Provisioning and Implementing Data Protection on VSP One Block 20 Storage Systems with Hitachi Ops Center Suite 11.0.2

v1.0

Quick Start Guide

This document describes how to provision and implement data protection with Global-active Device (GAD) on Hitachi Virtual Storage Platform One Block 20 (VSP One Block 20) storage systems using Hitachi Ops Center Administrator.

Hitachi Vantara

September 2024

© 2024 Hitachi Vantara LLC. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively, "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at https://support.HitachiVantara.com/ en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and
2) Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

Hitachi is a registered trademark of Hitachi, Ltd., In the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, Flash Copy, IBM, Lotus, MVS, OS/390, PowerPC, RS6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, BCPii™ and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or web site are properties of their respective owners.

Table of Contents

Table of Contents **3**

Preface **4**

About this document 4

Revision History 4

References 4

Accessing product downloads 4

Getting Help 5

Comments 5

Chapter 1: Introduction **6**

Key Components 6

High-Level Diagram 7

Chapter 2: Lab Scenarios **8**

Chapter 3: Lab Validation Procedures **9**

Preparing the Lab Environment 9

Provisioning using Hitachi Ops Center Administrator 9

Onboarding a Storage System in Ops Center Administrator 9

Creating a Pool using Ops Center Administrator 10

Creating a Volume 11

Onboarding a Server to Ops Center Administrator 12

Attaching a Volume to a Single Server 13

Creating a Server Group and Attaching a Volume 15

Data Protection with Global-active Device (GAD) using Ops Center Administrator and Protector 18

GAD Prerequisites 19

Configuring a VSM using Ops Center Administrator 19

Verifying a High Availability Setup in Ops Center Administrator 22

Verifying Integration of Ops Center Protector with Ops Center Administrator 23

Onboarding a Storage System in Ops Center Protector 24

Creating a Host Group for GAD 30

Creating a GAD Pair using High Availability 34

Conclusion **41**

Preface

About this document

This document describes how to manage Hitachi Virtual Storage Platform One Block 20 (VSP One B20) storage systems using the Ops Center Suite. In addition, this document provides step-by-step instructions for the following tasks:

- Basic storage provisioning using Ops Center Administrator.
- Data protection with Global-active Device (GAD) using Ops Center Administrator, integrated with Ops Center Protector.

This document serves as a quick start guide, covering key functionalities such as provisioning and implementing data protection. In summary, this is a concise, user-friendly document that enables customers to quickly set up their storage environment.

Note: The information provided here is specific to lab requirements, which involve a limited, controlled, low-stakes, and simplified environment. This can be used as a starting point only. However, you must conduct a proof-of-concept in a non-production, isolated test environment matching your production environment before implementing this solution. Additionally, this guide is not a replacement for the detailed user guides that provide in-depth information and explanations.

Revision History

Revision	Details	Date
v1.0	Initial Release	September 2024

References

- Hitachi Ops Center Documentation
- Ops Center System Requirements

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: https://support.hitachivantara.com/.

Log in and select Product Downloads to access the most current downloads, including updates that may have been made after the release of the product.

Getting Help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send your comments on this document to GPSE-Docs-Feedback@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Chapter 1: Introduction

Hitachi Virtual Storage Platform One Block (VSP One Block) storage appliances are specifically designed to meet the unique needs of mid-sized businesses. Offering unparalleled simplicity, sustainability, and security in a user-friendly package, VSP One Block empowers mid-sized businesses to manage data with greater ease and efficiency.

For some customers, deploying a suite of management tools alongside multiple storage systems might be the norm. At Hitachi Vantara, we value all our customers, and for those with extensive storage needs, we offer Hitachi Ops Center, a robust federated management solution. With Hitachi Ops Center, customers can manage their storage systems from day one with minimal setup time.

Key Components

The following lists the major components of this solution:

- **Hitachi Ops Center v11.0.2**: The Ops Center v11.0.2 suite was deployed using default OVAs in a VMware environment.

  Note: Ops Center can also be installed using the Express Installer.

- **Storage Systems**: Two VSP One B28 storage systems were used in the lab implementation. A third storage system, a VSP One B28, was used for the GAD quorum.

- **Network Switch**: A Cisco Nexus 9000 series switch was used to establish a LAN between the storage systems, Ops Center Server, and hosts.

- **SAN Switches**: Brocade 6510 FC switches were used for SAN connectivity between the storage systems and the host.

- **Host Server**: A Hitachi Advanced Server DS220 was used as the host.

- **Network Ports**: Ensured that all network ports and connectivity between servers, storage systems, and hosts are properly configured (LAN/FC).

High-Level Diagram

Figure 1 shows the high-level lab environment used for the implementation.

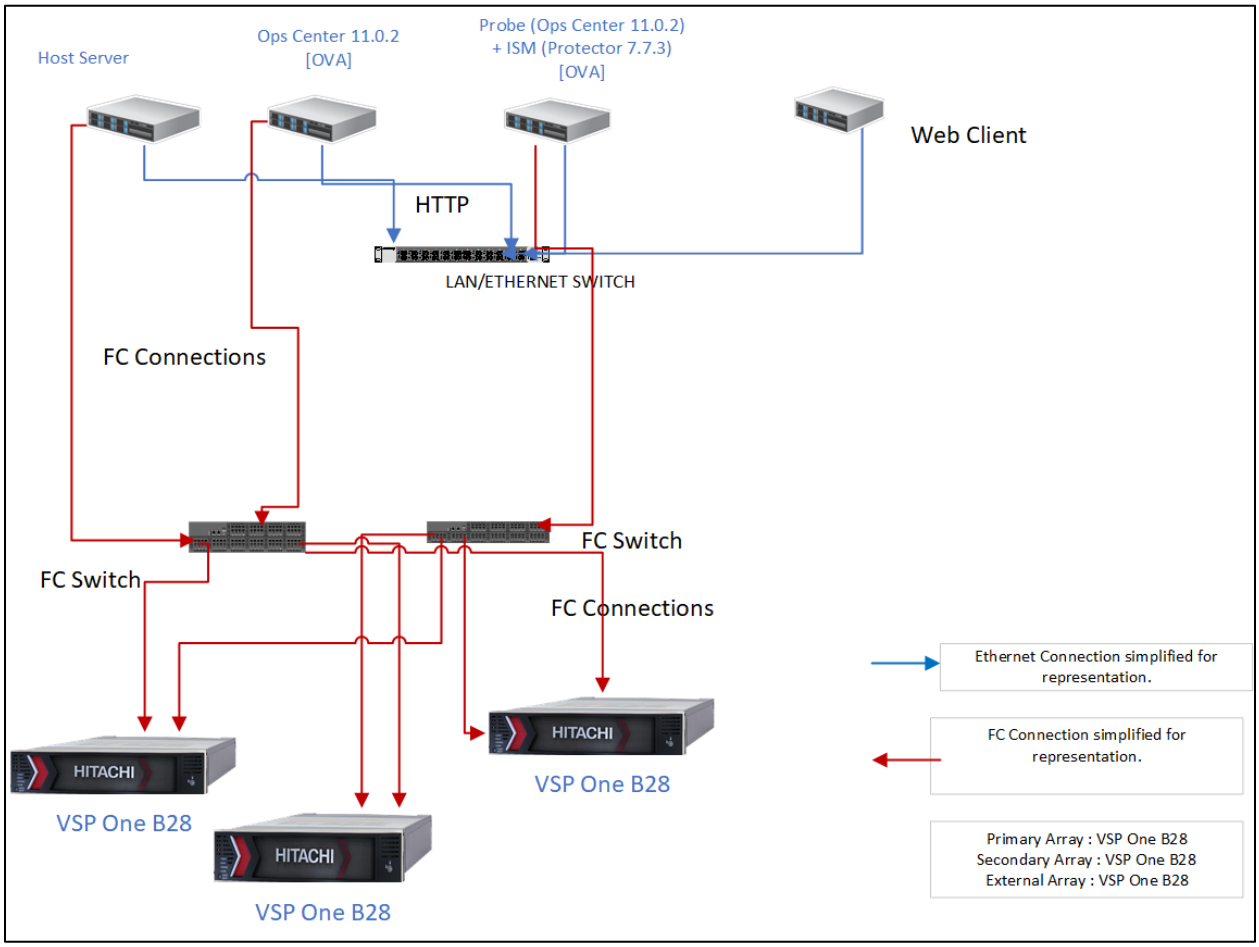


Figure 1: High-level diagram

Chapter 2: Lab Scenarios

Table 1 lists the high-level steps performed in the lab environment.

Table 1: High Level Steps

Step	Description
1	Preparing the Lab Environment: 1. Deploy Ops Center v11.0.2: a. Deploy Ops Center v11.0.2 using OVA templates on a VMware host or use the Express Installer for RHEL/OEL machines. b. Apply individual Ops Center product licenses to ensure proper functionality. 2. Configure the storage system, server, switch, and FC/LAN connections. Ensure all ports and connectivity between servers, storage systems, and hosts are properly set up (LAN/FC). 3. Set up zoning between the server HBAs and the storage ports.
2	Provisioning using Ops Center Administrator: 1. Onboard a storage system in Ops Center Administrator. 2. Create a pool using Ops Center Administrator. 3. Create a volume. 4. Onboard a server in Ops Center Administrator. 5. Attach a volume to a single server. 6. Create a server group and attaching a volume.
3	Data Protection with GAD using Ops Center Administrator and Protector: 1. GAD prerequisites: a. Configure VSM using Ops Center Administrator. b. Verify the high availability setup in Ops Center Administrator. c. Verify the integration of Ops Center Protector with Ops Center Administrator. d. Onboard storage in Ops Center Protector. 2. Create a host group for GAD. 3. Create a GAD pair using high availability.

Chapter 3: Lab Validation Procedures

This chapter describes how to provision and implement data protection with GAD using Ops Center Administrator and Protector.

Preparing the Lab Environment

To prepare a lab environment, complete the following steps:

1. Deploy Ops Center v11.0.2:

    a. Deploy Ops Center v11.0.2 using OVA templates on a VMware host or using the Express Installer. Set up IP, DNS, hostname, and NTP for RHEL/OEL machines.

    b. Apply individual Ops Center product licenses to ensure proper functionality.

2. Ensure that all prerequisites are met, such as configuring ports and connectivity between servers, storage systems, and switches (LAN/FC). For more details, see the Ops Center System Requirements Guide.

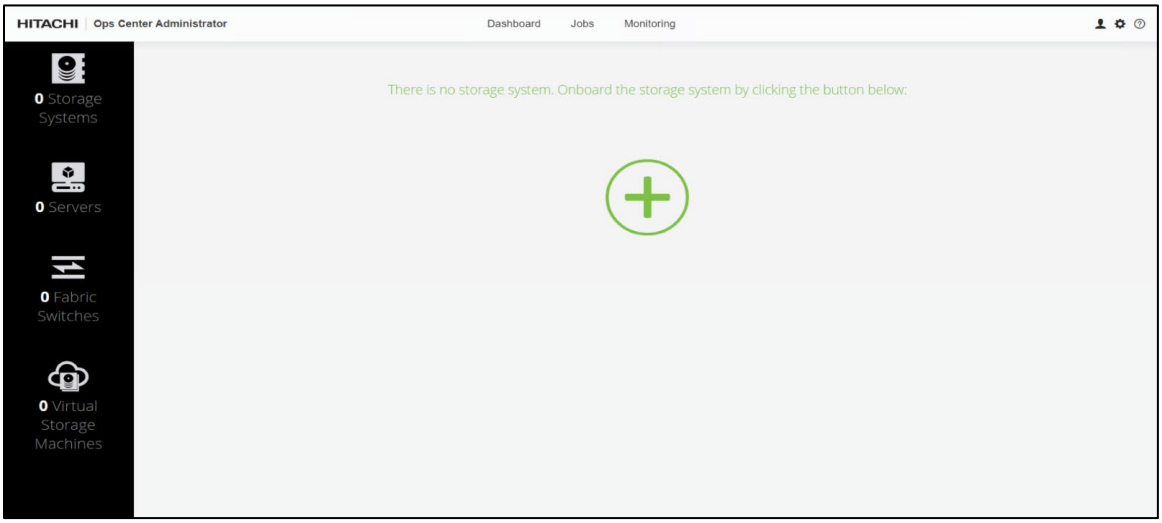
3. Ensure that zoning is configured between the server HBAs and the storage ports to verify that the provisioned volumes are visible on the host.

