SoftNAS CLOUD®

A Complete Platform for Highly Available Storage

SoftNAS™ High Availability Guide

Table of Contents

Introduction

Enterprise-Grade High-Availability with Low Complexity and Low Cost

SoftNAS™ SNAP HA™ High Availability delivers 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™ 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 no downtime or business impacts occur.

SNAP HA™ works hand in hand with **SoftNAS Cloud®** data protection features, including RAID, and automatic error detection and recovery, and as a result, reduces operational costs and boosting storage efficiency.

High Availability protects companies from lost revenue when access to their data resources and critical business applications would otherwise be disrupted with features that:
1) Protect against unplanned storage outages 24 x 7 x 365
2) Provide disaster recovery capabilities to quickly resume mission-critical operations in the event of a disaster (e.g., across availability zones or data centers)
3) Ensure failed components are quickly and automatically identified and isolated, so they do not cause data loss, application errors or downtime
4) Replicate data so there is an up-to-the-minute copy of any changes that have taken place
5) Prevent outdated or incorrect data from be made available due to multiple failures across the storage environment
6) Assure business owners that applications and IT infrastructure continue operating uninterrupted by unexpected failures in the storage environment
7) Enable IT administrators to take storage systems offline for maintenance and repair, without disrupting production IT systems or applications

Minimize Downtime from Host and Storage Failures

SoftNAS™ SNAP HA™ High Availability delivers the availability required by mission-critical applications running in virtual machines and cloud computing environments, independent of the operating system and application running on it. HA provides uniform, cost-effective failover protection against hardware and operating system outages within virtualized IT and cloud computing environment. HA:

• Monitors **SoftNAS Cloud®** storage servers to detect hardware and storage system failures
• Automatically detects network and storage outages and re-route NAS services to keep NFS and Windows servers and clients operational
• Restarts **SoftNAS Cloud®** storage services on other hosts in the cluster without manual intervention when a storage outage is detected
• Reduces application and IT infrastructure downtime by quickly switching NAS clients over to a another storage server when an outage is detected
• Maintains a fully-replicated copy of live production data for disaster recovery
• Is quick and easy to install by any IT administrator, with just a few mouse clicks using the automatic setup wizard

Extend and Enhance Data Protection Across Enterprise Infrastructure

Most availability solutions are tied to specialized hardware or require complex setup and configuration. In contrast, an IT administrator configures **SoftNAS SNAP HA™** with a few clicks from within the **SoftNAS**

StorageCenter™ client interface. With simple configuration and minimal resource requirements, **SNAP HA™** allows administrators to:

• Provide uniform, automated data protection and availability for all applications without modifications to the application or guest operating system
• Establish a consistent first line of data protection defense for an entire IT infrastructure
• Protect data and applications that have no other failover options, which might otherwise be left unprotected and subject to extended outages and downtime
• In Amazon Web Services cloud environment, provide storage HA across AWS availability zones
• Compatible with **SoftNAS Cloud®** advanced NFS file servers, Windows CIFS file servers, and iSCSI SAN servers.

Highly-Available NAS Services

SoftNAS SNAP HA™ provides NFS, CIFS and iSCSI services via redundant storage controllers. One controller is active, while another is a standby controller. Block replication transmits only the changed data blocks from the source (primary) controller node to the target (secondary) controller. Data is maintained in a consistent state on both controllers using the ZFS copy-on-write filesystem, which ensures data integrity is maintained. In effect, this provides a near real-time backup of all production data (kept current within 1 to 2 minutes).

Storage Monitoring

A key component of **SNAP HA™** is the HA Monitor. The HA Monitor runs on both nodes that are participating in **SNAP HA™**. On the secondary node, HA Monitor checks network connectivity, as well as the primary controller's health and its ability to continue serving storage. Faults in network connectivity or storage services are detected within 10 seconds or less, and an automatic failover occurs, enabling the secondary controller to pick up and continue serving NAS storage requests, preventing any downtime.

Storage Failover

Once the failover process is triggered, either due to the HA Monitor (automatic failover) or as a result of a manual takeover action initiated by the admin user, NAS client requests for NFS, CIFS and iSCSI storage are quickly re-routed over the network to the secondary controller, which takes over as the new primary storage controller. Takeover on VMware typically occurs within 20 seconds or less. On AWS, it can take up to 30 seconds, due to the time required for network routing configuration changes to take place.

Operation in AWS Virtual Private Cloud

In AWS, **SNAP HA™** is applied to SoftNAS storage controllers running in a Virtual Private Cloud (VPC). It is recommend to place each controller into a separate AWS Availability Zone (AZ), which provides the highest degree of underlying hardware infrastructure redundancy and availability.

Virtual IP Setup

Each AZ operates on a separate subnet; e.g.. 10.0.1.0/24 and 10.1.0.0/24 (choose how to organize the subnet addresses in the VPC based on expected requirements). **SoftNAS SNAP HA™** can now take advantage of Virtual IPs. One virtual IP address is assigned to each VPC instance, set up within the same CIDR block. A third lone IP address is set up on a separate CIDR block, to manage NAS client traffic requirements.

Virtual IPs are isolated from internet traffic completely, increasing the security of your HA VPC setup. For this reason, a Virtual IP driven private HA setup is our recommended best practice.

HA storage traffic uses a dedicated network interface (interface 1), which further isolates storage traffic.

Elastic IP setup

Traditionally, an elastic IP provided NAS clients across all AZs access to HA storage. Until recently Elastic IPs were the only IPs capable of re-routing network traffic across AZs. **SoftNAS SNAP HA™** enhances the standard elastic IP provided by AWS, creating a patent-pending "Elastic HA™" (EIP). Elastic HA IPs are managed by the HA controller, ensuring NAS client traffic is properly routed to the active primary storage controller at all times.

HA storage traffic uses a dedicated network interface (interface 1), which further isolates storage traffic.

There's a common misconception that elastic IPs are only useful for Internet-based access to EC2 instances. While that is the most common use case by far, Elastic HA IP addresses are typically configured using a Security Group which restricts access within the AZ private network only. This prevents any possible Internet-based access to Elastic HA IPs.

VPCs can also be configured for use with VPNs, which enables secure access from an administrator's office location to the private network (no other inbound Internet access is typically available). It is possible to attach optional elastic IP addresses to interface 0 on each SoftNAS controller instance for remote administration (restricted IP range access recommended).

Operation in VMware Private Clouds

On VMware, it is common to dedicate a non-routable VLAN to storage traffic. The storage VLAN segregates primary storage traffic (e.g., VMDKs attached to VMs over NFS or iSCSI) from other traffic. Data replication traffic can also be placed on its own separate non-routed VLAN. **SoftNAS StorageCenter™** is typically placed on a routable VLAN (the default network), where it can be readily accessed by admins from a web browser from anywhere within the organization (or via a VPN).

A Virtual IP (VIP) address is employed to route NAS client traffic to the primary storage controller. In the event of a failover or takeover, the VIP is reassigned to the other controller, which immediately re-routes NAS client traffic to the proper controller.

High-integrity Data Protection

A number of measures are taken to ensure the highest possible data integrity of the HA storage system. An independent "witness" HA controller function ensures there is never a condition that can result in what is known as "split-brain", where a controller with outdated data is accidentally brought online. **SNAP HA™** prevents split-brain using a number of industry-standard best practices, including use of a 3rd party witness HA control function that tracks which node contains the latest data. On AWS, shared data stored in highly-redundant S3 storage is used. On VMware, a separate HA Controller VM is used.

Another HA feature is "fencing". In the event of a node failure or takeover, the downed controller is shut down and fenced off, preventing it from participating in the cluster until any potential issues can be analyzed and corrected, at which point the controller can be admitted back into the cluster.

Finally, data synchronization integrity checks prevent accidental failover or manual takeover by a controller which contains data which is out of date.

The combination of high-integrity features built into **SNAP HA™** ensures data is always protected and safe, even in the face of unexpected types of failures or user error.

Scales to Hundreds of Millions of Files

SNAP HA™ has been validated in real-world enterprise customer environments and is proven to handle hundreds of millions of files efficiently and effectively. The use of block replication instead of file replication supports hundreds of millions of files and directories.

Paravirtualization (PV) vs Hardware Assisted Virtual instances (HVM)

Paravirtualization (PV) is an efficient and lightweight virtualization technique introduced by the Xen Project team, later adopted by other virtualization solutions. PV does not require virtualization extensions from the host CPU and thus enables virtualization on hardware architectures that do not support Hardware-assisted virtualization. This has become less and less an issue in recent years. With the increase in popularity of virtualization, chip manufacturers like Intel and AMD implemented hardware virtualization support beginning in 2006. Today's hardware platforms such as Intel's Ivy Bridge used in EC2's R3, C3, I2 instance types have very complete technology support for HVM.

Unlike PV guests, HVM guests can take advantage of hardware extensions that provide fast access to the underlying hardware on the host system. HVM AMIs are required to take advantage of enhanced networking and GPU processing. In order to pass through instructions to specialized network and GPU devices, the OS needs to be able to have access to the native hardware platform; HVM virtualization provides this access.

Traditionally, Paravirtual guests performed better for storage and network operations than hardware assisted guests because they could leverage special drivers for I/O that avoided the overhead of emulating network and disk hardware. In contrast, HVM guests had to translate these instructions to emulated hardware. Recently, this has changed. These PV drivers are now available for HVM guests, so operating systems that could not be ported to run in a paravirtualized environment (such as Windows) can still see performance advantages in storage and network I/O by using them. With these PV on HVM drivers, HVM guests can get the same, or better, performance than paravirtual guests, even on workloads that traditionally performed better on PV.

In other words, HVM guests now have the best of both worlds, and automatically select the path that provides best performance. Paravirtualization is slowly being phased out, or the best parts of it integrated with HVM. PV is still a strong option for legacy hardware scenarios, but will be less and less useful as companies upgrade their hardware to newer chipsets with hardware virtualization support.

System Requirements

Minimum System Requirements

The following minimum system requirements must be met for **SNAP HA™**:
• 2 GB RAM
• 4 vCPU

AWS Minimum Requirements
• Virtual Private Cloud (VPC)
• 1 Elastic or Virtual IP address, used to route NAS client traffic across availability zones
• 2 SoftNAS storage controller EC2 instances (**Note:** micro instance is not compatible with only 640 MB RAM)
• Amazon S3 storage (2 MB of S3 storage will be allocated in same region as EC2 instances
• Two 1 GB virtual interfaces on each instance
• EBS disks and/or S3 Cloud Disks for each storage controller's local storage

VMware Minimum Requirements
• 2 SoftNAS storage controller VMs
• HA Controller VM is required, with a recommended min. of 500 MB RAM and 1 vCPU
• One 1 Gb virtual NIC (shared for admin, replication and HA monitor - not recommended best practice, minimum for demo systems)
• Two 1 GbE physical NICs
• One or more VMDK virtual disks for storage

Recommended Configurations
The following configurations are recommended best practices for **SoftNAS SNAP HA™**:
• 8 to 64 GB RAM
• 4 vCPU (8 vCPU if volume data compression will be used extensively)
• SSD for read cache and write log
• Separate replication and storage traffic to dedicated physical networks

Note: SNAP HA relies on time settings in both the primary and secondary instances. It is important to use the same time for each. If an NTP is used, configure both with the same URL.

AWS Requirements
• Virtual Private Cloud (VPC)
• 3 Virtual IP addresses 1) one used to route NAS client traffic across availability zone. This IP address must be in a separate CIDR block. 2) one for each instance for **SoftNAS StorageCenter™** remote administration. Virtual IP setup is recommended.
• Alternatively, 3 Elastic IP addresses: 1) one used to route NAS client traffic across availability zones, 2) one each for **SoftNAS StorageCenter™** remote administration.
• Alternatively, use a VPC with private VPN access to **SoftNAS StorageCenter™** for administration, with 1 Elastic IP address for NAS client traffic
• 2 each SoftNAS storage controller EC2 instances

Note: micro instance is not compatible with only 640 MB RAM

• Amazon S3 storage (2 MB of S3 storage will be allocated in same region as EC2 instances
• 2 virtual interfaces on each instance. First interface is used for **SoftNAS StorageCenter™** and replication, second interface for Elastic HA IP for NAS traffic
• For storage VLAN, choose EC2 instance types for NAS clients and **SoftNAS StorageCenter™** that support MTU 9000 (required for 10 GbE maximum throughput)
• EBS disks and/or S3 Cloud Disks for each storage controller's local storage
• For highest throughput, use HVM instances with local, ephemeral SSDs for read cache, high-IOPS EBS volume (SSD) for write log and EC2 instances with 10 GbE network interfaces

• Use EBS volumes for primary storage in RAIDz-2 configuration for best data density and RAID-10 with high-IOPS EBS volumes for best IOPS in database and transactional applications
• Use S3 disks for lower IOPS, highly-redundant mass-storage up to 4 PB per S3 disk device

VMware Requirements

• HA Controller VM is required, the recommended minimum is 500MB of RAM and 1vCPU
• 2 each SoftNAS storage controller VMs
• 1 each HA Controller VM with 500 MB RAM and 1 vCPU configured to use VMware FT (fault-tolerance) to ensure HA Controller is always available
• 3 each virtual NICs - separate vNIC and VLAN allocated to: 1) **SoftNAS StorageCenter™** administration (E1000), 2) **SnapReplicate™** block replication (E1000), 3) storage VLAN (VMXNet3)
• For storage VLAN, configure for MTU 9000 (required for 10 GbE maximum throughput)
• DirectPath pass-through disk controller providing direct disk access (requires Intel VT-d and disk controller supported by CentOS). This is required for best small block 4K/8K I/O and synchronous write-log and read cache performance with VMware
• Separate disk controllers for 1) booting VMware from RAID-1 mirrored disks and 2) storage I/O
• 4 each 10 GbE or 1 GbE physical NICS (2 active/active for VMware host management and SoftNAS administration and replication, 2 active/active for data storage)

Optional

• Boot VMware from 32 GB USB, and dedicate disk controller for DirectPath disk I/O
• VMDKs for SATA and SAS storage and read cache
• Infiniband NIC for data storage pathway

Installation and Setup

System Requirements for SoftNAS SNAP HA™ Installation

If you have already created the VPCs that are to be made highly available, then skip the **Amazon Web Services VPC** section in favor of the chapters for **Virtual IP Setup**, or **Elastic IP**, depending on the setup desired. Virtual IP Setup is our strong best practice recommendation.

The following requirements must be met for a successful **SNAP HA™** install:

Software Requirements

• The **SnapReplicate™** feature must be enabled.

Note: No separate HA license is required for SoftNAS Cloud® at any level of service.

Supported Platforms

SNAP HA™ can be enabled on the following platforms:

• **Amazon Web Services VPC**
• **VMWare vSphere**

Adding HA pairings to Active Directory

The process for joining your HA pairing to Active Directory can be found in the **SoftNAS Installation Guide: Active Directory Configuration**. If connecting SoftNAS instances in a High Availability pairing to Active Directory, it is **very important** that the process is performed twice, once on each node. Active Directory configurations do not carry over to the second node automatically because the target node's NAS services (amongst others) are not running while the node is dormant. Settings cannot be automatically triggered upon takeover. In order for the second instance to remain in Active Directory after a failover the second node must be added as well.

Amazon Web Services VPC

Amazon AWS Installation Overview

This section describes how to set up an Amazon AWS Virtual Private Cloud (VPC) in high availability (HA) mode to work with **SoftNAS SNAP HA™**. SoftNAS SNAP HA for EC 2 now supports the use of Virtual IPs, and is our best practice recommendation. Configuration with Elastic IPs is still fully supported.

The following is required

- Create the VPC in AWS.
- Specify the **IAM User for SoftNAS Cloud®**
- Configure the routing tables.
- Launch an Instance of **SoftNAS Cloud®** into the VPC.
- Create and Associate the Required Elastic or Virtual IPs.
- Set up **SoftNAS Cloud®** for HA.

Note: The HA IAM Role is caps sensitive, and must be named **SoftNAS_HA_IA**M.

Creating the VPC

A VPC is a private, isolated section of the AWS cloud that can be set up in a variety of configurations.

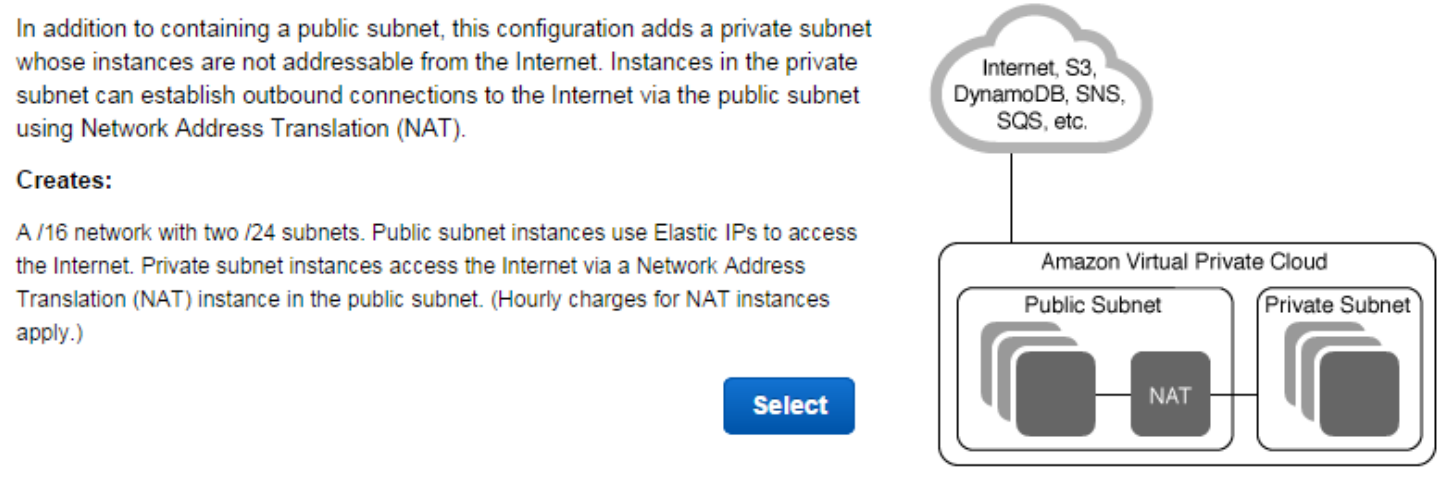
1. From the VPC Dashboard, click on **Start VPC Wizard.**

2. Select **VPC with Public and Private Subnets** as the configuration scenario.

3. Click on **Select.** The **Create an Amazon Virtual Private Cloud** screen is displayed.

Note: Private subnet instances access the Internet via a Network Address Translation (NAT) instance in the public subnet. (Hourly charges for NAT instances apply.)

