HITACHI
Inspire the Next

Building a Multi-tenancy, Multi-cloud Solution with HNAS 5000

Using Hitachi Cloud Connect for Equinix

Hitachi Vantara
May 2023

HITACHI
Inspire the Next

Table of Contents

Notices and Disclaimer

About This Guide

Introduction

This reference architecture documents how to set up a multi-tenant, multi-cloud solution with Hitachi NAS Platform (HNAS) to provide network attached storage (NAS) services to clients in multiple, distinct clouds.

Intended Audience

This document is intended for Hitachi Vantara staff and IT professionals of Hitachi Vantara customers and partners who are responsible for planning and deploying such as solution.

Document Revisions

Revision Number	Date	Author	Details
v1.0	May 2023	Hitachi Vantara LLC	Initial Release

References

- Virtual SMU Administration Guide: https://knowledge.hitachivantara.com/Documents/Storage/NAS_Platform/14.4/NAS_Installation_and_Configuration_Guides/Virtual_SMU_Administration_Guide
- HNAS Administration Guides: https://knowledge.hitachivantara.com/Documents/Storage/NAS_Platform/14.4/NAS_Administration_Guides
- HNAS Multi-tenancy Implementation and Best Practices Guide: https://knowledge.hitachivantara.com/Documents/Storage/NAS_Platform/Best_practices/HNAS_Multi-tenancy_Implementation_and_Best_Practice_Guide

Comments

Send any comments on this document to GPSE-Docs-Feedback@hitachivantara.com. Include the document title, including the revision level, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you.

Executive Summary

This reference architecture documents how to set up a multi-tenant, multi-cloud solution with the Hitachi NAS Platform (HNAS) to provide network attached storage (NAS) services to clients in multiple, distinct clouds. HNAS uses Enterprise Virtual Servers (EVSs) to provide file services such as SMB shares and NFS exports. You can deploy multiple EVSs on the same HNAS server or cluster while maintaining unique network and security settings. You can create up to 64 EVSs on an HNAS server or cluster.

The environment used for this validation includes an HNAS 5300 cluster with storage provided by a Hitachi Virtual Storage Platform 5200 (VSP 5200) storage system. The equipment was placed in a near-cloud colocation datacenter operated by Equinix. This location was selected because it offered high-speed and low latency connections to the major hyperscalers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). In fact, Hitachi Vantara collaborated with Equinix to create a new near-cloud hybrid solution called **Hitachi Cloud Connect for Equinix**.

This offering allows clients to locate Hitachi VSP enterprise-class storage at Equinix International Business Exchange™ (IBX) data centers worldwide and includes the option for customers to procure this solution through one agreement and invoice, greatly simplifying and accelerating their time to market. By using Equinix IBX data centers and Equinix Fabric™ to interconnect sources of data to applications, VSP storage systems enable organizations to locate their data next to clouds while still maintaining control by enabling applications such as data protection and back-up for hybrid- and multi-cloud data availability.

If you want to discuss options for hosting these types of solutions at Equinix, contact your Hitachi Vantara sales team. For more information, visit the Hitachi Cloud Connect for Equinix webpage at: https://hitachivantara.com/en-us/products/storage/flash-storage/cloud-connect-for-equinix.html.

Introduction

The environment used for this validation includes a HNAS 5300 cluster, with backend storage provided by a VSP 5200 storage system. The equipment was placed in a near-cloud colocation datacenter operated by Equinix. This location was selected because it offered high-speed and low latency connections to the major hyperscalers, such as AWS, Microsoft Azure, and GCP.

To summarize, our hybrid cloud environment consisted of two domains. The relationship between the two sites is shown is *Figure 1*.

- A near-cloud Equinix colocation data center (named SV5), located in San Jose, California.
- Hyperscalers, including AWS, Azure, and GCP, hosted in Northern California.

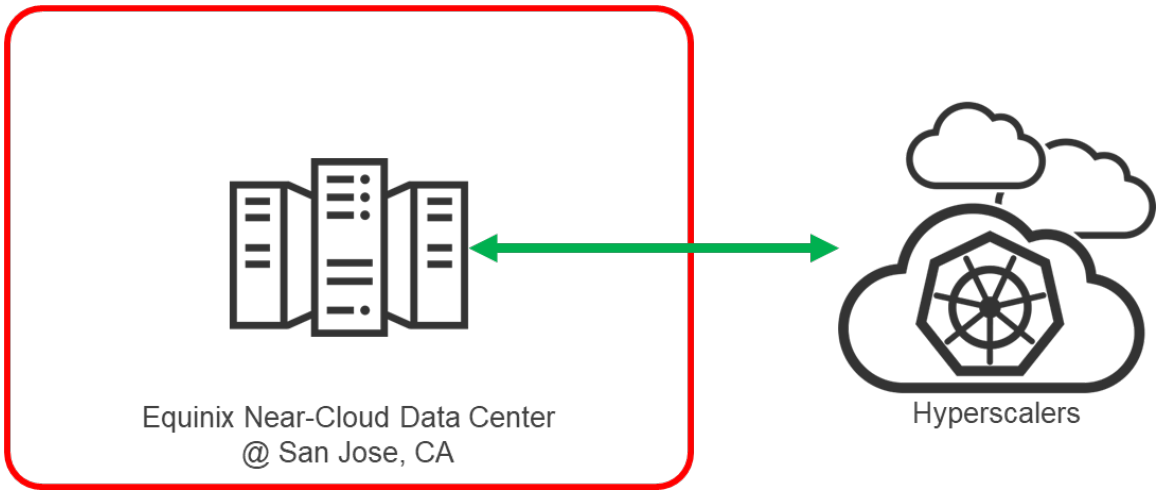


Figure 1: High Level Diagram

Note: The information shared here is specific to our requirements. It can be used as a guideline or a starting point, but we recommend conducting a proof-of-concept in a non-production, isolated test environment matching your production environment before implementing this solution.

Solution Overview

HNAS multi-tenancy provides companies, such as application service providers, with the ability to support more than one customer service on a single HNAS server or cluster, while keeping them logically separate. *Table 1* compares the capabilities that HNAS multi-tenancy adds.

Capabilities	Stand-alone	Multi-tenancy
Multiple EVSs per HNAS	x	x
Logically separate serving environments on a single HNAS or cluster		x
Combining multiple EVSs into one EVS		x
Per-EVS security with global namespaces	x	x
Legacy VLANs (deprecated)	x	
VLAN-interface	x	x
Duplicate or overlapping IP address support		x
EVS crosstalk checking		x
Per-EVS routing	x	x
Multi-tenancy-aware protocols		x

Table 1: *Multi-tenancy Capabilities*

To enable and use multi-tenancy mode, ensure that the following requirements are met:

- The per-EVS Security license must be installed.
- All EVSs present on the NAS server or cluster must be configured with individual security settings.
- An EVS can use a VLAN interface, or an aggregation interface, but VLANs configured with the vlan command are not supported. VLAN interfaces are configured using the vlan-interfaces command.
- No cluster name space (CNS) can be configured (an EVS name space is supported).
- Active Directory Server (ADS) entries must be used instead of NT domains.
- For clusters, all nodes must be running a version of software that supports multi-tenancy.
- When enabling multi-tenancy mode for a cluster, all cluster nodes must be online.

For the complete requirements list, see the HNAS Server and Cluster Administration Guide.

Business Benefits

The following lists the benefits of a multi-tenancy, multi-cloud HNAS solution with the Hitachi Cloud Connect for Equinix program.

- HNAS multi-tenancy improves resource utilization by allowing the same hardware to be shared among multiple tenants.
- Equinix Fabric provides connectivity to major hyperscalers at low latency and high throughput.
- HNAS file-serving protocols, CIFS/SMB, NFS, FTP, and iSCSI, are naturally compatible with modern operating systems and applications (in the cloud and on-premises).

Key Components

The following lists the major components of the solution. For specifications, see the Hardware and Software section.

- Hitachi NAS Platform: Two HNAS 5300 systems configured in a cluster.
- VSP Storage System: A VSP 5200 storage system was used as the backend storage system for the HNAS cluster.
- System Management Unit (SMU): A virtual SMU was used to manage the HNAS cluster.
- Network Switch: A Cisco Nexus 9000 Series switch was used to connect the HNAS system to the Equinix Fabric, which provided the uplink to the hyperscalers.
  - 10/25Gbase-LR-S Optics: Long Range transceivers to connect long distances.
  - Single-Mode Fiber Cables: For long distance communications.
- Equinix Fabric: Connected equipment at the Equinix near-cloud data center to the hyperscalers.
- AWS Cloud: Equipment at Equinix was connected to AWS cloud using a 10 Gbps Direct Connect link. On AWS, a Virtual Private Cloud was created in the region us-west-1.
- Azure Cloud: Equipment at Equinix was connected to Azure cloud using a 10 Gbps Express Route link. On Azure, a Virtual network was created in the region West US.
- GCP Cloud: Equipment at Equinix was connected to Google cloud using a 10 Gbps Google Cloud Interconnect link. On GCP, a Virtual Private Cloud was created in the region us-west1-b.

Validation

This section describes the method, test environment, hardware and software, and test scenarios used in the validation.

Validation Method

To validate the solution, three EVSs were created to provide SMB and NFS file services to clients in the three hyperscalers. All three EVSs shared a single ethernet aggregate. Routing was configured between each EVS to the respective hyperscaler. We created one file system for each EVS. Then, SMB shares and NFS exports were configured so each file system could be accessed by clients running in the clouds.

Additionally, we validated running the SMU in Azure (instead of on-premises in the near-cloud data center) to demonstrate the ability to add an extra layer of resiliency.

High Level Diagram

Figure 2 shows the test environment used to run the validation.