Provisioning using Hitachi Ops Center Administrator

Onboarding a Storage System in Ops Center Administrator

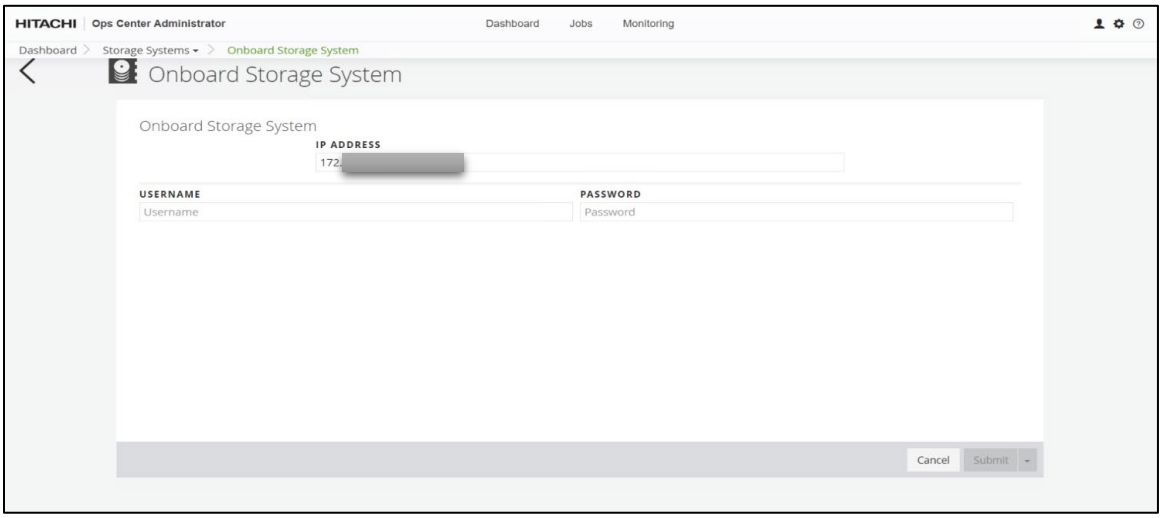
To onboard a VSP One B20 storage system in Ops Center Administrator, complete the following steps:

1. From the Ops Center Administrator dashboard, click the '**+**' icon.



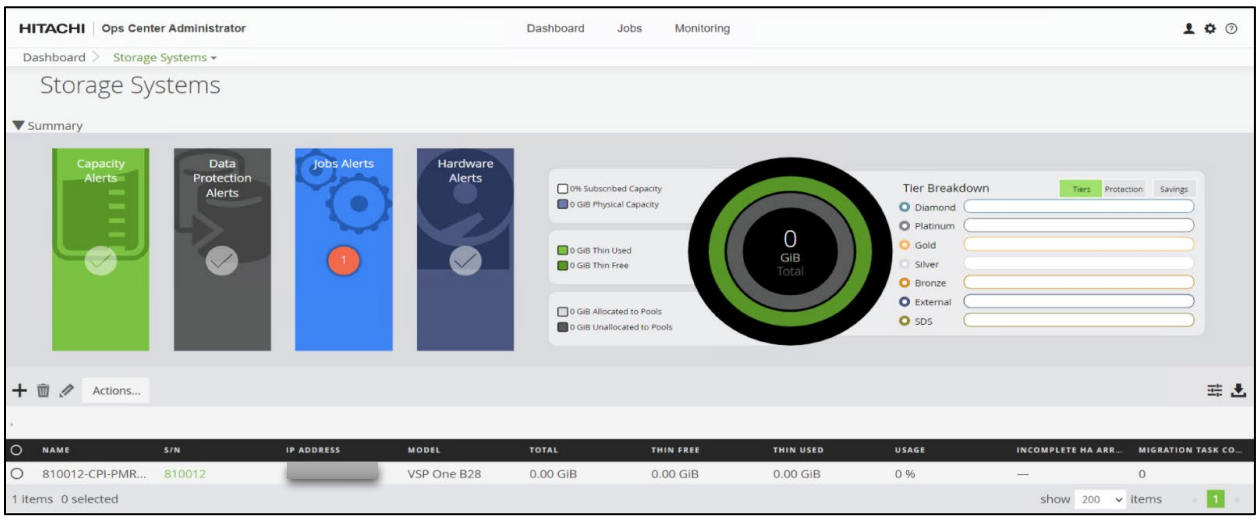
2. Enter the storage system IP address and user credentials as shown in the following screenshot.

   Note: VSP One B20 storage systems must be registered using the Service (ESM) IP.



Creating a Pool using Ops Center Administrator

After onboarding the storage system to Ops Center Administrator, it appears under Storage Systems.

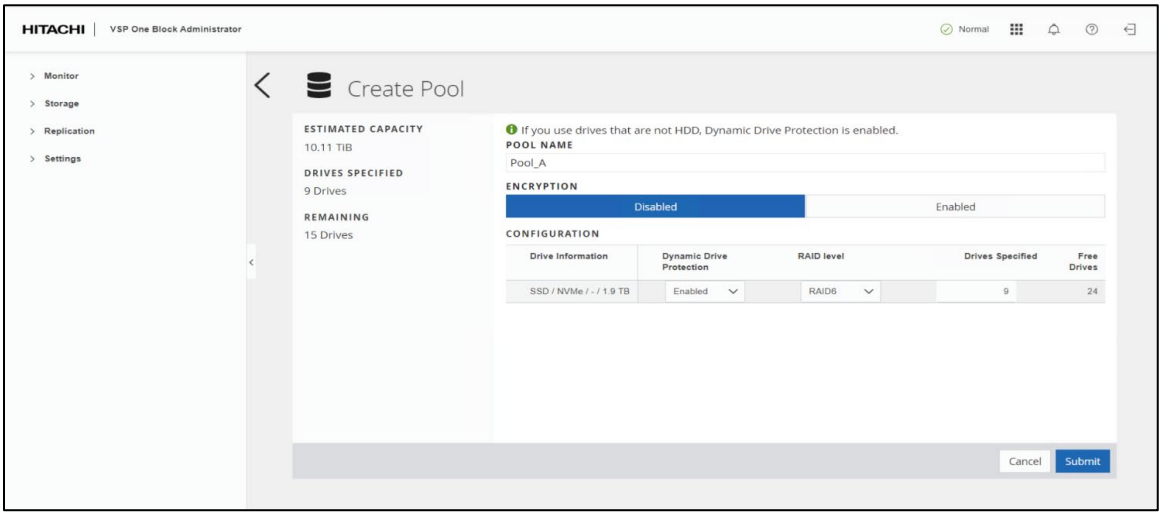


To create a pool from Ops Center Administrator, complete the following steps:

1. To access the storage system from the Ops Center Administrator dashboard, click the serial number.

2. To create a pool, navigate to **Pools**, then click the '**+**' icon.

The ‘Create Pool’ page opens in a new tab.



3. To create a pool, enter the information as shown in the screenshot, and then click **Submit**.

When the pool is created, it is visible in Ops Center Administrator.

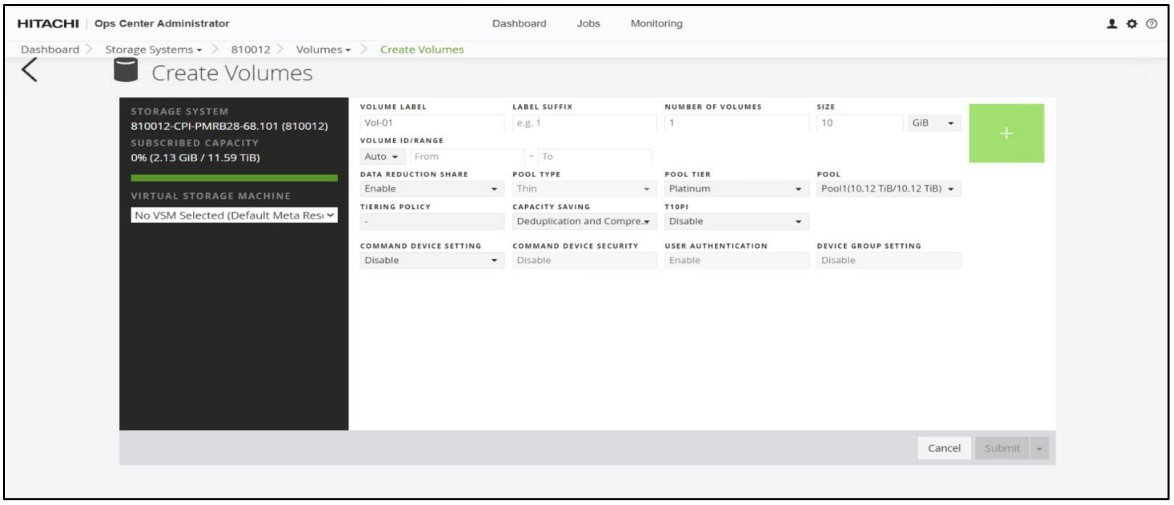
Note:

- **Dynamic Drive Protection** is enabled by default and cannot be modified.
- **RAID6** is selected by default and cannot be modified.
- Ops Center Administrator does not create the pool. Instead, it redirects you to the VSP One Administrator GUI to create the pool.
- Dynamic Drive Protection (DDP) is a new feature introduced in VSP One Block 20 that significantly reduces rebuild and recovery time during a drive failure, enhancing overall system reliability. DDP is exclusively supported for RAID 6 configurations and requires one additional drive compared to traditional RAID 6. While traditional RAID 6 in VSP storage systems requires 8 drives, DDP-enabled RAID 6 requires 9 drives.
- For our lab environment, a RAID 6 pool was created using 9 drives with DDP enabled and encryption disabled.

Creating a Volume

After pool creation, you must create volumes. To create a volume, complete the following steps:

1. From the Ops Center Administrator dashboard, navigate to **Storage Systems** > **Volumes**, and then click the ‘**+**’ icon.
2. Enter the information, as shown in the following screenshot:



3. To create a new volume, click the '**+**' icon on the right, and click **Submit**.

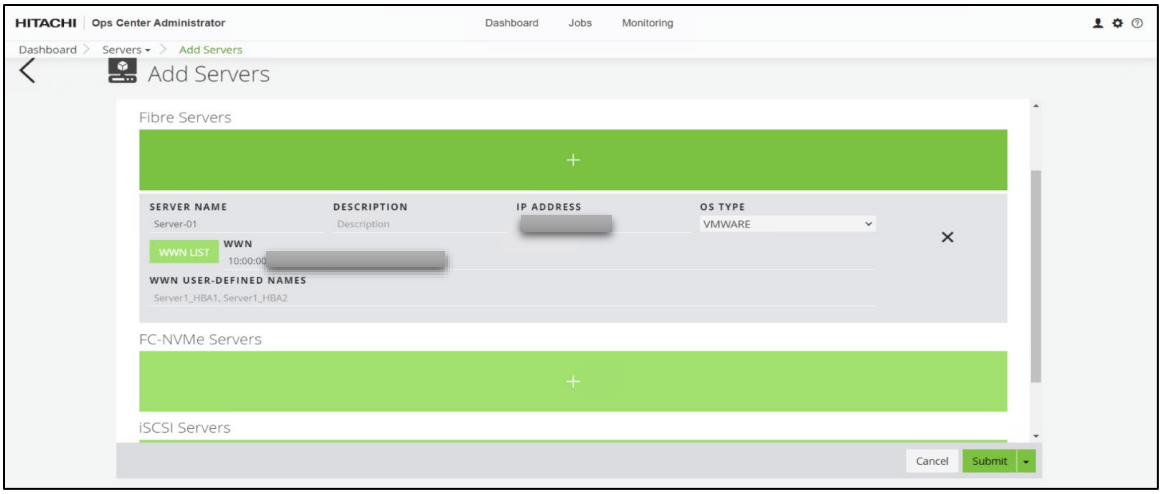
   Note:

   - For our lab environment, we created a 10GB DRS (Data Reduction Shared) volume. The Capacity Saving was set to "Deduplication and Compression". **T10P1** and **Command Device Settings** were disabled.
   - You can select the pool manually using the dropdown list (recommended), or Ops Center Administrator selects the pool automatically.
   - Ops Center Administrator only allows the creation of DRS and DRD volumes (DRS is default).
   - Ops Center Administrator does not create DP Volumes.

Onboarding a Server to Ops Center Administrator

To onboard a server to Ops Center Administrator, complete the following steps:

1. From the Ops Center Administrator dashboard, navigate to **Servers**.
2. To add a server, click the '**+**' icon.
3. Select **Fiber Server,** enter the **IP Address**, **OS Type**, and **WWN(s)** as shown in the following screenshot, and then click **Submit**.



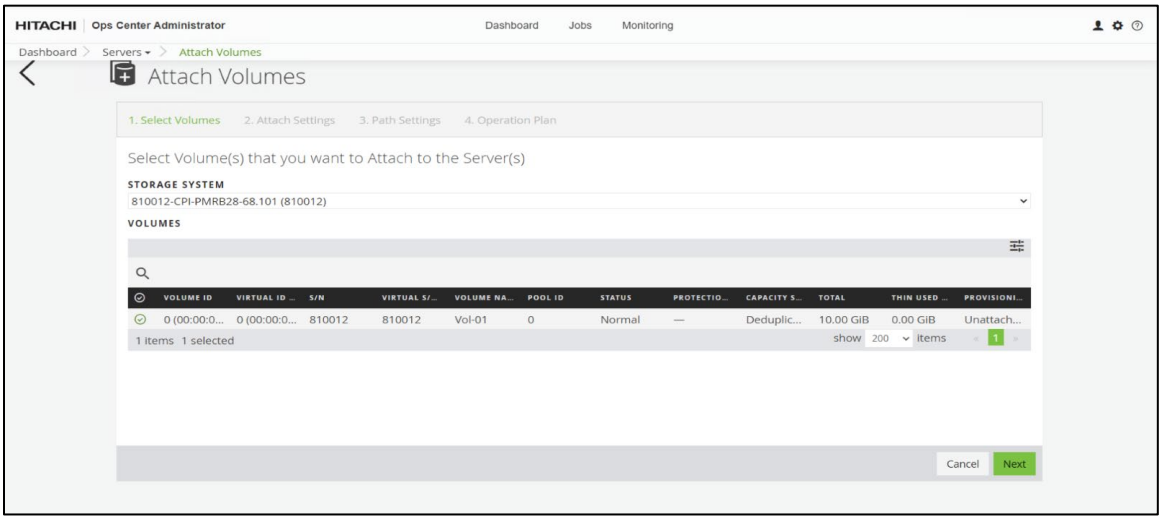
The server is successfully onboarded to Ops Center Administrator.

Note: For our lab environment, a single server was used with 2 WWNs (for multipathing.)