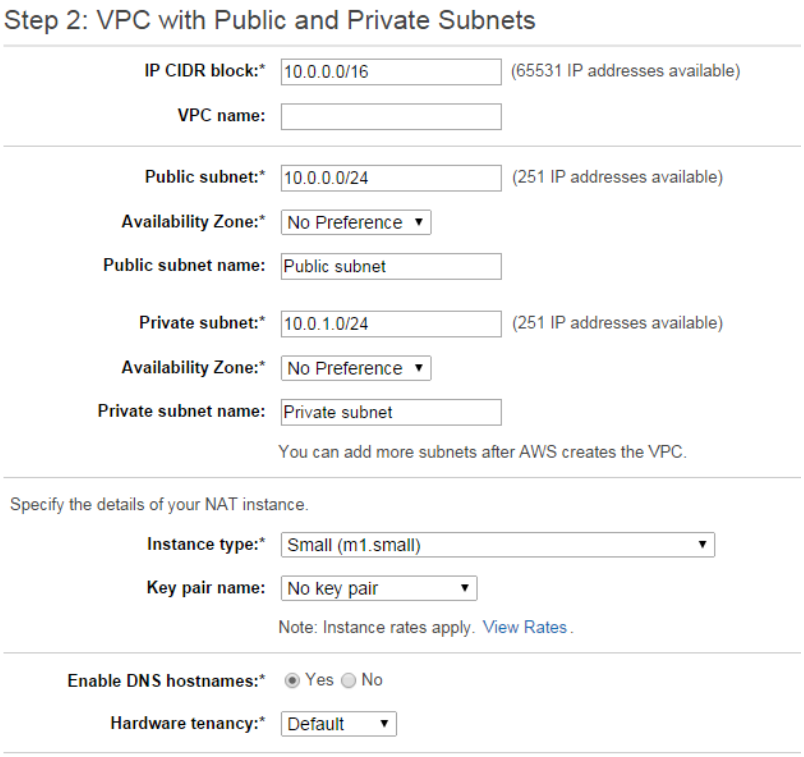
Note: You may not require NAT setup if setting up a Private instance using Virtual IPs. While not required for Private instances, there are some organization specific instances where set up of NAT is relevant.



4. Configure the IP CIDR block, Public and Private Subnets, and all other settings as appropriate. In this guide's example, the 70.0.0.0/16 VPC will be used for configuration procedures.

Configuration Best Practices to Consider Now:

- Select different availability zones when configuring the subnets for the greatest level of VPC redundancy.
- Select the proper instance type for intended usage, including anticipated networking and storage needs.
- Select a valid Key Pair that is secured and available for use.



5. Click on **Create VPC.** AWS will create the VPC with the Public and Private subnets.

Note: If a NAT instance is not required for the local **SoftNAS Cloud®** deployment, delete the NAT instance and release any assigned Elastic IPs. Amazon hourly charges apply to NAT instances.

Specify the IAM User for SoftNAS Cloud®

About Amazon IAM Users

AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon RDS, and the AWS Management Console. With IAM, centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

Create an AWS IAM User for **SoftNAS Cloud®**. This will allow **SoftNAS Cloud®** instances to use the credentials of the AWS IAM User when accessing the VPC. For a step-by-step guide to setting up your IAM user, see **Creating the SoftNAS Cloud® IAM Role for AWS**.

Setting Up the Routing Tables

In the routing tables configuration, ensure that both the private and public subnets are associated to the main routing table of the VPC and that the default route uses the IP gateway. This will enable access to the VPC using an elastic IP address.

To set up the routing tables

1. From the VPC Dashboard, click **Route Tables**.

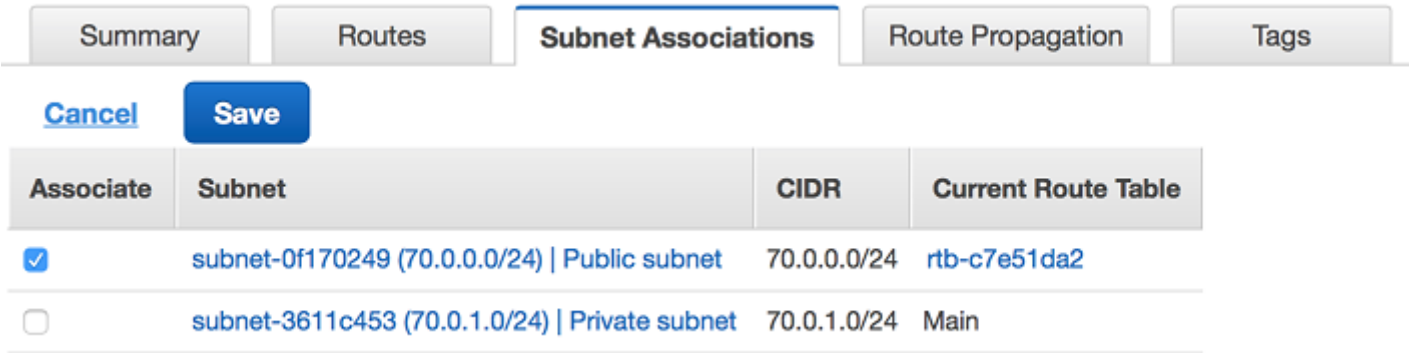
2. The available routing tables are displayed. In the screenshot below, the main routing table for the 70.0.0.0 VPC has no associated subnets. We want to ensure that both the public and private subnets are associated to the main routing table.

	Route Table ID	Associated With	Main	VPC
☐	rtb-d17087b4	1 Subnet	No	vpc-de6597bb (70.0.0.0/16)
☐	rtb-4a4a5e28	1 Subnet	No	vpc-1a667378 (60.0.0.0/16)
☐	rtb-454a5e27	1 Subnet	Yes	vpc-1a667378 (60.0.0.0/16)
☐	rtb-d67087b3	0 Subnets	Yes	vpc-de6597bb (70.0.0.0/16)
☐	rtb-eea8b18c	1 Subnet	No	vpc-4e29312c (10.0.0.0/16)
☐	rtb-c72f80a6	2 Subnets	Yes	vpc-c52f80a4 (50.0.0.0/16)
☐	rtb-e8a8b18a	0 Subnets	Yes	vpc-4e29312c (10.0.0.0/16)

3. Click on the main routing table to select it. The route table settings will appear at the bottom of the screen.

4. Click on **Subnet Associations**, and ensure that both the private and public subnets are associated to the main routing table. Click the down arrow to select the subnet for association.

5. Click **Edit**. Select the desired subnets from the available subnets menu provided and **Save**.



Default Routes:

When creating a VPC, the default route for the main routing table is the NAT instance. However, depending on the networking environment, it may be required to redirect this route to an internet gateway.

Note: The following procedure is optional. Use of the NAT gateway may be appropriate depending on the networking setup.

1. From the main route table settings, click on **Routes.** The default route to the NAT device is displayed.

2. Click **Remove** next to the default route.

3. Click **Yes** when prompted by the Delete Route screen.

4. Recreate the default route (0.0.0.0/0) and point it to the internet gateway, by selecting it from the **Target** dropdown.

Launch An Instance of SoftNAS Cloud® into the VPC

To launch an instance of **SoftNAS Cloud®** into the already-set-up VPC, the following is required:

• Select the appropriate **SoftNAS Cloud® AMI** from the Marketplace AMI section of EC2 services.
• Select at least the small instance
• Configure the instance details
    a. Launch instance into the subnet
    b. Add an additional ethernet interface
    c. Add storage as required
    d. Tag the instance
    e. Set up security groups
    f. Select a key pair for SSH

• The above procedure is repeated to create a second **SoftNAS Cloud®** instance for HA.

Selecting the SoftNAS Cloud® AMI

1. For **SoftNAS Cloud®**, navigate to AWS Marketplace AMIs.

2. Select the **SoftNAS AMI** from the **Community AMI** section of **EC2** services.

3. From EC2 services, click on **Launch Instance>Marketplace AMIs** and enter **SoftNAS** in the search text box**.**

4. Select the appropriate **SoftNAS Cloud®** version for expected need (Express, Standard, or Enterprise).

Choosing an Instance Type

SoftNAS requires at least the use of a small instance type.

1. From **Step 2. Choose an Instance Type**.

2. Select the appropriate machine type for expected usage from the matrix given. For more information on Amazon Instance types, click **here**.

3. Click on **Next: Configure Instance Details.**

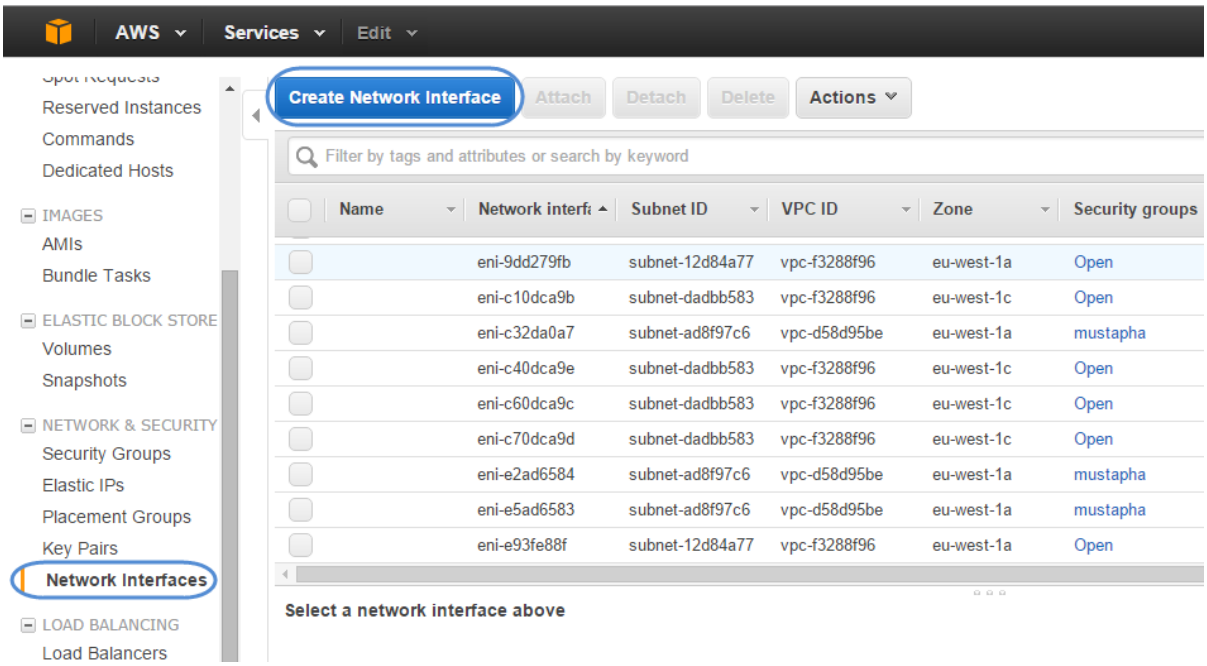
Instance Details

1. For **Network**, select the previously configured VPC.

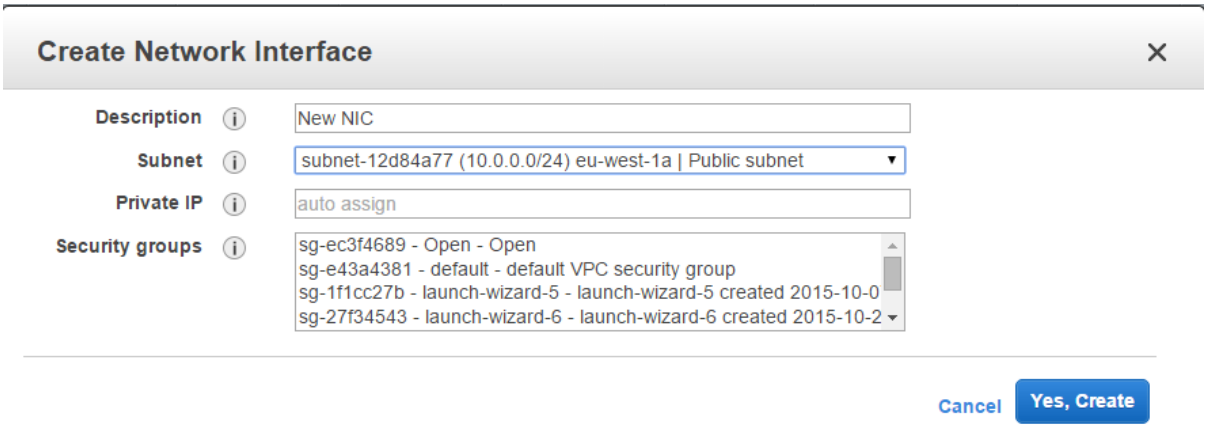
2. Select one of the available public or private subnets to associate with this instance.

3. Scroll to **Network Interfaces**, expand, and click **Add Device**. If using Elastic IPs for your HA instance, it is very important to add an additional **NIC** here as well as your storage.
To add an additional NIC:

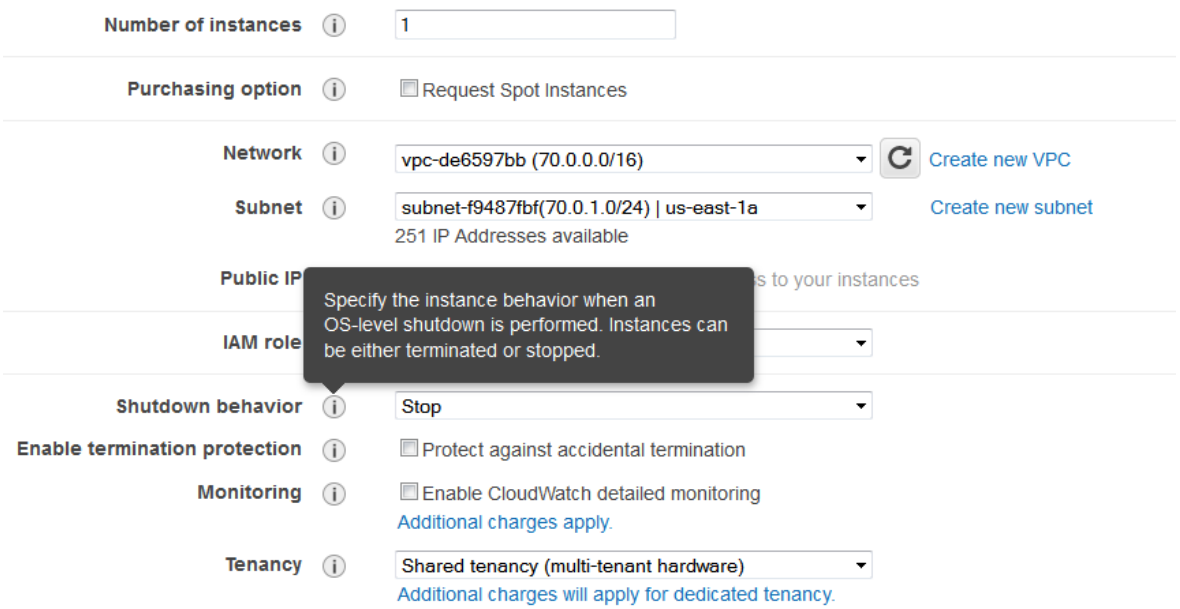
a) Select Network Interfaces from within the EC2 console, then **Create Network Interface**.



b) Provide a name, select your subnet and a security group. Click **Create**.



4. Click on **Next: Add Storage.**



Adding Storage and Tagging

1. From the storage screen, add storage volumes as necessary. Ensure that **Delete on Termination** is selected.

2. Click **Next**: **Tag Instance** and add an instance name to the **Value** field.

3. Click **Next: Configure Security Group**

Note: Disk names for EBS volumes must follow **SoftNAS Cloud®** storage naming conventions. For more information, see the document **SoftNAS Installation Guide**.

Security Groups

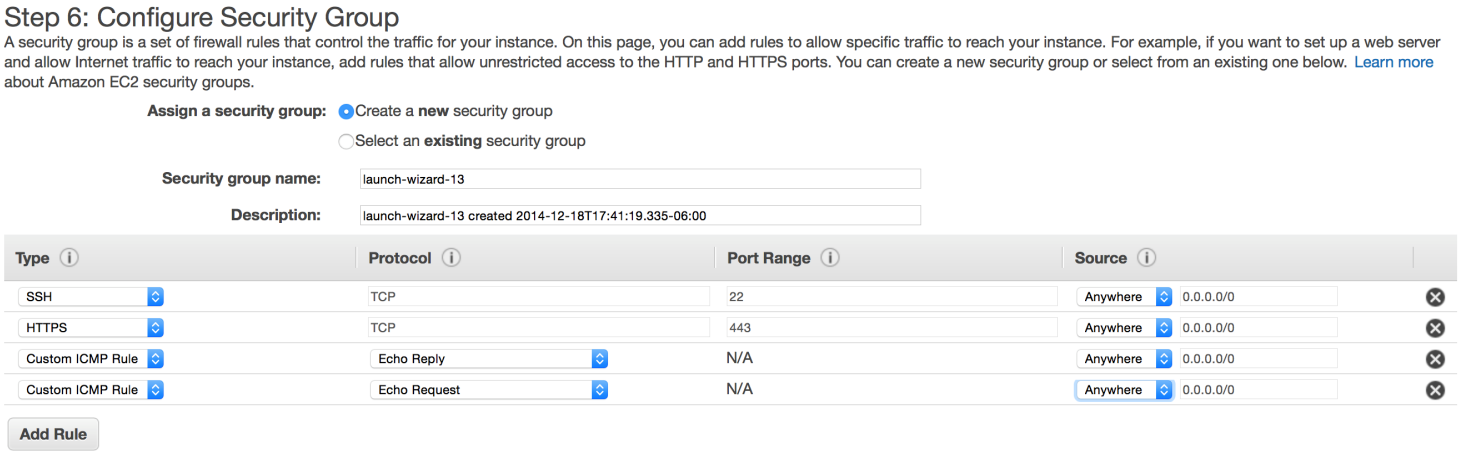
Security groups for **SoftNAS Cloud®** must include TCP 443, TCP 22, and ICMP Echo Reply and Echo Response. **Source** can be locked down per security requirements.

Note: When assigning the Security Group for a **SoftNAS Cloud®** instance, either create a new Security Group or select a preexisting security Group. Regardless of decision, ensure it includes the above mentioned rules.

Create the required rules for the security group

1. From the available selection, choose **Create**.

2. Select **Custom ICMP Rule**. **Source** can be set to "Anywhere, My IP, or Custom IP," based on local security requirements. Assign **Type** and **Port** as appropriate.



Repeat the above procedure to add the Custom TCP Rule for ports 443 and 22.

Enable ICMP **Echo Reply** and **Request** as seen above. For ping requests to work correctly, enable ICMP echo reply and request.

Note: It is recommend to restrict the Source IP address to a range of valid address, not "Anywhere" as shown in this example, for best security.

3. Click on **Review and Launch.**

4. Provide the appropriate key pair when prompted.

Note: Keep in mind that two instances are required for **HA.** Create a second instance at this time

In order to complete the set up high availability for Amazon Web Services VPCs in either a Virtual IP or Elastic IP setup, select the appropriate link below:

Amazon Web Services VPC: Virtual IP Setup

Amazon Web Services VPC: Elastic IP

Amazon Web Services VPC: Virtual IP Setup

SoftNAS now supports the set up of highly available VPCs with private subnets using virtual IPs. Elastic IP setup is still supported for legacy purposes. However, Virtual IP setup, more secure because it does not require a public facing IP, is our recommended best practice.

