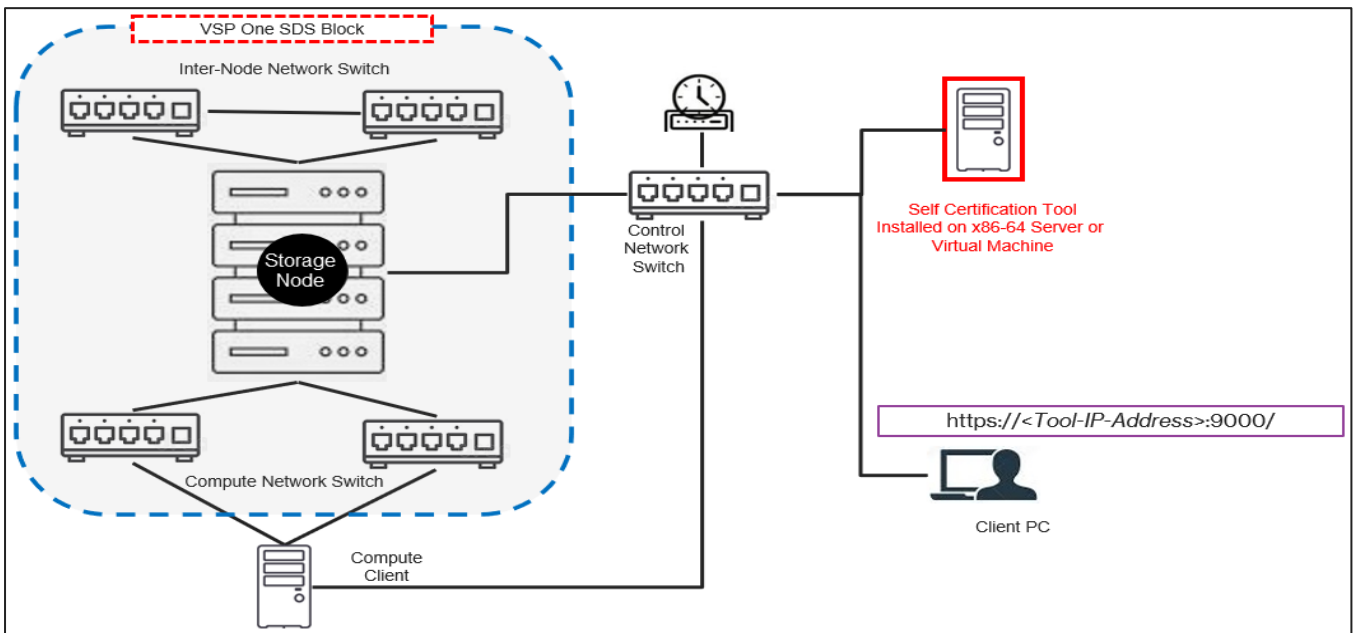


Self Certification Tool: Validate, Configure, and Certify Third-Party Infrastructure for VSP One SDS Block

Use the Hitachi Self Certification tool to certify vendor-agnostic infrastructure that enables the building of a virtual storage system, providing high-performance, high-capacity block storage as part of Hitachi Virtual Storage Platform One Software-Defined Storage Block (VSP One SDS Block) hybrid cloud data platform.

Get started with these high-level steps to validate, configure, and certify third-party infrastructure for VSP One SDS Block.



Step 1: Complete the prerequisites

1. Obtain the Minimum Self Certification Requirement form from a Hitachi Vantara representative. This form will verify that all hardware components, including switches, servers, disks, and network interface cards (NICs), meet the minimum requirements for VSP One SDS Block compatibility.

The following table lists the minimum supported hardware components for SDS nodes:

Component	Description
Server	SLES 15 Certified Server model
CPU	Intel Xeon 2 nd -5 th Gen
Memory	Minimum 256GiB, any vendor
Ethernet Adapter	SLES15 SP5 inbox driver-supported drivers
Fibre Channel Adapter	Host bus adapter (HBA) built on Q-Logic chipset
Disk Controller	SLES15 SP5 inbox driver-supported controllers
System/User Data Drives	Any vendor
Internode/Compute Switches	Any vendor

2. Make sure that the VSP One SDS Block cluster, composed of multiple storage nodes and switches as depicted in the diagram, is freshly installed with no users or pools created.
3. Complete the form and submit it to a Hitachi Vantara representative. Once verified, you will receive an email with a link to download the self certification ISO file, associated installation documents, and a Unique Certification ID.

Step 2: Configure compute client

Set up your compute client for operating system, network, date and time, and Fibre Channel (FC) zoning.

Configure compute client for FC

1. Install Red Hat Enterprise Linux 8.4, 8.5, or 9.3 (x86 or x64) using the default settings on a local hard disk.
2. Select US English (`en_US.UTF-8`) as the language.
3. Configure the compute client with an IPv4 address and set up the root user password for SSH and Self Certification tool access.

Note the compute client IPv4 address and root user credentials.

4. Log in to the compute client and retrieve the FC HBA WWN information.

```
cat /sys/class/fc_host/host<number>/port_name
```

Example:

```
cat /sys/class/fc_host/host1/port_name
0x21000024ff86a661
```

```
cat /sys/class/fc_host/host2/port_name
0x21000024ff86a660
```

The FC HBA port_name/wwn values are: "21000024ff86a661" and "21000024ff86a660".

5. Set the compute client date and time to UTC and synchronize with an NTP server.
6. Verify that the packages are installed:
 - `dnf search device-mapper-multipath`
 - `yum search device-mapper-multipath`
7. Configure yum with a local repository or subscribe to the OS vendor repository to install any missing software.
8. Download the latest Vdbench tool from [Vdbench Downloads](#) and copy the package to the root directory.
9. Configure switch zoning using the FC HBA port_name/wwn and compute port_name/wwn.

Configure compute client for iSCSI

1. Install Red Hat Enterprise Linux 8.4, 8.5, or 9.3 (x86 or x64) using the default settings on a local hard disk.
2. Select US English (`en_US.UTF-8`) as the language.
3. Configure the compute client with an IPv4 address and set up the root user password.

Note the compute client IPv4 address and root user credentials.

4. Log in to the compute client and assign IPv4 addresses to the Ethernet/NIC adapter.
5. Verify connectivity between the compute client and storage node compute ports.
6. Retrieve the iSCSI initiator name from the compute client.

```
cat /etc/iscsi/initiatorname.iscsi
```

7. Set the compute client date and time to UTC and synchronize with an NTP server.
8. Verify that the packages are installed:
 - `dnf search device-mapper-multipath`
 - `yum search device-mapper-multipath`
9. Configure yum with a local repository or subscribe to the OS vendor repository to install any missing software.
10. Download the latest Vdbench tool from [Vdbench Downloads](#) and copy the package to the root directory.

Configure compute client for NVMe/TCP

1. Install Red Hat Enterprise Linux 9.3 (x86 or x64) using the default settings on a local hard disk.
2. Select US English (`en_US.UTF-8`) as the language.
3. Configure the compute client with an IPv4 address and set up the root user password.

Note the compute client IPv4 address and root user credentials.

4. Log in to the compute client and assign IPv4 addresses to the Ethernet/NIC adapter.
5. Verify connectivity between the compute client and storage node compute ports.
6. Retrieve the host NQN name from the compute client.

```
cat /etc/nvme/hostnqn
```

7. Set the compute client date and time to UTC and synchronize with an NTP server.
8. Verify that the packages are installed:
 - `dnf search nvme-cli`
 - `yum search nvme-cli`
9. Configure yum with a local repository or subscribe to the OS vendor repository to install any missing software.
10. Download the latest Vdbench tool from [Vdbench Download](#) and copy the package to the root directory.

Step 3: Install the tool

The tool is provided as an ISO image with the Debian operating system. It can be installed on either a bare metal server or a virtual machine (VM).

Install on a bare metal server

The following procedure uses the Dell BMC utility as an example. BMC utilities may vary depending on the bare metal server. If a different vendor BMC utility is used, refer to the vendor documentation for specific instructions.

1. Download and save the self certification ISO file to a local machine.
2. Connect to the bare metal server through the BMC console.
3. Open the server management console and launch the virtual console.