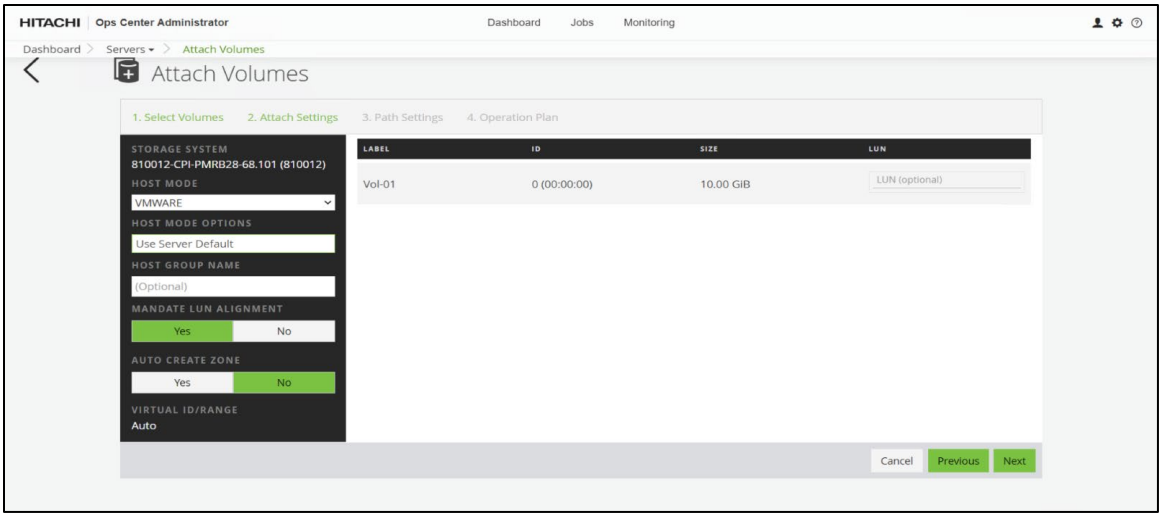
Attaching a Volume to a Single Server

To attach a volume to a server, complete the following steps:

1. From the Ops Center Administrator dashboard, navigate to **Servers**.
2. Select the server for volume attachment.
3. On the top-right-hand side, click **Attach Volumes**, then select **Attach Existing Volumes**.
4. Select the volume for attachment, then click **Next**.



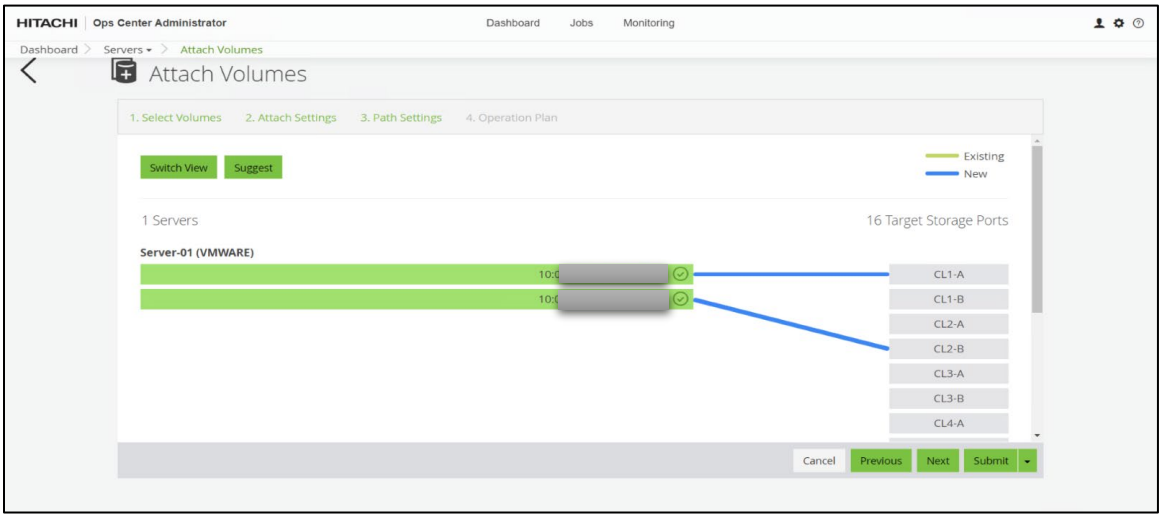
5. In the ‘Attach Settings’ page, enter the information as shown in the following screenshot, and then click **Next**.



Note: For our lab environment, we set the Host Mode to **VMWARE** and selected **Use Server Default** for the Host Mode Options. Additionally, selected **Yes** for Mandate LUN Alignment and **No** for Auto Create Zone.

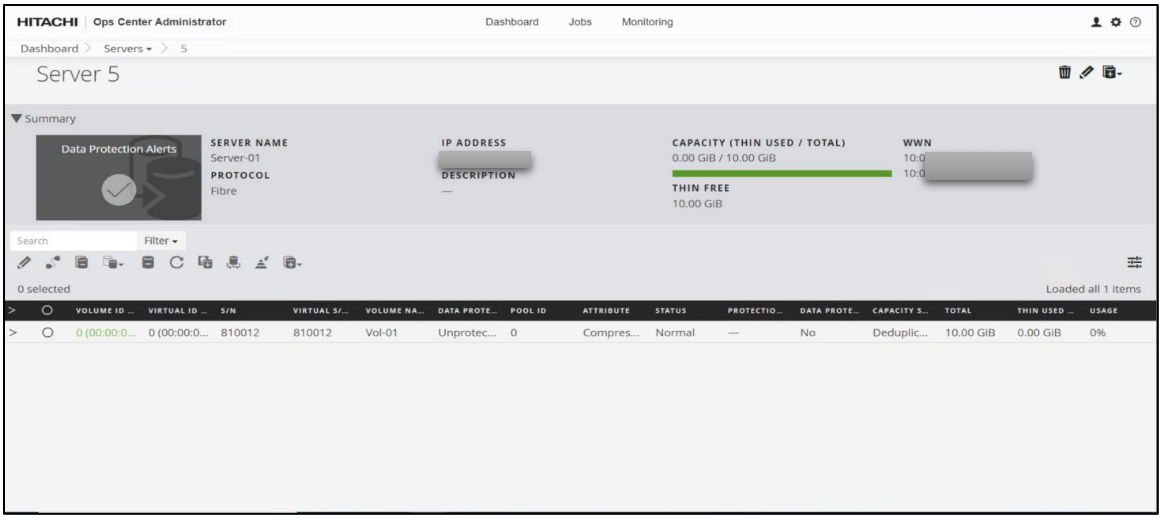
6. In the 'Path Settings' page, attach the server to a storage port by selecting the server, selecting the storage port, and then clicking **Submit**.

   Note: Single or multiple paths can be created between the host and the storage ports. In a production environment, multiple paths are recommended.



7. To view the newly attached volume, navigate to **Servers** and click the server.

   The list of attached volumes appears as shown in the following screenshot:

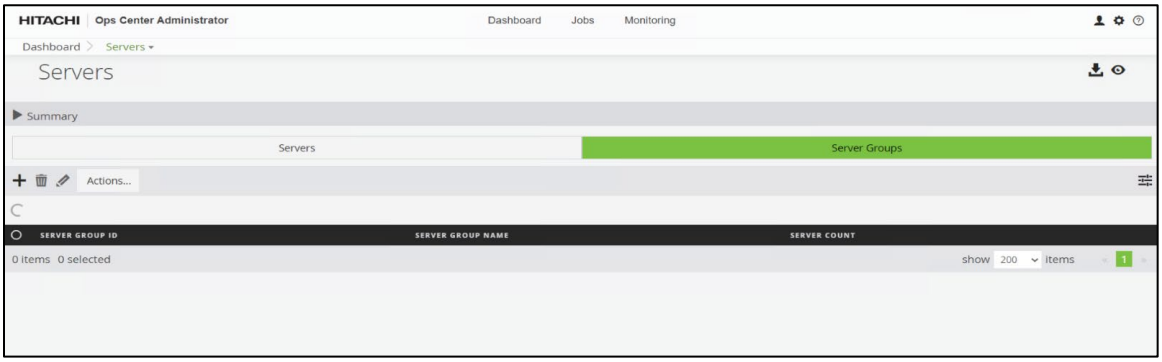


Creating a Server Group and Attaching a Volume

Server Groups are created to simplify server management by allowing multiple servers to be managed simultaneously.

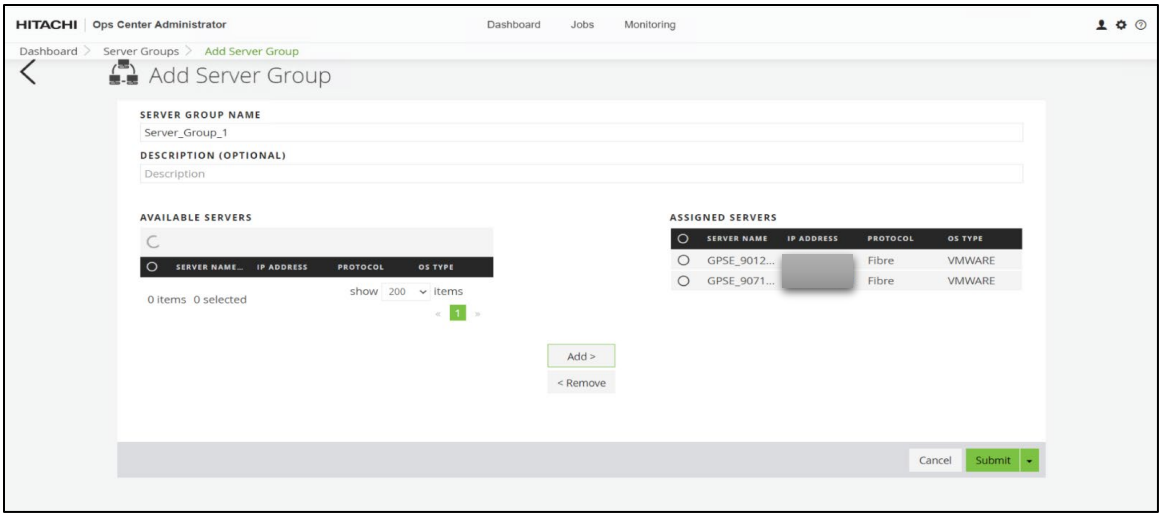
To create a server group, complete the following steps:

1. From the Ops Center Administrator dashboard, navigate to **Servers** > **Server Groups** and click the '**+**' icon.

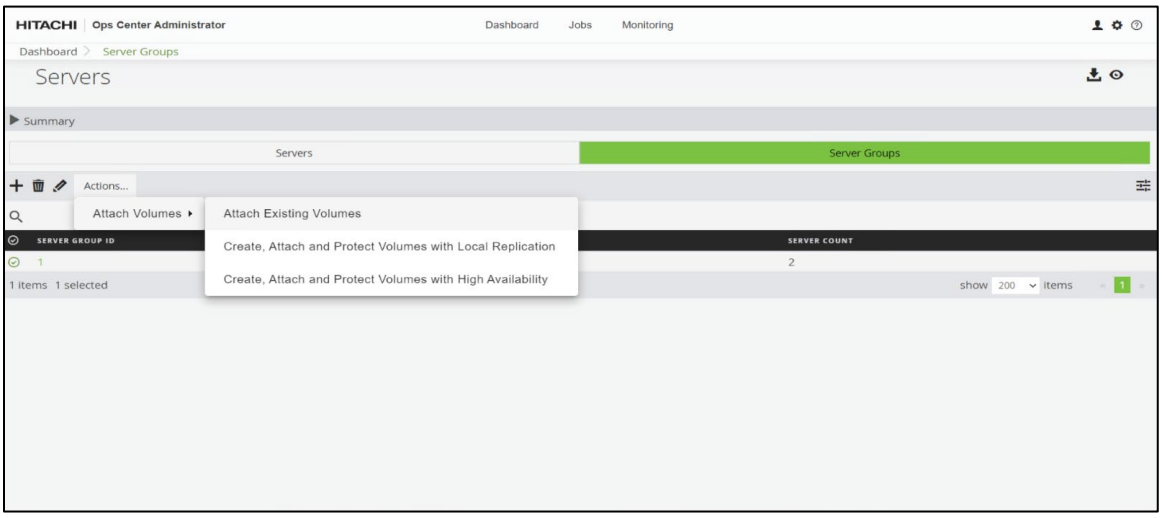


2. To add a server to the server group, enter the Server Group Name and Description (Optional), select one or more servers from the Available Servers list, and then click **Add**.

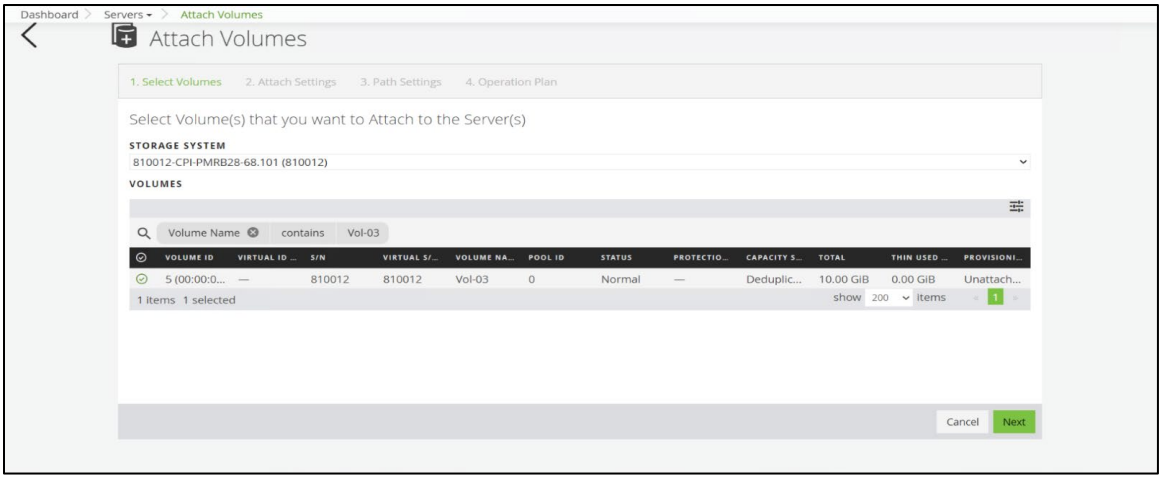
3. When the servers are added, create the server group by clicking **Submit**.



