU are added at run-time.

**Note:** Add memory with the system powered down and disable hot add of memory at run-time.
Performance Tuning for VMware vSphere

Achieving peak storage performance in the VMware environment involves tuning the VMware configuration beyond default values. The following are recommended best practices for tuning VMware for use with SoftNAS.

VMDirectPath

VMDirectPath provides a means of passing a disk controller device directly through to the guest operating system (i.e., CentOS Linux).

To enable VMDirectPath Configuration page in the vSphere Client

1. Select the ESX host from Inventory.
2. Select the Configuration tab.
3. Select Advanced Settings under Hardware.
4. Edit and select device (storage controller, physical NIC)

Note that Intel VT-d (or equivalent) processor feature is required for support of VMDirectPath.

VM SCSI Controller - Set to Paravirtual

In VMware, change the SCSI controller type to "Paravirtual", which provides more efficient access to storage.

Physical NIC Settings

A host physical NIC can have settings, which can provide better utilization and performance improvement:

Most 1GbE or 10GbE NICs (Network Interface Cards) support a feature called interrupt moderation or interrupt throttling, which coalesces interrupts from the NIC to the host so that the host does not get overwhelmed and spend too many CPU cycles processing interrupts.

To disable physical NIC interrupt moderation on the ESXi host execute the following from ESXi SSH session.

Find the appropriate module parameter for the NIC by first finding the driver using the ESXi command:

```
# esxcli network nic list
```

Then find the list of module parameters for the driver used:

```
# esxcli system module parameters list -m <driver>
```

This example applies to the Intel 10GbE driver called ixgbe.

```
# esxcli system module parameters set -m ixgbe -p "InterruptThrottleRate=0"
```

Also, check the host for SR-IOV support, which provides additional performance and throughput in virtualized systems like VMware.

Adjust Network Heap Size for high network traffic

By default, the ESX server network stack allocates 64MB of buffers to handle network data. Increase buffer allocation from 64MB to 128MB memory to handle more network data.
To change Heap Size ESX Host:

Go to the Configuration tab for the ESX Server host, and select Advanced Settings-VMkernel - Boot-VMkernel.Boot.netPktHeapMaxSize

Virtual NIC Settings

VM’s virtual adapter has many tuning options, which can also provide much better throughput:

Configure jumbo frames (MTU 9000) in vSwitch and virtual network adapter (be sure physical switch supports MTU 9000)

We recommend VMXNET 3 virtual NICs.

Disable virtual interrupt coalescing for VMXNET 3 virtual NICs as follows:

Go to the vSphere Client, then to VM Settings - Options tab - Advanced General - Configuration Parameters and add an entry for ethernetX.coalescingScheme with the value of disabled.

An alternative way to disable virtual interrupt coalescing for all virtual NICs on the host which affects all VMs, not just the latency-sensitive ones, is by setting the advanced networking performance option (Configuration -Advanced Settings - Net) CoalesceDefaultOn to 0 (disabled).

Disable LRO

Reload the vmxnet3 driver in the SoftNAS CentOS guest operating system. Log into the SoftNAS Cloud® VM using SSH (or the Desktop Console) and su root:

# modprobe -r vmxnet3

Add the following line in /etc/modprobe.conf:

(options vmxnet3 disable_lro=1)

Then reload the driver using:

# modprobe vmxnet3

Physical Host BIOS Settings

On most servers, these BIOS Settings can improve the overall performance of the host:

- Turn on Hyper-threading in BIOS
- Confirm that the BIOS is set to enable all populated sockets for all cores
- Enable “Turbo Mode” for processors that support it
- Confirm that hardware-assisted virtualization features are enabled in the BIOS
- Disable any other power-saving mode in the BIOS
- Disable any unneeded devices from the BIOS, such as serial and USB ports
- In order to allow ESXi to control CPU power-saving features, set power management in the BIOS to “OS Controlled Mode” or equivalent. Even without planning to use these power-saving features, ESXi provides a convenient way to manage them.
- C-states deeper than C1/C1E (i.e., C3, C6) allow further power savings, though with an increased chance of performance impacts. We recommend, however, enabling all C-states in BIOS, then use ESXi host power management to control their use.