Dashboard			System			Storage			Configuration			Maintenance			iDRAC Settings		
License												<input checked="" type="checkbox"/> Enterprise Edit					
Recent Logs view all																	
Severity	Description	Date and Time															
<input checked="" type="checkbox"/>	The chassis is closed while the power is off.	Wed 16 Mar 2022 05:59:29															
<input checked="" type="checkbox"/>	The chassis is open while the power is off.	Wed 16 Mar 2022 05:59:24															
<input checked="" type="checkbox"/>	The chassis is closed while the power is off.	Tue 01 Mar 2022 15:27:49															
<input checked="" type="checkbox"/>	The chassis is open while the power is off.	Tue 01 Mar 2022 15:27:45															
<input checked="" type="checkbox"/>	The chassis is closed while the power is off.	Thu 10 Dec 2020 01:16:08															
<input checked="" type="checkbox"/>	The chassis is open while the power is off.	Thu 10 Dec 2020 01:16:02															
<input checked="" type="checkbox"/>	The chassis is closed while the power is off.	Tue 11 Aug 2020 08:00:57															
<input checked="" type="checkbox"/>	The chassis is open while the power is off.	Tue 11 Aug 2020 08:00:52															
<input checked="" type="checkbox"/>	The chassis is closed while the power is off.	Mon 10 Aug 2020 06:28:45															
<input checked="" type="checkbox"/>	The chassis is open while the power is off.	Mon 10 Aug 2020 06:28:40															

4. Use Connect Virtual Media to mount the ISO image.

Virtual Media

Virtual Media is connected [Disconnect Virtual Media](#)

Map CD/DVD

Image File [Map Device](#)

Read Only

Map Removable Disk

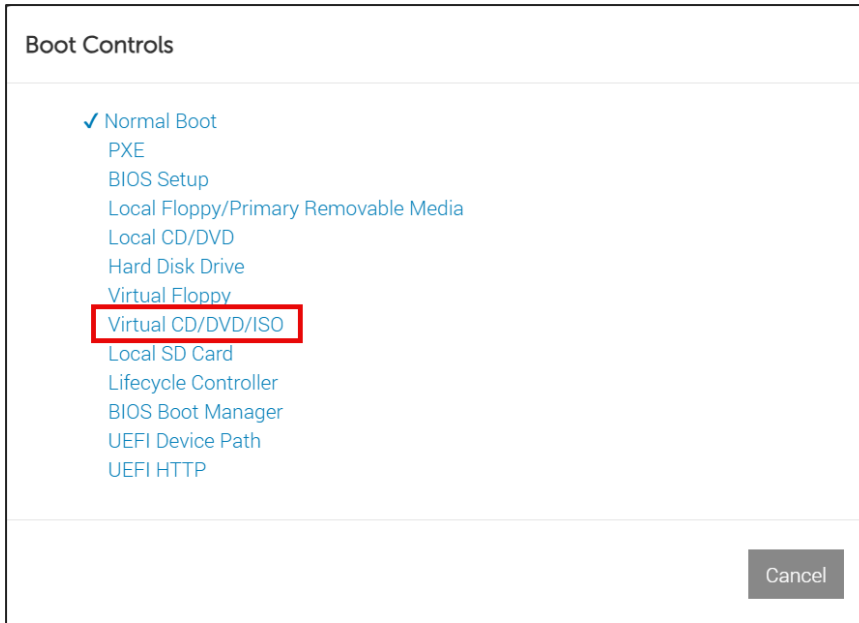
Image File [Map Device](#)

Read Only

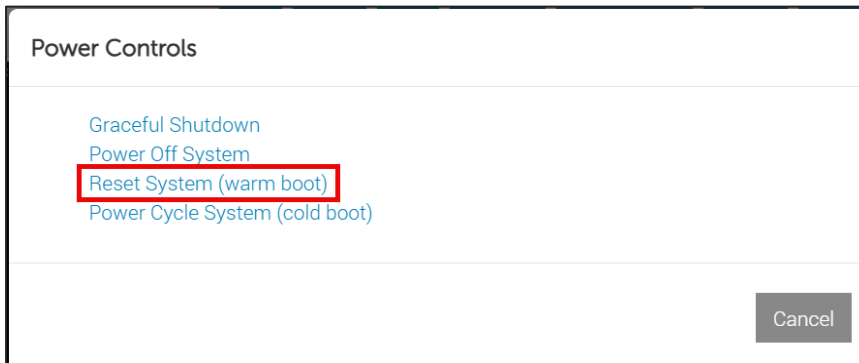
Resets the USB State for redetection. [Reset USB](#)

[Close](#)

5. Set the BIOS boot sequence to prioritize the Virtual CD/DVD/ISO.

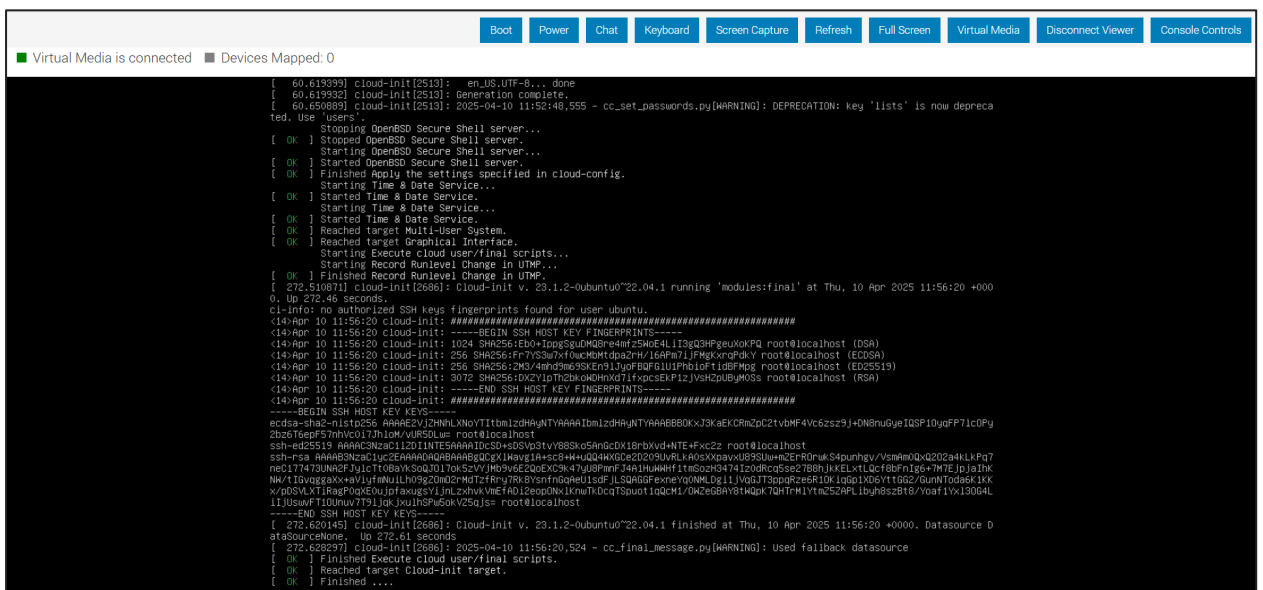


6. Restart the server.

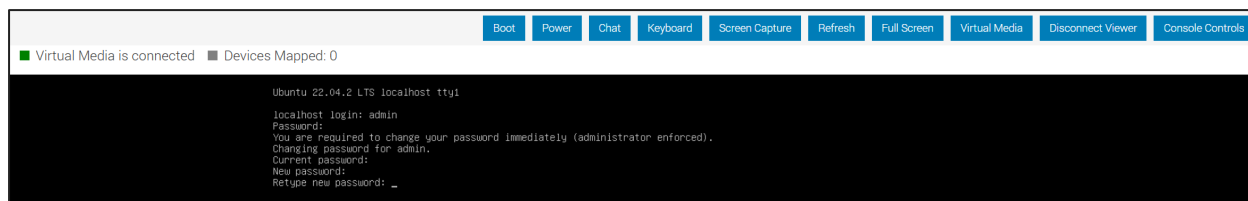


The system loads the ISO image, presents “Auto Install Self Certification Application,” and initiates installation automatically.