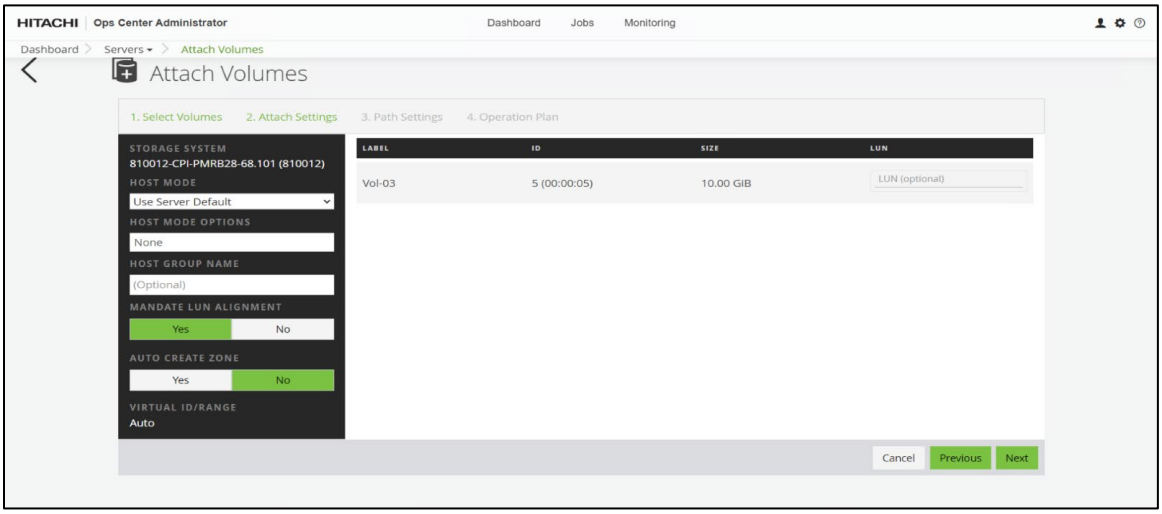
4. To attach a volume to a server group, navigate to **Servers** > **Server Groups** and select the required server group. Then, from the Actions menu, select **Attach Volumes** > **Attach Existing Volumes**.



5. To attach the storage system and volume to the server group, select the required storage system and volume, then click **Next**.



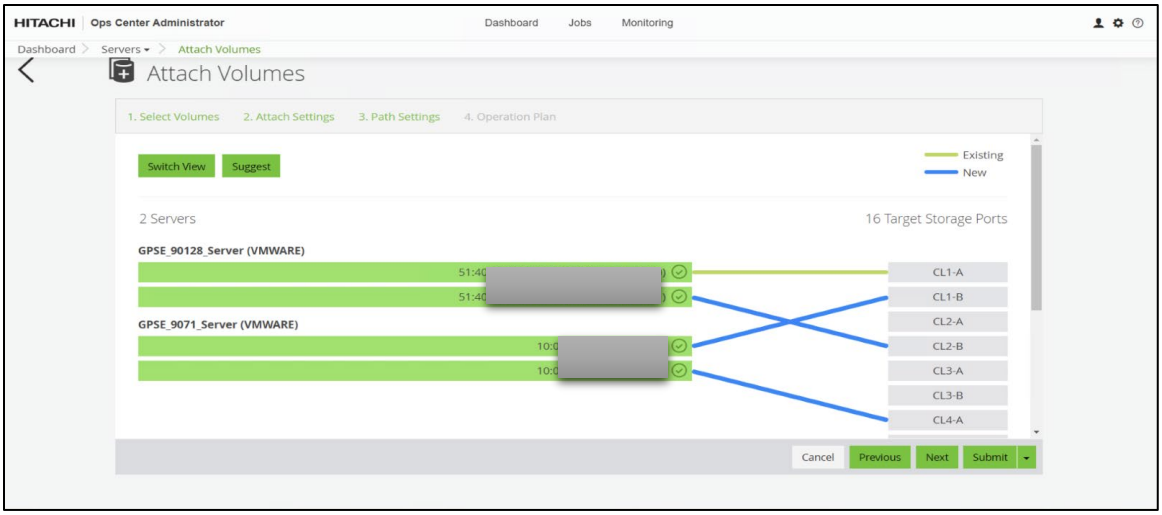
6. In the ‘Attach Settings’ page, enter the information as shown in the following screenshot, and then click **Next**.



Note: We used the default settings for our lab environment.

8. In the ‘Path Settings’ page, attach the server to a storage port by selecting the server, selecting the storage port, and then clicking **Submit**.

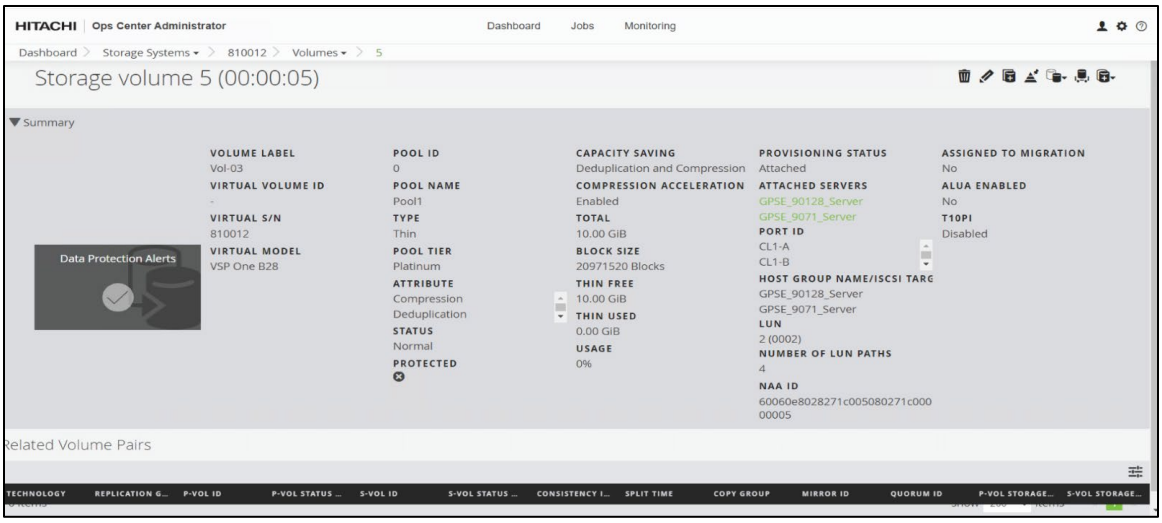
Note: Single or multiple paths can be created between the host and the storage ports. In a production environment, multiple paths are recommended.



The volumes are attached to the existing servers in the server group.

7. To verify that the volumes are attached to the servers, navigate to **Storage Systems** > **Volumes** and click the required volume.

   The volume information page displays the list of servers it's attached to. An example is shown in the following screenshot:



Data Protection with Global-active Device (GAD) using Ops Center Administrator and Protector

Ops Center Administrator supports Hitachi Block-based replication technologies allowing users to view the current state of replications and control the related activities. When establishing a replication, the storage system copies all data to the secondary volume, which can take time depending on the volume size.

In this section, Ops Center Administrator is used to create and manage GAD- based data protection policies after replications and snapshots are created.

Note: Ops Center Administrator must be integrated with Ops Center Protector because pair management is managed through Protector.

GAD Prerequisites

The following prerequisites must be met for setting up GAD:

- Configure RCU (Remote Control Unit) - MCU (Main Control Unit) between the primary and secondary storage systems. This configuration can be done using CCI or VSP One Block Administrator.
- Attach a third VSP One B20 storage system as a quorum disk to both the primary and secondary storage systems.
- Configure a command device on both primary and secondary storage systems (both FC and IP Command Devices are supported).
- Onboard primary and secondary storage systems as Hitachi Block Devices to Ops Center Protector.

Additional prerequisites explained in subsequent sections include:

- Configuring a VSM on both primary and secondary storage systems using Ops Center Administrator.
- Verifying a high availability setup in Ops Center Administrator.
- Verifying integration of Ops Center Protector with Ops Center Administrator.
- Onboarding a storage system in Ops Center Protector.

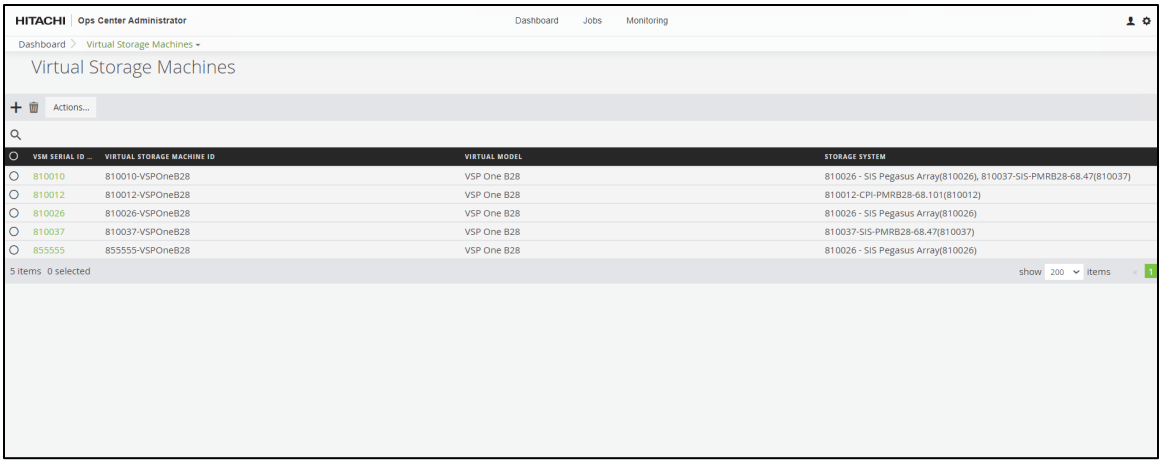
Configuring a VSM using Ops Center Administrator

Ops Center Administrator enables users to create Virtual Storage Machines (VSMs) and manage associated resources, such as volumes, ports, and host groups. In addition, users can add or remove both defined and undefined resources to or from an existing VSM, offering flexible storage infrastructure management.

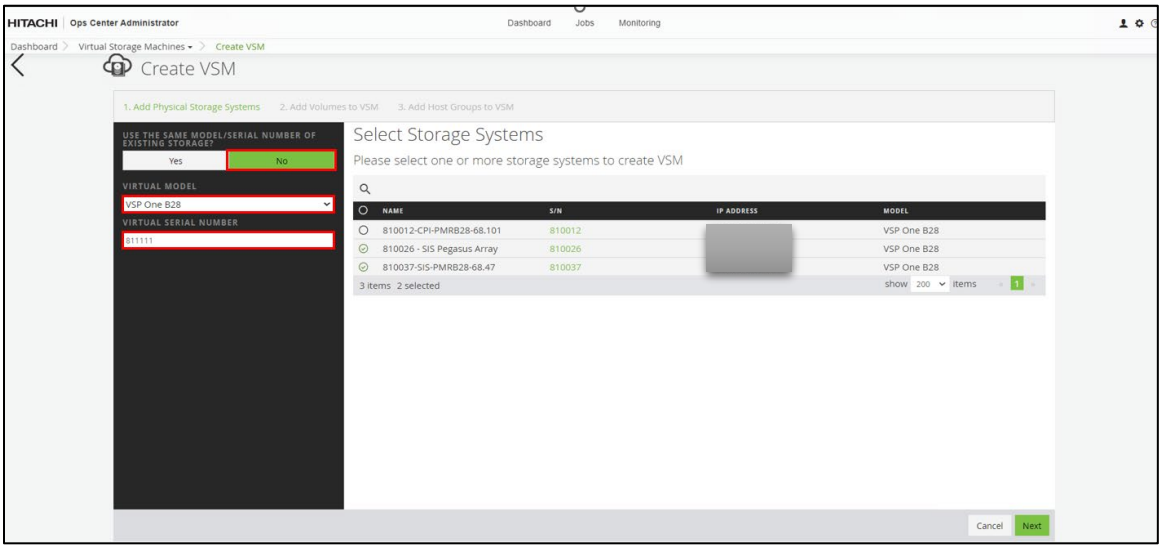
To configure VSM using Ops Center Administrator, complete the following steps:

1. From the Ops Center Administrator dashboard, navigate to **Virtual Storage Machines** and click the '**+**' icon.



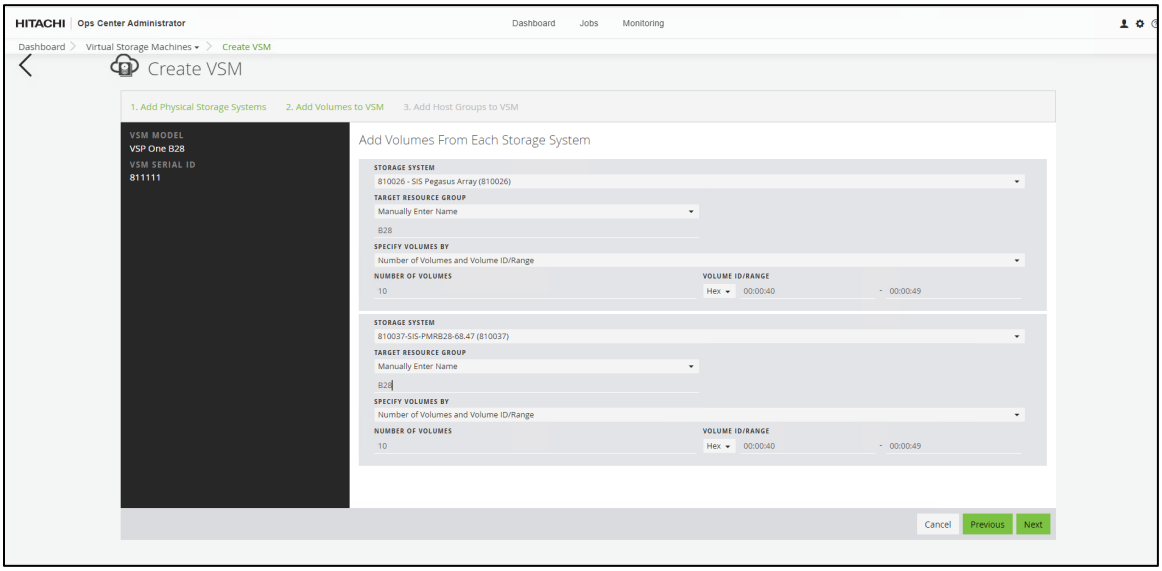


2. In the ‘Create VSM’ page, add a physical storage system by entering the information as shown in the following screenshot, and then click **Next**.