Secure Administrative Access in VPC

Without a public facing IP, the only way to access a Virtual IP VPC is by connecting to the private subnet upon which it is based. There are multiple ways to configure secure administrative access to the **SoftNAS SNAP HA™** storage controllers:

1) VPN - this is the most secure stand-alone solution, and a recommended minimum best practice for limiting access to the private IPs of each **SoftNAS Cloud®** controller. In this case, use DNS to assign a common name to each controller (e.g., "nas01.localdomain.com", "nas02.localdomain.com"), making routing to each **SoftNAS Cloud®** controller convenient for administrators

2) Admin Desktop - an even more secure approach is to combine VPN access with an Administrator's desktop, (sometimes referred to as a jumpbox) typically running Windows and accessed via RDP. This secure admin desktop adds another layer of authentication, namely Active Directory (or local account) authentication. Once an administrator has gained secure, encrypted access to the Admin Desktop, she opens up a web browser to connect to the **SoftNAS StorageCenter™** controller.

Amazon Private IP AWS Installation Overview

This section describes how to set up an Amazon AWS Virtual Private Cloud (VPC) in high availability (HA) mode to work with **SoftNAS SNAP HA™**.

The following is required

- Create the VPC in AWS.
- Specify the **IAM User for SoftNAS Cloud®**
- Configure the routing tables.
- Launch an Instance of **SoftNAS Cloud®** into the VPC.
- Create and Associate the Required Virtual IPs.
- Set up ICMP echo/reply to use "ALL TRAFFIC" for the VIP (for example, 40.40.40.40 will need ICMP entries)
- ALL TRAFFIC needs to be added specifically to the Security Group used for the SoftNAS nodes.
- Set up **SoftNAS Cloud®** for HA.

See **Amazon Web Services VPC** for detailed setup of the VPC, if you have not already done so.

Note: The HA IAM Role is caps sensitive, and must be named SoftNAS_HA_IAM.

SoftNAS Setup for Virtual IPs

If setting up SoftNAS SNAP HA with virtual IPs, there is no need to create Elastic IPs. A total of **3 IP addresses** will be required. The two IPs statically assigned or assigned via DHCP to your VPCs at instance creation time can be retained. Each VPC instance must have an IP in the same CIDR block. A third, human-configured (chosen by you) IP starting with a different octet will be selected during the HA wizard setup. This 3rd IP address will be used to access the share. Staring with a different octet means that if your VPC range is 172.16.0.0/16, the VIP you select must not start with 172, it must start with something else, for example: 10 or 12 or 175.

More information on adding IP addresses to your AWS/SoftNAS VPC can be found in **IP Addressing in your VPC.**

Setting Up for SNAP HA™

To set up **SoftNAS for SNAP HA™**, log into the **SoftNAS Cloud®** instances and access storage via the **SoftNAS StorageCenter™** interface. Via the **SoftNAS StorageCenter™** interface, set up **SoftNAS Cloud®** with the required Disk Devices, Storage Pools, and Volumes. Once this is complete for both instances, set up replication and **SoftNAS SNAP HA™**.

Log In to SoftNAS StorageCenter™

Logging in to **SoftNAS StorageCenter™** requires the public IP of the **SoftNAS Cloud®** instance, as well as the Instance ID (default password).

1. Obtain the virtual private IP of the **SoftNAS Cloud®** instance, as listed on the Instances screen. (the one starting with a different octet than the VPC instances)

2. Select the desired **SoftNAS Cloud®** instance.

3. Copy the Instance ID.

4. Navigate a local web browser to **https://[Virtual Private IP of the instance]**. (the one starting with a different octet than the VPC instances)

5. When prompted, use "softnas" as the username and the Instance ID (e.g., "i-99abc991") as the password. Change the password when convenient as dictated by security best practices.

The **SoftNAS StorageCenter™** interface will load.

Setting Up SoftNAS Cloud®

After accessing the **SoftNAS StorageCenter™** interface, set up the Disk Devices, Storage Pools, and Volumes that will ultimately be required for **SNAP HA™**.

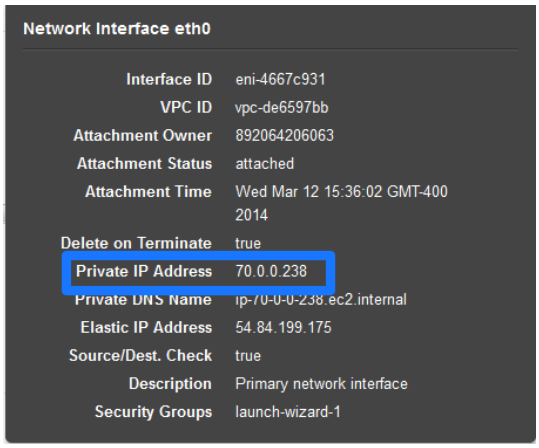
For more information, see the document **SoftNAS Installation Guide**.

Note: When setting up storage pools for replication, they have to have the same name or replication will not work properly. Also, a volume must be created on the source side node.

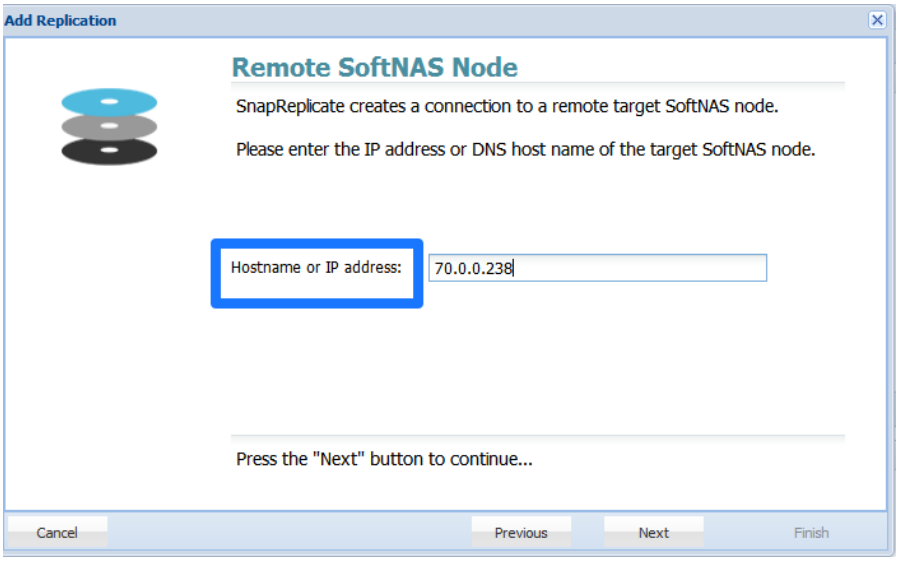
Setting Up Replication and SNAP HA™

Set up Replication

1. Log on to a **SoftNAS Cloud®** instance and select the **SnapReplicate / SNAP HA™** menu in the file tree.
2. Click **Add Replication.**
3. Enter the private IP for Ethernet 0 of the secondary node to be replicated to from AWS setup.



4. Provide this private IP address when prompted by the **SoftNAS StorageCenter** wizard, as seen below.



4. Provide the **SoftNAS Cloud®** instance credentials.

5. Click **Finish.**

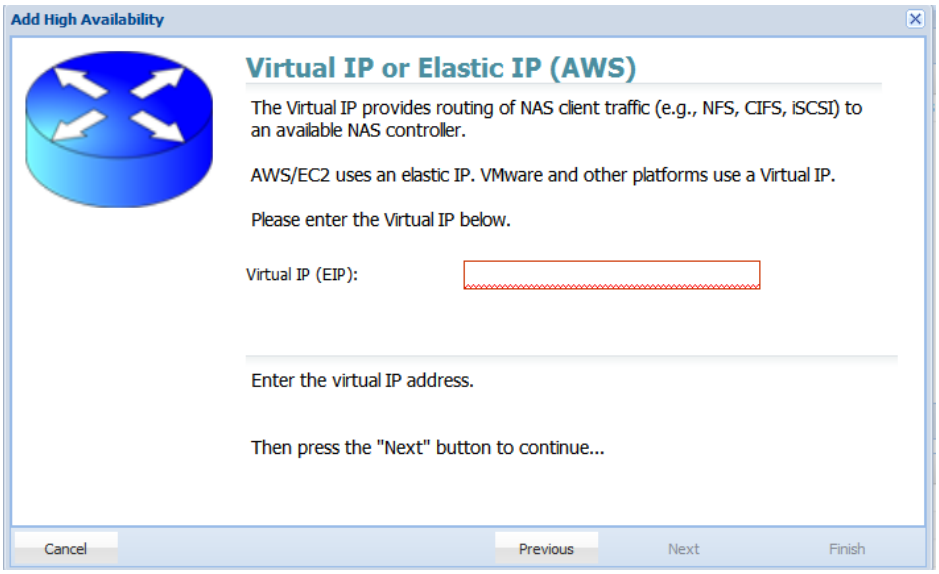
This will establish replication.

Set Up HA

1. From the **SoftNAS SnapReplicate™** panel, click on **Add SNAP HA** and click **Next**.

2. Select the type of HA you want to use. In this case we are creating a **Virtual IP** set up. Select **Virtual IP**.

3. Add the remaining Virtual IP which was previously configured in AWS. This is the **3rd Virtual IP** that we previously selected/created that is outside the CIDR block of the two instances. This IP is chosen by you, and requires no configuration. Select any IP address that is outside the CIDR block of the IPs selected for each SoftNAS instance.



4. Provide the Amazon **IAM User credentials** that will be used with **SoftNAS Cloud®**. Click **Next**.

5. Click **Finish**.

At this point, **SoftNAS Cloud®** will do the heavy lifting required to establish HA without the need for any user intervention. This process may take several minutes. After completion, a high availability **SoftNAS Cloud®** pair has been successfully set up across availability zones in AWS.

Amazon Web Services VPC: Elastic IP

Amazon AWS Installation Overview

This section describes how to set up an Amazon AWS Virtual Private Cloud (VPC) in high availability (HA) mode to work with **SoftNAS SNAP HA™**. Using Elastic IPs is the traditional setup for High Availability EC2 nodes. With SoftNAS Storage Center, use of Elastic IPs are no longer a requirement. Because use of Elastic IPs require a public facing IP, providing a potential security risk, a Virtual IP setup is SoftNAS' recommendation. Both setups are fully supported by SoftNAS.

The following is required:

• Create the VPC in AWS.
• Specify the **IAM User for SoftNAS Cloud®**
• Configure the routing tables.
• Launch an Instance of **SoftNAS Cloud®** into the VPC.
• Create and Associate the Required Elastic IPs.
• Set up **SoftNAS Cloud®** for HA.

See **Amazon Web Services VPC** for detailed setup of the VPC, if you have not already done so.

Note: The HA IAM Role is caps sensitive, and must be named SoftNAS_HA_IAM.

Secure Administrative Access in VPC

With Elastic IPs, direct internet access to the SoftNAS instance is possible. However, this is not recommended for obvious security reasons.
There are multiple ways to configure secure administrative access to the **SoftNAS SNAP HA™** storage controllers:

1) VPN - this is the most secure and recommended best practice for limiting access to the private IPs of each **SoftNAS Cloud®** controller. In this case, use DNS to assign a common name to each controller (e.g., "nas01.localdomain.com", "nas02.localdomain.com"), making routing to each **SoftNAS Cloud®** controller convenient for administrators

2) Admin Desktop - an even more secure approach is to combine VPN access with an Administrator's desktop, typically running Windows and accessed via RDP. This secure admin desktop adds another layer of authentication, namely Active Directory (or local account) authentication. Once an administrator has gained secure, encrypted access to the Admin Desktop, she opens up a web browser to connect to the **SoftNAS StorageCenter™** controller.

3) Direct Internet Access - the least secure, yet simplest form of providing administrators with access to **SoftNAS StorageCenter™** is to assign two additional Elastic IP addresses, one per **SoftNAS Cloud®** controller (see Figure 3 below). Of course, a corresponding security group, locked down to restrict the IP addresses allowed access to the controllers is necessary to properly secure this configuration. While not recommended for production systems, this configuration is most commonly seen during evaluation and for development systems, where full VPC deployment has not yet taken place.

Associating the Required Elastic IPs to the SoftNAS Cloud® Instances

If setting up **SoftNAS SNAP HA™** with Elastic IPs, **three elastic IPs** will be required. One IP is associated to each VPC instance, and a third IP is associated to the VIP interface.

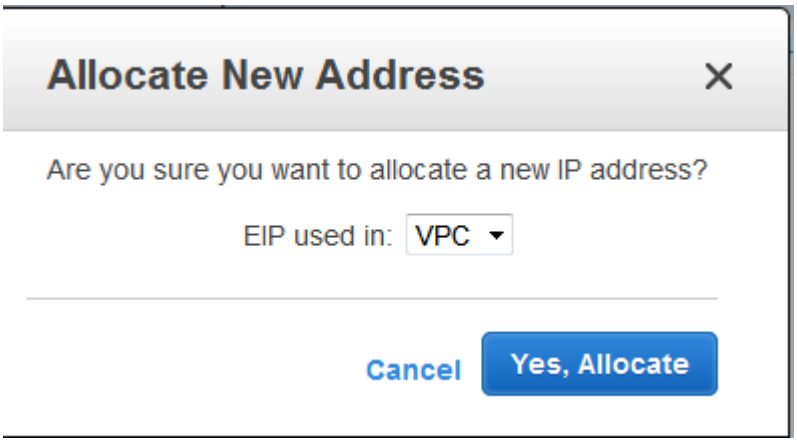
Creating the Elastic IPs

Create three Elastic IPs for use with **SoftNAS Cloud®**.

1. From the EC2 Services Dashboard, click on **Elastic IPs.**

2. Click on **Allocate New Address.**

3. For **EIP used in**, select "VPC."



4. Click **Yes, Allocate**.

Repeat the procedure to create three new elastic IPs for the VPC.

Associating the Elastic IPs to the SoftNAS Cloud® Instances.

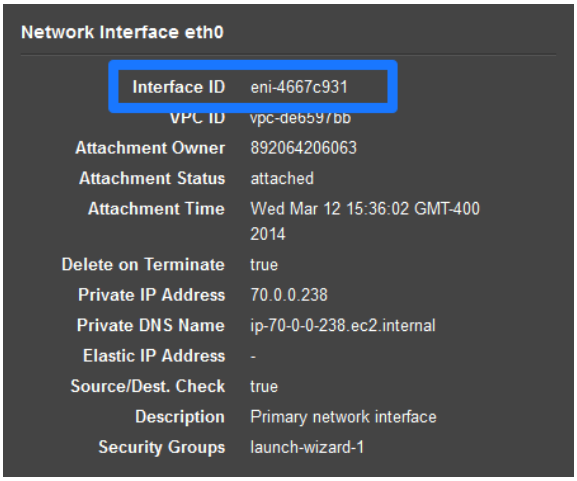
To associate the Elastic IPs to the instances, take note of the Interface ID for the **SoftNAS Cloud®** instance. This can then be used to associate an Elastic IP.

1. From the EC2 Services Dashboard, click on **Instances.**

2. Select one of the **SoftNAS Cloud®** instances.

3. Scroll down to the **Network interfaces** settings.

4. Click on "eth0" and take note of the Interface ID.

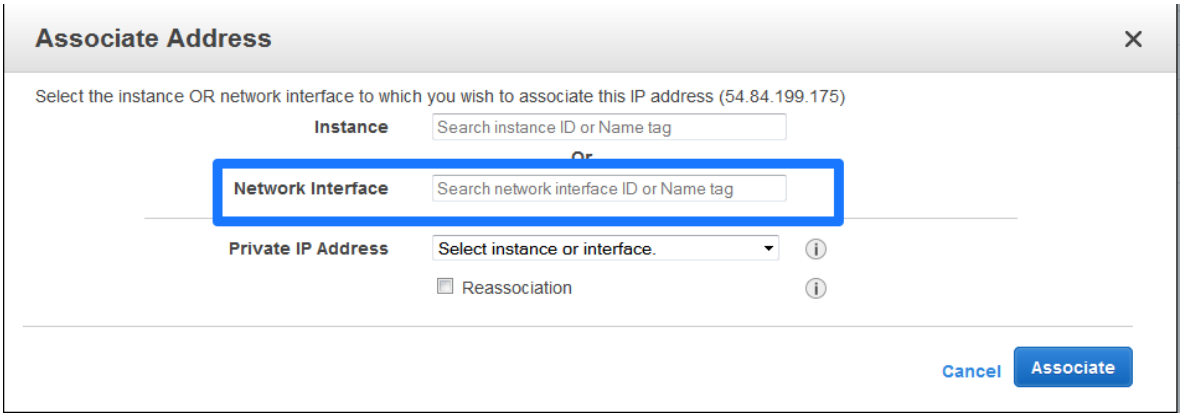


5. Click on **Elastic IPs.**

6. Select the Elastic IP of choice.

7. Click on **Associate Address.**

8. From the **Associate Address** window, select the corresponding **Network Interface** from the dropdown.



9. Click on **Associate.**

The Elastic IP is associated with the **SoftNAS Cloud®** instance.

Repeat the above procedure to associate another Elastic IP to the other **SoftNAS Cloud®** instance.

Setting Up for SNAP HA™

To set up **SoftNAS for SNAP HA™**, log into the **SoftNAS Cloud®** instances and access storage via the **SoftNAS StorageCenter™** interface. Via the **SoftNAS StorageCenter™** interface, set up **SoftNAS Cloud®** with the required Disk Devices, Storage Pools, and Volumes. Once this is complete for both instances, set up replication and **SoftNAS SNAP HA™**.

Log In to SoftNAS StorageCenter™

Logging in to **SoftNAS StorageCenter™** requires the public IP of the **SoftNAS Cloud®** instance, as well as the Instance ID (default password).

1. Obtain the public IP of the **SoftNAS Cloud®** instance, as listed on the Instances screen.

2. Select the desired **SoftNAS Cloud®** instance.

3. Copy the Instance ID.

4. Navigate a local web browser to **https://[Public IP of the instance]**.

5. When prompted, use "softnas" as the username and the Instance ID (e.g., "i-99abc991") as the password. Change the password when convenient as dictated by security best practices.

The **SoftNAS StorageCenter™** interface will load.

Setting Up SoftNAS Cloud®

After accessing the **SoftNAS StorageCenter™** interface, set up the Disk Devices, Storage Pools, and Volumes that will ultimately be required for **SNAP HA™**.

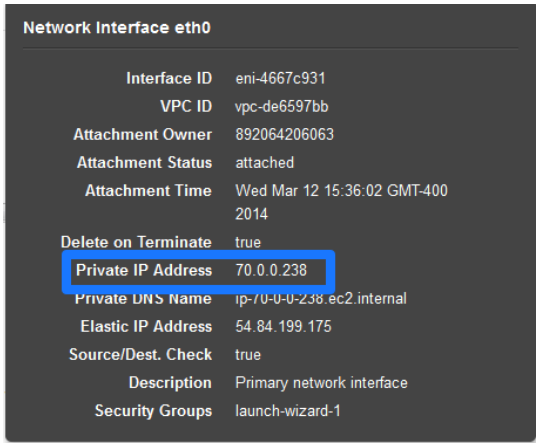
For more information, see the document **SoftNAS Installation Guide**.