7. Press **Enter** after installation to access the login prompt.



8. If the virtual drive fails to automatically unmount the ISO image file, manually unmount it and proceed with restarting the server.
9. Use the tool virtual console to log in with the username "admin" and the default password "selfCertif1c@ti0n".
10. When prompted, create a new password that is at least 14 characters long and includes at least one digit, one uppercase letter, one lowercase letter, and one special character.



```

Virtual Media is connected  Devices Mapped: 0

Ubuntu 22.04.2 LTS localhost tty1
localhost login: admin
Password:
You are required to change your password immediately (administrator enforced).
Changing password for admin.
Current password:
New password:
Retype new password:

```

11. Configure the network: assign IP address, CIDR, gateway IP, NTP server, and optionally nameserver:

```

aip <IP/CIDR -- Mandatory> <Gateway -- Mandatory> <NTP server IP -- Mandatory>
<Nameserver -- Optional>

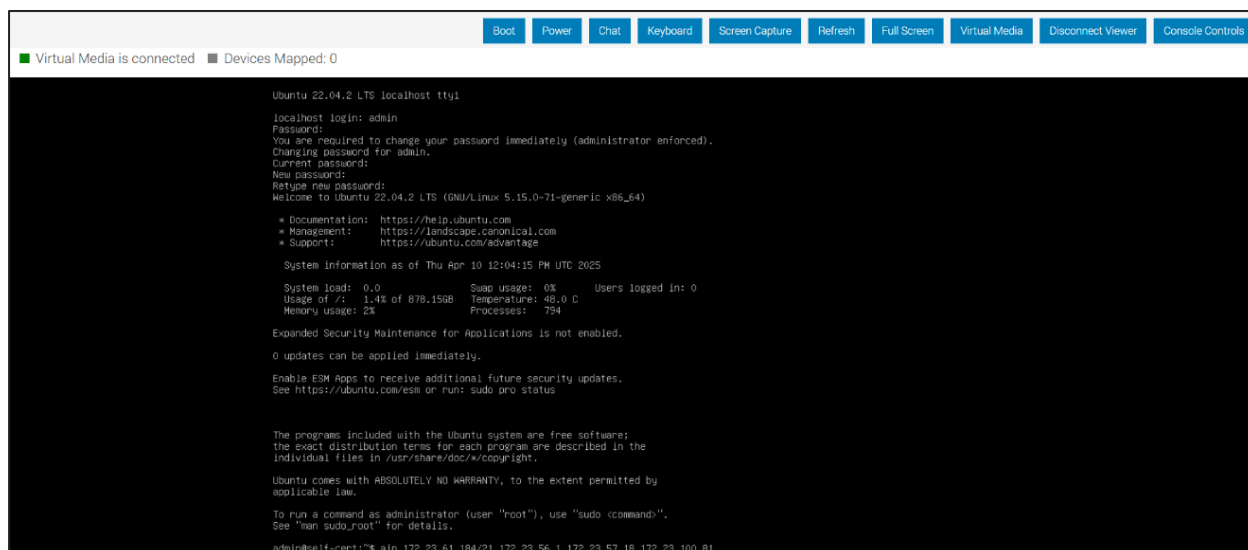
```

Example:

```

aip "172.23.61.184/21" "172.23.56.1" "172.23.57.18" "172.23.100.81"

```



```

Virtual Media is connected  Devices Mapped: 0

Ubuntu 22.04.2 LTS localhost tty1
localhost login: admin
Password:
You are required to change your password immediately (administrator enforced).
Changing password for admin.
Current password:
New password:
Retype new password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-71-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Apr 10 12:04:15 PM UTC 2025

System load: 0.0          Swap usage: 0%          Users logged in: 0
Usage of /:   1.4% of 878.15GB      Temperature: 48.0 C
Memory usage: 2%          Processes: 794

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

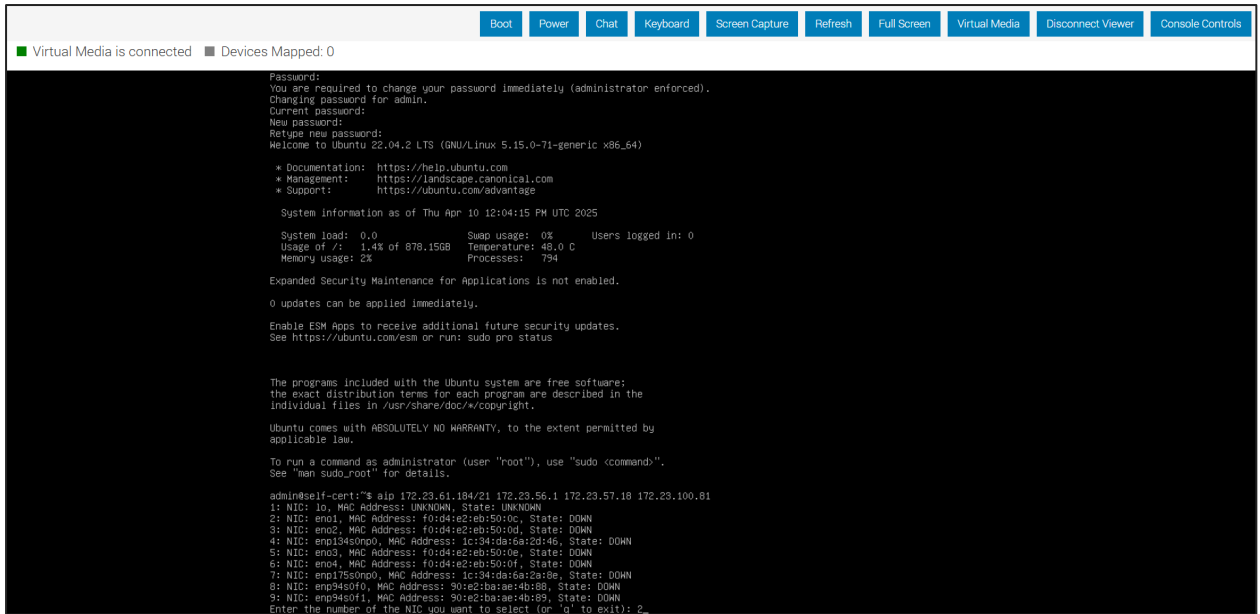
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

adminself-cert:~$ aip 172.23.61.184/21 172.23.56.1 172.23.57.18 172.23.100.81

```

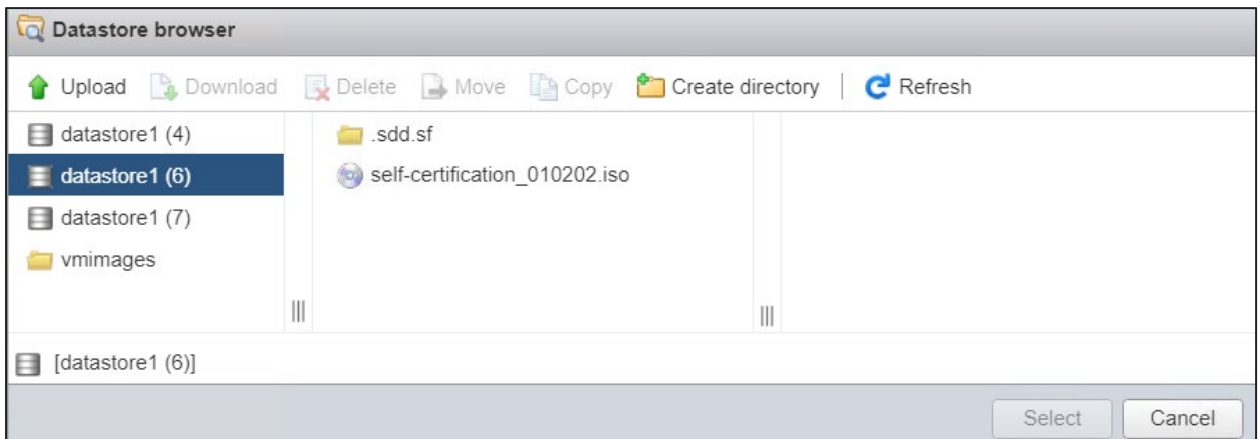
12. Select the NIC with the correct MAC address.