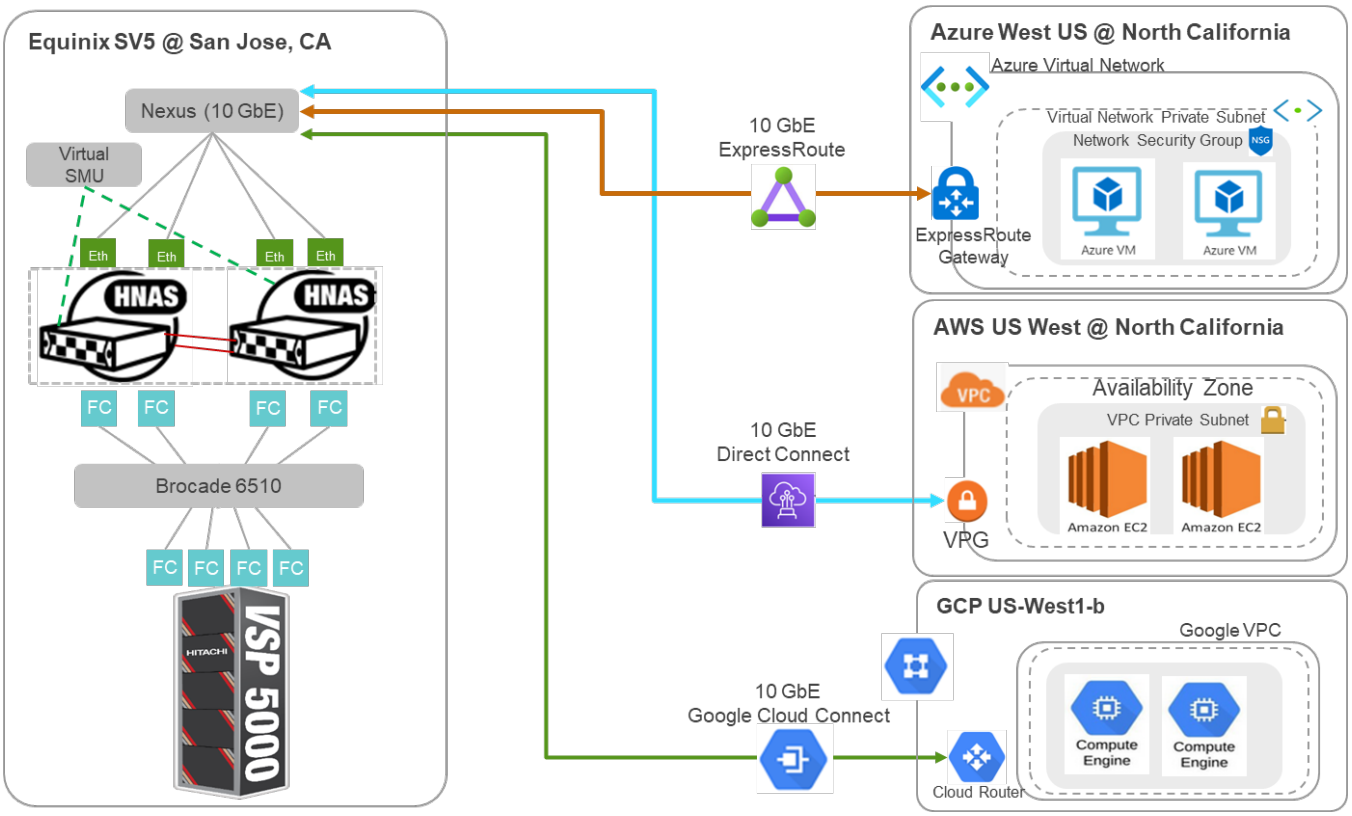


Figure 2: *Test Environment*

Hardware and Software

Table 2 provides the hardware specifications for the equipment used in this validation.

Item	Description	Version	Function
HNAS 5300	HNAS 5300	Firmware 14.4.7322.05	2-node HNAS cluster
VSP 5200	1 TB cache (2) 20-core MPUs (4) RAID6 6D+2P parity groups (4) 32 Gbps FC ports	SVOS RF 9.8.2 90-08-61-00/00-M104	Backend storage system
Brocade 6510	16 Gbps Fiber Channel switch	FOS 8.2.1	Provides FC connectivity between the VSP 5200 and HNAS cluster.
Cisco Nexus C93180YC-FX	Cisco Nexus C93180YC-FX 10 GbE Switch	NXOS 9.3(4)	Network switch

Table 2: *Hardware Components*

Table 3 provides the software specifications used in this validation.

Item	Version	Function
Virtual System Management Unit	14.4.7322.05	Manages HNAS clusters
Microsoft Windows Server 2019 Datacenter	Windows Server 2019 Datacenter	Operating system of SMB hyperscalers clients
Red Hat Enterprise Linux	Red Hat Enterprise Linux 8.6	Operating system of NFS hyperscalers clients

Table 3: *Software Components*

Table 4 provides the configuration details of HNAS 5300 used in this validation.

Item	Description
HNAS Model	HNAS 5300
HNAS Firmware	14.4.7322.05
Number of HNAS Nodes	2
Number of System Drives	32
Capacity per System Drive	6 TB
Number of Storage Pools	1
Capacity of Storage Pool	192 TB
Number of File Systems	3
Capacity per File System	5 TB
Number of NFS Export per File System	1
Number of SMB Share per File System	1
Number of Backend FC Ports	2 per HNAS node

Item	Description
Number of Frontend 10 GbE Ports	2 per HNAS node
HNAS Deduplication	Enabled

Table 4: *Characteristic of HNAS 5300*

Test Scenarios

Table 5 lists the test scenarios performed in the validation.

#	Description	Success Criteria
1	Prepare the environment: 1. Provision (32) 6 TB DP volumes on VSP 5200 storage system to HNAS nodes. 2. Deploy virtual SMU at Equinix near-cloud data center. 3. Build HNAS cluster using two HNAS 5300 systems. 4. AWS cloud: Deploy one Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine. 5. Azure cloud: Deploy one Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine. 6. GCP cloud: Deploy one Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine.	Environment is set up as per specifications.
2	Configure HNAS multi-tenancy: 1. Install EVS Security license, if not already installed. 2. Enable multi-tenancy. 3. Create EVS and enable routing by EVS. 4. Configure DNS for each EVS. 5. Add each EVS to Windows Active Directory. 6. Provision SMB shares and NFS exports. 7. Validate whether the network clients in the cloud can access the HNAS file system.	HNAS file services are accessible to network clients in all three hyperscalers.
3	Deploy virtual SMU in Azure: 1. Create Azure storage account and upload SMU virtual disk. 2. Create managed disk. 3. Create a virtual machine. 4. Set static IP address on the virtual machine. 5. Install SMU software.	Virtual SMU on Azure can administer near-cloud HNAS cluster.

Table 5: *Test Scenarios*

Guidelines and Recommendations

This section describes the lessons learned from this validation, along with guidelines and recommendations.

- HNAS used a single ethernet aggregate to provide the optimum resource utilization. However, you can use separate ethernet aggregates, for instance, to provide more bandwidth.
- Ensure that the network configuration is performed correctly between the near-cloud colocation site and between cloud providers in advance. All the required VLAN configurations responsible for different cloud providers must be carefully designed and implemented within the network switch and tested well in advance. For example, in the tested environment, before the exercise, physical cable connections were set up between the near-cloud site and cloud providers, and VLANs were created within the network switch. Then, we verified that the communication between near-cloud site and cloud worked correctly.
- Ensure that EVS security license for HNAS multi-tenancy is installed.
- Enabling multi-tenancy in HNAS causes a temporary loss of service.
- We recommend using effective EVS naming conventions for ease-of-use when multiple cloud providers are connected with the EVSs. For example, the EVS connected with AWS can be named AWSEVS and the EVS connected with Azure can be named AZEVS. This helps to identify EVSs during the configuration.
- The SMU requires a static IP address if it is used as an HNAS cluster quorum (which is a common deployment option).

Validation Results

This section shows specific steps and screenshots for each test scenario.

Test 1: Prepare the Environment

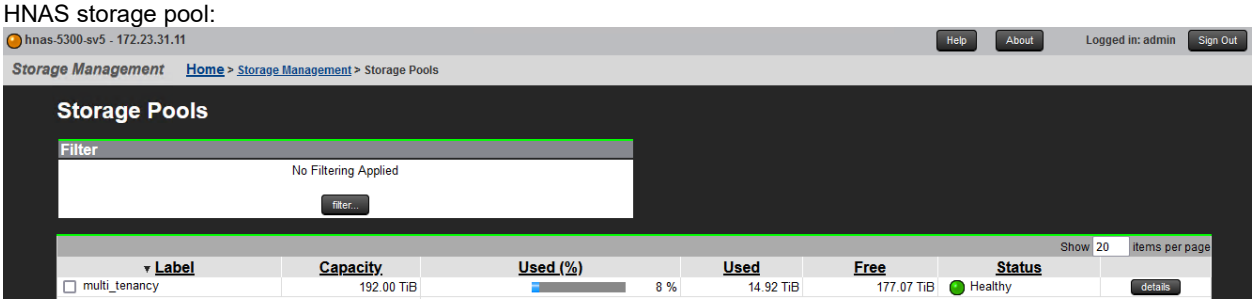
This test case describes the configuration of the components used in the validation.

Prerequisites

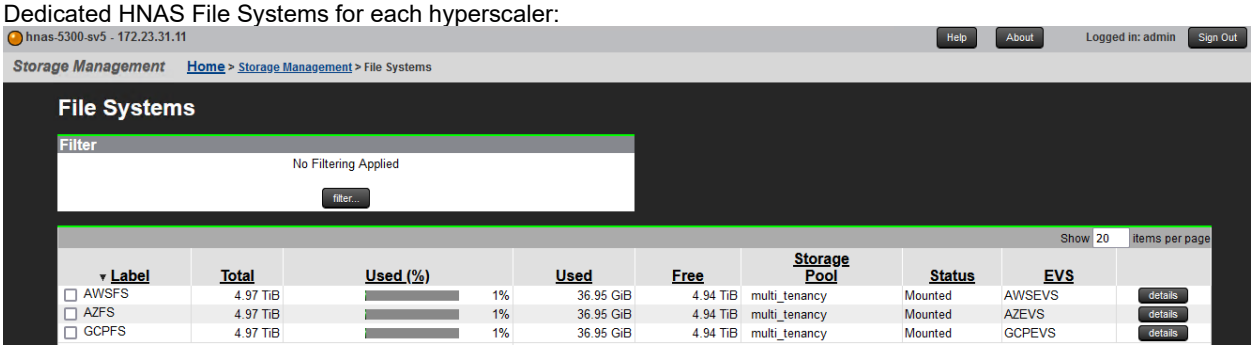
Note that the following prerequisites are outside the scope of this document, so we do not describe them in detail.

- Physical LAN and FC connections for the HNAS cluster.
- Network configuration to allow communication between the HNAS cluster and AWS, Azure, and GCP.
- Virtual SMU: See Installing and Configuring Virtual SMU.
- Configure the HNAS cluster: See Create HNAS Cluster using NAS manager.
- Provision volumes from VSP 5200 storage system to the HNAS cluster.
- Create virtual machines that will act as file share clients:
  - AWS cloud: One Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine.
  - Azure cloud: One Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine.
  - GCP cloud: One Windows Server 2019 virtual machine and one RHEL 8.6 virtual machine.
- The following screenshots show the storage pool and file systems created on the HNAS cluster. For instructions on how to set up these objects, see HNAS Administration Guides.

HNAS storage pool:

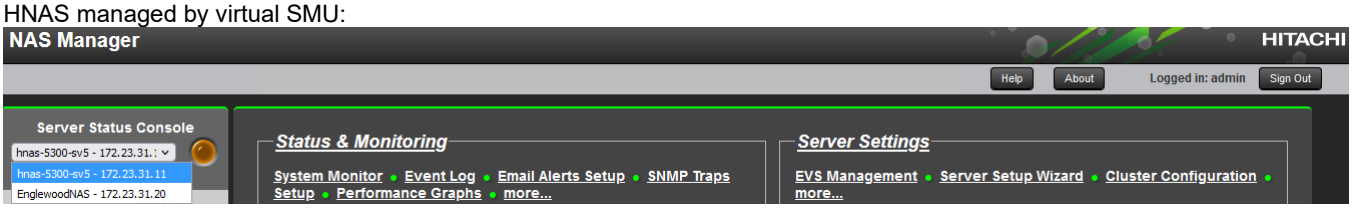


Dedicated HNAS File Systems for each hyperscaler:

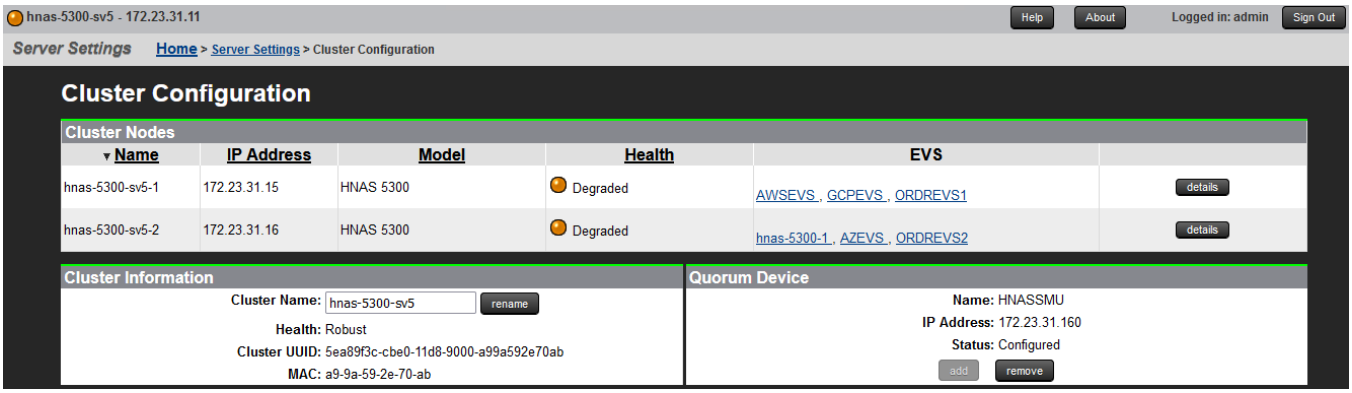


- The following screenshots show the HNAS cluster as a managed server under the virtual SMU. For usage information, see the Virtual SMU Administration Guide.