Note: When setting up storage pools for replication, they have to have the same name or replication will not work properly. Also, create a volume on the source side node.

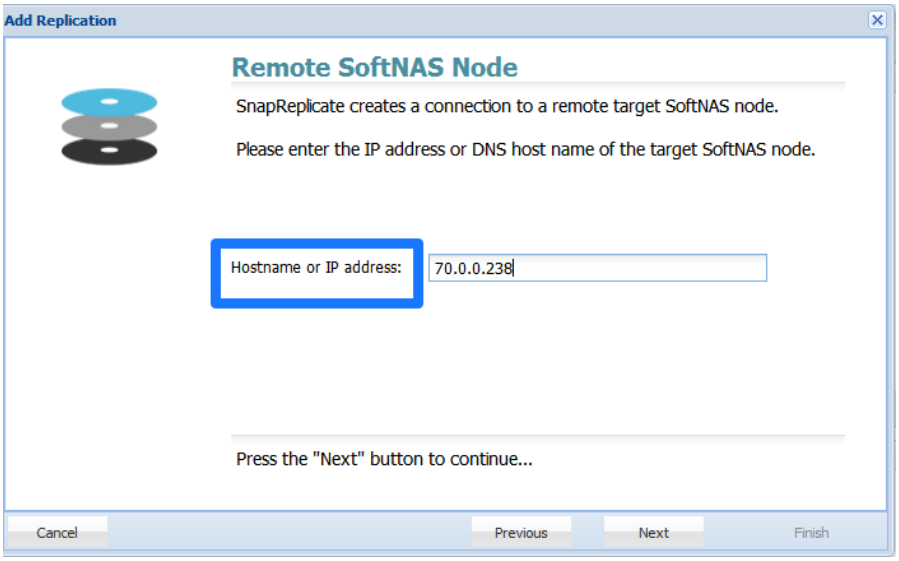
Setting Up Replication and SNAP HA™

Set up Replication

1. Log on to a **SoftNAS Cloud®** instance and select the **SnapReplicate / SNAP HA™** menu in the file tree.
2. Click **Add Replication.**
3. Enter the private IP for Ethernet 0 of the secondary node to be replicated to from AWS setup.



4. Provide this private IP address when prompted by the **SoftNAS StorageCenter** wizard, as seen below.



4. Provide the **SoftNAS Cloud®** instance credentials.

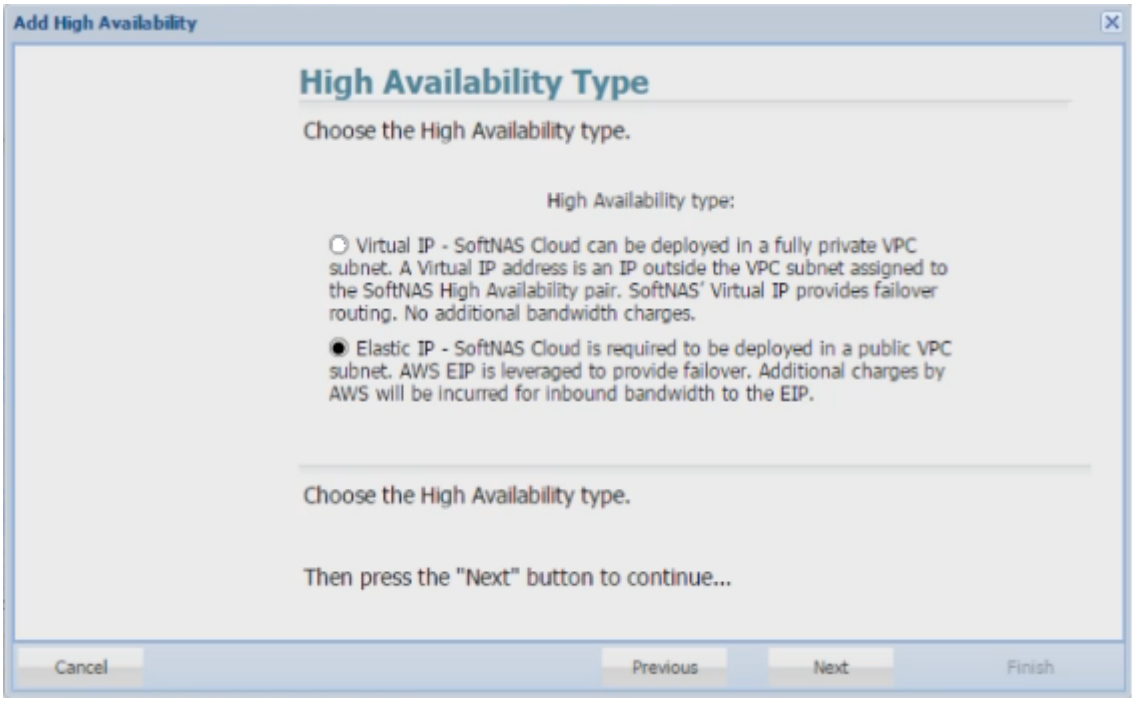
5. Click **Finish.**

This will establish replication.

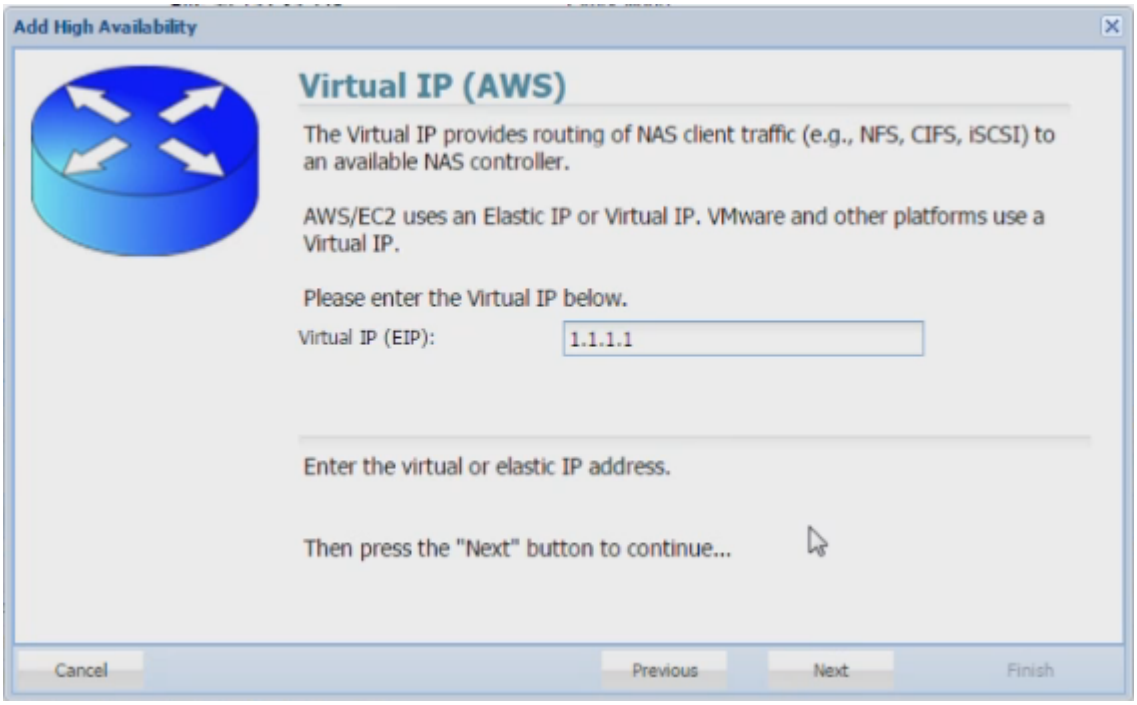
Set Up HA

1. From the **SoftNAS SnapReplicate™** panel, click on **Add SNAP HA** and click **Next**.

2. Select **Elastic IP** from High Availability type when the option is presented.



3. Add the **Elastic IP** which was previously configured in AWS. This is the **Elastic IP** that we previously created, but did not assign to a VPC.



4. Provide the Amazon **IAM User credentials** that will be used with **SoftNAS Cloud®**. Click **Next**.

5. Click **Finish**.

At this point, **SoftNAS Cloud®** will do the heavy lifting required to establish HA without the need for any user intervention. This process may take several minutes. After completion, a high availability **SoftNAS Cloud®** pair has been successfully set up across availability zones in AWS.

VMware

Overview

Set up **SNAP HA™** in any VMWare virtualized environment. In order to set up **SNAP HA™** the following is required:

• 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 SNAP HA™** Controller node is **required**. This 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.

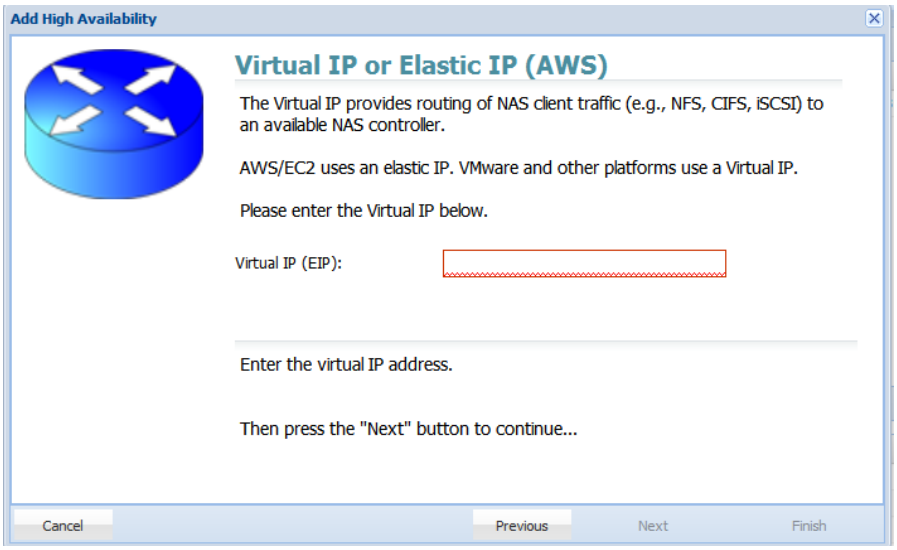
For more information about **SNAP HA™** networking best practices, see section **HA Design Principles.**

For more information about common **SoftNAS Cloud®** installation procedures, see the document **SoftNAS Installation Guide**.

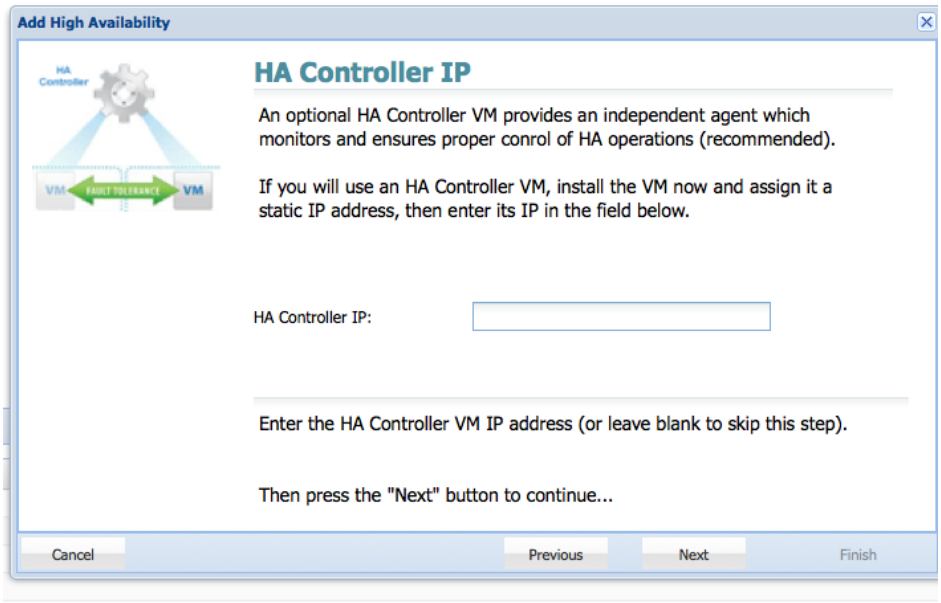
Setting Up SNAP HA™ for VMWare

After the above networking requirements have been fulfilled, **SNAP HA™** may be set up.

1. Navigate to the **SoftNAS StorageCenter™** interface of the primary node.
2. From the **SoftNAS SnapReplicate™** panel click on **Add Snap HA.**
3. Enter the virtual IP of an unassigned VIP address in the storage VLAN subnet. Click on **Next.**



5. Add the static IP of a third **SoftNAS Cloud®** virtual machine that will act as the HA Controller. It is recommended that this machine be deployed in fault tolerant mode.



6. Click on **Next**.
7. Click on **Finish.**

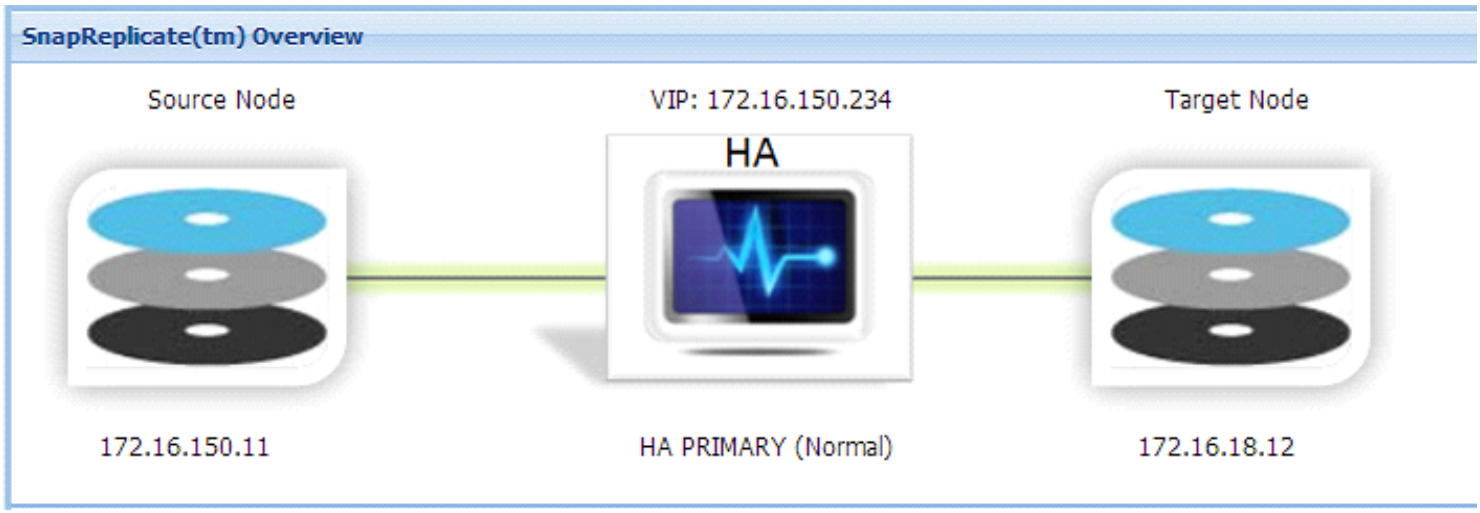
HA iSCSI on VMware

ISCSI HA VMware Setup

To configure iSCSI for HA operation with VMware, use the following instructions.

1. Locate the Virtual IP address assigned during **SNAP HA™** installation.

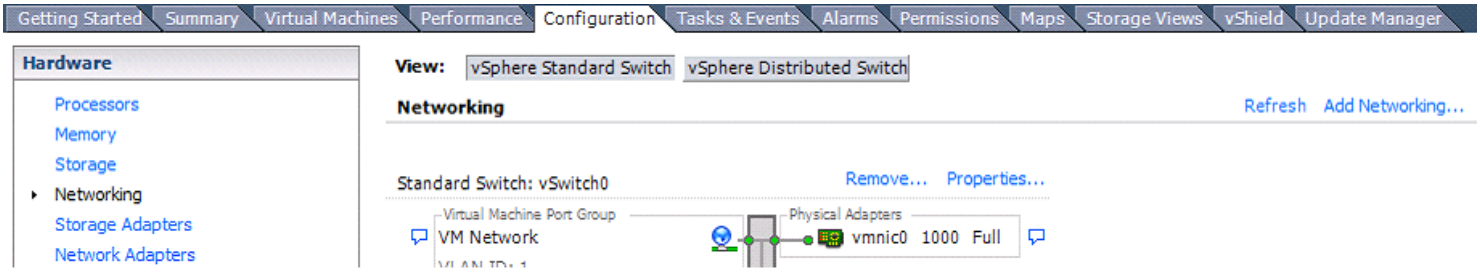
Note: The example for this guide will use 172.16.150.234.



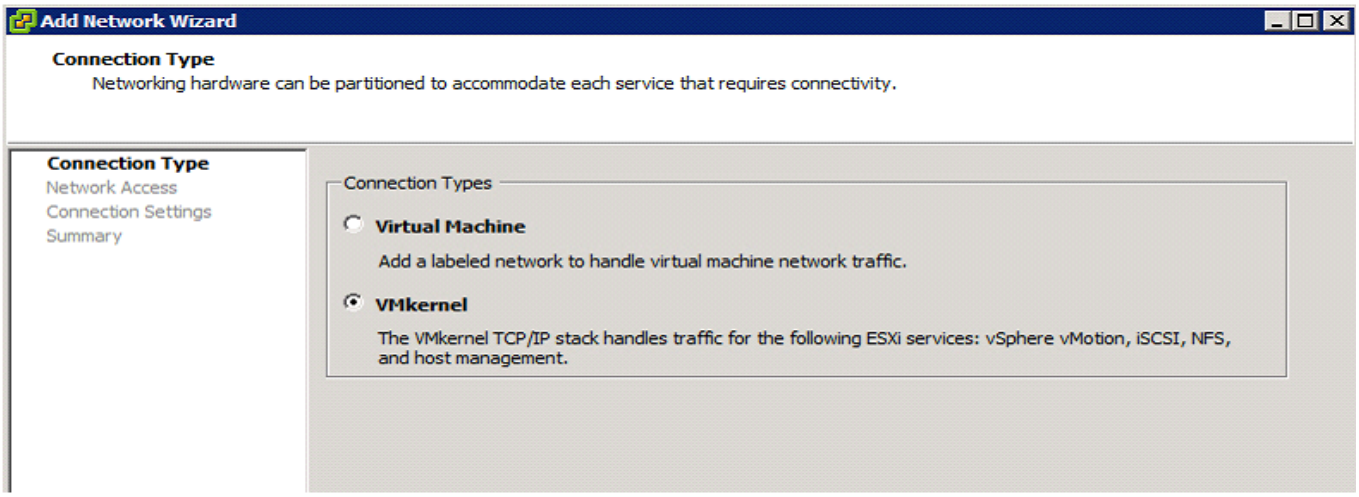
Go to the ESXi host through VI client and create a new standard switch with a new vmkernel. Align the IP with the same subnet of the existing VIP.

Note: Ensure a free physical NIC on the ESXi host.