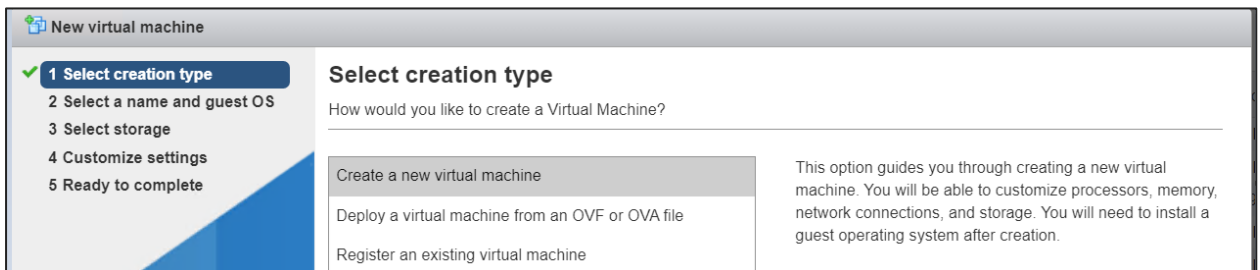
The server hosting the tool will reboot automatically.

Install on a VM

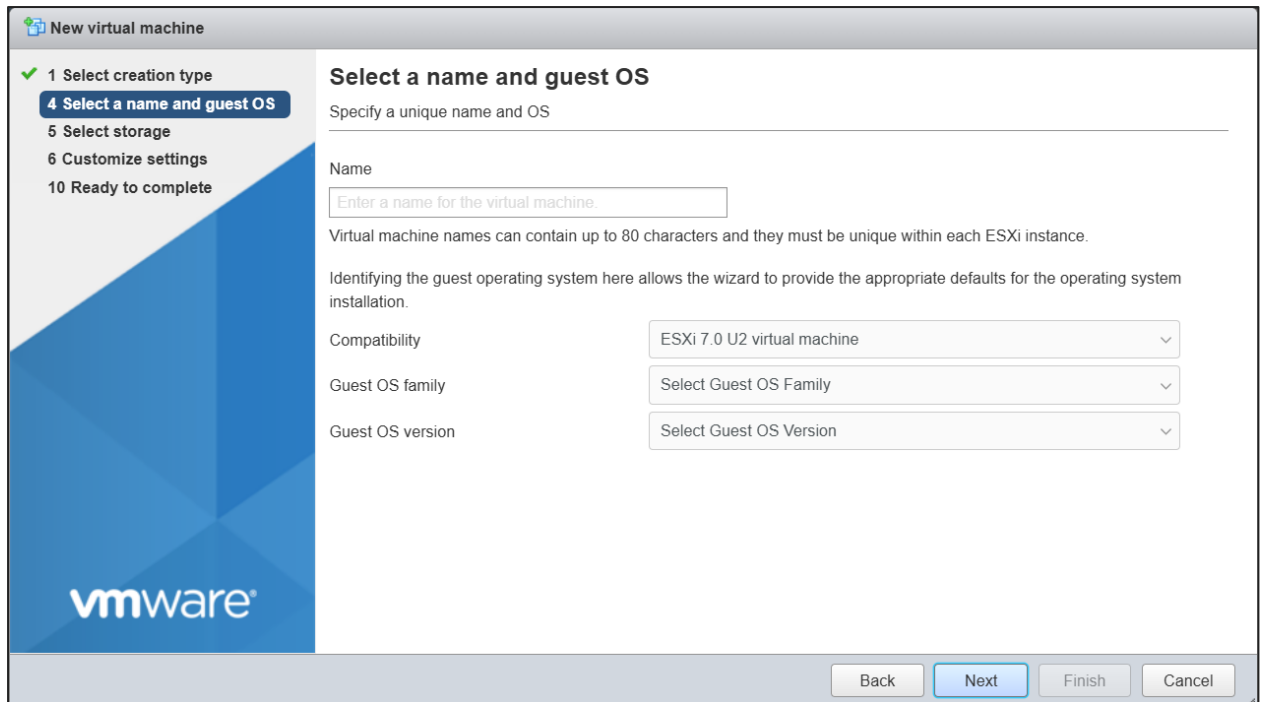
1. Log in to the VMware ESXi host.
2. Upload or copy the self certification ISO file to the VMware datastore.



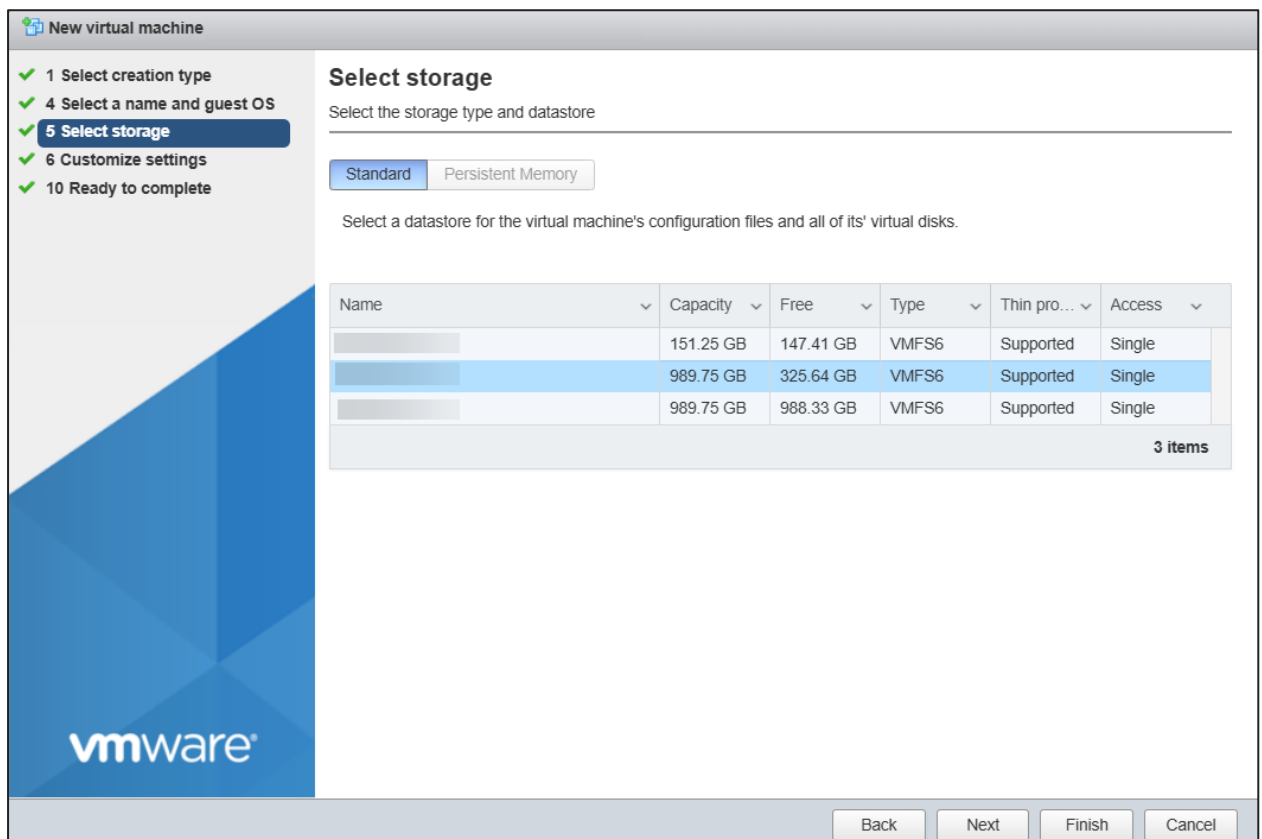
3. Select **Create a new virtual machine** to set up a new VM.