HNAS managed by virtual SMU:



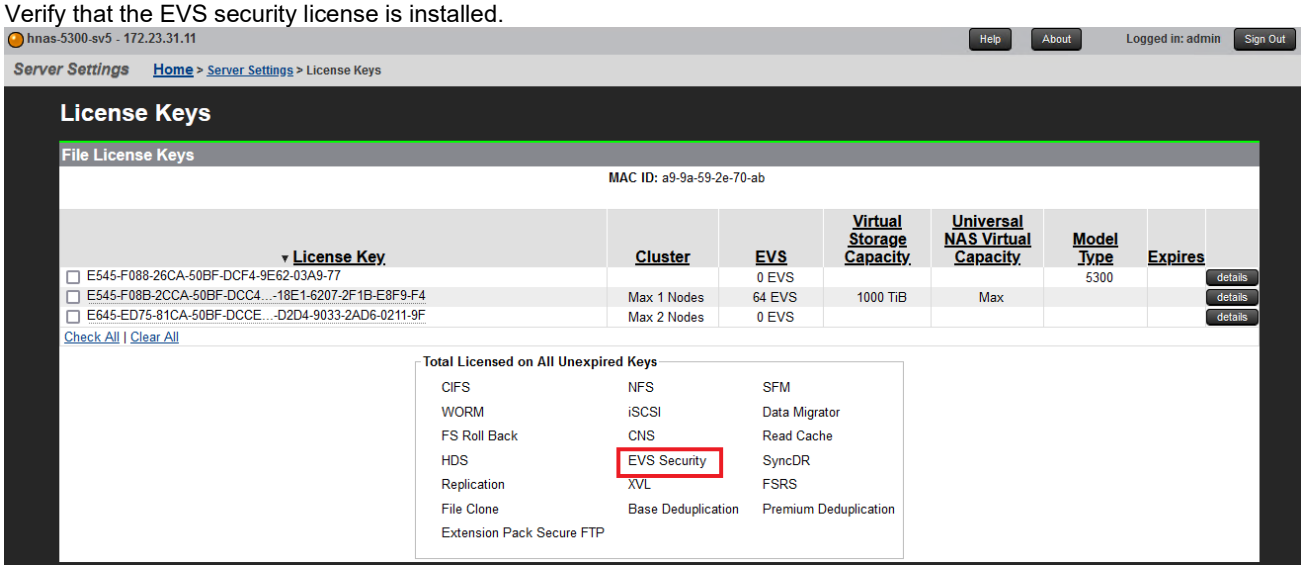
Status of HNAS nodes in the cluster:



Test 2: Configure HNAS Multi-tenancy

This test case describes the process of implementing multi-tenancy and connections to different cloud providers. For more in-depth information on multi-tenancy, see the HNAS Multi-tenancy Implementation and Best Practice Guide.

1. Verify that the EVS security license is installed.



Enable multi-tenancy as follows:

```
hnas-5300-sv5-2:$ cn all multi-tenancy-show
Cluster node 1:
Multi-tenancy is disabled.
Cluster node 2:
Multi-tenancy is disabled.
hnas-5300-sv5-2:$ cn all multi-tenancy-enable
Cluster node 1:
Warning: Enabling multi-tenancy significantly affects the configuration of the HNAS.
Have you read and understood the multi-tenancy man page?(Y/N)[N]:
Y
Have you read and understood the multi-tenancy-enable man page?(Y/N)[N]:
Y
Do you understand that once enabled, multi-tenancy cannot be disabled until all file serving EVSs have been deleted?(Y/N)[N]:
Y
Warning: All active connections, including any remote console sessions, will be disconnected to allow the network service to support multi-tenancy.
Do you want to proceed?(Y/N)[N]:
YConnection closed by foreign host.
```

```
hnas-5300-sv5-2:$ cn all multi-tenancy-show
Cluster node 1:
Multi-tenancy is enabled.
Cluster node 2:
Multi-tenancy is enabled.
```

2. Create an EVS and enable EVS routing.
   a. Create three EVSs, one for each cloud provider. The naming was selected for ease of identification: AWSEVS is used to communicate with AWS, AZEVS is used for Azure, and GCPEVS is used for GCP.

```
Hitachi NAS OS Console
MAC ID : 81-36-D3-B0-02-98
Cluster MAC ID : A9-9A-59-2E-70-AB

hnas-5300-sv5-2:$ evs create -l AWSEVS -i 172.23.31.27 -m 255.255.254.0 -p ag2
Service EVS 3 created successfully.
hnas-5300-sv5-2:$ evs create -l AZEVS -i 172.23.31.28 -m 255.255.255.0 -p ag2
Service EVS 4 created successfully.
hnas-5300-sv5-2:$ evs create -l GCPEVS -i 172.23.31.29 -m 255.255.255.0 -p ag2
Service EVS 5 created successfully.
```

The following screenshot shows the three EVS after creation:

```
hnas-5300-sv5-2:$ evs list

Node EVS ID    Type           Label Enabled Status       IP Address Port
---- ------ ------- --------------- ------- ------ ---------------- ----
   1         Cluster hnas-5300-sv5-1     Yes Online 172.23.31.15     eth1
   1      1 Service        ORDREVS1     Yes Online 172.23.31.17      ag1
   1      3 Service          AWSEVS     Yes Online 172.23.31.27      ag2
   1      5 Service          GCPEVS     Yes Online 172.23.31.29      ag2
   2         Cluster hnas-5300-sv5-2     Yes Online 172.23.31.16     eth1
   2      0   Admin     hnas-5300-1     Yes Online 172.23.31.11     eth0
   2      2 Service        ORDREVS2     Yes Online 172.23.31.18      ag2
   2      4 Service          AZEVS     Yes Online 172.23.31.28      ag2
```

b. Before enbling EVS routing, set evs-security to ‘individual’ using the followng command:

`evs-security individual -e <evs-id>`

The following screenshot shows the EVS security setting:

```
hnas-5300-sv5-2:$ evs-security list

EVS id     Per EVS security status
------     -----------------------
     1                  individual
     2                  individual
     3                  individual
     4                  individual
     5                  individual
```

c. Enable routing by EVS as follows:

```
hnas-5300-sv5-2:$ cn all routing-by-evs-show
Cluster node 1:
routing-by-EVS is enabled
Warning: routing-by-evs is active as multi-tenancy is enabled
Cluster node 2:
routing-by-EVS is enabled
Warning: routing-by-evs is active as multi-tenancy is enabled
```

d. Configure routing for each of the three EVSs as follows:

Routing for AWS:

```
hnas-5300-sv5-2:$ vn 3 route-net-add 10.77.24.0/23 -g 172.23.30.1 -m 9000
Route cache flushed.
hnas-5300-sv5-2:$ vn 3 route
route: executing on cluster node 2, though the EVS in context (3) is currently on cluster node 1
Routes for EVS 3:
Destination                   Gateway                   MTU     Flags
10.77.24.0/23                 172.23.30.1               9000
```

Routing for Azure:

```
hnas-5300-sv5-2:$ vn 4 route-net-add 10.77.27.0/24 -g 172.23.30.1 -m 9000
Route cache flushed.
hnas-5300-sv5-2:$ vn 4 route
Routes for EVS 4:
Destination                    Gateway                    MTU      Flags
10.77.27.0/24                  172.23.30.1                9000
```

Routing for GCP:

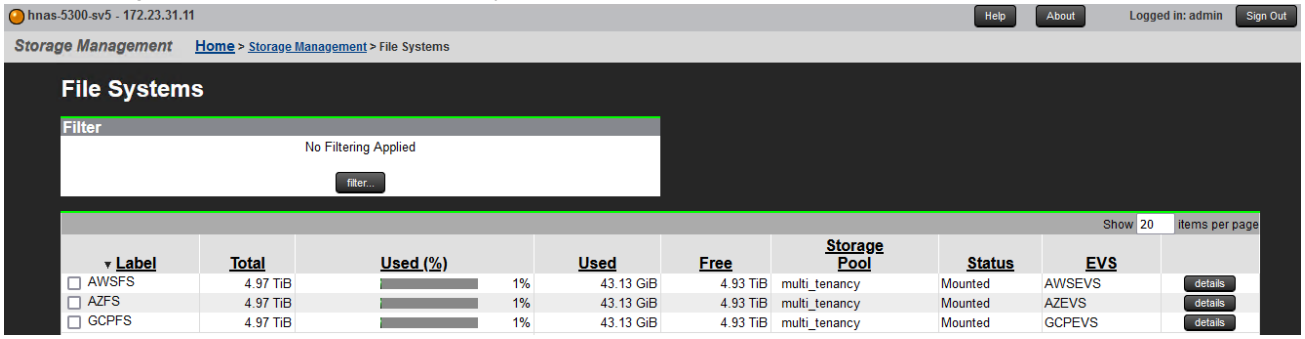
```
hnas-5300-sv5-2:$ vn 5 route-net-add 10.77.30.0/24 -g 172.23.30.1 -m 9000
Route cache flushed.
hnas-5300-sv5-2:$ vn 5 route
route: executing on cluster node 2, though the EVS in context (5) is currently on cluster node 1
Routes for EVS 5:
Destination                    Gateway                    MTU      Flags
10.77.30.0/24                  172.23.30.1                9000
```