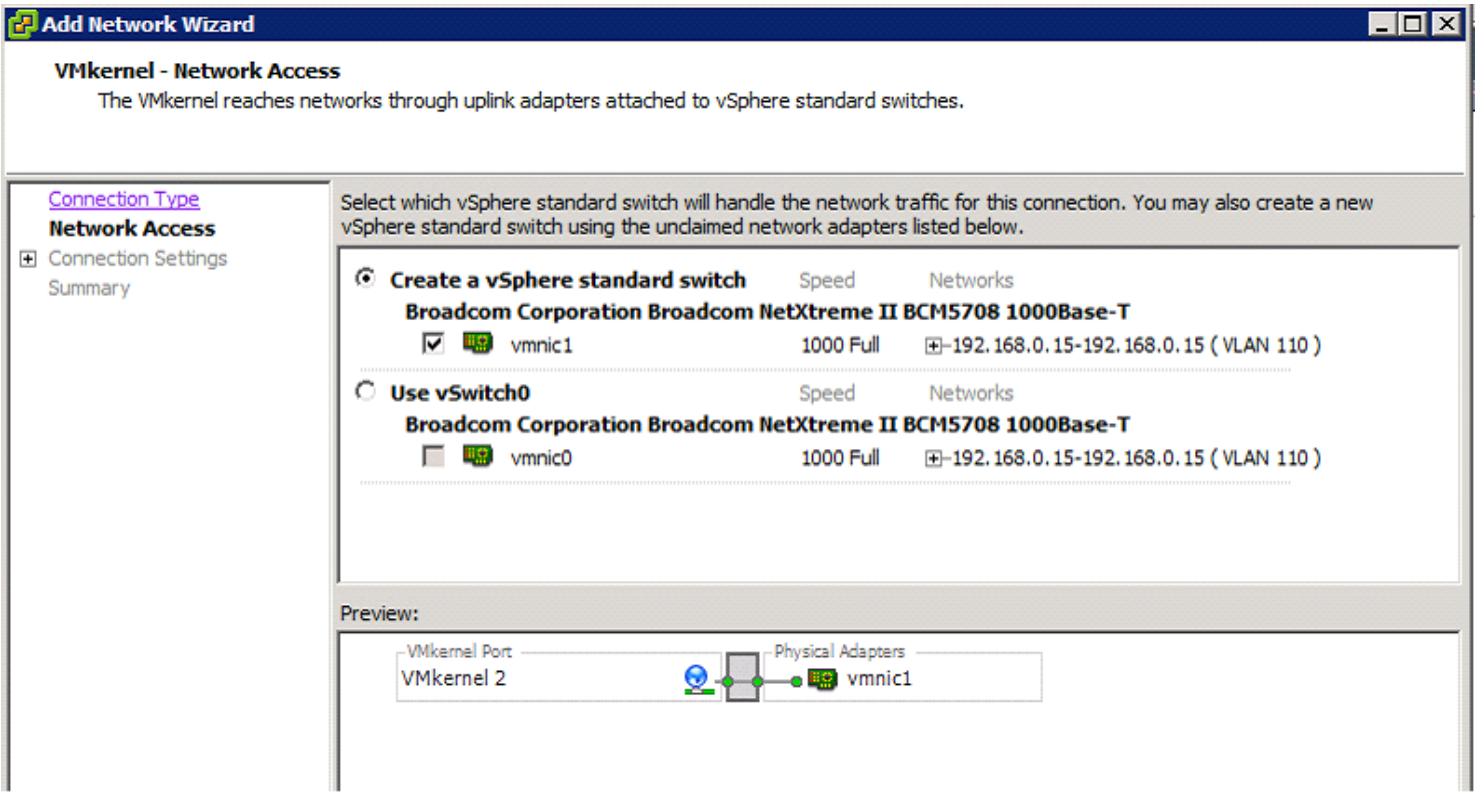
Within the ESXi host: .**Configuration > Networking > Add Networking**



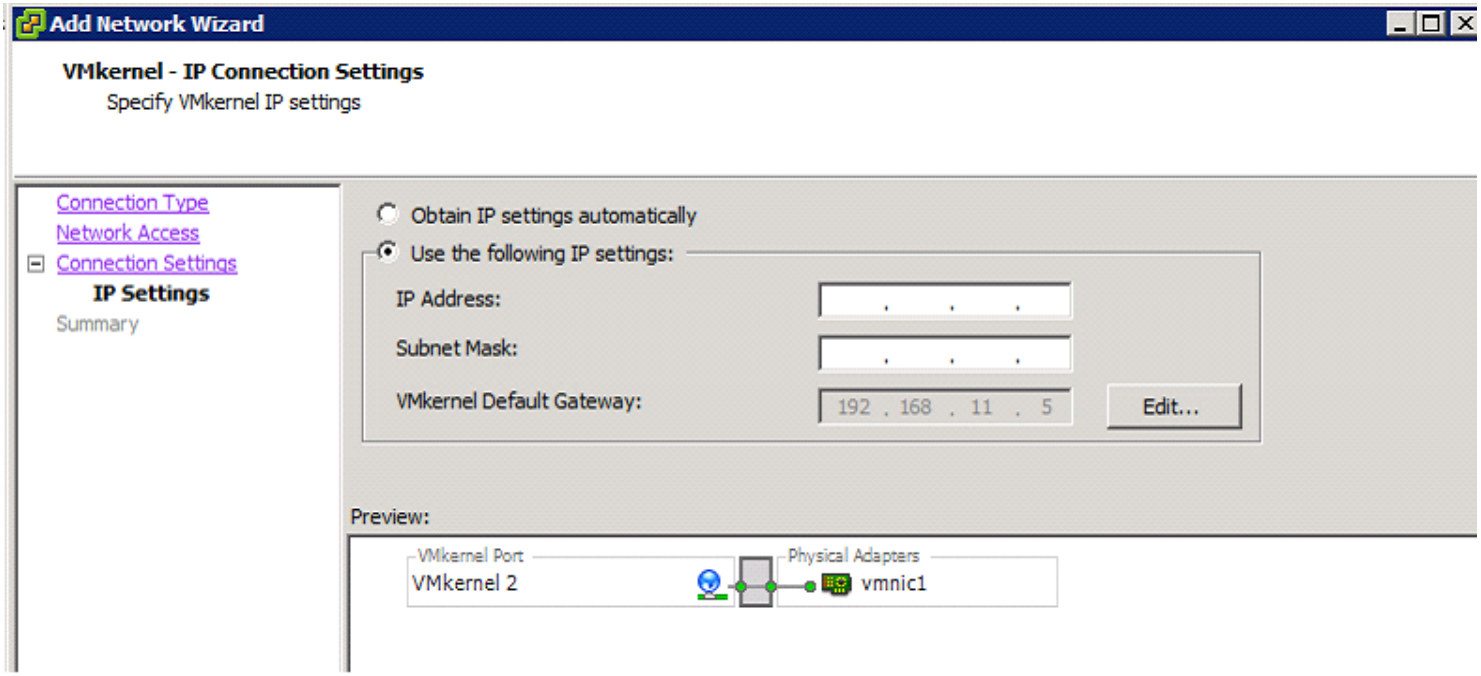
Choose **VMkernel** and click **Next.**

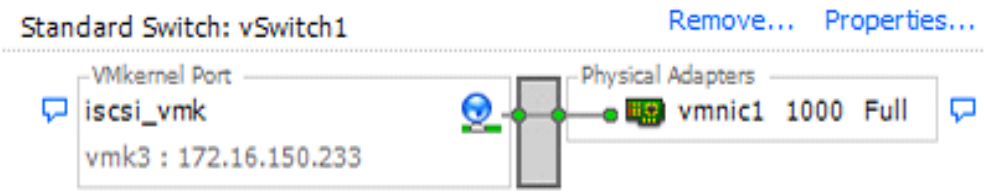


Choose an available physical NIC. Click **Next.**

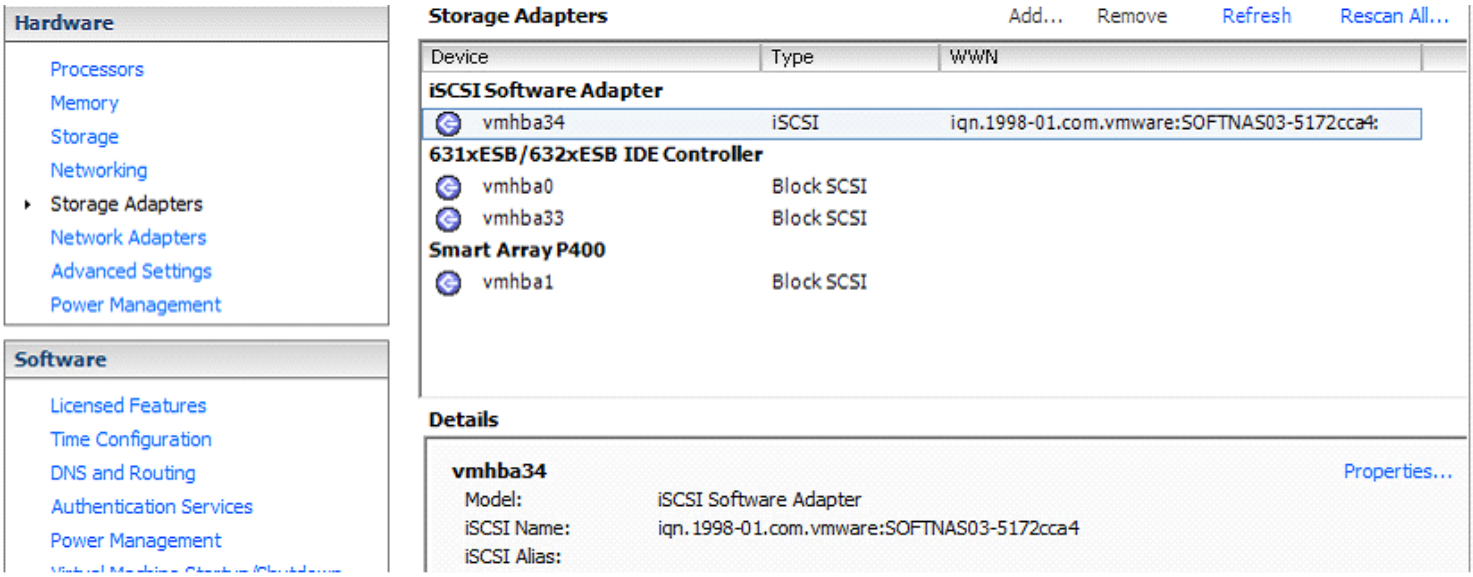


Enter an IP that corresponds to the existing VIP's subnet. Click **Next** and then **OK**.

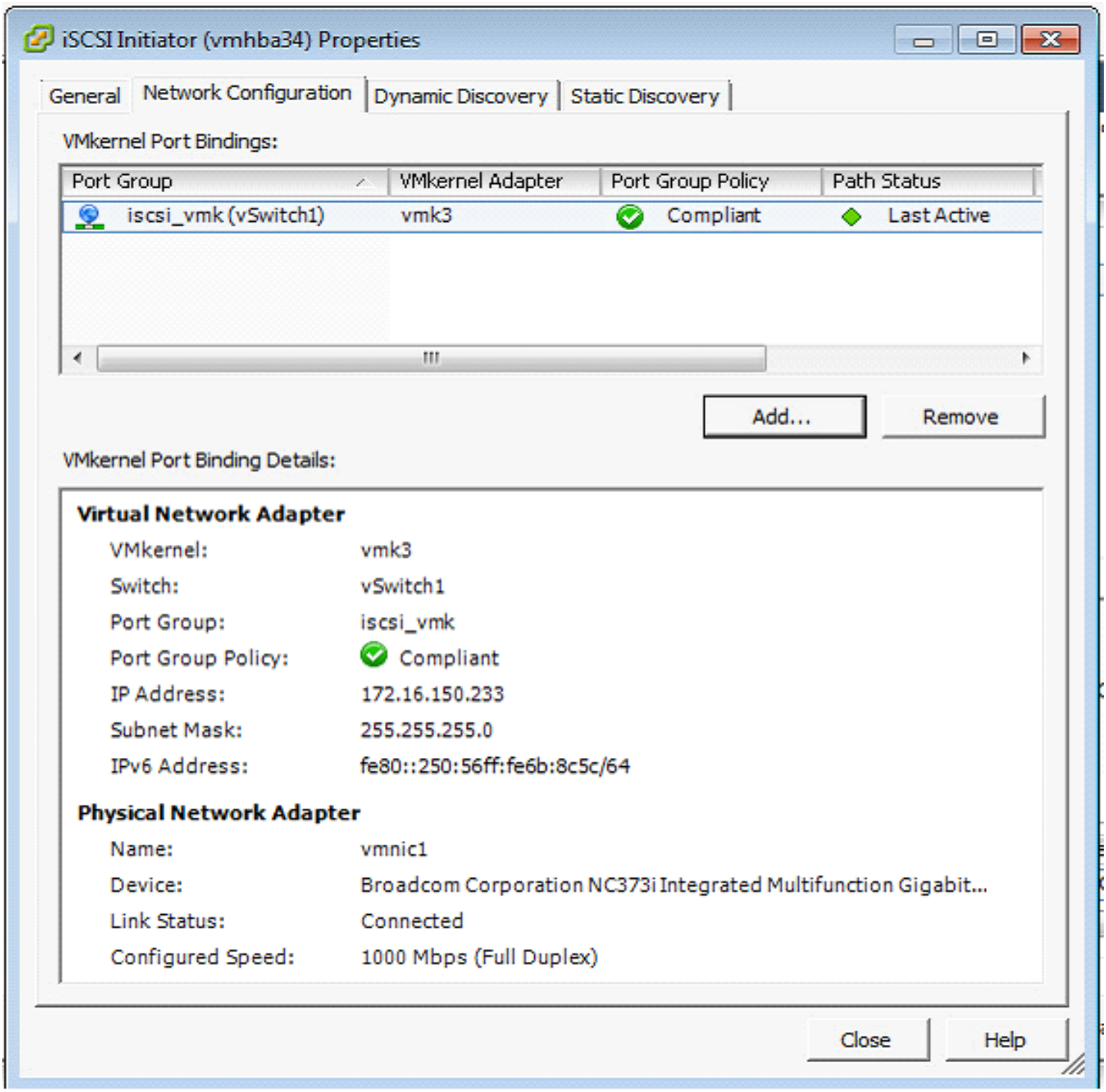




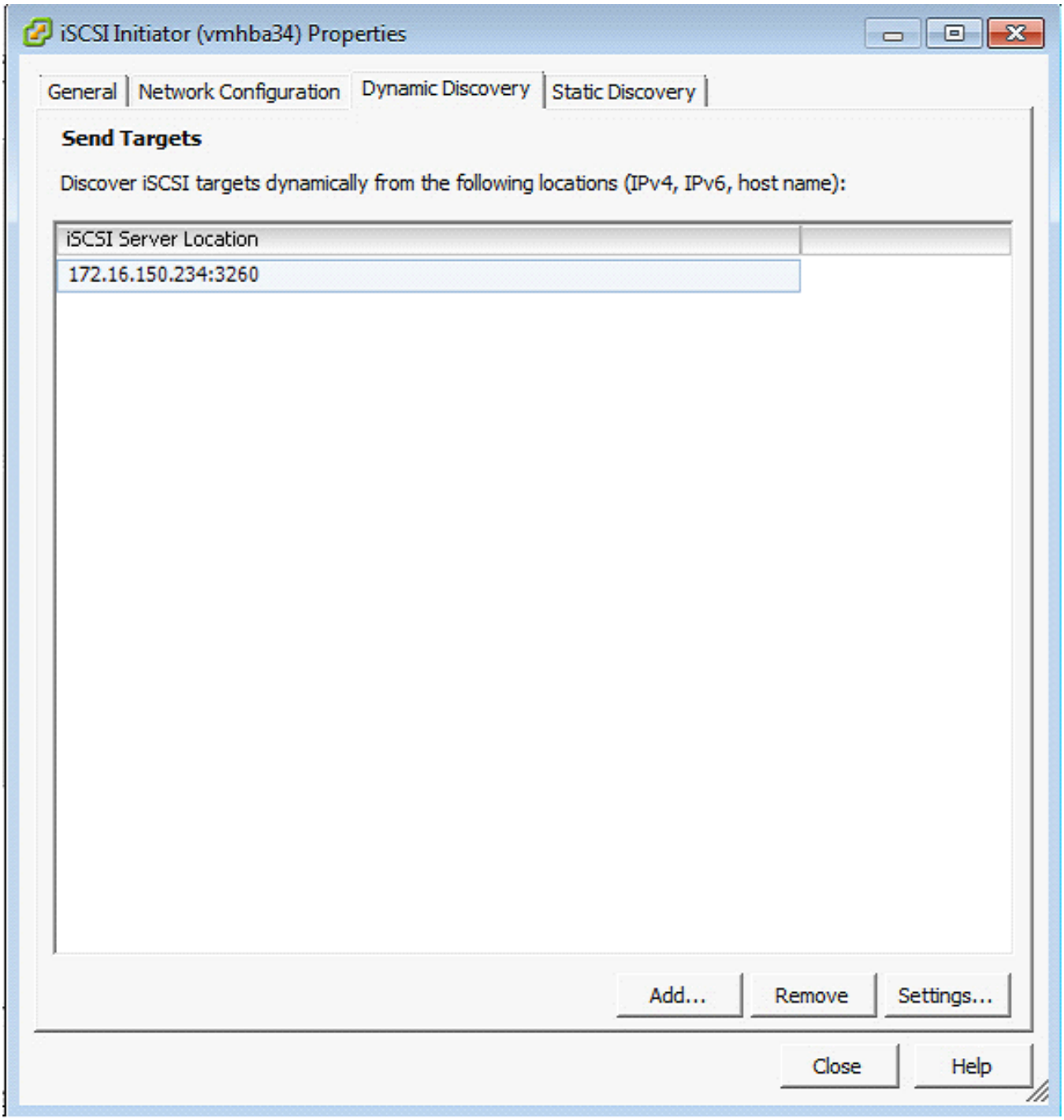
Next go to configuration tab -- > storage adapters and click properties

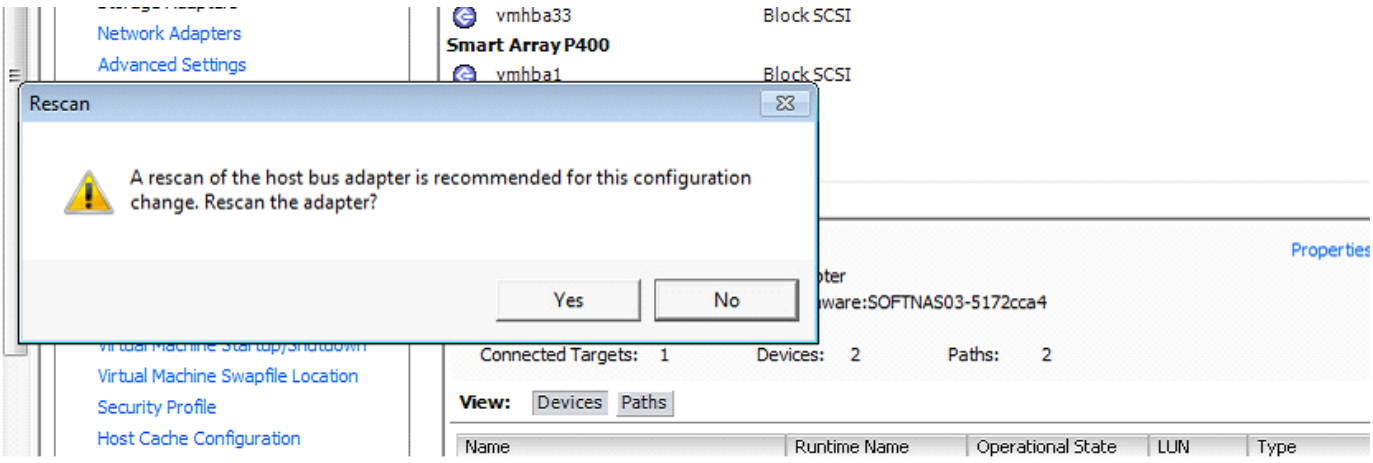


On the network configuration tab click add to add the vmkernel which we will use for iscsi port binding