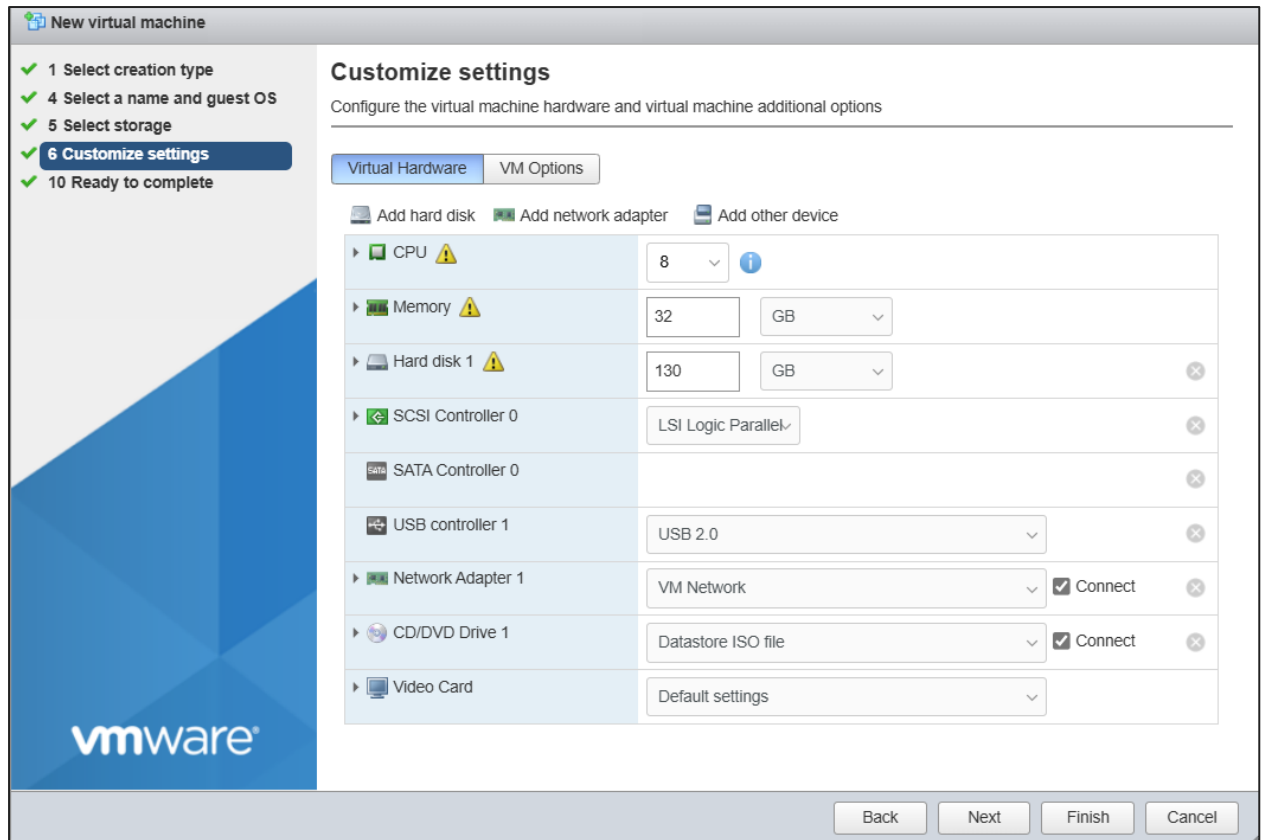
4. Enter the VM name and select **Compatibility, Guest OS family and version**, then click **Next**.



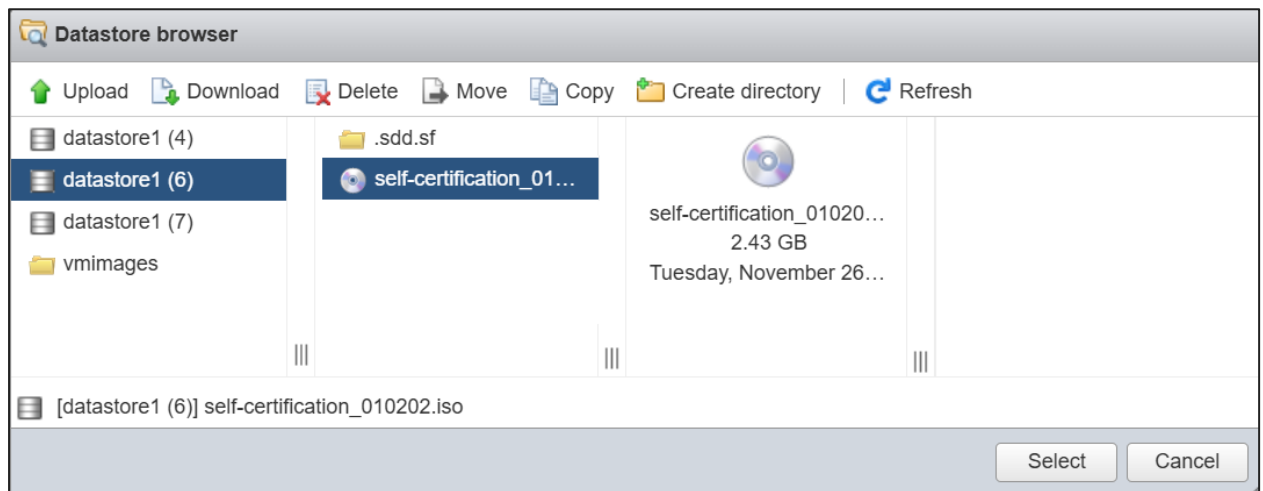
5. Select a datastore with at least 130 GB of free space and click **Next**.



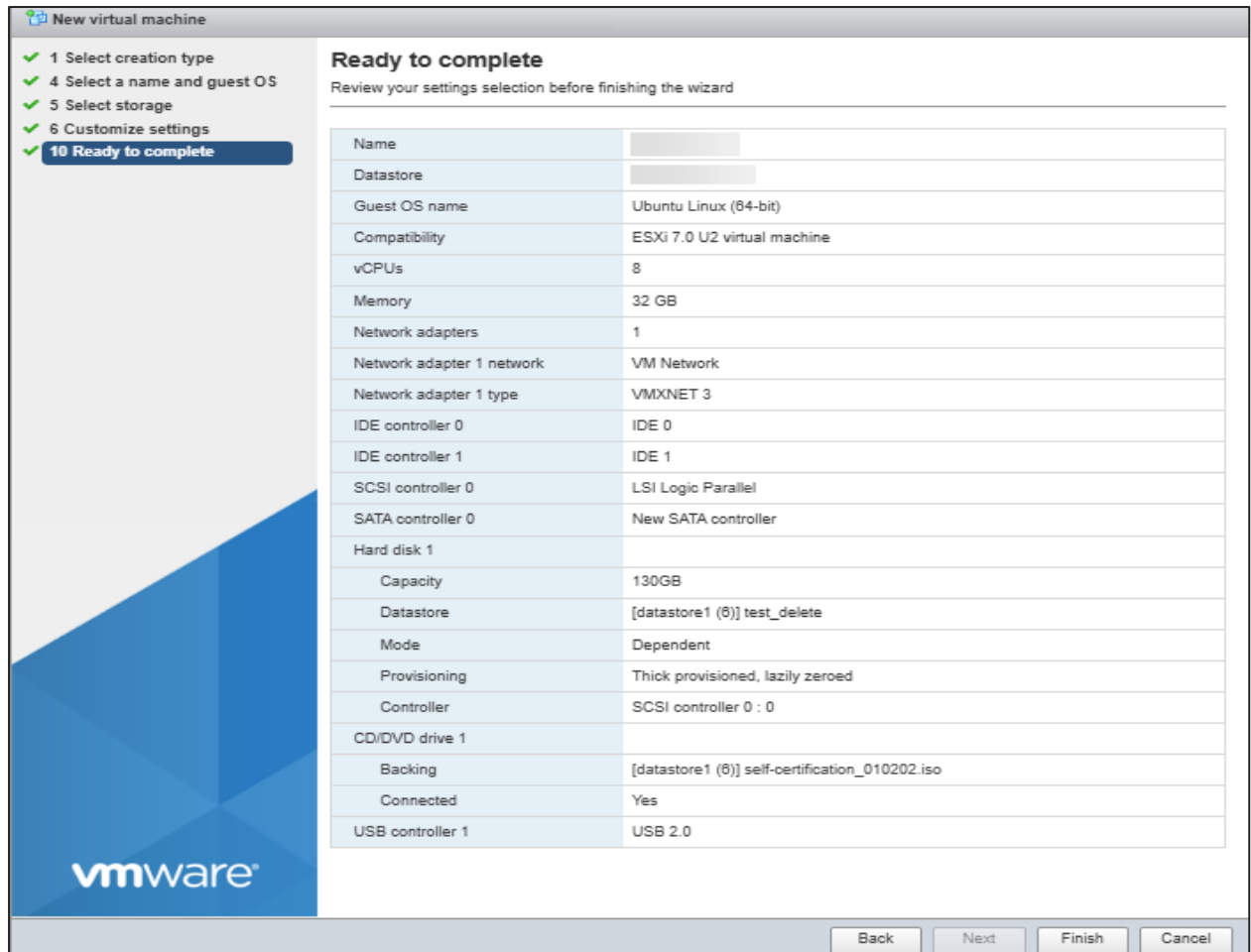
6. Allocate a minimum of 8 CPUs, 32GB memory, and 130GB hard disk, then click **Next**.