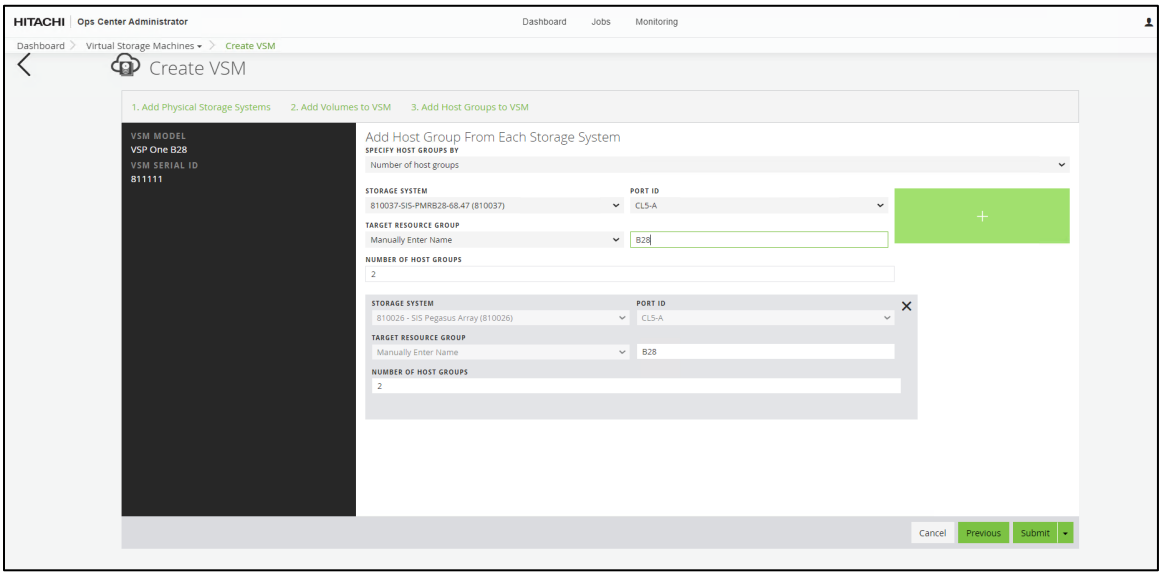


Note: For our lab environment, we selected both the primary and secondary storage systems while creating the VSM. Selected ‘VSP One B28’ as the Virtual Model and assigned ‘811111’ as the Virtual Serial Number.

3. In the ‘Add Volumes to VSM’ page, select the **Storage System**, enter the **Target Resource Group** manually or automatically, enter the **Number of Volumes**, and specify the **Volume ID/Range** as shown in the following screenshot, and then click **Next**.



4. In the ‘Add Host Groups to VSM’ page, select the **Storage System**, select the **Port ID** reserved for GAD, select the **Target Resource Group**, and enter the **Number of Host Groups** as shown in the following screenshot, and click the ‘**+**’ icon, then click **Submit**.

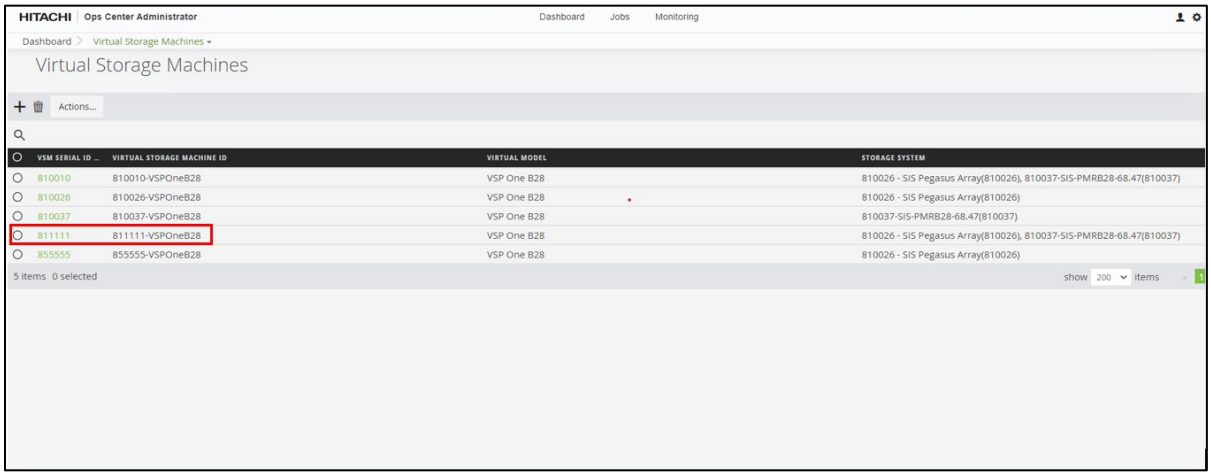


Note:

- By clicking the ‘**+**’ icon, the lower half of the window displays the selections made.

- You can add multiple host groups, if required.

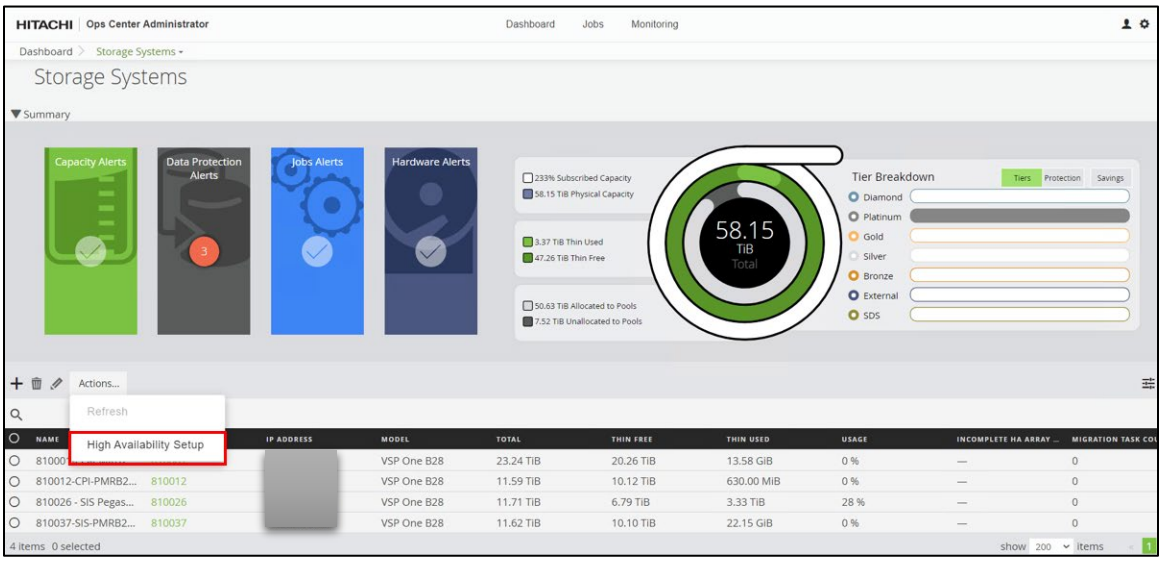
The new VSM appears in the ‘Virtual Storage Machines’ page as shown in the following screenshot:



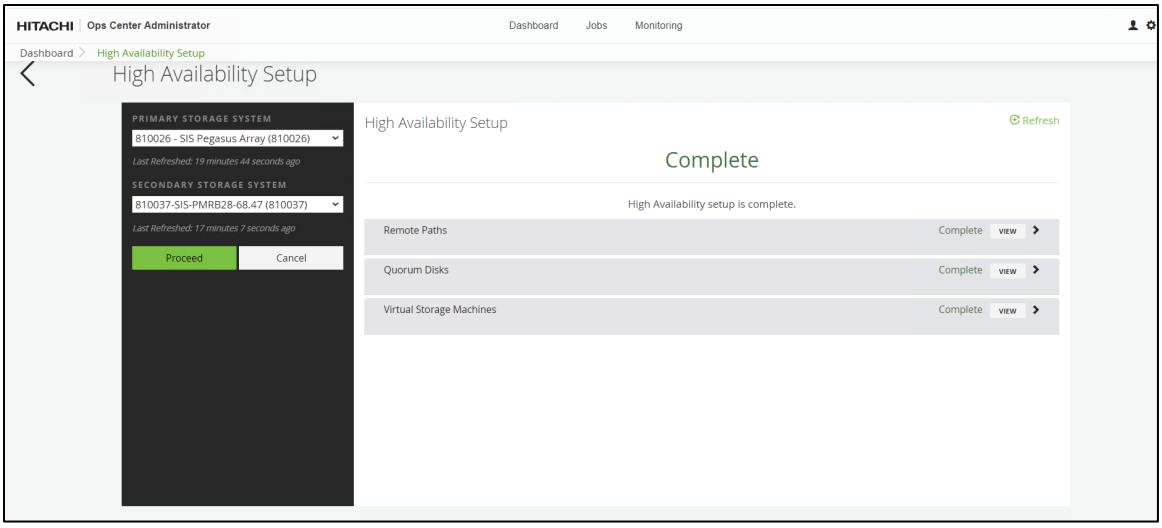
Verifying a High Availability Setup in Ops Center Administrator

To verify High Availability between primary and secondary storage systems, complete the following steps:

1. From the Ops Center Administrator dashboard, navigate to **Storage Systems** > **Actions** menu, then click **High Availability Setup**.



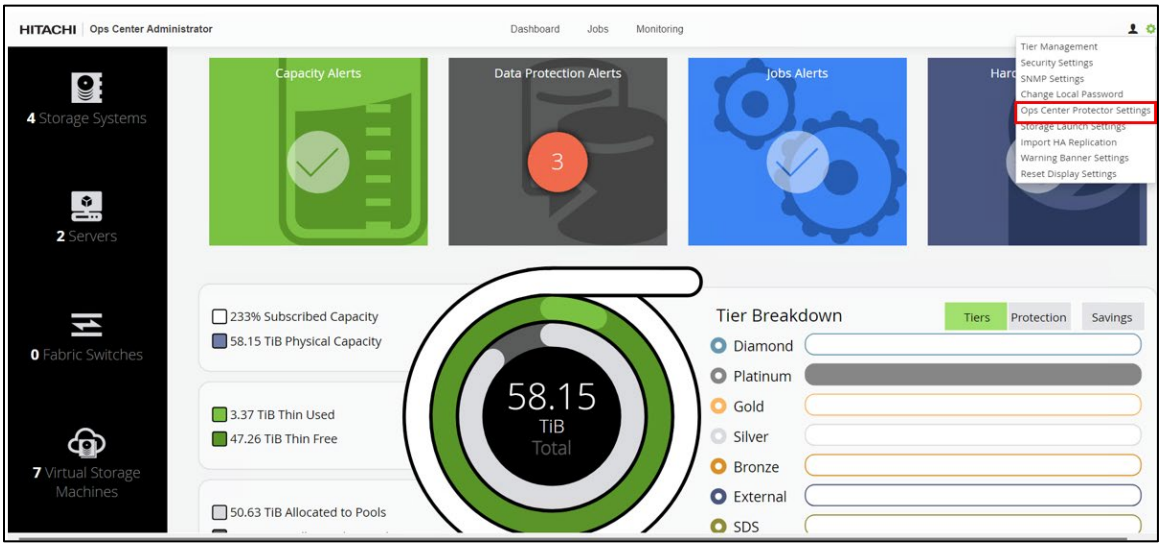
2. To verify the status of the High Availability setup, select the primary and secondary storage systems, then click **Proceed** as shown in the following screenshot:



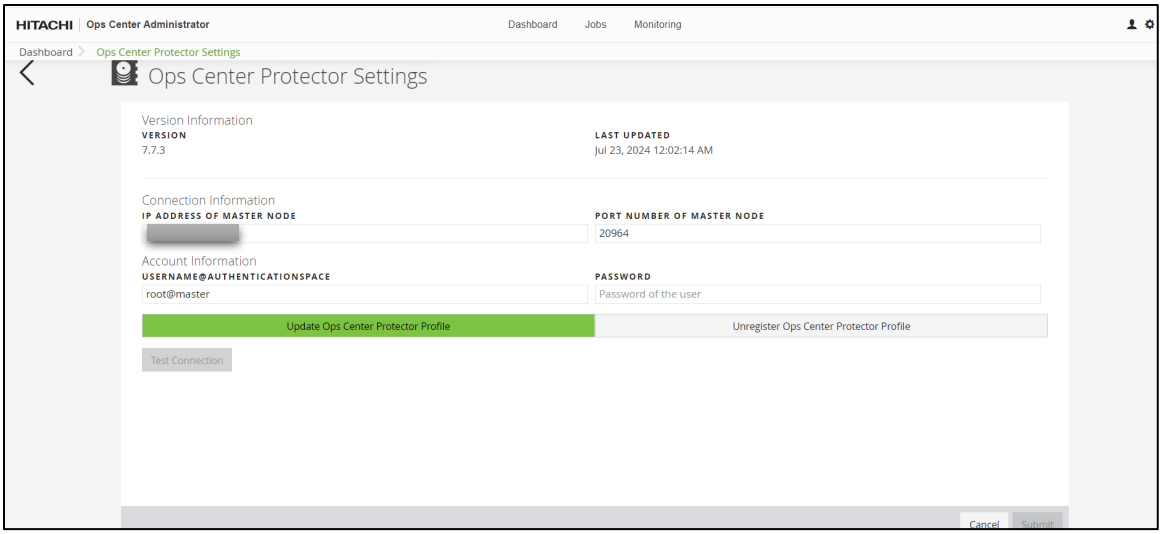
Verifying Integration of Ops Center Protector with Ops Center Administrator

Before setting up the GAD configuration, verify the connection between Ops Center Administrator and Ops Center Protector.