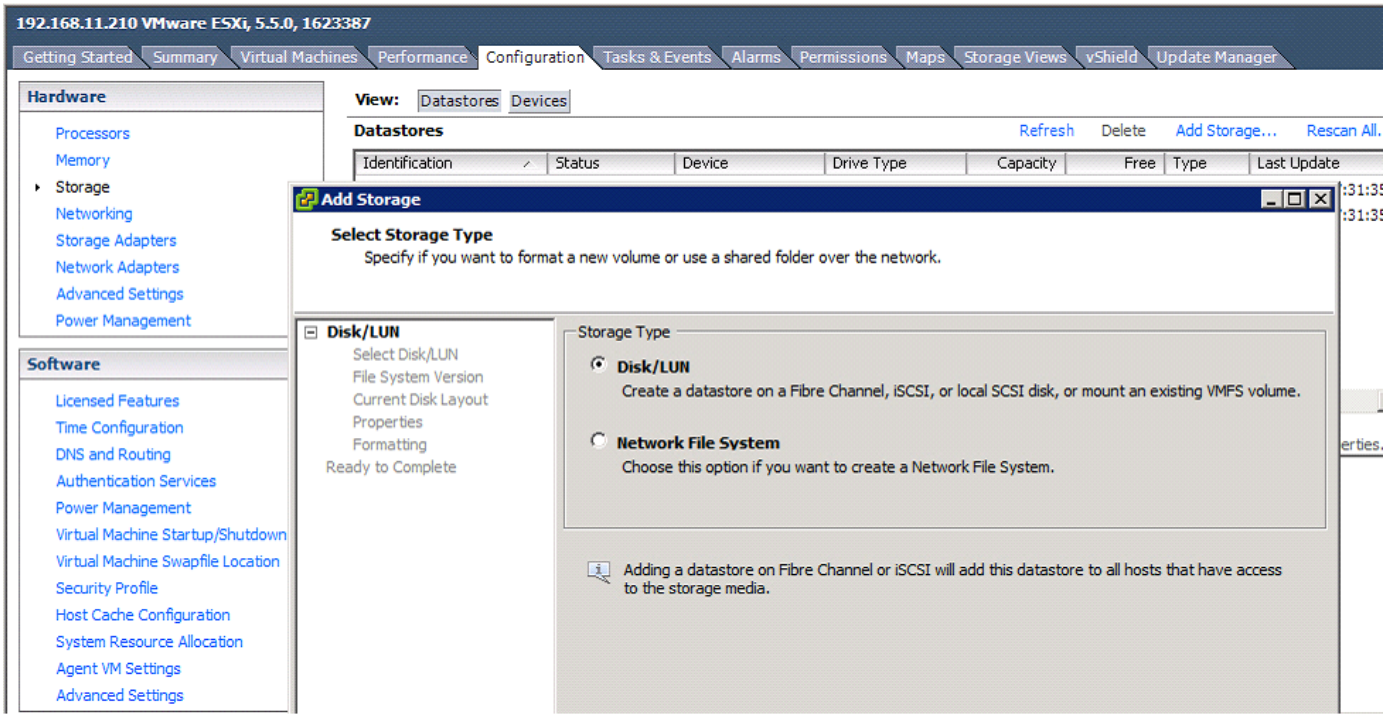
Then on “Dynamic discovery” click “Add” to put our VIP address press OK and on rescan choose yes.


iSCSI Initiator (vmhba34) Properties
General
Network Configuration
Dynamic Discovery
Static Discovery
Send Targets
Discover iSCSI targets dynamically from the following locations (IPv4, IPv6, host name):
iSCSI Server Location
172.16.150.234:3260
Add...
Remove
Settings...
Close
Help


Network Adapters
Advanced Settings
vmhba33
Block SCSI
Smart Array P400
vmhba1
Block SCSI
Rescan
A rescan of the host bus adapter is recommended for this configuration change. Rescan the adapter?
Yes
No
Properties
ware:SOFTNAS03-5172cca4
Connected Targets: 1
Devices: 2
Paths: 2
Virtual Machine Swapfile Location
Security Profile
Host Cache Configuration
View:
Devices
Paths
Name
Runtime Name
Operational State
LUN
Type

ESXi has now found the ISCSi controller. Add the Datastore and follow the prompts.

Configuration > Storage > Add Storage > Disk LUN



HA Operations

The following operations with **SoftNAS SNAP HA™:**

- **Manual Takeover and Giveback**
- **Automatic Failover**
- **Maintenance Mode**

Manual Takeover and Giveback

Configure **SNAP HA™** to perform Manual Takeovers and Givebacks.

Setting Up Manual Takeover and Giveback

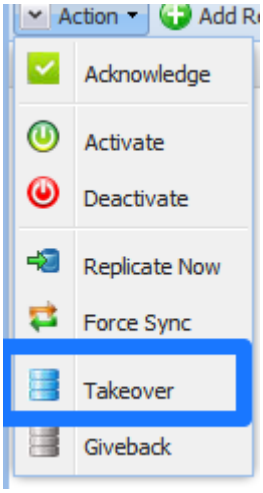
When a takeover is initiated, the **SNAP HA™** Controller will ensure that data is not being written to a node in the process of a switch over. This will avoid the split brain condition.

The HA controller will authorize the switch over, reassign the IPs, and change the primary/secondary designation for the **SoftNAS Cloud®** instances. Also, as part of the takeover the problematic instance is shutdown.

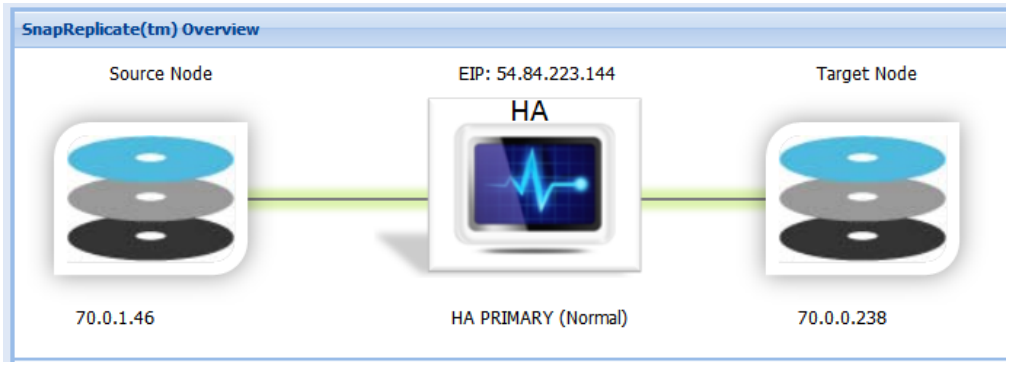
Takeover

1. From the **SoftNAS StorageCenter™** interface of the good node, navigate to the **SnapReplicate™** panel.

2. Click on **Actions>Takeover.** Confirm at the prompt.



3. The takeover process begins. This process will shut down the source node and allow the target to take over as primary. After the process has completed successfully, the good node will display as the HA Primary.

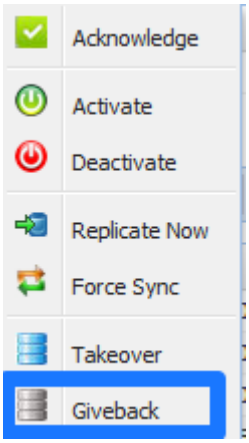


After the problematic node has been fixed, bring the node back up.

Giveback

After rebooting the node shut down by the takeover process, perform a Giveback from the secondary instance to allow the **SNAP HA™** controller to safely and securely perform the switch over to protect data integrity.

1. From the **SoftNAS SnapReplicate™** screen, click on **Giveback.**



2. Confirm the action by clicking **Yes.**

Automatic Failover

Auto Failover

Automatic Failover is one of the features included with **SNAP HA™.** Once **SNAP HA™** is set up, no additional configuration is required to make Automatic Failover work.

SNAP HA™ Automatic Failover works via the use of the **SoftNAS Cloud®** health monitor. When the health monitor detects a failure or is unable to reach the **SoftNAS Cloud®** node, it will automatically failover to the other node and move all NAS services over to the other side.

Maintenance Mode

Warning: If putting only one node into maintenance mode, synchronization need not occur. If both HA nodes need to be placed into maintenance, a forced synchronization will need to occur.

For major **SoftNAS StorageCenter** upgrades that require downtime, **SoftNAS** has provided a way to protect replications and SNAP HA pairings while also keeping storage connectivity and data access uninterrupted. To check whether an upgrade is required, click **Settings > Software Updates** in the main menu on the left.

Sync & Deactivate

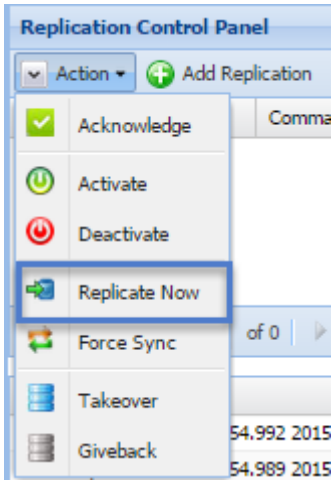
Sync SNAP HA in StorageCenter

Ensure that both nodes are in sync by forcing the event through **SoftNAS StorageCenter**. Sign in to each node of the HA pair to be upgraded in separate browsers to more easily switch between nodes.

Note: Ensure that target and source nodes have been established. For the purposes of this document, the following terminology will be used:

Original Status	Document Reference
Source Node	Node A
Target Node	Node B

In the **SoftNAS StorageCenter** interface for **Node A**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Replicate Now** as shown below.



To verify sync completion, watch the **Event Log** at the bottom of the UI. Click **Refresh** to ensure current status visibility if necessary.

Deactivate

In the **SoftNAS StorageCenter** interface for **Node A**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Deactivate.**

Upgrade Nodes & Transfer Workload

This critical section ensures that storage and compute capacities remain at expected levels during a disruptive update.

Upgrade Node B

Navigate to the **SoftNAS StorageCenter** for **Node B**, then to **Settings > Software Updates** and click **Apply Update.** Click **Yes** to confirm.

Wait for the confirmation that the update has been successful and allow the browser to refresh itself.

Reactivate

In the **SoftNAS StorageCenter** interface for **Node A**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Activate.** Click **Yes** to confirm.

If only one node needs maintenance, then the process ends here, with the reactivation of SnapReplicate. However, if both nodes require maintenance, additional steps must occur:

Deactivate

In the **SoftNAS StorageCenter** interface for **Node B**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Deactivate.** Click **Yes** to confirm.

Upgrade Node A

Navigate to the **SoftNAS StorageCenter** for **Node A**, then to **Settings > Software Updates** and click **Apply Update.**

Wait for the confirmation that the update has been successful and allow the browser to refresh itself.

Restore HA

Reactivate Replication

In the **SoftNAS StorageCenter** interface for **Node B**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Activate.** Click **Yes** to confirm.

The system will then automatically synchronize.

Product Upgrade

Warning: In order to upgrade, both nodes of the HA pairing will require a forced synchronization to complete the process.

For major **SoftNAS StorageCenter** upgrades that require downtime, **SoftNAS** has provided a way to protect replications and SNAP HA pairings while also keeping storage connectivity and data access uninterrupted. To check whether an upgrade is required, click **Settings > Software Updates** in the main menu on the left.

Sync & Deactivate Pair

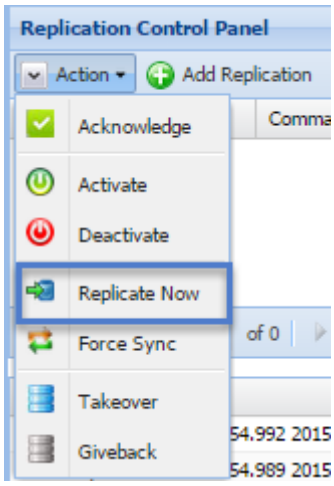
Sync SNAP HA in StorageCenter

Ensure that both nodes are in sync by forcing the event through **SoftNAS StorageCenter**. Sign in to each node of the HA pair to be upgraded in separate browsers to more easily switch between nodes.

Note: Ensure that target and source nodes have been established. For the purposes of this document, the following terminology will be used:

Original Status	Document Reference
Source Node	Node A
Target Node	Node B

In the **SoftNAS StorageCenter** interface for **Node A**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Replicate Now** as shown below.



To verify sync completion, watch the **Event Log** at the bottom of the UI. Click **Refresh** to ensure current status visibility if necessary.

Deactivate

In the **SoftNAS StorageCenter** interface for **Node A**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Deactivate.**

Upgrade Nodes & Transfer Workload

This critical section ensures that storage and compute capacities remain at expected levels during a disruptive update.

Upgrade Node B

Navigate to the **SoftNAS StorageCenter** for **Node B**, then to **Settings > Software Updates** and click **Apply Update.** Click **Yes** to confirm.

Wait for the confirmation that the update has been successful and allow the browser to refresh itself.

Reactivate

In the **SoftNAS StorageCenter** interface for **Node A**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Activate.** Click **Yes** to confirm.

Perform Takeover

In the **SoftNAS StorageCenter** interface for **Node B**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Takeover.** Click **Yes** to confirm.

Deactivate

In the **SoftNAS StorageCenter** interface for **Node B**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Deactivate.** Click **Yes** to confirm.

Upgrade Node A

Navigate to the **SoftNAS StorageCenter** for **Node A**, then to **Settings > Software Updates** and click **Apply Update.**

Wait for the confirmation that the update has been successful and allow the browser to refresh itself.

Restore HA

Reactivate Replication

In the **SoftNAS StorageCenter** interface for **Node B**, navigate to the **SnapReplicate / SNAP HA** menu. Click **Action** and then **Activate.** Click **Yes** to confirm.

The system will then automatically synchronize via a forced sync.

HA Design Principles

This section provides an overview of **SNAP HA™** architecture and provides design principles to apply when planning HA implementation. Softnas cloud offers two approaches to extending a common IP across AZs. Virtual IPs provided the capabiltiy through routing, and permit fully private VPCs. Virtual IPs are SoftNAS' best practice recommendation, as they ensure none of your IP addresses are public-facing, improving the security of your deployment.

Alternatively, Elastic IPs are the legacy solution, and were previously the only supported cross-zone routable IP addresses available in the AWS VPC environment. In practice, EIPs add very little latency or other overhead to storage traffic, and provide routing redundancy across the zones.

SoftNAS SNAP HA™ takes a basic EC2 elastic IP and layers on additional patent-pending functionality that turns it into an Elastic HA IP - a cross-zone IP suitable for highly-available network-attached storage. Both solutions are fully supported and can be implemented using the information below.

AWS VPC Architecture: Virtual IP - How to design an HA storage solution for a VPC using Virtual IPs in Amazon Web Services

AWS VPC Architecture: Elastic IPs - How to design an HA storage solution for a VPC using Elastic IPs in Amazon Web Services

Premise-based HA Architecture - How to design an HA storage solution for a private cloud using VMware

AWS VPC Architecture: Virtual IP

On AWS, **SoftNAS SNAP HA™** is designed to operate within the Virtual Private Cloud (VPC). VPCs can be as simple as a single subnet, with or without a VPN security gateway, or as complex as public / private compartmentalized subnets, as depicted in the figures herein. In figure 1 below, we see a VPC configured to operate across two availability zones (AZ), with separate private subnets. **SoftNAS Cloud®** controllers are placed into the private subnet for Virtual IP address routing purposes.

About Virtual IP Addresses

SoftNAS Cloud® storage is normally not accessible from the public Internet. With a Virtual IP setup, none of your IP addresses are public facing, increasing the security of the deployment. A Virtual IP address is configured with a security group setting that restricts its access to only the internally-routable, private IPs assigned to the VPC; e.g., in this example, only EC2 instances within the VPCs internal 10.0.0./16 private network are routable to the Virtual IP.

Why use a Virtual IP? Virtual IPs (VIP) are completely private cross-zone routable IP addresses available in the AWS VPC environment. In practice, VIPs add very little latency or other overhead to storage traffic, and provide routing redundancy across the zones, all without the risks inherent in using a public facing IP. For this reason Virtual IPs are our recommended best practice.

AWS Virtual IP Cross-Availability Zone Architecture Overview

Please refer to Figure 1 shown below for the remaining discussion. This drawing depicts a typical HA deployment, but is not the only possible design. In fact, **SoftNAS SNAP HA™** can be deployed with dual controllers located within a single AZ on a VPC (there is no requirement to split controllers across AZs, but it is a recommended best practice for maximum availability).

We see a VPC created in a /16 network in AWS US East (Virginia) data center, with subnets allocated in Zone A and Zone B. This topology provides the best overall redundancy and availability within the AWS AZ architecture.