7. Select the self certification tool ISO from the datastore.



8. In the Ready to complete section, confirm settings and click **Finish**.



9. Power on the VM.

The system loads the ISO image, presents “Auto Install Self Certification Application,” and initiates installation automatically.

10. Press **Enter** after installation to access the login prompt.

11. If the virtual drive fails to automatically unmount the ISO image file, manually unmount it and proceed with restarting the server.

12. Use the tool virtual console to log in with the username "admin" and the default password "selfCertif1c@ti0n".

13. When prompted, create a new password that is at least 14 characters long and includes at least one digit, one uppercase letter, one lowercase letter, and one special character.

14. Configure the network: assign IP address, CIDR, gateway IP, NTP server, and optionally nameserver:

```
aip <IP/CIDR -- Mandatory> <Gateway -- Mandatory> <NTP server IP -- Mandatory>
<Nameserver -- Optional>
```

Example:

```
aip "172.23.61.184/21" "172.23.56.1" "172.23.57.18" "172.23.100.81"
```

15. Select the NIC with the correct MAC address.

The server hosting the tool will reboot automatically.

Step 4: Perform the initial setup

1. Access the tool using the URL: `https://<Tool-IP-Address>:9000/`.

2. Enter your **Username** and **Password** and then click **Log in**.

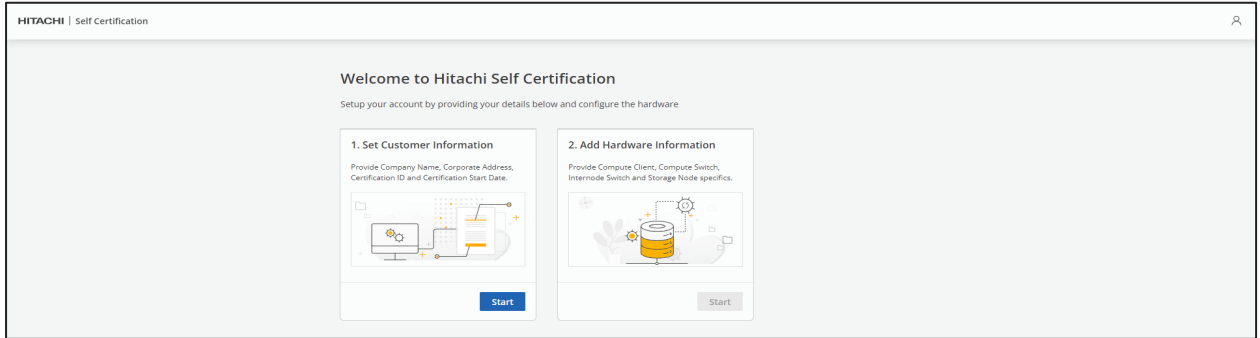
If you are logging in for the first time, use the default credentials:

- **Username:** admin
- **Password:** sdsblock@1234

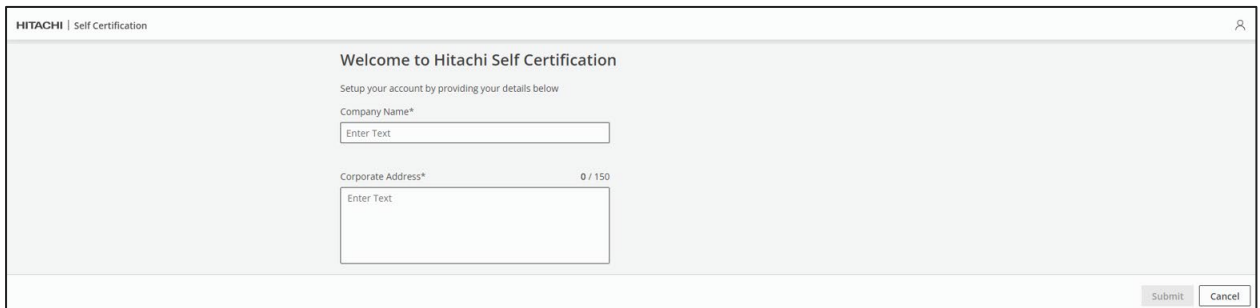
3. Enter the current and new passwords when prompted, then click **Submit**.

The new password must be at least 14 characters long and include at least one digit, one uppercase letter, one lowercase letter, and one special character.

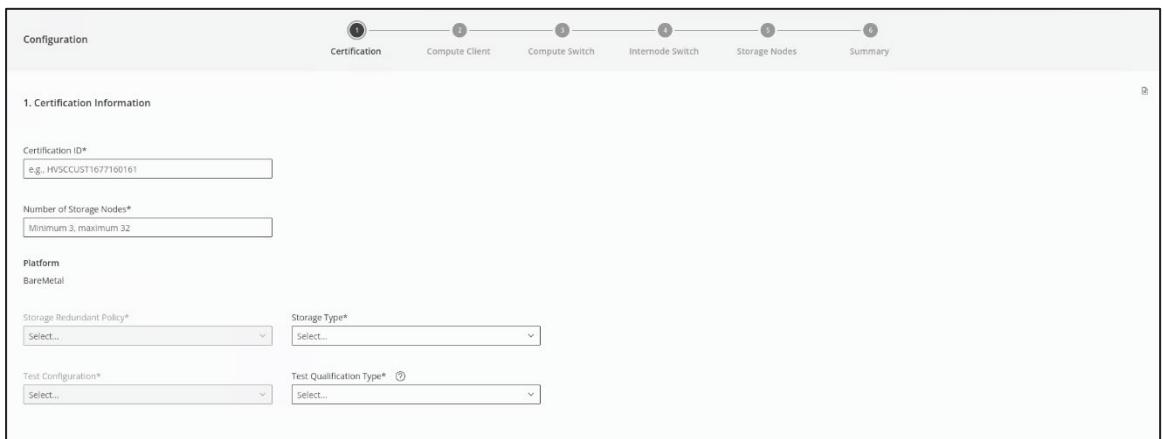
4. Log in to the tool again to display the Self Certification wizard.



5. In the Set Customer Information panel, click **Start**. Enter your Company Name and Corporate Address, then click **Submit**.