NUMA Settings
NUMA systems are advanced server platforms with more than one system bus. They can harness large numbers of processors in a single system image with superior price to performance ratios. The high latency of accessing remote memory in NUMA (Non-Uniform Memory Access) architecture servers can add a non-trivial amount of latency to application performance.

For best performance of latency-sensitive applications in guest OSes, all vCPUs should be scheduled on the same NUMA node and all VM memory should fit and be allocated out of the local physical memory attached to that NUMA node.

Processor affinity for vCPUs to be scheduled on specific NUMA nodes, as well as memory affinity for all VM memory to be allocated from those NUMA nodes, can be set using the vSphere Client under VM Settings – Options tab – Advanced General – Configuration Parameters and adding entries for “numa.nodeAffinity=0, 1, …,” where 0, 1, etc. are the processor socket numbers.

**Networking Tips**

10 Gigabit Network Configurations on VMware vSphere

By default, the **SoftNAS Cloud® VM** (on **VMware vSphere**) ships with the default E1000 virtual NIC adapter and VMware defaults to MTU 1500.

For best performance results above 1 gigabit, follow the steps outlined below:

1. Replace the **E1000** virtual NIC adapter with a **vmxnet3** on the **SoftNAS Cloud® VM**.

2. Use **MTU 9000** instead of **MTU 1500** for **vmKernel** and physical switch configurations. Be sure to configure the network interface in SoftNAS for **MTU 9000** also.

3. Refer to the **MTU 9000** section for more information.

A dedicated VLAN for storage traffic is recommended. For VMware, refer to the **Performance Tuning for VMware vSphere** section for details.

**iSCSI Multi-pathing**

To increase performance throughput and resiliency, use of **iSCSI** multipathing is recommended by VMware and other vendors.

Since **SoftNAS** operates in a hypervisor environment, it is possible to configure multi-path operation as follows:

1. On the **VMware** host where the **SoftNAS Cloud® VM** runs, install and use multiple physical NIC adapters.

2. Assign a dedicated **vSwitch** for each incoming **iSCSI** target path (one per physical NIC).

3. Assign the **SoftNAS Cloud® VM** a dedicated virtual NIC adapter for each incoming iSCSI target path (per **vSwitch** physical NIC).

4. Assign a unique IP address to each corresponding Linux network interface (for each virtual NIC attached to the **SoftNAS Cloud® VM**).

5. Restart the **SoftNAS iSCSI** service and verify connectivity from the iSCSI initiator client(s) to each iSCSI target path.

A dedicated VLAN for storage traffic is recommended.
Customers using our product for the first time, or introduced to our newest HA feature, Dual Controller HA, for the first time, may be uncertain of which option best suits their needs. Each high availability option has its own benefits and limitations, which will be covered below, allowing you to make an informed decision. Bear in mind that this does not mean a decision must be made between the two, as both solutions can be used in conjunction with the other. Dual Controller HA is an integrated part of SNAP HA™ but for the purposes of this discussion, SNAP HA will refer to our standard SNAP HA™ replication technology, and Dual Controller HA (or DCHA) will refer to our shared object storage solution.

SNAP HA™

Existing customers will need no introduction to our SNAP HA™ product, which offers a low-cost, low-complexity solution for high-availability clustering that is easy to deploy and manage. A robust set of HA capabilities protect against data center, availability zone, server, network and storage subsystem failures to keep business running without downtime. SNAP HA™ for Amazon Web Services (AWS) includes patent-pending Elastic HA™ technology, providing NAS clients in any availability zone uninterrupted HA access to the storage cluster across availability zones.

SNAP HA™ operates by maintaining a redundant copy of all storage on the primary node, and constantly replicating this data to a secondary node, ensuring that both copies remain synchronized through our patented SnapReplicate™ technology. SNAP HA™ then monitors all critical storage components, ensuring they remain operational and when there is an unrecoverable failure in a system component, another storage controller detects the problem and automatically takes over, ensuring that no downtime and no business impacts (or very limited business impacts) occur. The data on the second storage controller is identical to the primary node and is presented immediately and seamlessly, ensuring that the end-user never knows an outage occurred.

Key Differences:

- **Duplication of Storage:** Standard SNAP HA™ replicates data from one node to another. This means that the target node will have copies of the pools and volumes on the primary. This means that each node must maintain an equivalent amount of storage.