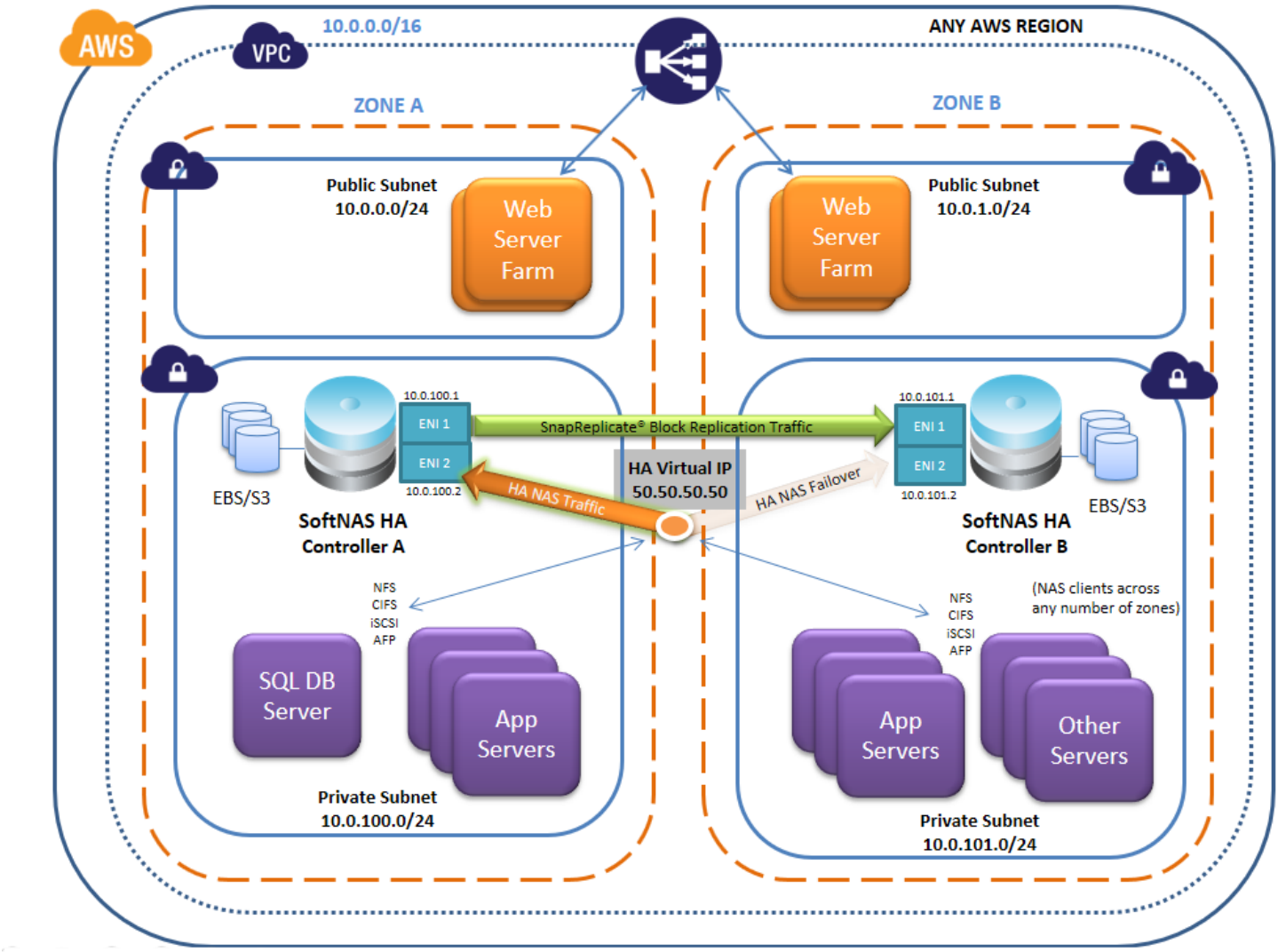


Figure 2 - AWS Virtual IP VPC with SoftNAS SNAP HA™

Two **SoftNAS Cloud®** controller EC2 instances are deployed - one per AZ. If optional private subnets are configured in one or more AZs, they will also have access to the Virtual IP(VIP) for NFS client storage access via NFS, CIFS and iSCSI protocols.

The drawing shows **SNAP HA™** replication traffic flowing from Controller A to Controller B. This traffic is allocated to interface 0. Interface 0 is also used for administration using the **SoftNAS StorageCenter™** GUI. Block replication keeps a warm copy of the data from node A on node B, in case a failover is necessary.

The drawing shows two orange arrows emanting from an orange and white circle, which represents the Virtual IP. The black lock symbol represents the EC2 Security Group associated with the Virtual IP. The shadowed orange arrow represents re-routed storage requests flowing to Controller B after an automatic failover or manual takeover. This Virtual IP must be in a completely separate CIDR block from the two instance IPs.

When an automatic failover or manual takeover occurs, NAS traffic is re-routed via the Virtual IP from Controller A to Controller B, as indicated by in the diagram above. When a Virtual IP switches over from one controller to another, NAS client traffic is rapidly re-routed to the new controller, typically in just a few seconds. NAS clients typically experience a brief switch-over delay of up to 20 seconds or so, and automatically reconnect after the switch-over event takes place.

AWS VIP Cross-Availability Zone Network Design

Each **SoftNAS Cloud®** controller has two NICs assigned - interface 0 (default) and one additional interface 1 (added during EC2 instance configuration).

1) Admin and Replication, Interface 0 - the first (default) NIC is used for **SoftNAS StorageCenter™** access and **SnapReplicate™** data replication across controllers.

2) **SoftNAS Cloud®** Storage, Interface 1 - the second NIC is dedicated to NAS storage traffic, and is used for Virtual IP routing of storage-related traffic (NFS, CIFS, iSCSI).

Note in the following diagrams the IP addresses shown are for illustration purposes only, and actual IP addresses will be assigned by AWS.

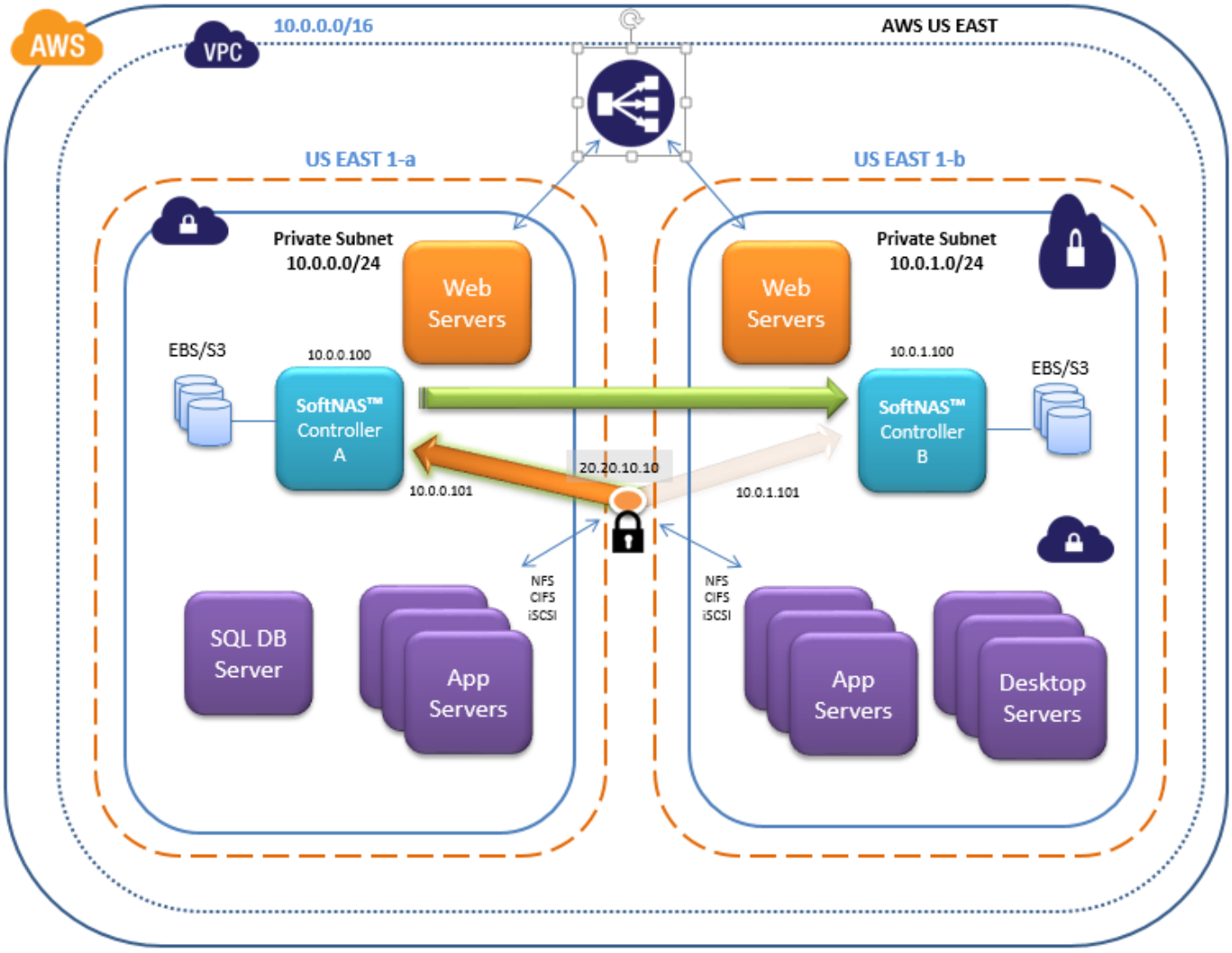


Figure 2 - AWS Cross-AZ Network Architecture

The remaining EC2 instances constitute NAS clients; that is, EC2 instances that connect using NFS, CIFS or iSCSI protocols to access NAS services across the private network. Although only two AZs are shown in these diagrams, NAS clients can access HA NAS services from any zone within the region allowed access to the Virtual IP.

Secure Administrative Access in VPC

Without a public facing IP, the only way to access a Virtual IP VPC is by connecting to the private subnet upon which it is based. There are multiple ways to configure secure administrative access to the **SoftNAS SNAP HA™** storage controllers:

1) VPN - this is the most secure stand-alone solution, and a recommended minimum best practice for limiting access to the private IPs of each **SoftNAS Cloud®** controller. In this case, use DNS to assign a common name to each controller (e.g., "nas01.localdomain.com", "nas02.localdomain.com"), making routing to each **SoftNAS Cloud®** controller convenient for administrators

2) Admin Desktop - an even more secure approach is to combine VPN access with an Administrator's desktop, (sometimes referred to as a jumpbox) typically running Windows and accessed via RDP. This secure admin desktop adds another layer of authentication, namely Active Directory (or local account) authentication. Once an administrator has gained secure, encrypted access to the Admin Desktop, she opens up a web browser to connect to the **SoftNAS StorageCenter™** controller.

HA Controller in AWS

On AWS, shared data stored in highly-redundant S3 storage is used as an HA Controller. A single S3 bucket is created in the same region as the VPC.

HA controller bucket names in S3 are of the form "hacontroller-<haUUID>", where haUUID is a unique ID created by **SNAP HA™** and assigned to represent a customer's HA cluster; e.g., "hacontroller-02c8a87d-8af7-4295-962e-8313e1ff6c7d" is an HA controller bucket stored on S3. The HA controller bucket occupies very little space.

AWS VPC Architecture: Elastic IPs

On AWS, **SoftNAS SNAP HA™** is designed to operate within the Virtual Private Cloud (VPC). VPCs can be as simple as a single subnet, with or without a VPN security gateway, or as complex as public / private compartmentalized subnets, as depicted in the figures herein. In figure 1 below, we see a VPC configured to operate across two availability zones (AZ), with separate subnets for public and private use. **SoftNAS Cloud®** controllers are placed into the public subnet for elastic IP address routing purposes.

About Elastic HA™ IP Addresses

SoftNAS Cloud® storage is normally not accessible from the public Internet. A special "Elastic HA™" IP address is configured with a security group setting that restricts its access to only the internally-routable, private IPs assigned to the VPC; e.g., in this example, only EC2 instances within the VPCs internal 10.0.0./16 private network are routable to the Elastic HA IP.

Why use an Elastic IP? Elastic IPs (EIP) were previously the only supported cross-zone routable IP addresses available in the AWS VPC environment. In practice, EIPs add very little latency or other overhead to storage traffic, and provide routing redundancy across the zones.

SoftNAS SNAP HA™ takes a basic EC2 elastic IP and layers on additional patent-pending functionality that turns it into an Elastic HA IP - a cross-zone IP suitable for highly-available network-attached storage.

AWS Cross-Availability Zone Architecture Overview

Please refer to Figure 1 shown below for the remaining discussion. This drawing depicts a typical HA deployment, but is not the only possible design. In fact, **SoftNAS SNAP HA™** can be deployed with dual controllers located within a single AZ on a VPC (there is no requirement to split controllers across AZs, but it is a recommended best practice for maximum availability).

We see a VPC created in a /16 network in AWS US East (Virginia) data center, with subnets allocated in US East 1-a and 1-b. This topology provides the best overall redundancy and availability within the AWS AZ architecture.

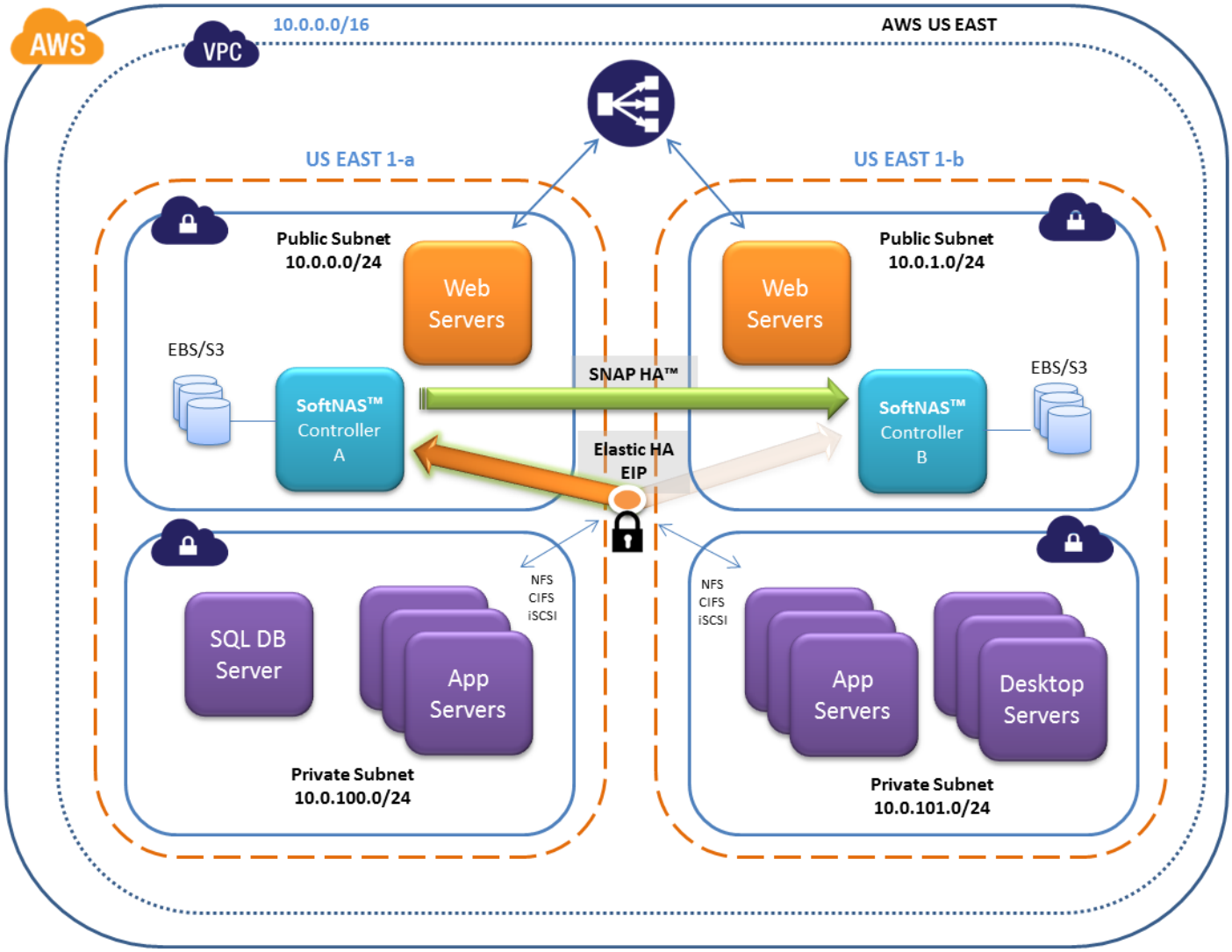


Figure 1 - AWS VPC with SoftNAS SNAP HA™

Two **SoftNAS Cloud®** controller EC2 instances are deployed - one per AZ. If optional private subnets are configured in one or more AZs, they will also have access to the Elastlc HA IP for NFS client storage access via NFS, CIFS and iSCSI protocols.

The drawing shows **SNAP HA™** replication traffic flowing from Controller A to Controller B. This traffic is allocated to interface 0. Interface 0 is also used for administration using the **SoftNAS StorageCenter™** GUI. Block replication keeps a warm copy of the data from node A on node B, in case a failover is necessary.

The drawing shows two orange arrows emanting from an orange and white circle, which represents the Elastic HA IP. The black lock symbol represents the EC2 Security Group associated with the Elastic HA IP. The shadowed orange arrow represents re-routed storage requests flowing to Controller B after an automatic failover or manual takeover.

When an automatic failover or manual takeover occurs, NAS traffic is re-routed via the Elastic HA IP from Controller A to Controller B, as indicated by in the diagram above. When an Elastic HA switches over from one controller to another, NAS client traffic is rapidly re-routed to the new controller, typically in just a few seconds. NAS clients typically experience a brief switchover delay of up to 20 seconds or so, and automatically reconnect after the switch over event takes place.

AWS Cross-Availability Zone Network Design

Each **SoftNAS Cloud®** controller has two NICs assigned - interface 0 (default) and one additional interface 1 (added during EC2 instance configuration).

1) Admin and Replication, Interface 0 - the first (default) NIC is used for **SoftNAS StorageCenter™** access and **SnapReplicate™** data replication across controllers.

2) **SoftNAS Cloud®** Storage, Interface 1 - the second NIC is dedicated to NAS storage traffic, and is used for Elastic HA IP routing of storage-related traffic (NFS, CIFS, iSCSI).

Note in the following diagrams the IP addresses shown are for illustration purposes only, and actual IP addresses will be assigned by AWS.

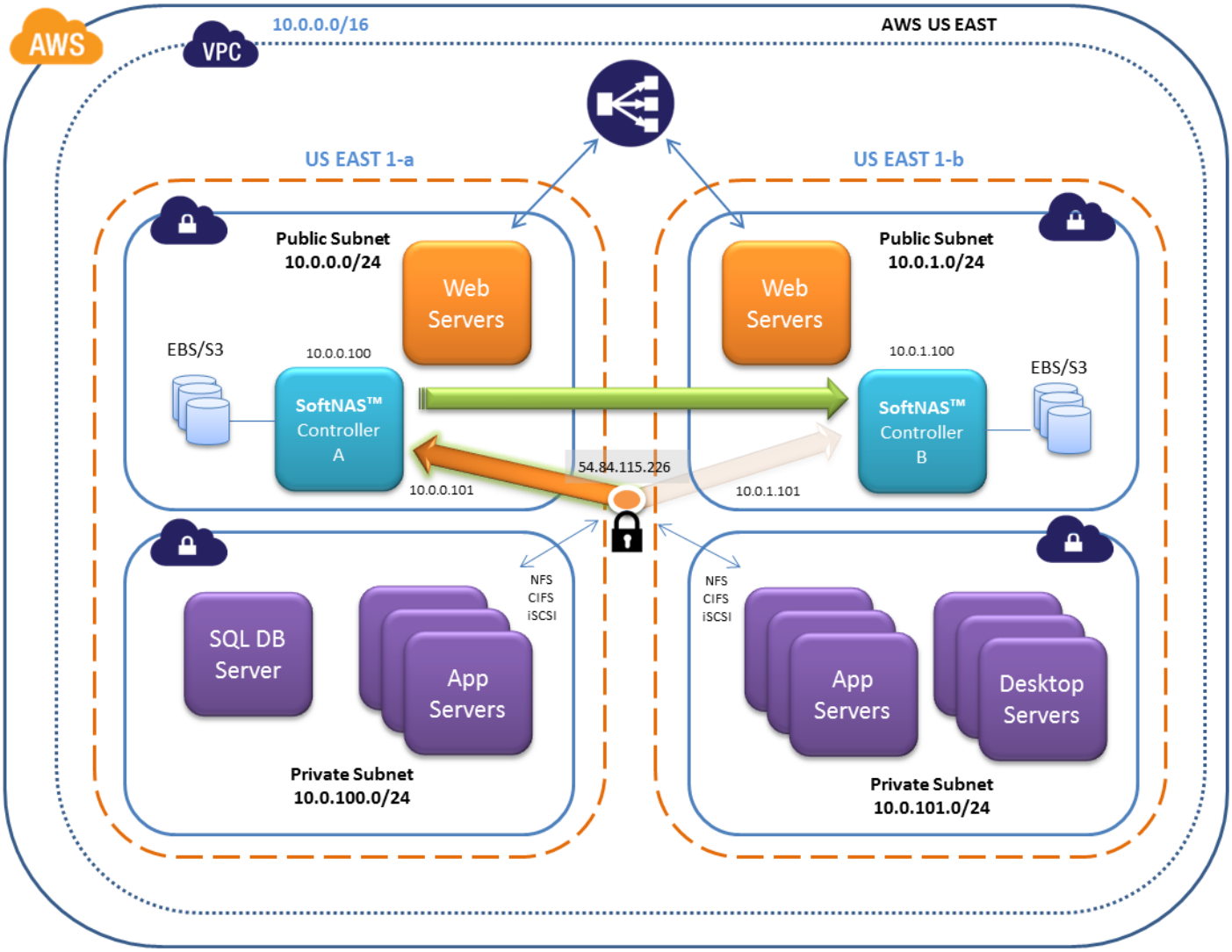


Figure 2 - AWS Cross-AZ Network Architecture

The remaining EC2 instances constitute NAS clients; that is, EC2 instances that connect using NFS, CIFS or iSCSI protocols to access NAS services across the private network. Although only two AZs are shown in these diagrams, NAS clients can access HA NAS services from any zone within the region allowed access to the Elastic HA IP.