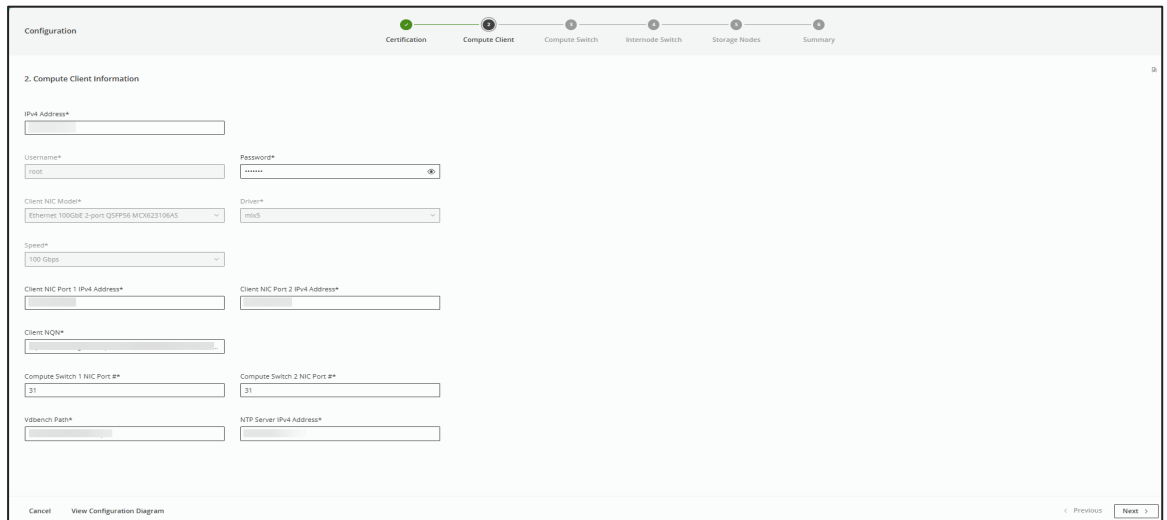


6. Configure hardware to certify.
 - a. In the Add Hardware Information panel, click **Start**.
 - b. In the Certification page, enter the following information:



- **Certification ID:** Enter the certification ID provided by the Hitachi Vantara representative.
- **Number of Storage Nodes:** Enter the number of storage nodes in the configuration.

- **Storage Redundant Policy:** Select the redundant policy for the storage system from the following based on the number of storage nodes:
 - **Mirroring:** 3 or 4 nodes.
 - **Mirroring and 4D + 1P** (Four data drives with one parity drive): 3, 4, or 5 nodes.
 - **Mirroring, 4D +1P, and 4D + 2P** (Four data drives with two parity drives): 6 nodes and above.
 - **Storage Type:** Select the storage system type from the following:
 - **FC:** Fibre Channel storage network.
 - **iSCSI:** IP based storage over Ethernet.
 - **NVMe/TCP:** NVMe storage over TCP/IP.
 - **Test Configuration:** Select the test configuration for validation based on the storage protocol and configuration type.
 - **Test Qualification Type:** Select the test qualification type from the following options:
 - **COMPUTE_SWITCH_QUALIFICATION:** Validates compute switch connectivity.
 - **DISK_QUALIFICATION:** Validates storage disk functionality.
 - **FULL_QUALIFICATION:** Performs full system validation.
 - **INTERNODE_SWITCH_QUALIFICATION:** Validates internode switch communication.
 - **NIC_QUALIFICATION:** Validates network interface cards.
 - **SERVER_QUALIFICATION:** Validates server hardware and configuration.
- c. Click **Next**, then **Yes, Submit** to finalize the certification submission.
- d. In the Compute Client page, enter the following information, then click **Next**.



Configuration

2. Compute Client Information

IPv4 Address*

Username* root Password*

Client NIC Model* Ethernet 100GbE 2-port QSFP56 MC823106AS Driver* mlx5

Speed* 100 Gbps

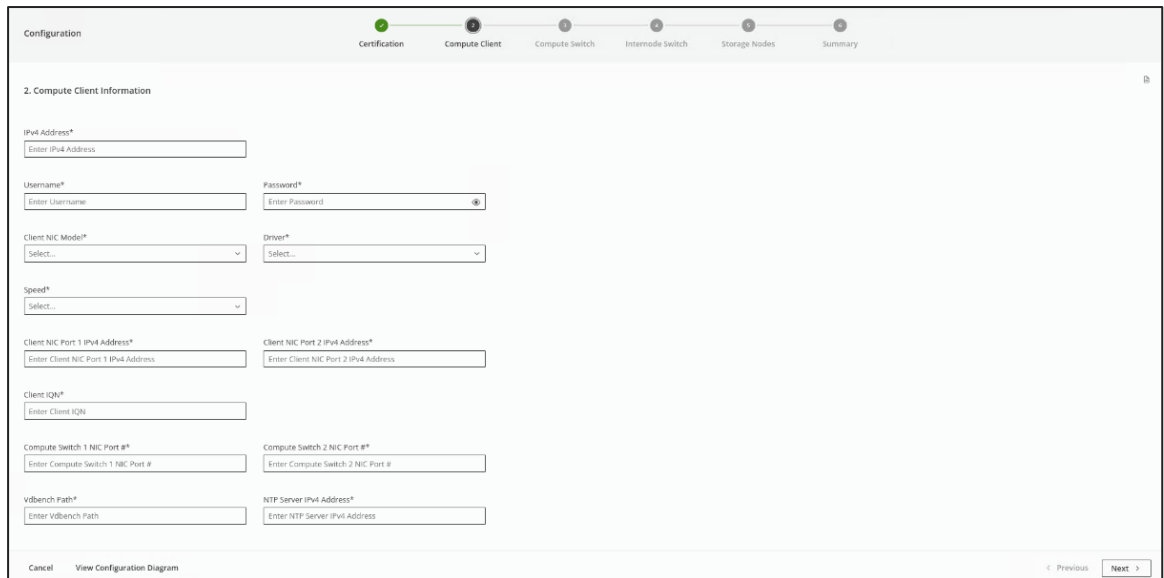
Client NIC Port 1 IPv4 Address* Client NIC Port 2 IPv4 Address*

Client NQN*

Compute Switch 1 NIC Port #* 31 Compute Switch 2 NIC Port #* 31

Vdbench Path* NTP Server IPv4 Address*

Cancel View Configuration Diagram Previous Next



Configuration

1 Certification 2 **Compute Client** 3 Compute Switch 4 Internode Switch 5 Storage Nodes 6 Summary

2. Compute Client Information

IPv4 Address*
Enter IPv4 Address

Username* Password*
Enter Username Enter Password

Client NIC Model* Driver*
Select... Select...

Speed*
Select...

Client NIC Port 1 IPv4 Address* Client NIC Port 2 IPv4 Address*
Enter Client NIC Port 1 IPv4 Address Enter Client NIC Port 2 IPv4 Address

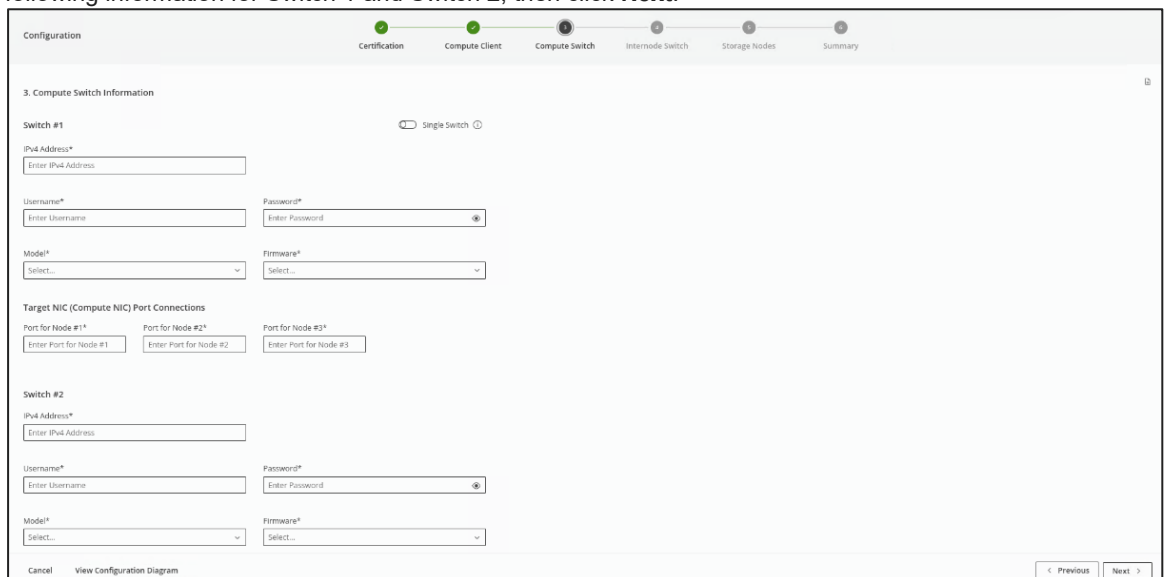
Client IQN*
Enter Client IQN

Compute Switch 1 NIC Port #* Compute Switch 2 NIC Port #*
Enter Compute Switch 1 NIC Port # Enter Compute Switch 2 NIC Port #