3. Configure DNS for each EVS.

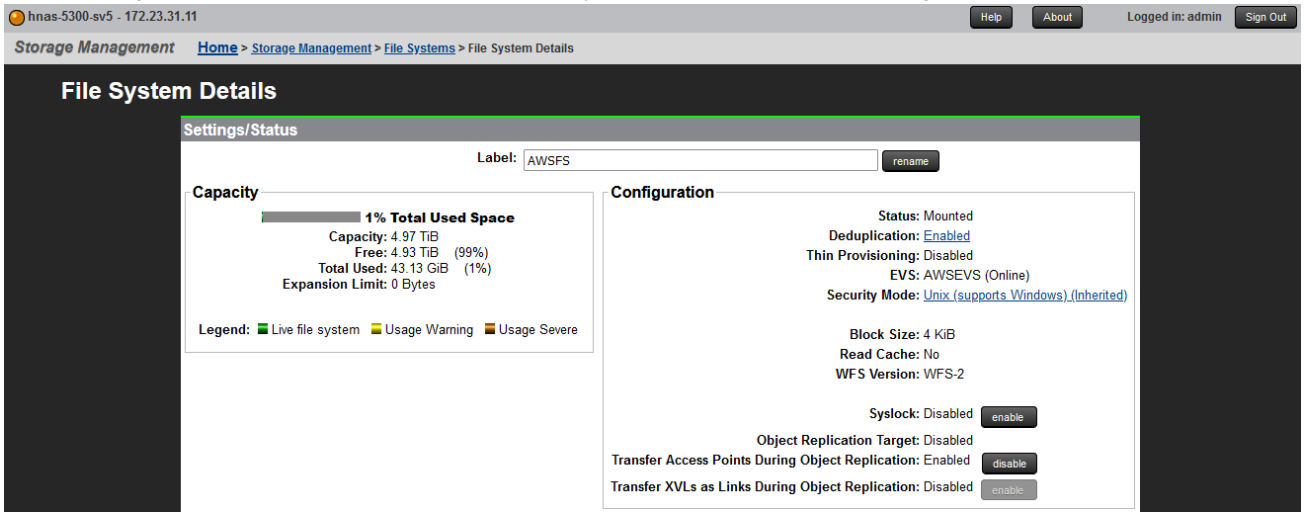
```
hnas-5300-sv5-2:$ vn 3 dnsserver add 172.23.30.70
hnas-5300-sv5-2:$ vn 3 dnsdomainname set juno.com
hnas-5300-sv5-2:$ vn 4 dnsdomainname set juno.com
hnas-5300-sv5-2:$ vn 4 dnsserver add 172.23.30.70
hnas-5300-sv5-2:$ vn 5 dnsserver add 172.23.30.70
hnas-5300-sv5-2:$ vn 5 dnsdomainname set juno.com
```

4. Create three file systems and attach them to the respective EVS.

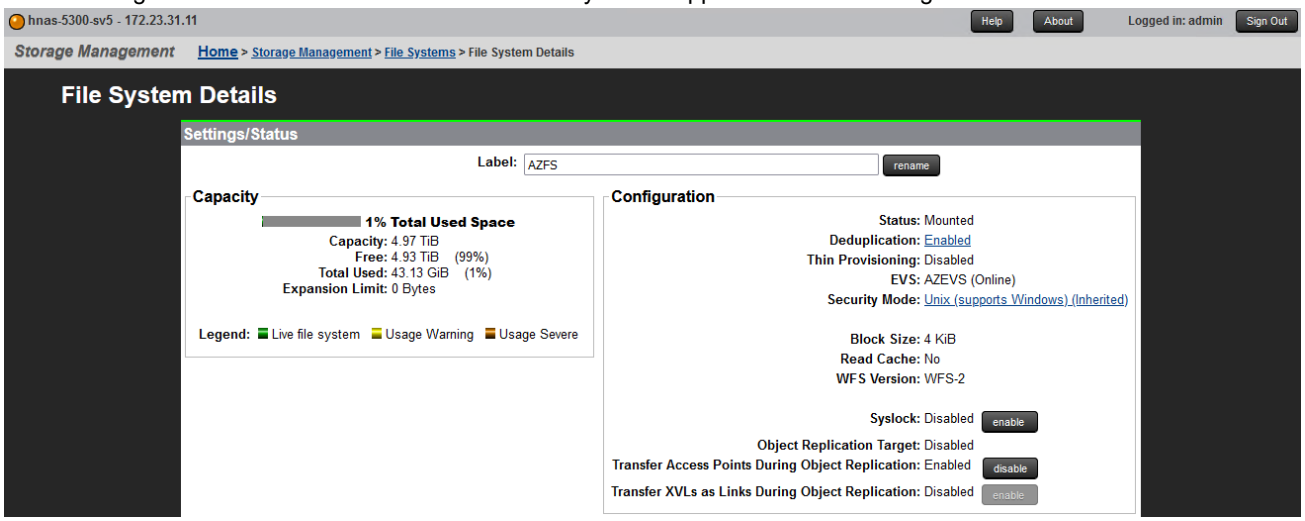
The following screenshot shows all three file systems:



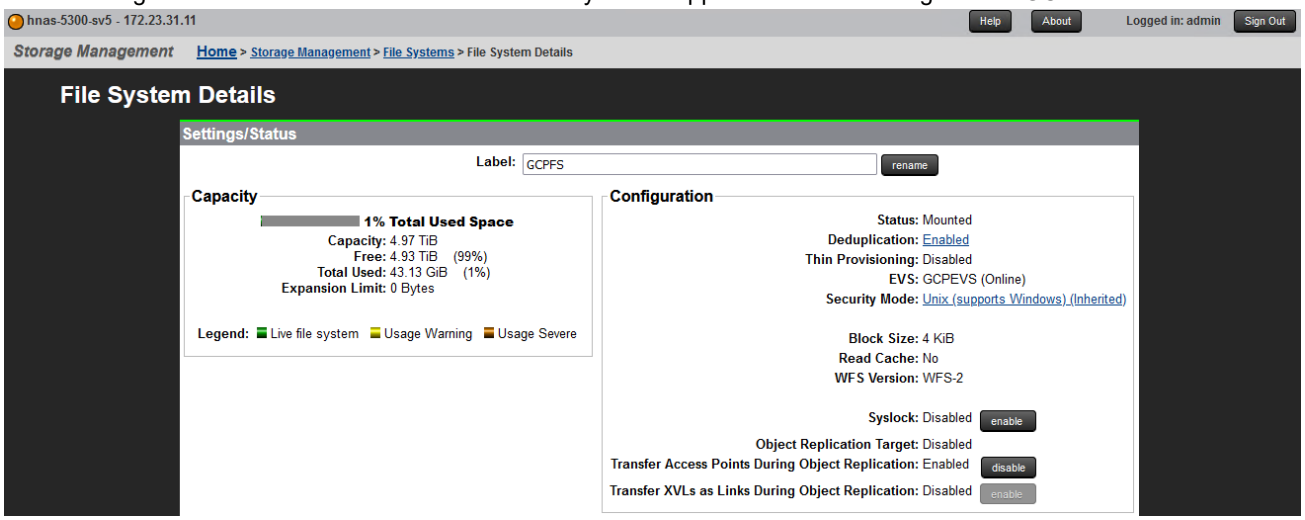
The following screenshot shows the details of the file system mapped to the EVS configured for AWS:



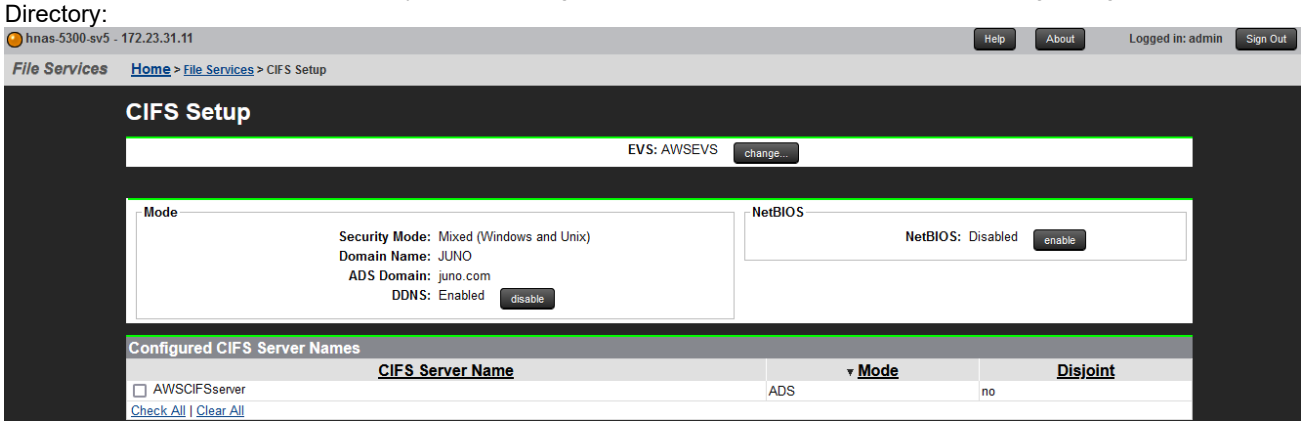
The following screenshot shows the details of the file system mapped to the EVS configured for Azure:

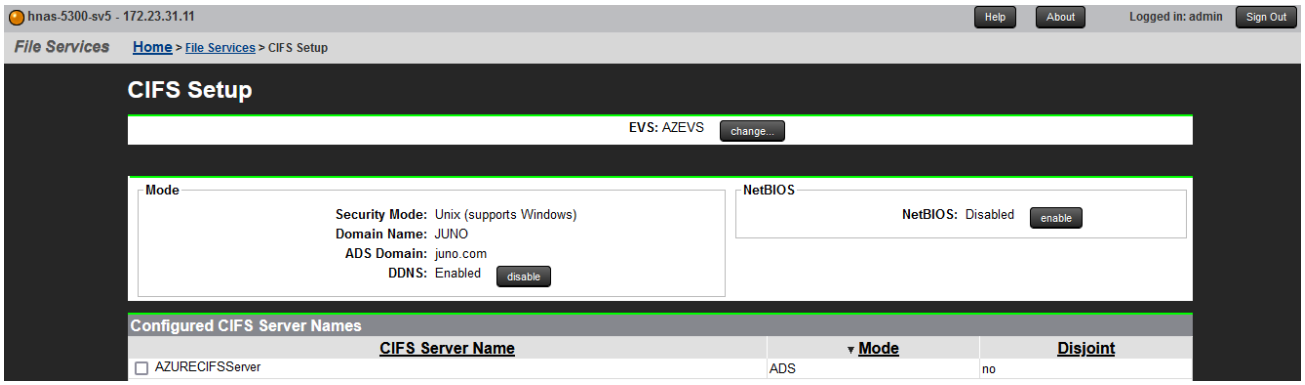


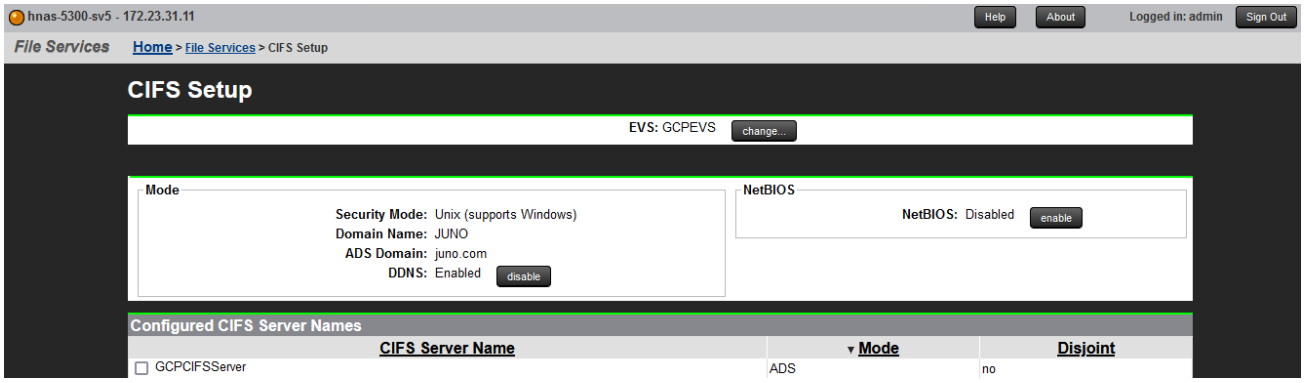
The following screenshot shows the details of the file system mapped to the EVS configured for GCP:



5. Add the three EVSs to Active Directory. The following screenshots show the three EVS after being configured in Active Directory:

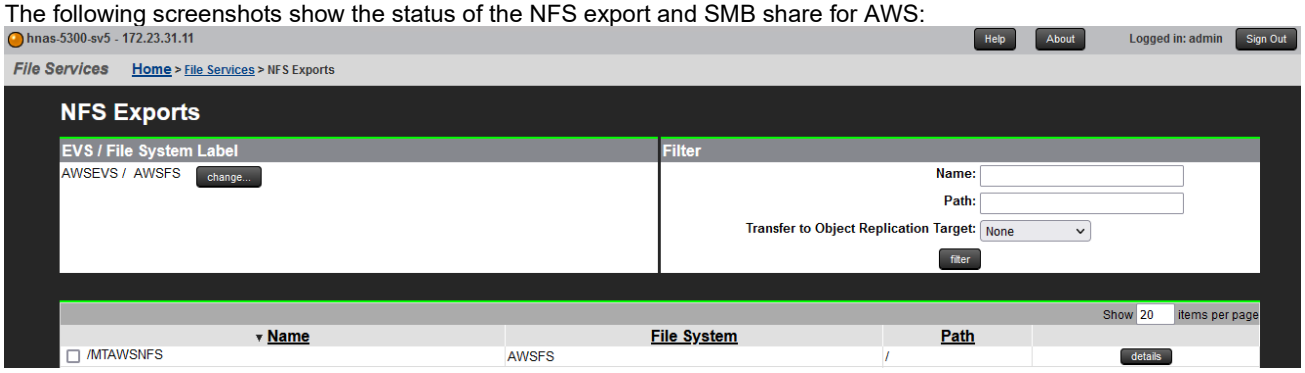


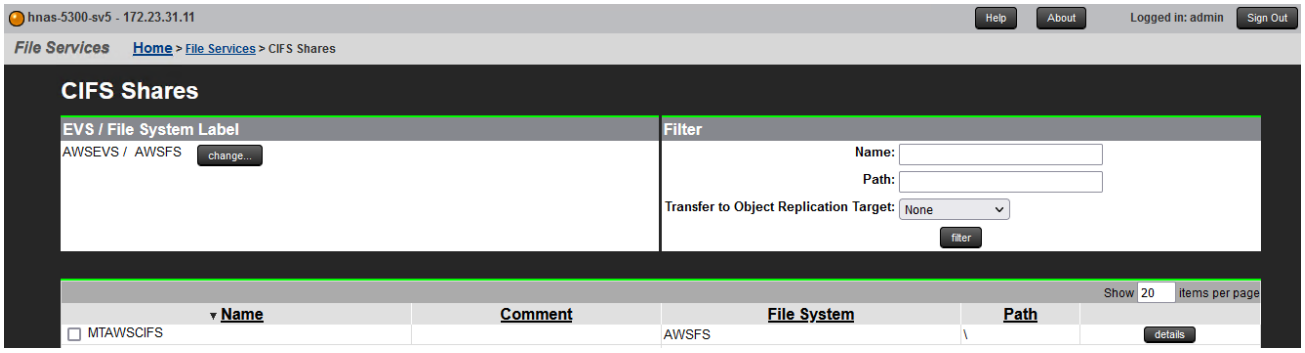




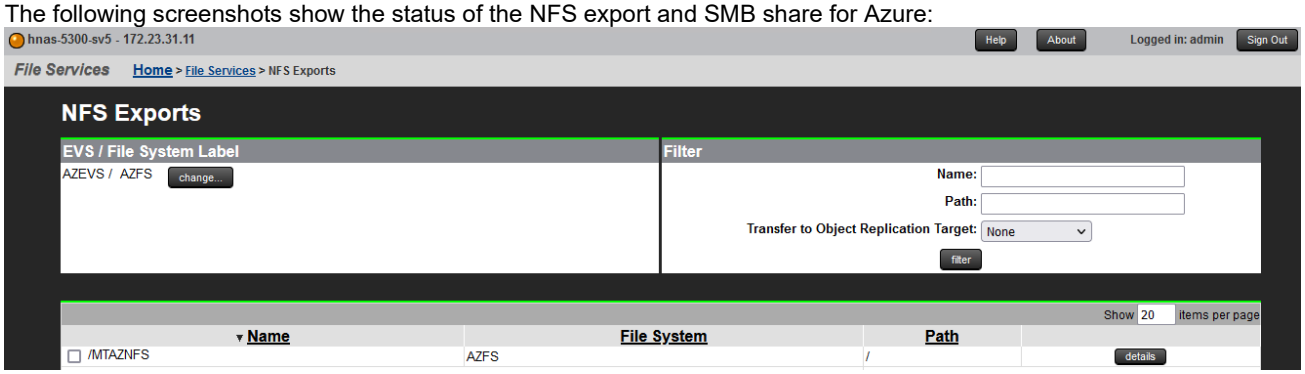
6. Configure NFS export and SMB shares in each file system to allow access from the corresponding cloud provider.

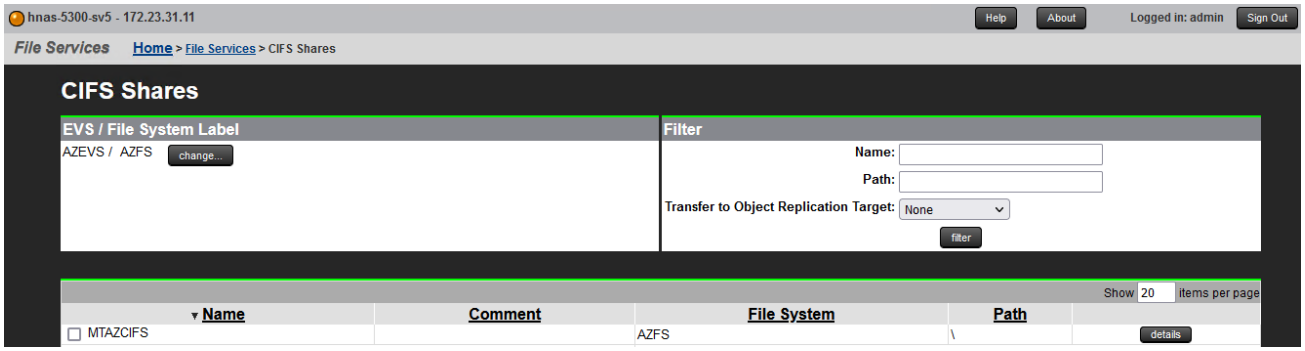
The following screenshots show the status of the NFS export and SMB share for AWS:



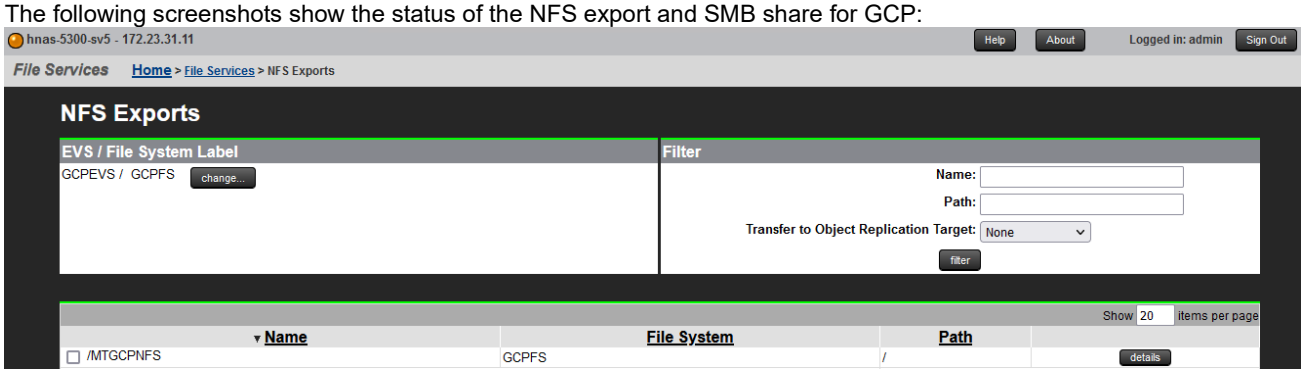


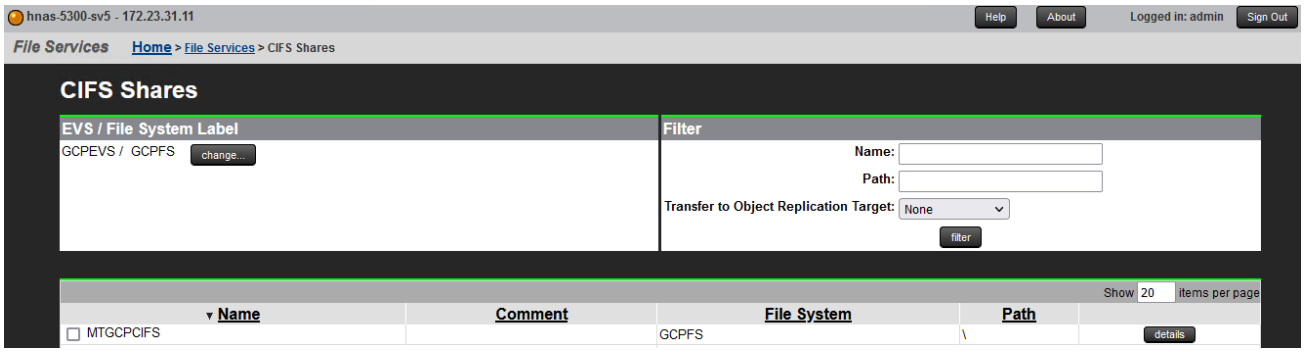
The following screenshots show the status of the NFS export and SMB share for Azure:





The following screenshots show the status of the NFS export and SMB share for GCP:





7. Access NFS exports and CIFS shares from the cloud providers.
    - Verify that the corresponding filesystem can be accessed from AWS.
    - Verify that the corresponding filesystem can be accessed from Azure.
    - Verify that the corresponding filesystem can be accessed from GCP.