- **Storage Type Flexibility:** SNAP HA™ can use any combination of block and object storage. Pools and Volumes can be created from:
  - **Block storage including:**
    - Azure Disk
    - AWS EBS
  - **Object Storage including:**
    - AWS S3
    - AWS S3 Infrequent
    - Azure Cold Blob
    - Azure Hot Blob
    - S3 compliant object storage

- **Separate Locations:** SNAP HA™ enables customers to rely on two completely separate storage systems - where data is completely replicated to 2 different locations ensuring any primary storage use cases remain operational. DCHA is reliant on object storage in a single location - if the cloud location is compromised (for example an AWS region-wide failure), the storage will become unavailable.

- **Faster Recovery:** For most use cases, our standard SNAP HA™ solution offers faster fail-over and recovery times in comparison to DCHA. This is because DCHA requires several ZFS checks behind the scenes to complete the transfer of ownership of the shared storage pool.

**Performance and Data Integrity Considerations:**
SoftNAS’ ZFS based solution provides a great deal of protection to ensure that your data is fully protected, but in a fail-over situation, default settings can potentially result in uncached write bursts not being committed to the target volumes. SoftNAS balances these concerns with performance considerations. If data integrity is of paramount importance, and you want the enhanced protection afforded by hosting your data in two separate locations, we recommend changing the Sync Mode when creating your pool to the ‘Always’ setting. This setting ensures every file system transaction is written and flushed to stable storage by a system call return, but at a significant performance cost. See Create a Storage Pool for more information about Sync Mode settings.

Alternatively, performance can be maintained while still further protecting against potential data loss by creating a ZIL, or as it is referred to within the SoftNAS UI, a Write Log. This process is covered in Configuring the Read Cache and Write Log.

**Dual Controller HA (DCHA)**

Dual Controller HA™ (or DCHA) is an extension to our existing SoftNAS Cloud® high availability solution, SNAP HA™. It is designed to provide high availability for a shared pool of object storage. DCHA only applies if a shared pool of object storage, such as AWS S3, or Azure Hot or Cool blob storage, is specified at storage pool creation. After adding object storage ‘disks’ via Disk Devices, and selecting Create in Storage Pools, the following dialog will appear. If Shared Storage is selected, Dual Controller HA™ will automatically be applied to the shared pool after SNAP HA™ is configured.

Regardless of whether it is a shared pool or dedicated, the customer must first define a SnapReplicate™ relationship between the primary and secondary node, then add the SNAP HA relationship. In other words, there is no change to the SnapReplicate/SNAP HA process. Adding a device to a shared storage pool results in the pool being excluded (skipped) by SnapReplicate; i.e., the data on the underlying device is already shared across nodes, so there is no need to replicate shared storage pools.

This allows SnapReplicate and SNAP HA to function across both types of pools, and to differentiate between them. Existing SNAP HA customer installations continue to operate uninterrupted, and new SoftNAS instances can be paired with both Dual Controller HA shared storage pools and dedicated pools asynchronously replicating via “standard” SNAP HA simultaneously. This also ensures that regardless of which type of pool selected, the customer can confidently set up SNAP HA with the same documentation.

**Key Differences**

- **No Duplication**: While both DCHA and SNAP HA require the configuration of two nodes, DCHA does not require the duplication of storage. Underlying storage devices, whether they be Azure Blob or AWS S3 object storage, are shared across the two nodes.

- **Object Storage Only**: DCHA applies only to object storage. Object Storage such as AWS S3, or Azure Hot or Cool blob storage, is typically accessed by network connection, allowing it to be accessed by two or more nodes (only two nodes are supported by DCHA for the moment). Block storage cannot be shared in the same way.

  DCHA can be used with the following:
  - AWS S3
  - AWS S3 Infrequent
  - Azure Cold Blob
  - Azure Hot Blob
  - S3 compliant object storage

- **Single Storage Location**: DCHA protects the storage controller and the storage media via object storage; however, it relies on a single data store that may be disrupted if a cloud element experiences an outage.

- **Slower Recovery**: Because standard SNAP HA™ only has to spin up local pre-existing storage, the failover window is much smaller than with Dual Controller HA™, which requires several ZFS data integrity checks to complete.