Vdbench Path* NTP Server IPv4 Address*
Enter Vdbench Path Enter NTP Server IPv4 Address

Cancel View Configuration Diagram < Previous Next >

- **IPv4 Address:** Enter the compute client network address.
 - **Username and Password:** Provide credentials for compute client access.
 - **Client NIC Model:** Select a virtual HBA model.
 - **Driver:** Select a driver for the HBA.
 - **Speed:** Select either **10 Gbps**, **25 Gbps**, or **100 Gbps** for the HBA connection.
 - **Client NIC Port 1 and 2:** Enter the compute client NIC port numbers.
 - **Client NQN:** Enter the NVMe Qualified Name (NQN) of the compute client.
 - **Compute Switch NIC Port 1 and 2:** Enter the corresponding compute switch port numbers.
 - **Vdbench Path:** Define the path to the Vdbench workload generator.
 - **NTP Server IPv4 Address:** Enter the NTP server address for time synchronization.
- e. In the Compute Switch page, keep Single Switch disabled to configure redundant switches. For Ethernet storage clusters, divide network segmentation for redundant compute paths or switches. Enter the following information for Switch 1 and Switch 2, then click **Next**.



Configuration

1 Certification 2 Compute Client 3 **Compute Switch** 4 Internode Switch 5 Storage Nodes 6 Summary

3. Compute Switch Information

Switch #1 Single Switch

IPv4 Address*
Enter IPv4 Address

Username* Password*
Enter Username Enter Password

Model* Firmware*
Select... Select...

Target NIC (Compute NIC) Port Connections

Port for Node #1* Port for Node #2* Port for Node #3*
Enter Port for Node #1 Enter Port for Node #2 Enter Port for Node #3

Switch #2

IPv4 Address*
Enter IPv4 Address

Username* Password*
Enter Username Enter Password

Model* Firmware*
Select... Select...

Cancel View Configuration Diagram < Previous Next >

- **IPv4 Address:** Enter the IP address of the compute switch.
- **Username and Password:** Provide credentials for compute switch authentication.

- **Model:** Select a compute switch model.
 - **Firmware:** Select the installed firmware version on the compute switch.
 - **Target NIC (Compute NIC) Port Connections:** Enter the compute NIC port connections for external and compute switches.
- f. In the Internode Switch page, enter the port settings for Switch 1 and Switch 2, ensure that the MTU value is set to 9216, then click **Next**.

- **IPv4 Address:** Enter the IP address of the internode switch.
 - **Username and Password:** Provide credentials for internode switch authentication.
 - **Model:** Select an internode switch model.
 - **Firmware:** Select the installed firmware version on the internode switch.
 - **Internode NIC Connections:** Enter the NIC port connections for external and internode switches.
- g. In the Storage Nodes page, enter the following information, then click **Next**.

- **Storage IPv4 Address:** Enter the IP address of the storage node.
- **New Password for Built-in User (admin):** Set a new password for the admin user.
- **Confirm Password for Built-in User (admin):** Re-enter the password to confirm.

- **New Test Username:** Enter the username for test operations.
- **New Test Password:** Set a password for the test user.
- **Confirm Test Password:** Re-enter the test user password to confirm.
- **Physical Server Information:** If the RAID level is set to RAID 1, select **Yes**; otherwise, select **No**.
- **Server Model:** Select a server model.
- **Server Firmware:** Select the installed firmware version of the server.

Configuration

5. Storage Nodes Information

Target NIC Model*
Select...

Target NIC Speed*
Select...

Internode NIC Model*
Select...

Internode NIC Speed*
Select...

Management Console Service*
Select...

Common Username of Management Console*
Common username

Common Password of Management Console*
Common password

IPv4 Addresses

Management Console Network #1*
Enter IPv4 address

Storage Node Control Port Network #1*
Enter IPv4 address

Management Console Network #2*
Enter IPv4 address

Storage Node Control Port Network #2*
Enter IPv4 address

Management Console Network #3*
Enter IPv4 address

Storage Node Control Port Network #3*
Enter IPv4 address

Cancel View Configuration Diagram

< Previous Next >

- **Target NIC Model:** Select a target NIC model.
- **Target NIC Speed:** Select either **10 Gbps**, **25 Gbps**, or **100 Gbps** for the target NIC speed.
- **Internode NIC Model:** Select an internode NIC model.
- **Internode NIC Speed:** Select either **10 Gbps**, **25 Gbps**, or **100 Gbps** for the internode NIC speed.
- **Management Console Service:** Select either **iLO** or **Manual**.
- **Common Username and Password:** Enter credentials for the management console.
- **IPv4 Addresses of Nodes:** Enter the port details for management console and storage node control.

h. In the Summary page, review the configuration information and click **Submit**.

Configuration

6. Summary

Verify the information provided.

Certification Information

Certification ID	Storage Nodes	Platform	Storage Redundant Policy
	3	BareMetal	Mirroring
Storage Type	Test Configuration	Test Qualification Type	
ISCSI	TEST_CONFIG_4	FULL_QUALIFICATION	

Compute Client Information

IPv4 Address	Username	Password	Client NIC Model
	root	Ethernet 10Gb 2-port SFP+ X710
Driver	Speed	Client NIC Port 1 IPv4 Address	Client NIC Port 2 IPv4 Address
i40e	100 Gbps		
Client IQN	Compute Switch 1 NIC Port #	Compute Switch 2 NIC Port #	vdbench Path
iqn.1994-05.com.redhat:59fe4224b7	3	4	/root/vdbench50407.zip
NTP Server IPv4 Address			

Cancel View Configuration Diagram

< Previous Submit

i. Click **View Test Dashboard** or close the popup to go to the Test Dashboard page.

Step 5: Run tests to certify

The tool runs several tests and automated test scenarios to validate third-party hardware compatibility.

1. Run all tests in the following sequence:
 - a. **Configuration:** Verifies the installation of the VSP One SDS cluster and configures the cluster and compute hosts for certification.
 - b. **Sustainability Endurance:** Verifies the hardware sustainability of the VSP One SDS Block through multiple stress operations.
 - c. **I/O Stability:** Ensures data integrity during I/O operations on the storage cluster under various disruptive scenarios.
 - d. **Fault Handling:** Simulates unplanned hardware errors, such as component failures and recoveries, to ensure fault tolerance.
 - e. **Switch Fault:** Tests error handling and storage recovery during switch faults or power failures.
 - f. **Maintenance:** Conducts planned maintenance to ensure business continuity in datacenter operations.
 - g. **Performance:** Evaluates read and write performance.
 - h. **Result Submission:** Runs the test to generate results, provides an option to download the test results, and necessitates the manual collection of switch logs.
2. Submit the test results and collected switch logs to a Hitachi Vantara representative for review and approval.

Test Overview		Total	In Progress	Passed	Failed
		32	0	3	0
✓	CONFIGURATION 3/3 Passed				
⊙	SUSTAINABILITY 0/4 Passed				
⊙	IO_STABILITY 0/5 Passed				
⊙	FAULT_HANDLING 0/7 Passed				
⊙	SWITCH_FAULT 0/4 Passed				
⊙	MAINTENANCE 0/7 Passed				
⊙	PERFORMANCE 0/1 Passed				
⊙	RESULT_SUBMIT 0/1 Passed				
Name	Status	Start Time	End Time	Log	
ExecuteTestResultCollection	⊙ Not Run Yet	—	—	—	Run

Summary

The tool simplifies third-party hardware validation for VSP One SDS Block. The tool enhances automation, flexibility, and performance validation, enabling seamless integration into existing infrastructure.

Reference

- [Self Certification Tool Getting Started Guide](#)
- [VSP One SDS Block](#)