Secure Administrative Access in VPC

There are multiple ways to configure secure administrative access to the **SoftNAS SNAP HA™** storage controllers:

1) VPN - this is the most secure and recommended best practice for limiting access to the private IPs of each **SoftNAS Cloud®** controller. In this case, use DNS to assign a common name to each controller (e.g., "nas01.localdomain.com", "nas02.localdomain.com"), making routing to each **SoftNAS Cloud®** controller convenient for administrators

2) Admin Desktop - an even more secure approach is to combine VPN access with an Administrator's desktop, typically running Windows and accessed via RDP. This secure admin desktop adds another layer of authentication, namely Active Directory (or local account) authentication. Once an administrator has gained secure, encrypted access to the Admin Desktop, she opens up a web browser to connect to the **SoftNAS StorageCenter™** controller.

3) Direct Internet Access - the least secure, yet simplest form of providing administrators with access to **SoftNAS StorageCenter™** is to assign two additional Elastic IP addresses, one per **SoftNAS Cloud®** controller (see Figure 3 below). Of course, a corresponding security group, locked down to restrict the IP addresses allowed access to the controllers is necessary to properly secure this configuration. While not recommended for production systems, this configuration is most commonly seen during evaluation and for development systems, where full VPC deployment has not yet taken place.

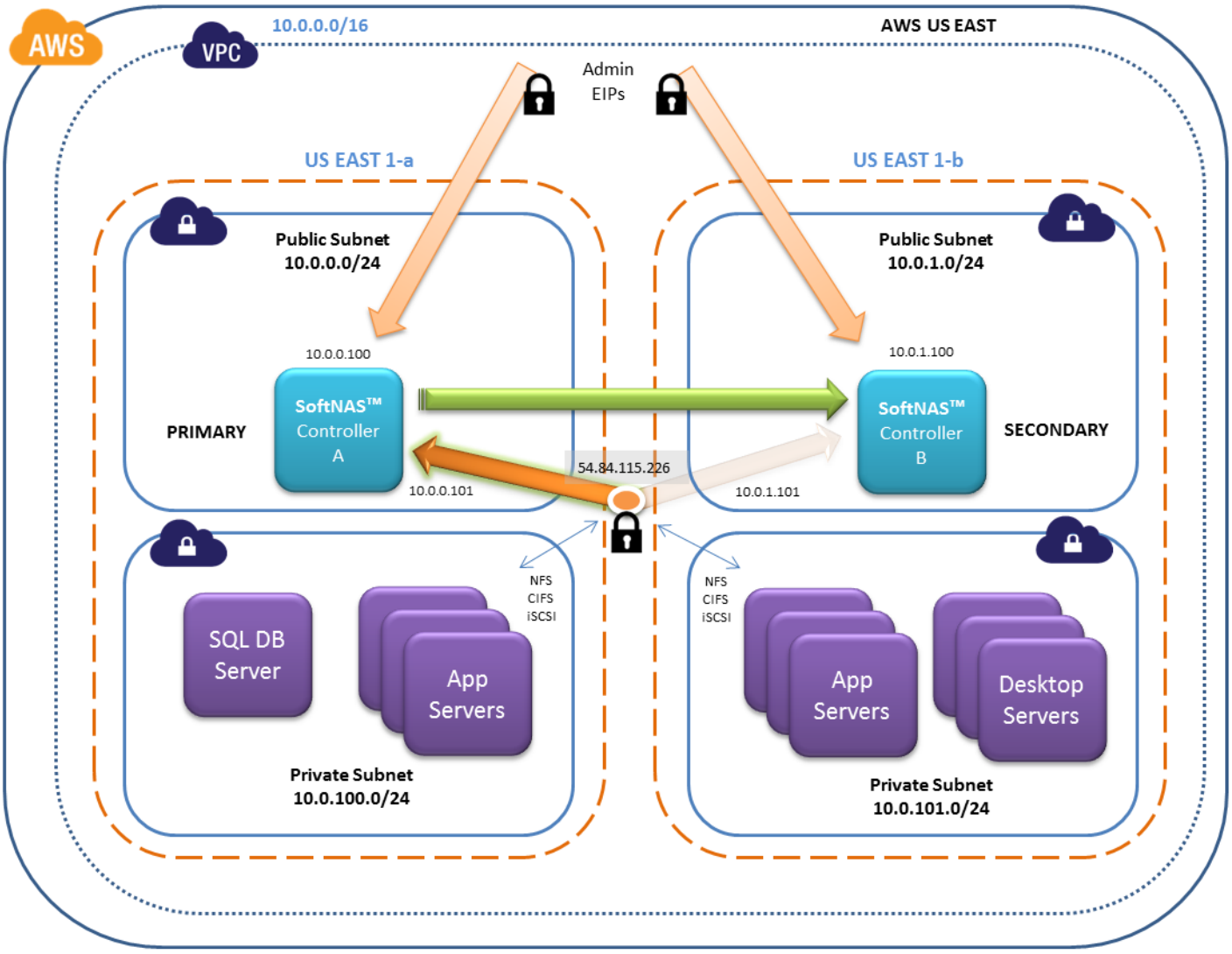


Figure 3 - Administrative Access, EIP Option

HA Controller in AWS

On AWS, shared data stored in highly-redundant S3 storage is used as an HA Controller. A single S3 bucket is created in the same region as the VPC.

HA controller bucket names in S3 are of the form "hacontroller-<haUUID>", where haUUID is a unique ID created by **SNAP HA™** and assigned to represent a customer's HA cluster; e.g., "hacontroller-02c8a87d-8af7-4295-962e-8313e1ff6c7d" is an HA controller bucket stored on S3. The HA controller bucket occupies very little space.

Premise-based HA Architecture

SoftNAS SNAP HA™ easily fits within a modern, virtualized data center. Today's data center is often running VMware, with a network architecture comprised of several VLANs used to segregate various classes of network traffic. Figure 4 below shows one such network topology, which implements best practices for **SoftNAS SNAP HA™** in the data center.

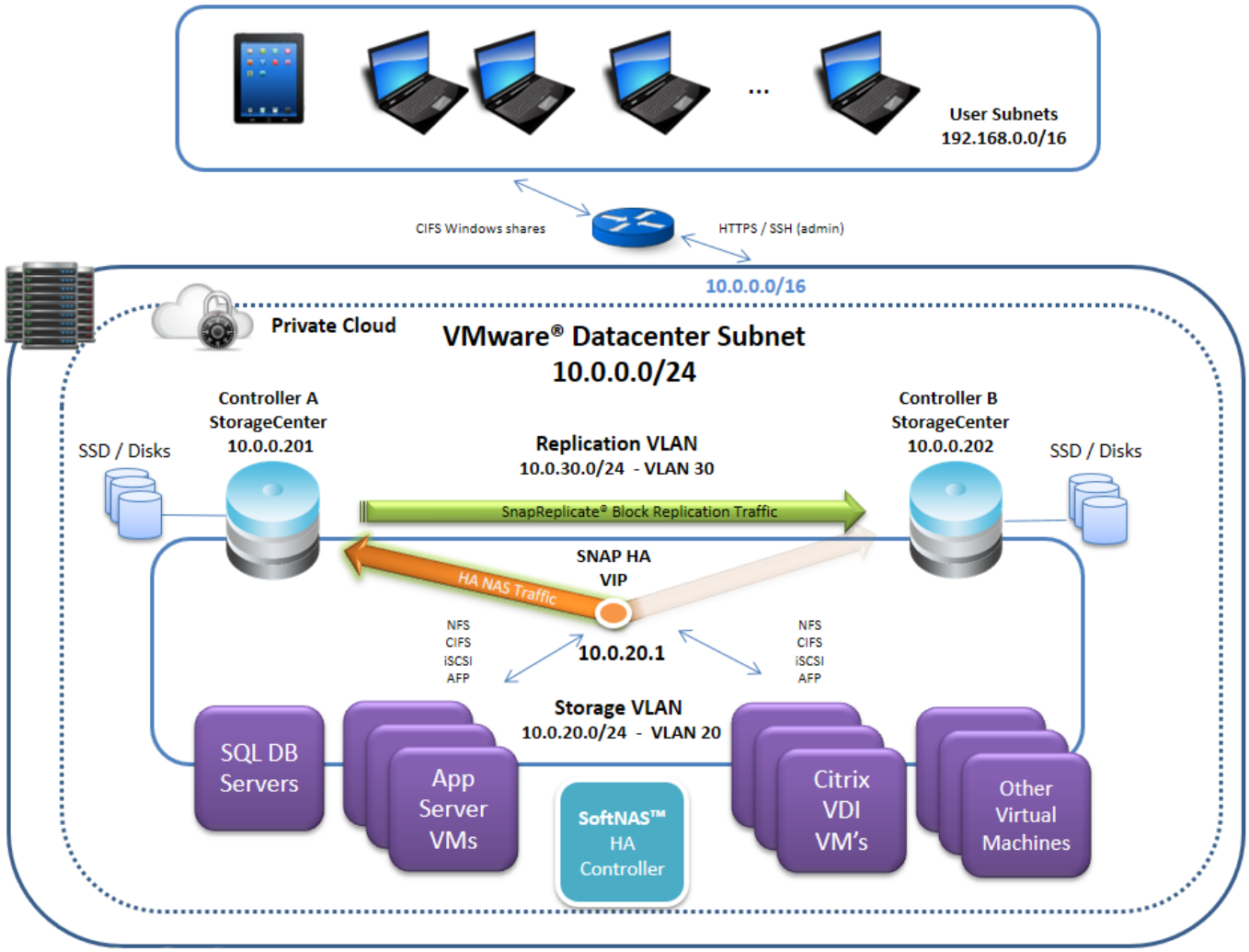


Figure 4 - Private Data Center with SoftNAS SNAP HA™

User subnets are allocated outside the data center network, and traverse one or more routers to reach the data center.

The data center network exists on its own /16 (or similar) layer 2 network, which we term the "Datacenter Primary Subnet". This subnet is used for administrative and other default traffic.

A separate "Replication VLAN" and corresponding subnet is allocated for **SoftNAS Cloud®** block replication traffic; i.e., **SnapReplicate™** is configured to flow across this dedicated VLAN, which prevents data replication traffic between controllers from impacting storage or other data center services. During high periods of I/O, data replication on a 1 GbE network can reach sustained levels of 120 MB/sec as multiple streams of block replication take place across controllers, so the replication VLAN is an important consideration.

A separate "Storage VLAN" and corresponding subnet is allocated for **SoftNAS Cloud®** primary virtualization storage traffic; i.e., NFS and iSCSI traffic between VMware vmKernels on each VM host responsible for storage access. Assigning a separate vSwitch and physical NICs to storage is essential for achieving maximum

throughput and IOPS, and for keeping storage access isolated from other network segments. If storage is not isolated on its own VLAN, vSwitch and physical NICs, performance will be impacted and high storage I/O loads will impact other services.

StorageCenter and routine, lower-priority storage traffic (e.g., from the User Subnets) can be routed across the default data center network, if simplicity of network topology is desired. Alternatively, certain protocols (e.g., CIFS for Windows shares) could be routed to the Storage VLAN and HTTP/HTTPS/SSH routed to the default data center network for **SoftNAS StorageCenter™** access and administration.

In the example shown above, VLAN 30 is assigned to **SNAP HA™** replication. VLAN 20 is assigned to as the Storage VLAN. A special "Elastic HA™" IP address is configured within the Storage VLAN subnet to act as a virtual IP address. **SoftNAS SNAP HA™** uses ARP IP aliasing to route the Elastic HA IP address to the proper **SoftNAS Cloud®** Controller.

Elastic HA IP

The Elastic HA IP in VMware is implemented as a virtual IP termed a "VIP"; that is, an IP address that can be quickly reassigned using a combination of ARP and local interface commands. Choose a VIP address that is within the Storage VLAN subnet. In the example show in Figure 4, a VIP of 10.0.20.100 would work fine. The VIP must not be manually assigned to any interface. During installation and set up of **SNAP HA™**, the VIP will be automatically configured and assigned to the primary controller and then managed by **SNAP HA™**.

HA Controller VM

In the VMware virtualization environments, a 3rd **SoftNAS Cloud®** VM is installed to act as the "HA Controller", shown below in Figure 5.

The HA Controller acts as an independent, 3rd party witness and controller to all **SNAP HA™** failover and takeover operations. The HA Controller keeps track of which **SoftNAS Cloud®** storage controller is, in fact, operating as the Primary controller. This prevents the possibility of "split-brain" or other potential cluster management maladies that could otherwise occur when only two cluster nodes are present, by fencing off failed controllers and ensuring they are not allowed to come back online and pose as a primary storage controller.

In VMware HA environment an HA Controller deployed as an "FT" (fault tolerant) VM is required. HA Controllers are relatively lightweight versions of **SoftNAS Cloud®**, only requiring 512 MB of RAM and 1 vCPU, and have relatively little network traffic or data change, so they pose relatively little resource overhead vs. the added peace of mind of always knowing that storage HA operations will remain consistent, no matter what takes place across the virtualization environment.

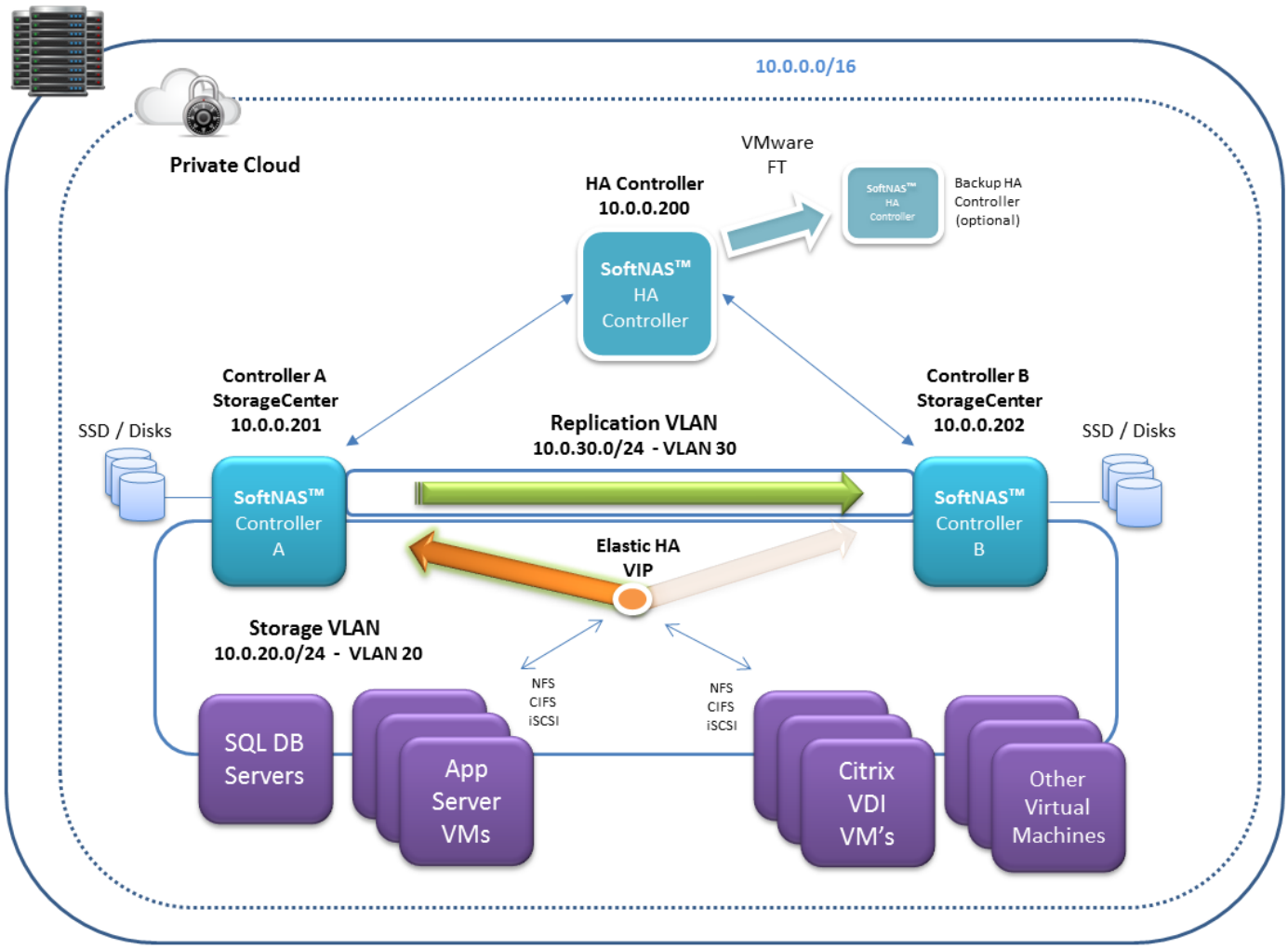


Figure 5 - HA Controller VM

The HA Controller is required for both production and test environments to ensure proper HA operation always takes place. If no HA Controller is deployed, IT administrators would instead have to assume all responsibility for keeping track of failovers and ensuring controllers with old data are not brought online before the most recent primary controller. As this would defeat the purpose of automated failovers, and the premise behind high availability, SoftNAS requires HA controllers for all VMware HA configurations.