1. In the right side of the dashboard, click the **Settings** icon, and then select **Ops Center Protector Settings**.



2. Enter all the information, then click **Test Connection**. If the test is successful, click **Submit** to save the settings.

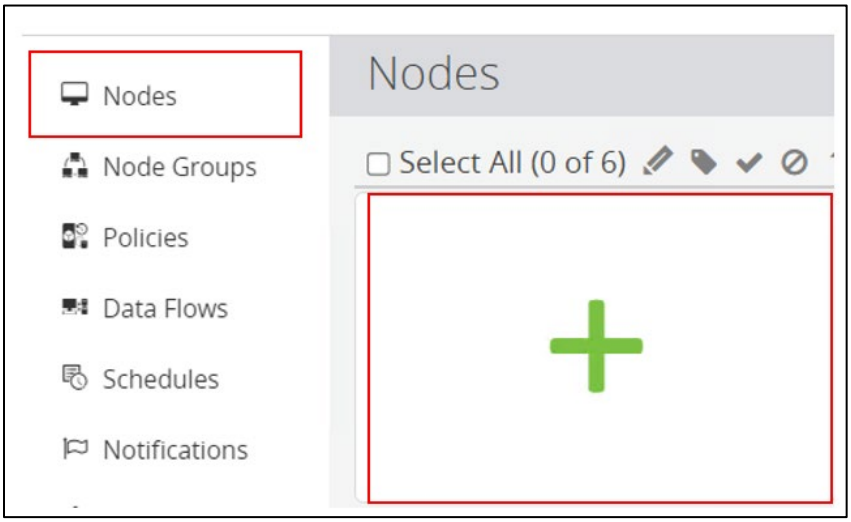


Note: You must enter the port number of the master node used during installation. The default port number is 44; however, the recommended port number is 20964.

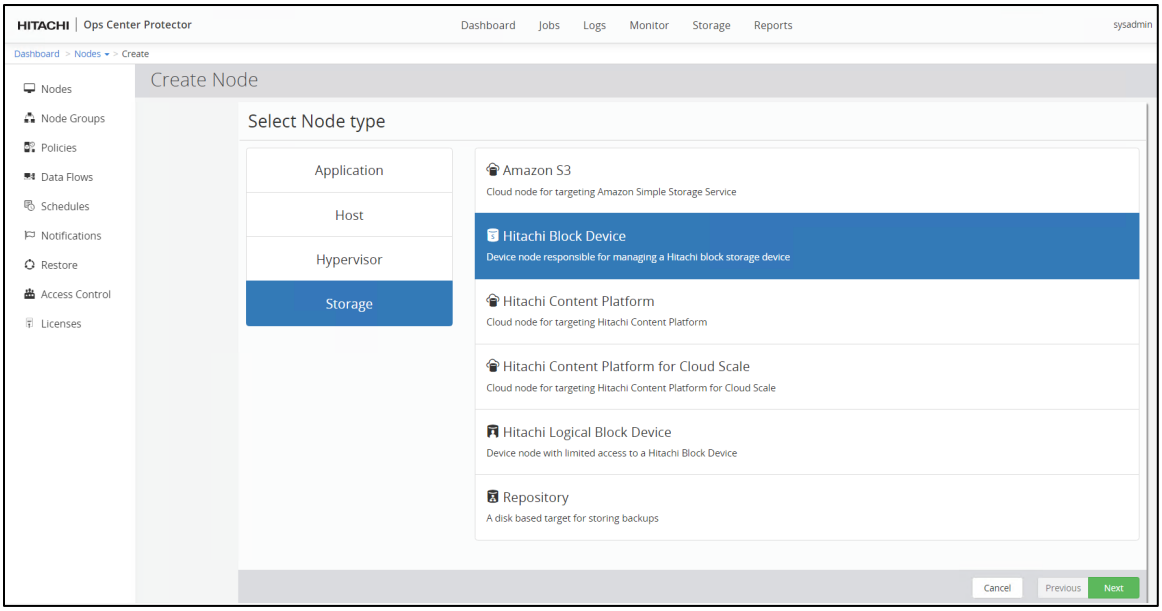
Onboarding a Storage System in Ops Center Protector

To onboard a storage system in Ops Center Protector, complete the following steps:

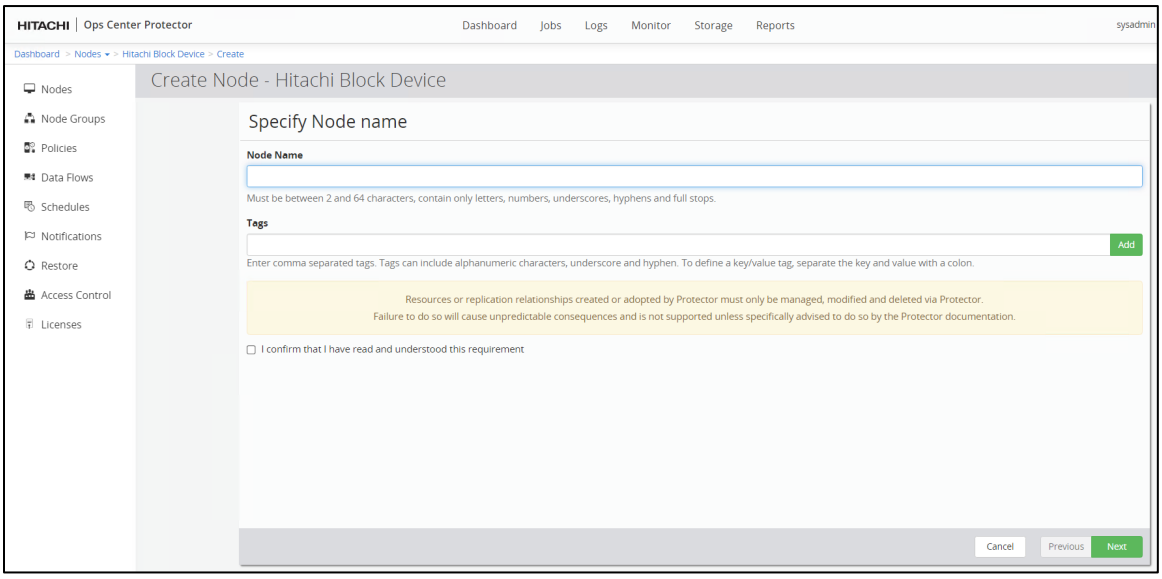
1. From the Ops Center Protector dashboard, navigate to **Nodes**, then click the '**+**' icon.



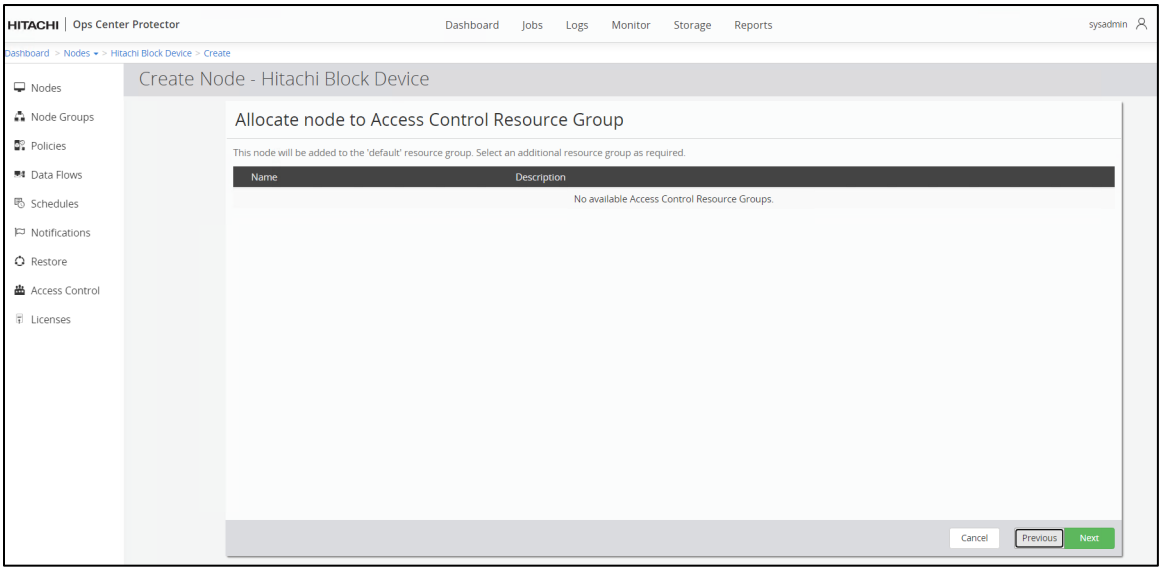
2. In the 'Create Node' page, select **Storage** as node type, and then select **Hitachi Block Device**.



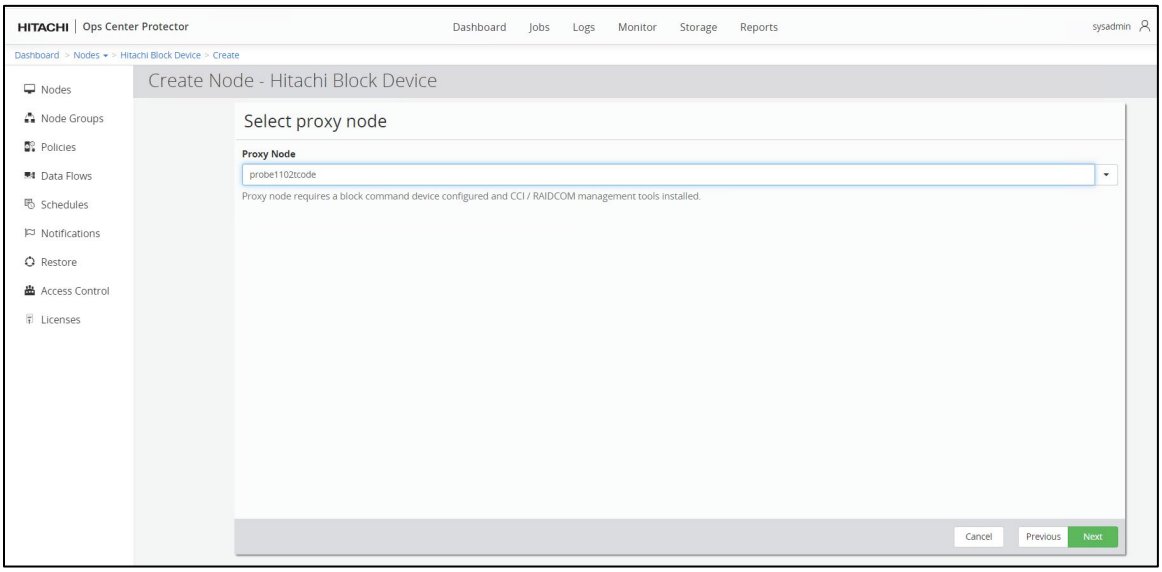
3. In the ‘Create Node - Hitachi Block Device’ page, enter the **Node Name**, select the confirmation box, and then click **Next**.



4. In the ‘Allocate node to Access Control Resource Group’ page, click **Next**.

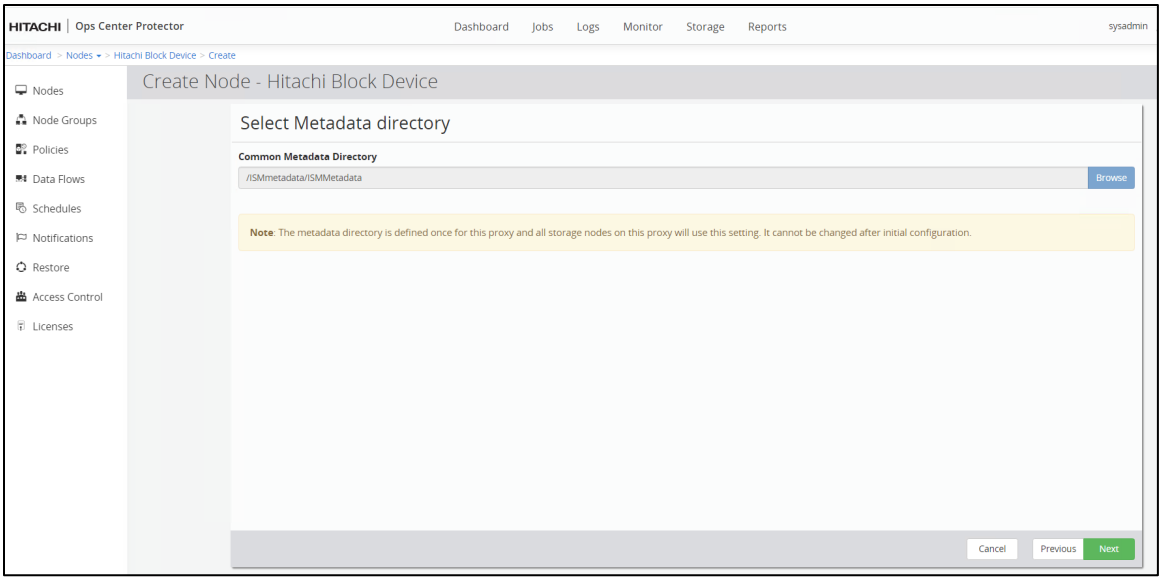


5. In the ‘Select proxy node’ page, select the Ops Center client node and click **Next**.



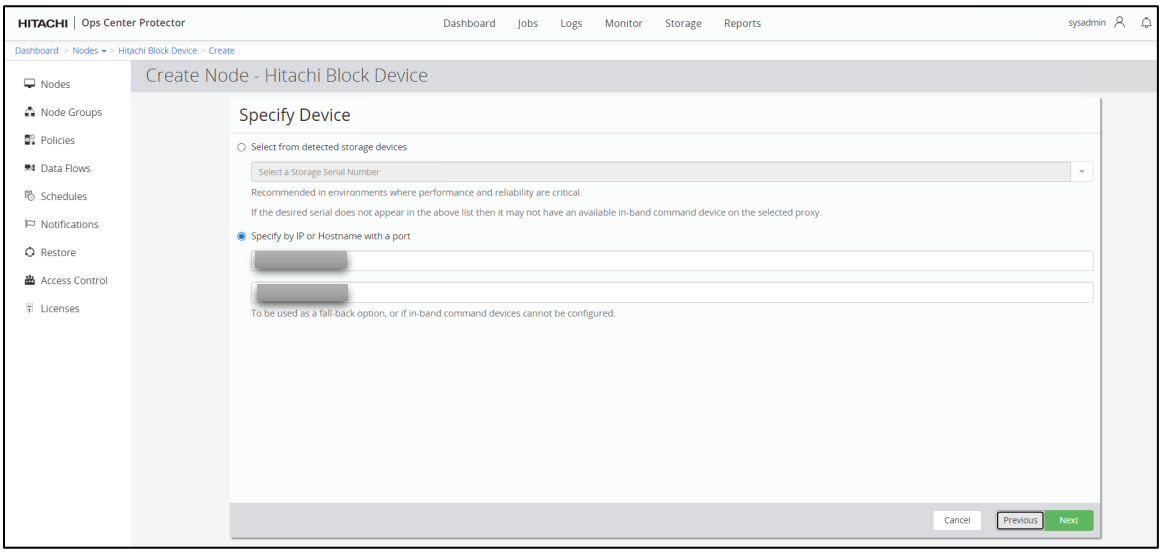
6. In the ‘Select Metadata directory’ page, select the directory and click **Next**.