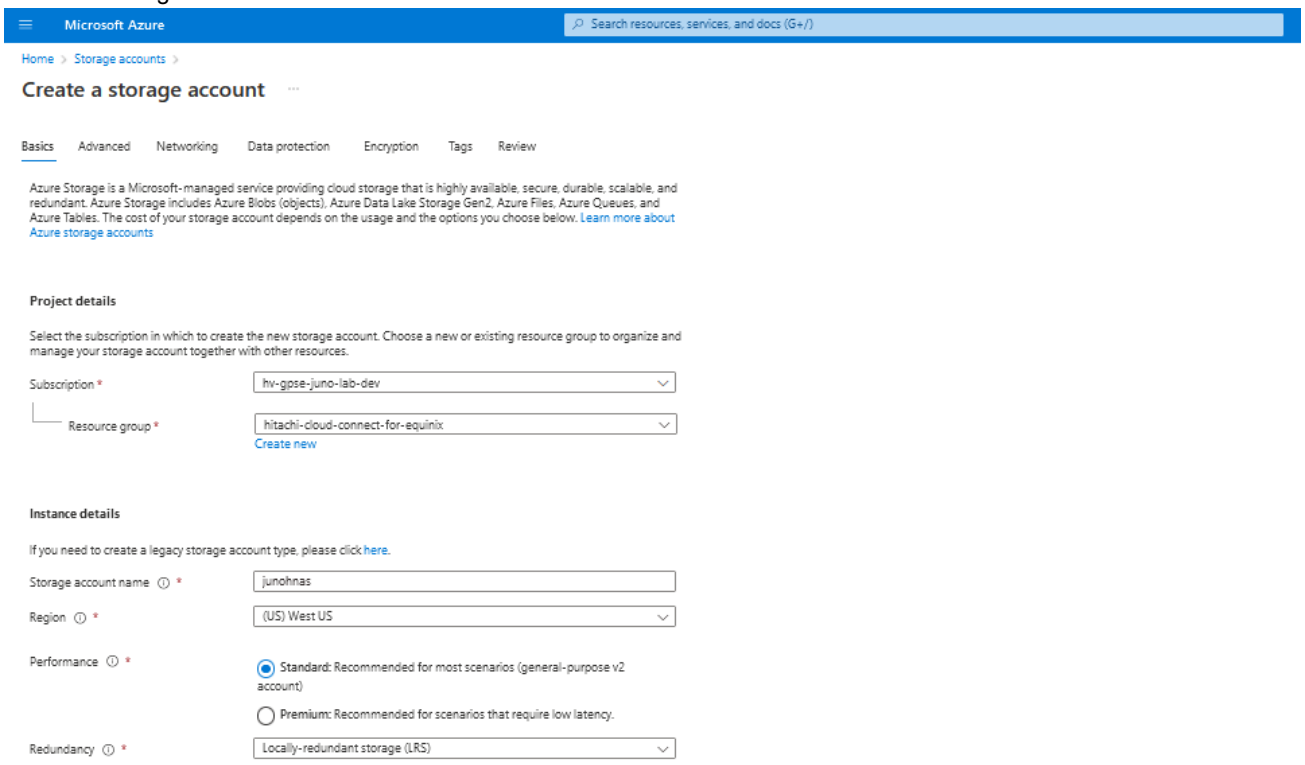
Test 3: Deploy Virtual SMU in Azure

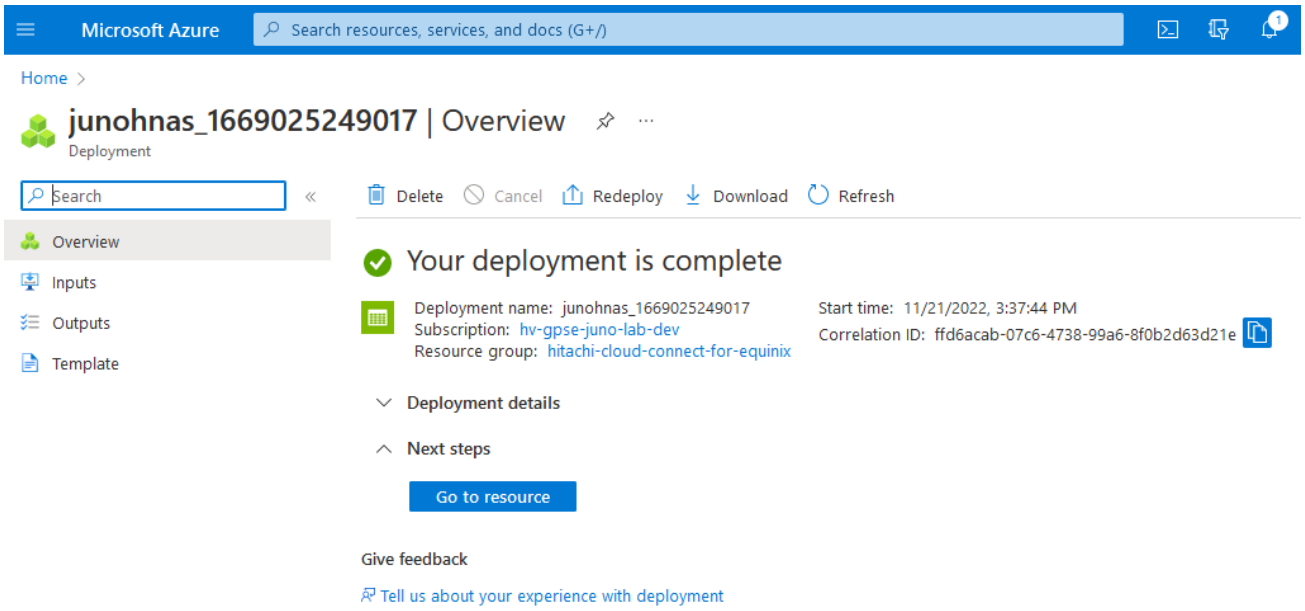
This test case describes the process of deploying a virtual SMU in Azure.

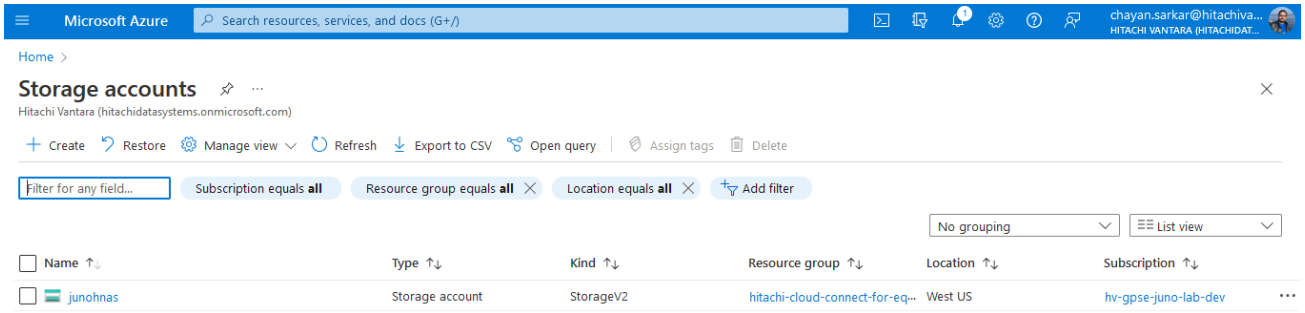
Prerequisites

- A Windows client with more than 100 GB of disk space available.
- For ease-of-work, Azure PowerShell modules can be installed in the Windows client. This helps in uploading the SMU disk image to Azure.
- Download the SMU Azure template file from Support Connect or TISC. The file is in ZIP format, so you must extract the file to upload to Azure.

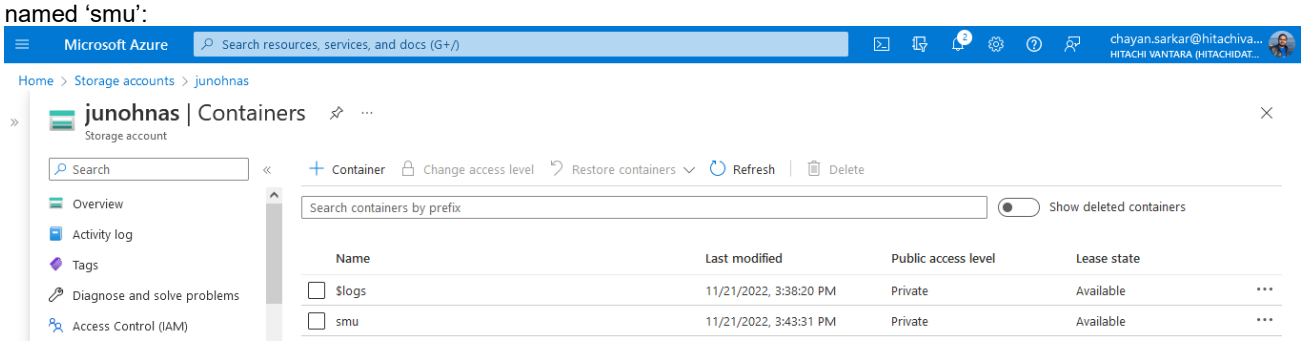
1. Create a storage account in Azure.





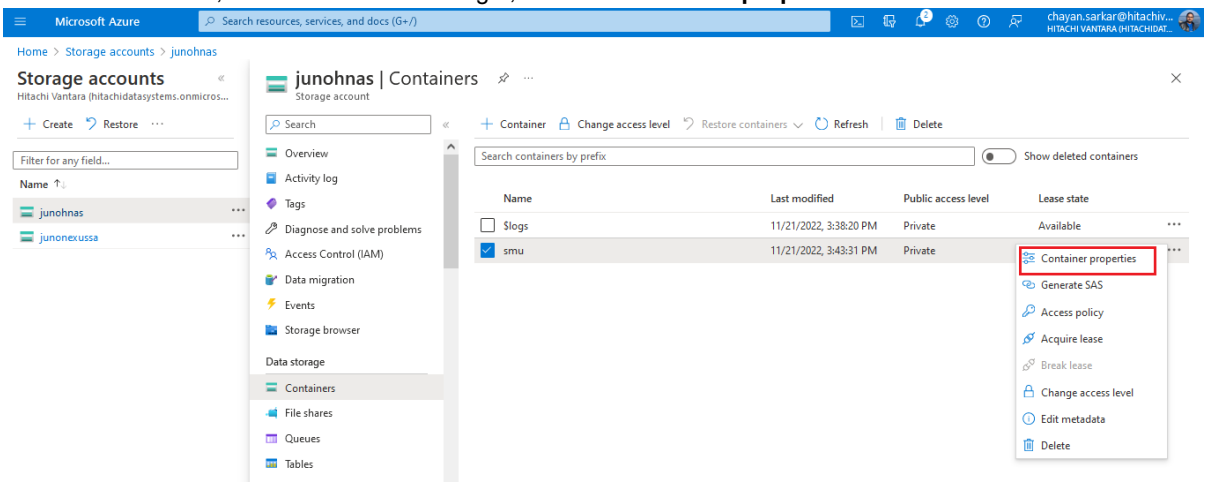


2. Create Blob service container under the new storage account. The following screenshot shows a Blob service container named ‘smu’:

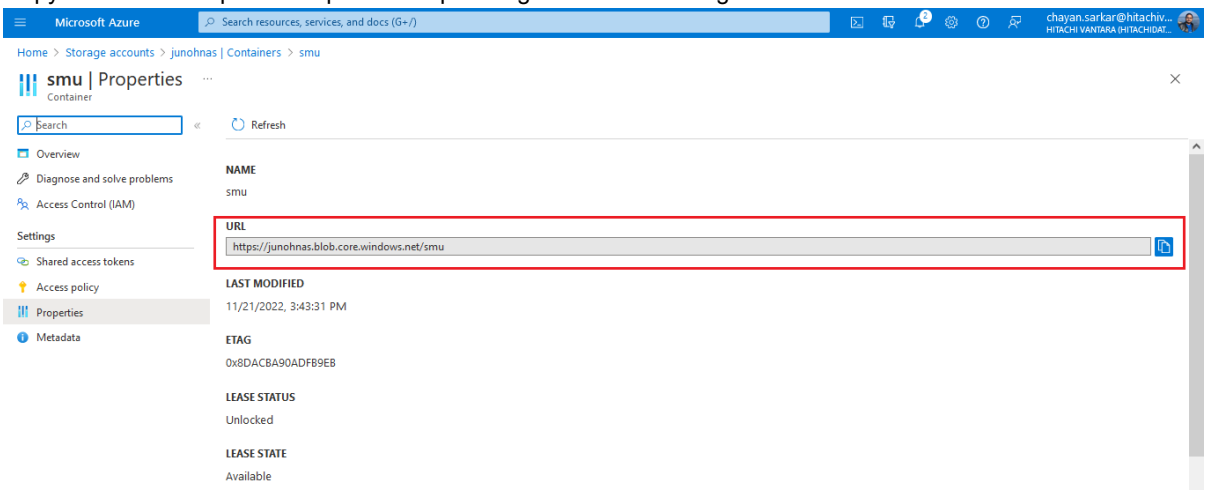


3. Upload the file to Azure.

a. Select the container, click the menu on the right, and click **Container properties**.



b. Copy the URL. This path is required for uploading the VHD file using PowerShell.