   Note: When adding a Block Device for the first time, create or define a new metadata directory. If not, the directory is selected by default.

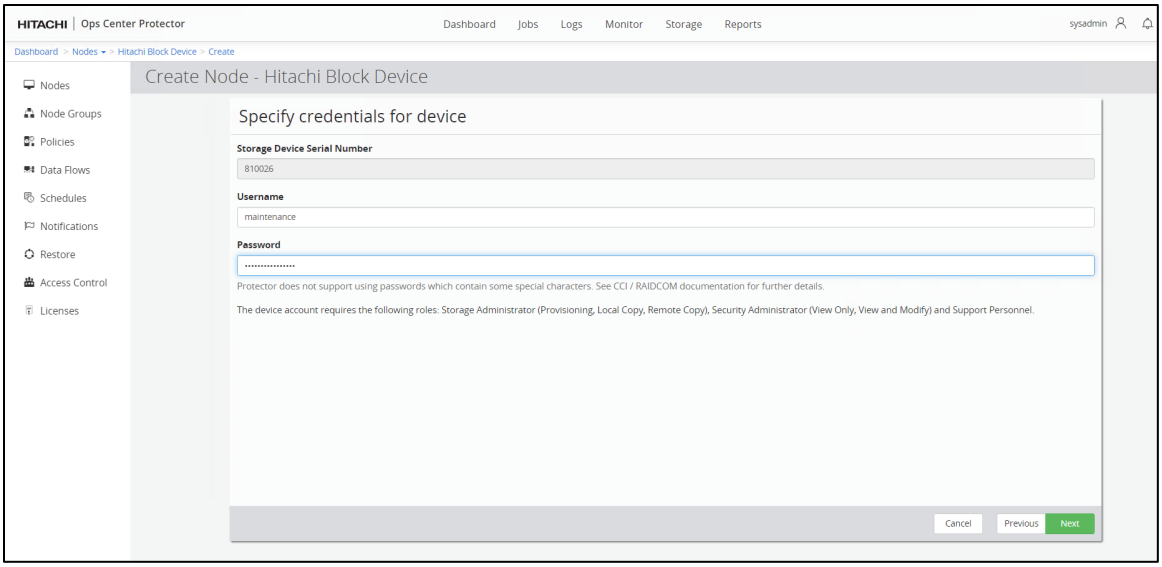


7. In the ‘Specify Device’ page, enter the IP address or Hostname and click **Next**.

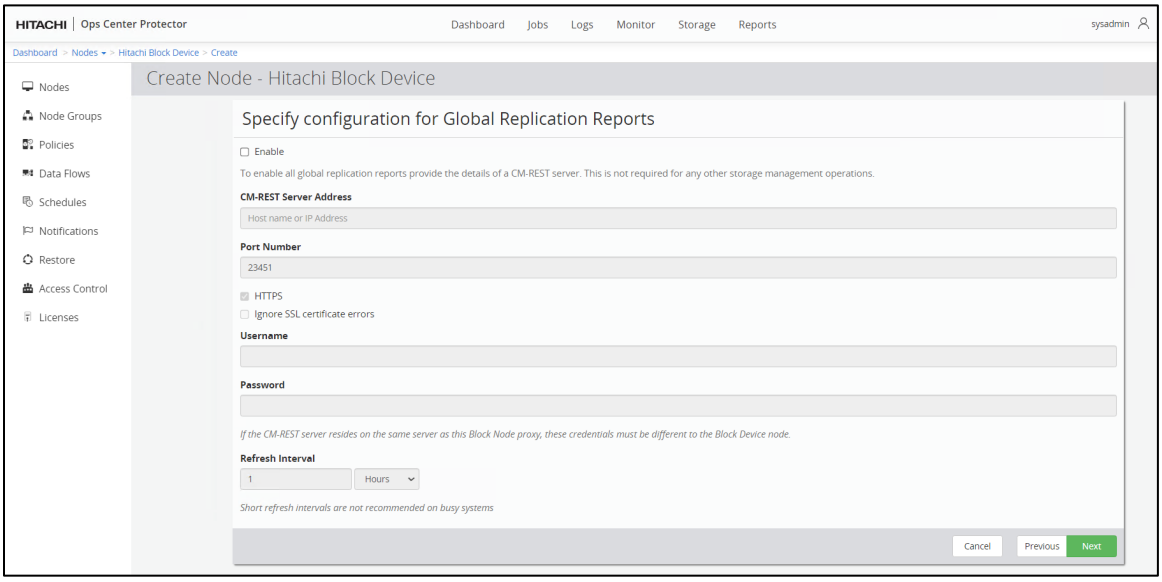
   Note: Use the default port.



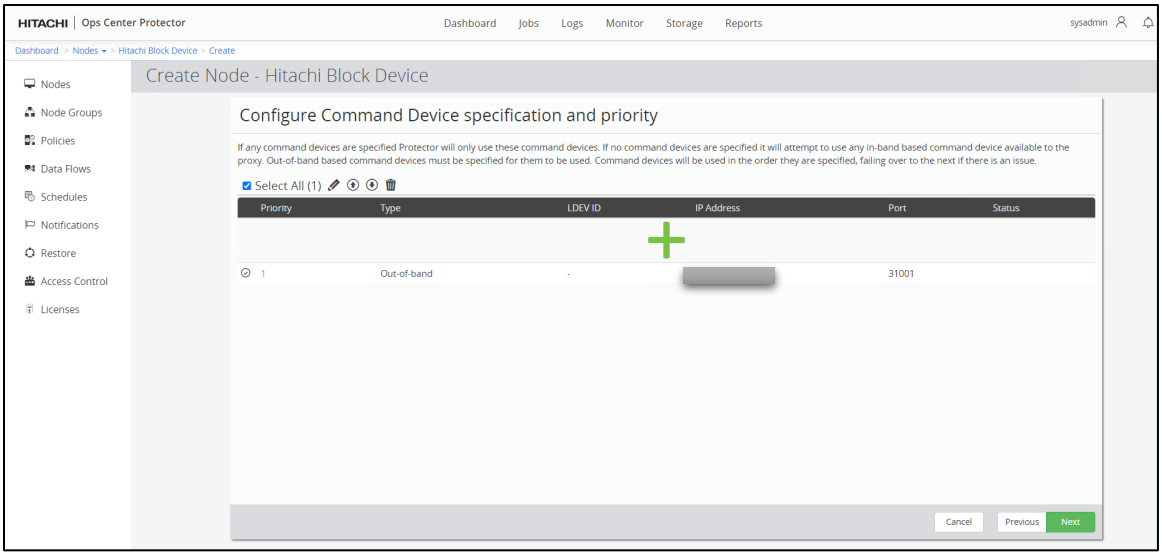
8. In the ‘Specify credentials for device’ page, enter the **Username** and **Password**, and then click **Next**.



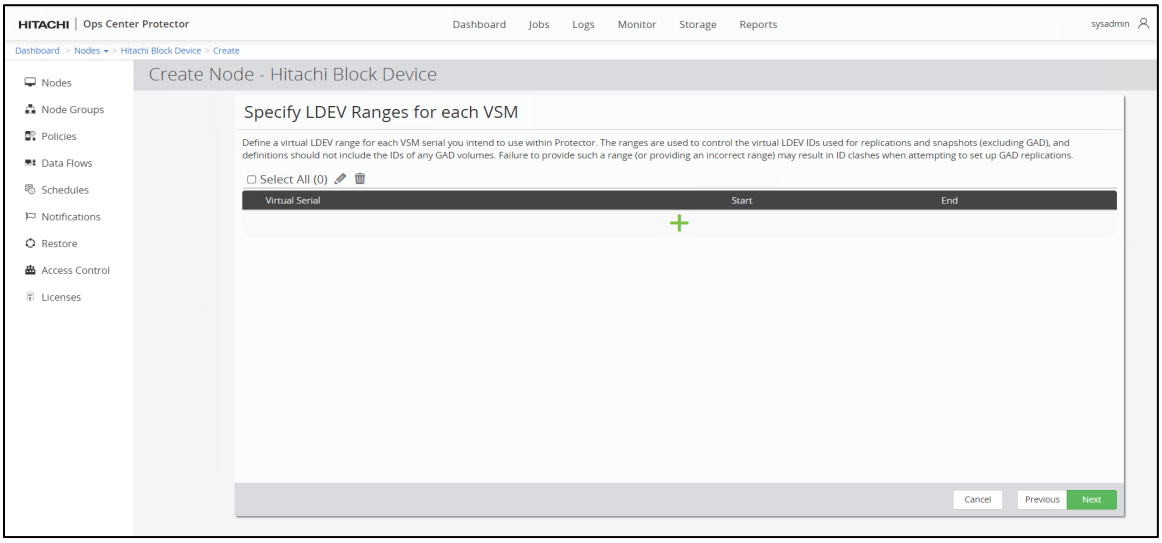
9. In the ‘Specify configuration for Global Replication Reports’ page, use the default values and click **Next**.



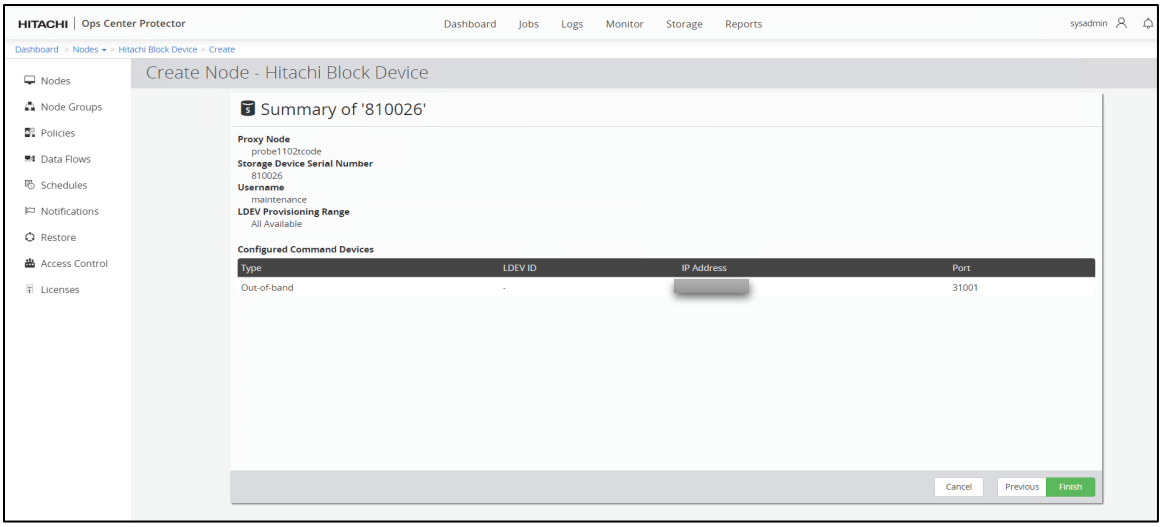
10. In the ‘Configure Command Device specification and priority’ page, select **Out-of-band** and click **Next**.



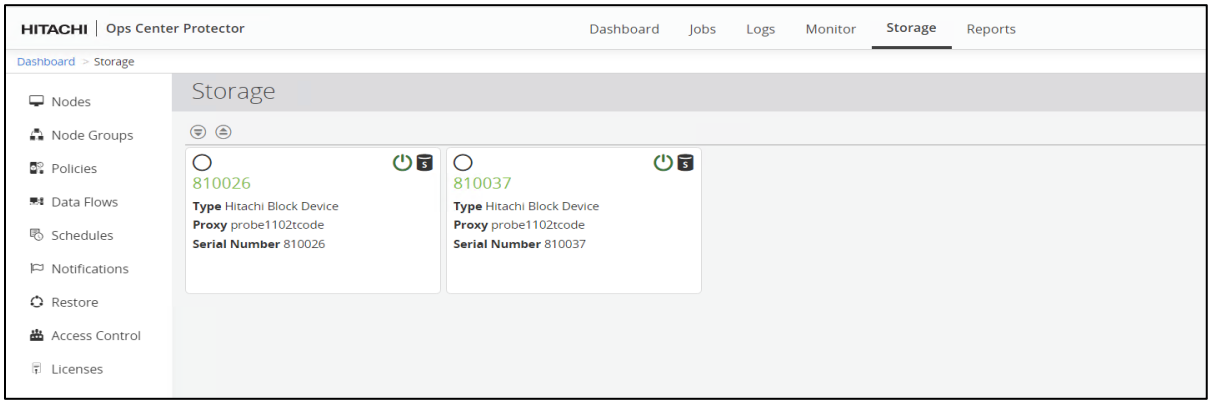
11. In the ‘Specify LDEV Ranges for each VSM’ page, click **Next**.