c. There are several ways to upload the VHD file to the Blob container. One of the easiest way is to use Azure PowerShell. Start by repairing the client from which the upload will take place by running the following commands:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
Install-Module -Name Az -Scope CurrentUser -Repository PSGallery -Force
```

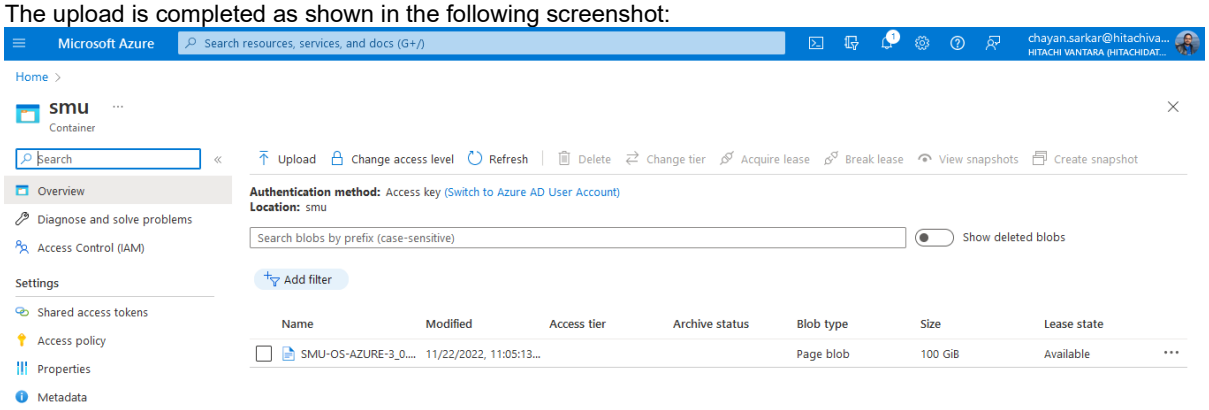
d. Log in to Azure using Azure Power Shell by running the following command. You will be prompted to log in to your Azure account. If you have several Azure subscriptions, you must change the context to the correct one and then begin the upload.

```
connect-azaccount
```

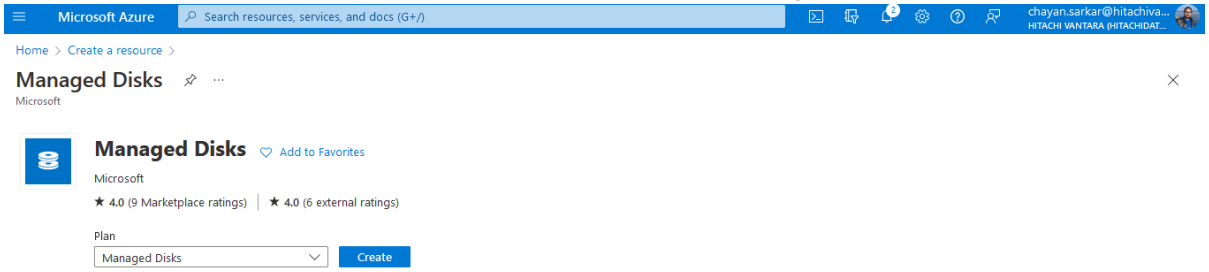
e. Start the upload by running the following command:

```
Add-AzVhd -ResourceGroupName <String> -Destination <Uri> -LocalFilePath <FileInfo>
```

The upload is completed as shown in the following screenshot:

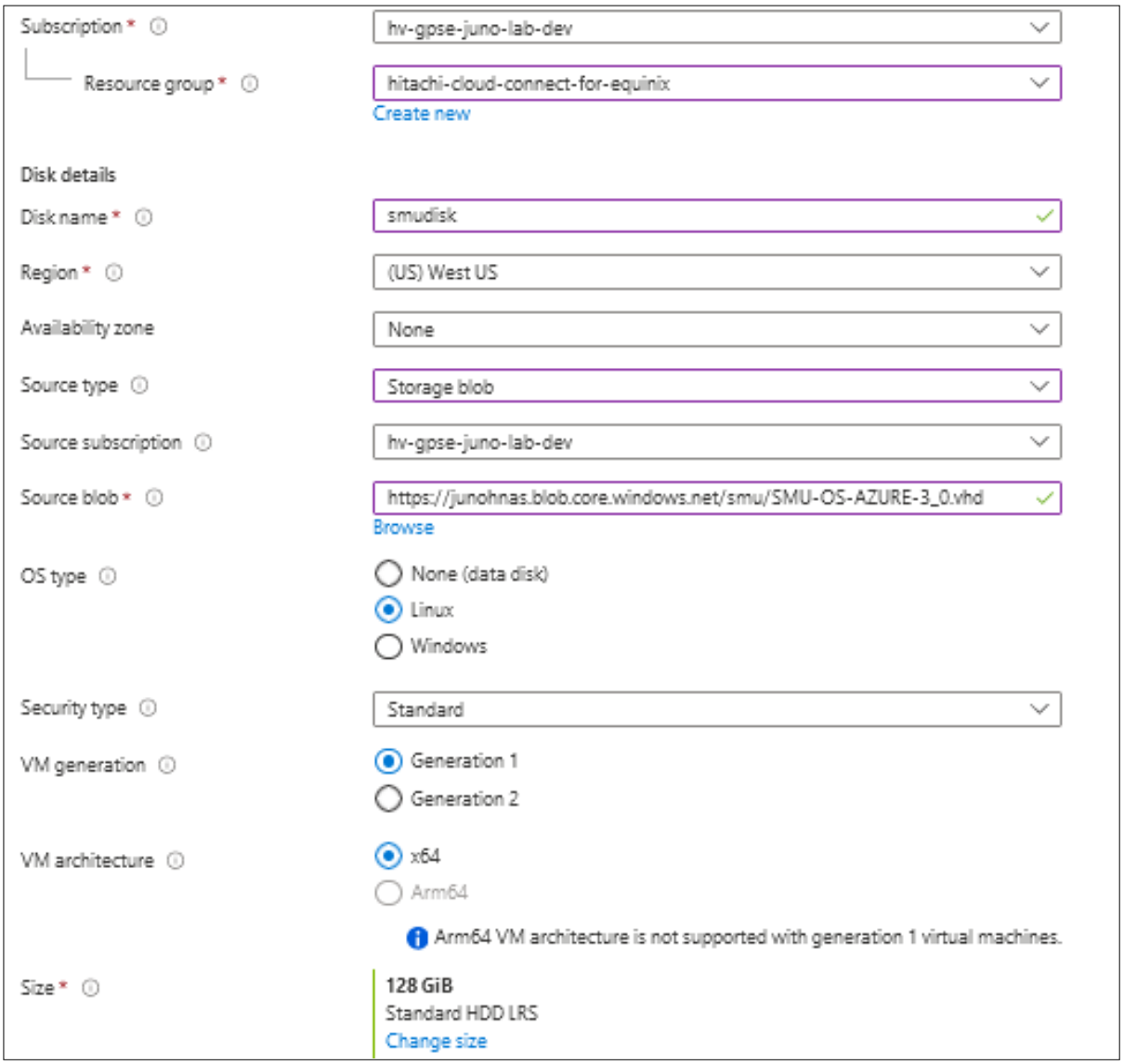


4. Create a managed disk.
   a. From the Azure main menu, click **Create a resource** and search for Managed Disks.

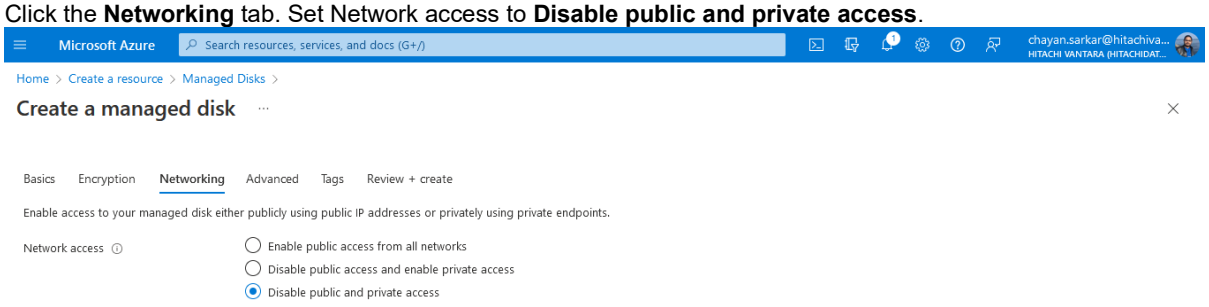


   b. Click **Create** and select the following options. See the following figure for an example of a filled out screen:
      - Source type: Storage Blob
      - Source Blob: Enter the URL which was used during the upload. You may need to browse to the location.
      - OS type: Linux
      - VM Generation: Generation 1
      - Size: Select the drive type based on the desired performance. The size must be manually set to 100 GB.

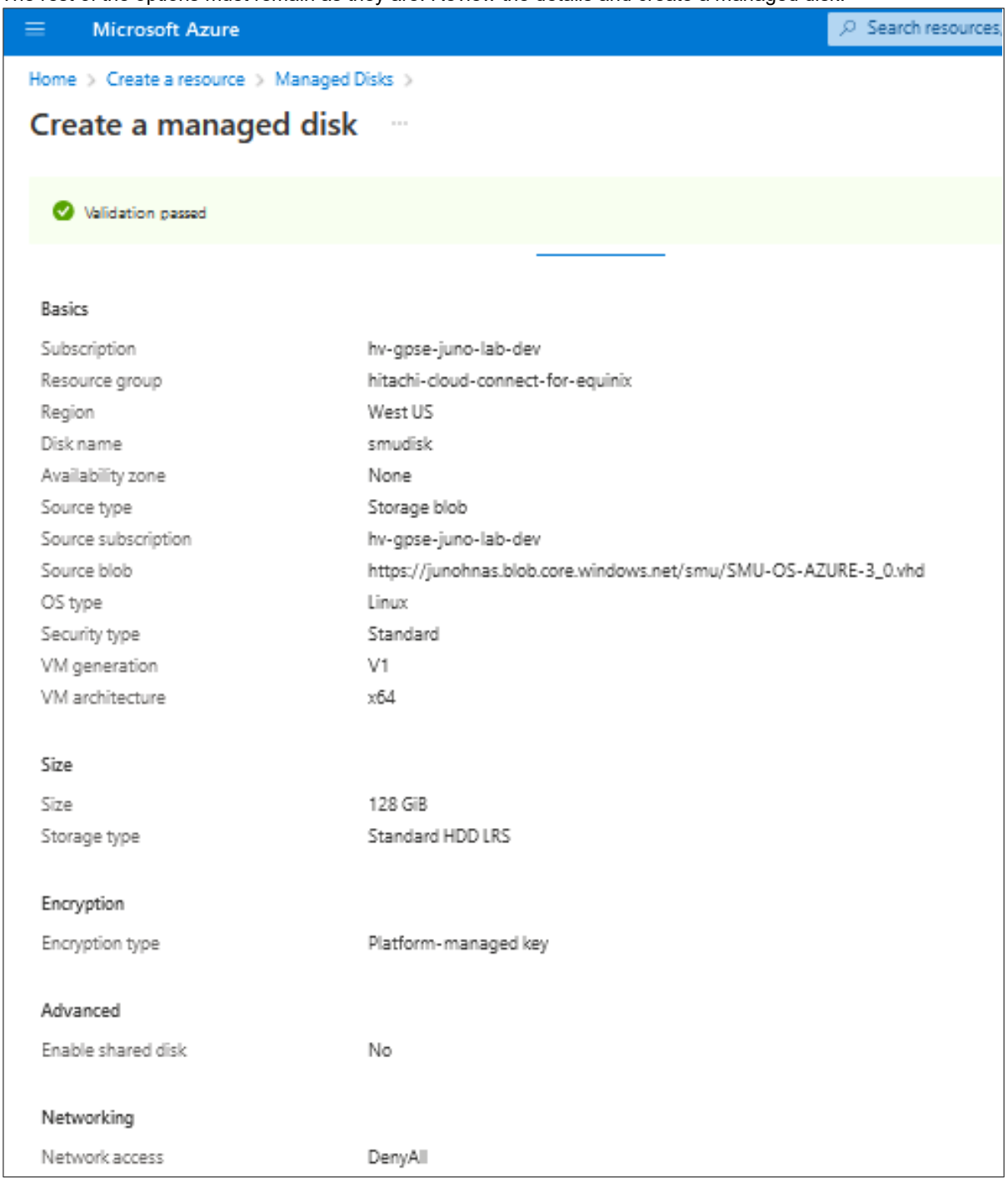
New managed disk:



c. Click the **Networking** tab. Set Network access to **Disable public and private access**.



d. The rest of the options must remain as they are. Review the details and create a managed disk.



5. After the managed disk is ready, create a virtual machine using the following options:

Basic:

- Select the newly created disk image.
- Size must be minimum 2 vCPU and 4GiB RAM.
- Availibility options: No infrastructure redundancy required
- Inbound port rules: None

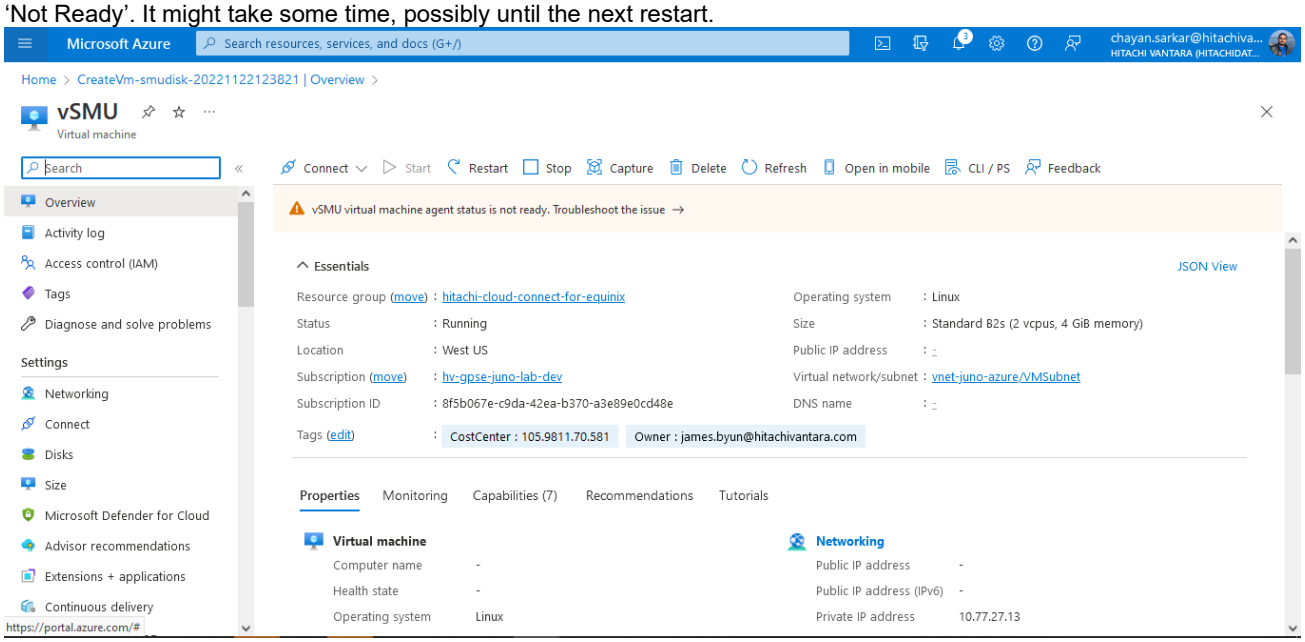
Disks:

- Delete OS disk with VM: Enabled

Networking:

- Virtual Network: <Select appropriate network>
- Public IP: None
- NIC Security Group: None
- Public inbound ports: None
- Delete NIC with VM: Enabled

After creating the virtual machine, the status must show as running. Note that sometimes, the agent status may show as 'Not Ready'. It might take some time, possibly until the next restart.

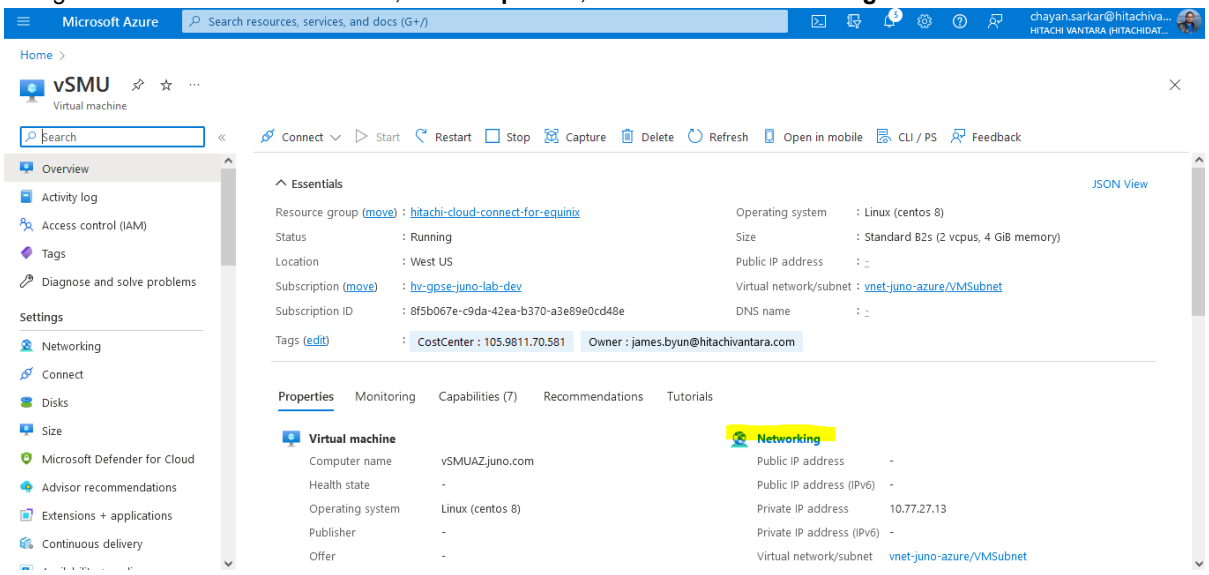


The SMU will have a dynamic IP address after the installation. A static IP address on the SMU is required for the following reasons:

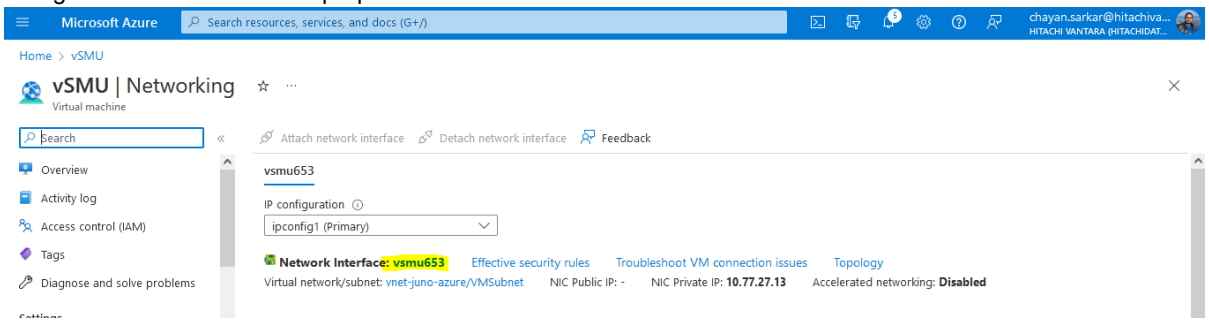
- SMU acting as a quorum for HNAS cluster
- Deploying Hitachi Disaster Recovery Solution

6. To reserve an IP address in Azure, complete the following steps.

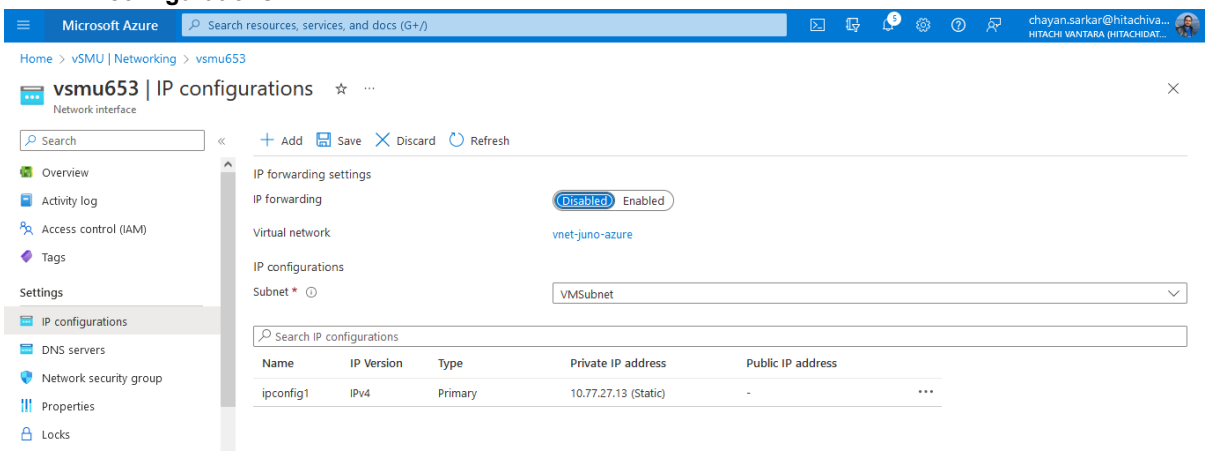
a. Navigate to the SMU virtual machine, click **Properties**, and then click **Networking**.



b. Navigate to network interface properties.



c. Select **IP configurations** on the left.



d. Click the IP address and change the assignment from **Dynamic** to **Static**. Additionally, you can change the IP address. However, in case of a new IP address, ensure that it is in the same IP network.

7. Install the SMU software on the virtual machine.
   a. Copy the SMU software ISO image to the virtual machine using SCP with the ‘smuinstall’ username. After copying, the image will be under `/home/smuinstall` directory.
   b. SSH to the virtual machine using the new static IP address.

c. Log in as a root user. Mount the ISO file using the following commands:
```
mkdir /media/iso
mount -o loop /home/smuinstall/<iso file> /media/iso
```
d. Initiate the installation. This restarts the virtual machine.

```
/media/iso/autorun
```

e. After restarting, log in to the virtual machine as a root user.
f. Configure the SMU software network settings by running the following command:

```
smu-config
```

g. When prompted, enter the static IP address, hostname, and domain. After this is completed, the SMU restarts.
h. Log in to the SMU UI by opening a web browser and pointing it to the SMU static IP address.
i. When prompted to run the ‘SMU Initial Setup Wizard’, select run and set the password for the user accounts.
j. Disable ‘smuinstall’ user.
k. Add the HNAS nodes to the SMU.