12. In the ‘Summary’ page, verify the details and click **Finish**.



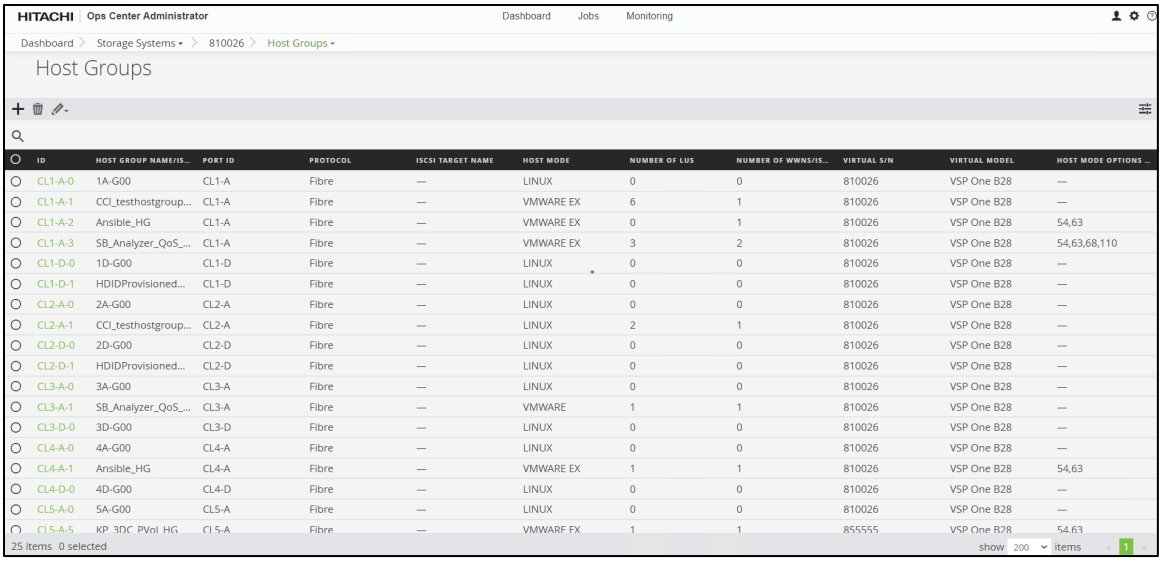
After onboarding, the added storage systems appear in the ‘Storage’ page.



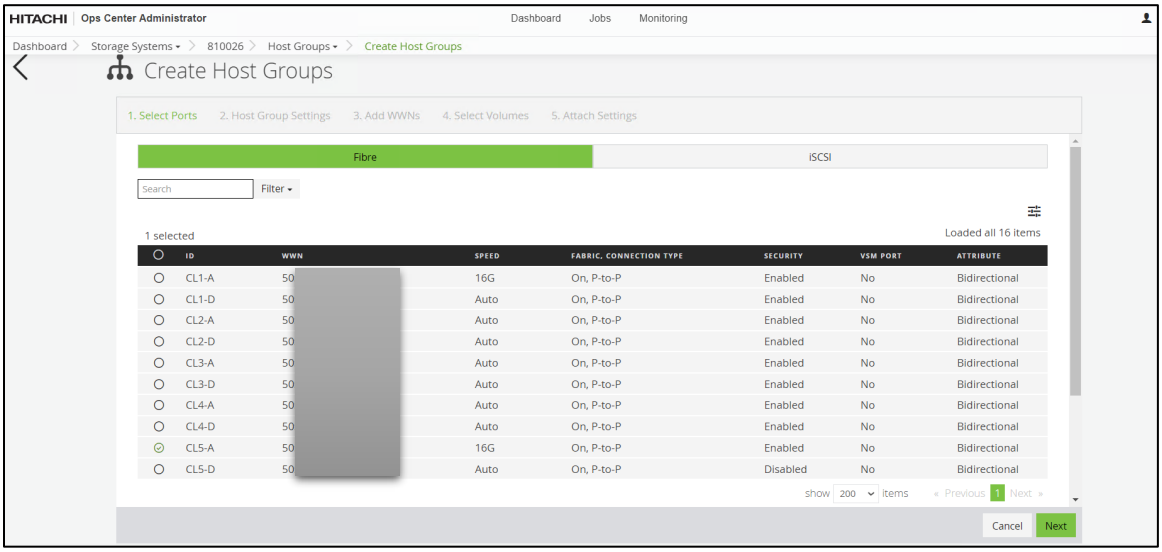
Creating a Host Group for GAD

To create a host group on the primary storage system, complete the following steps:

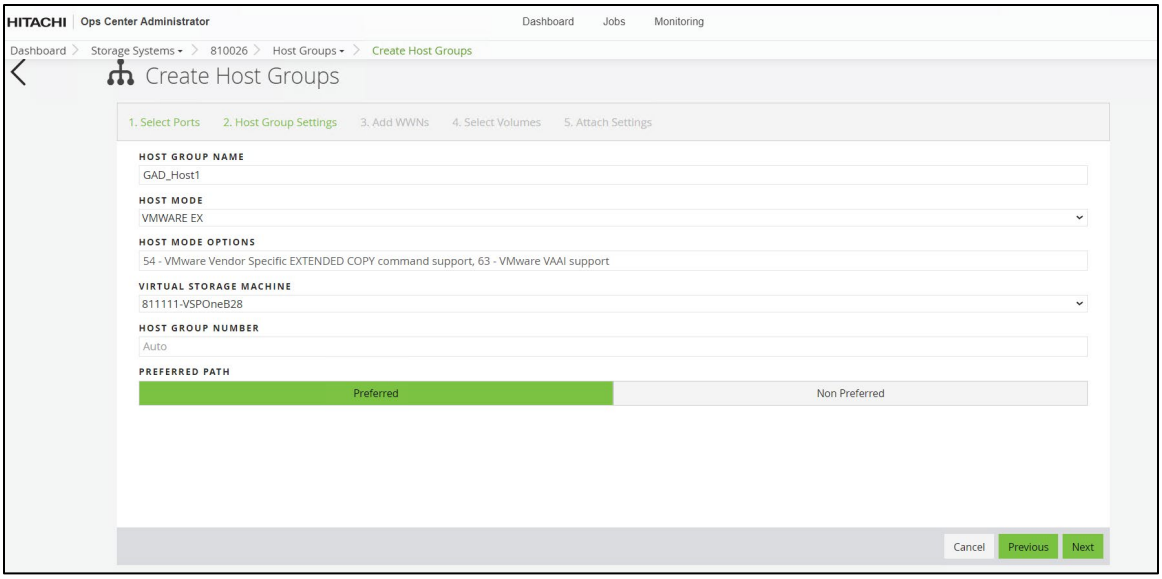
1. From the Ops Center Administrator dashboard, navigate to **Storage Systems** > **Host Group/iSCSI Target** and click the ‘**+**’ icon.



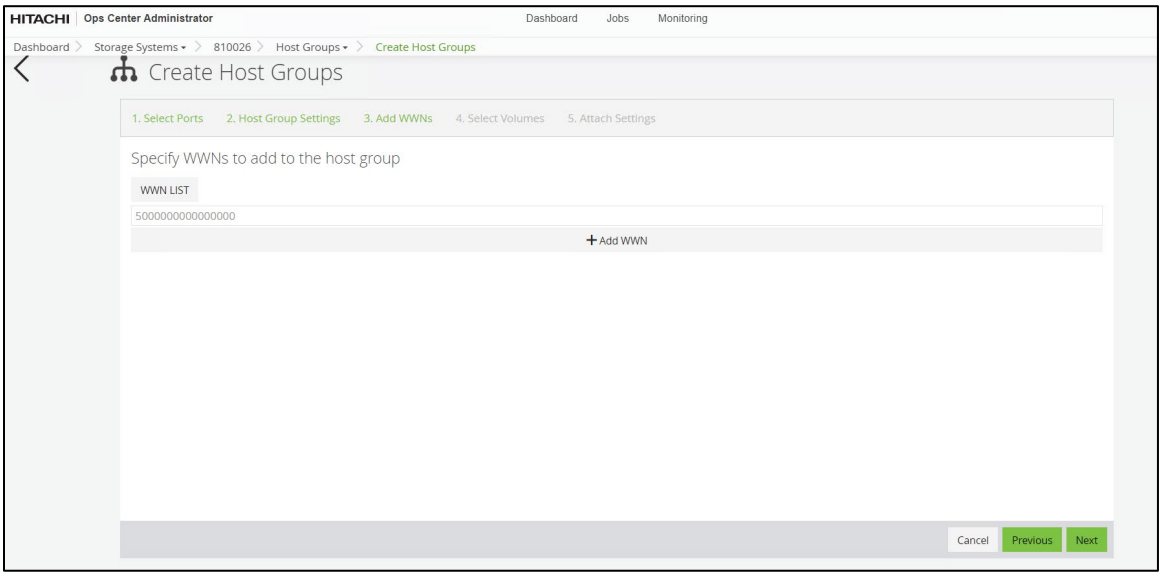
2. In the ‘Create Host Groups’ page, select the storage port and click **Next**.

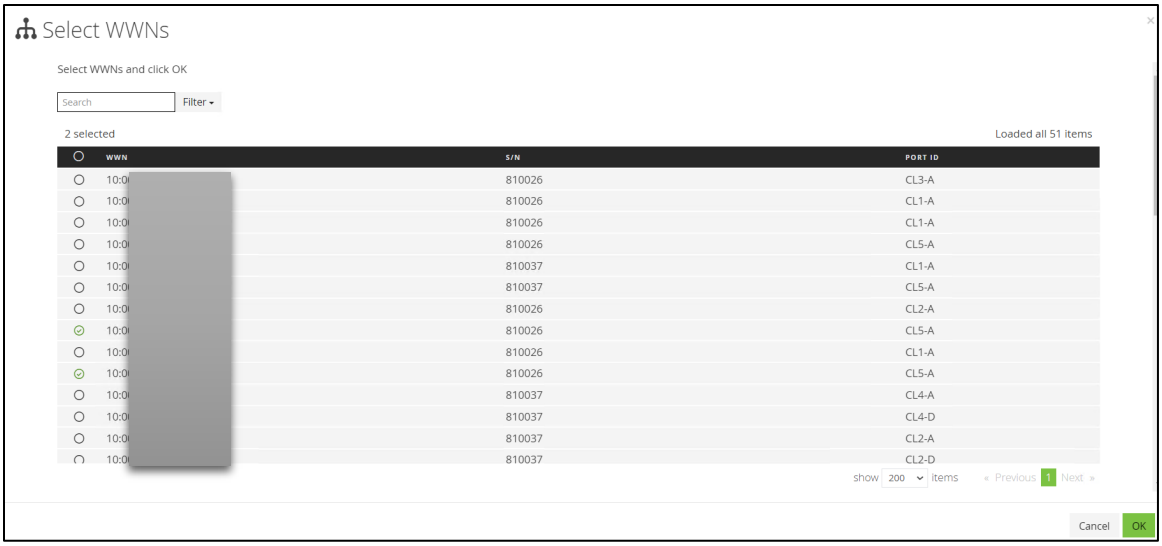


3. In the ‘Host Group Settings’ page, enter the information as shown in the following screenshot, and then click **Next**.

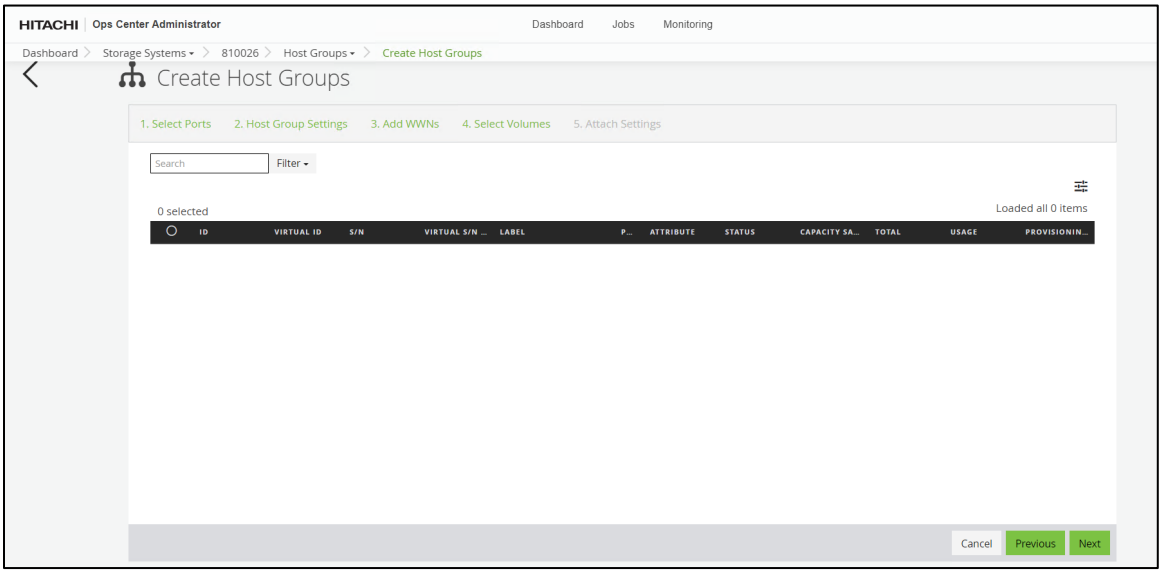


4. To add a WWN, click **WWN LIST**. Select the WWN that corresponds to the new server.

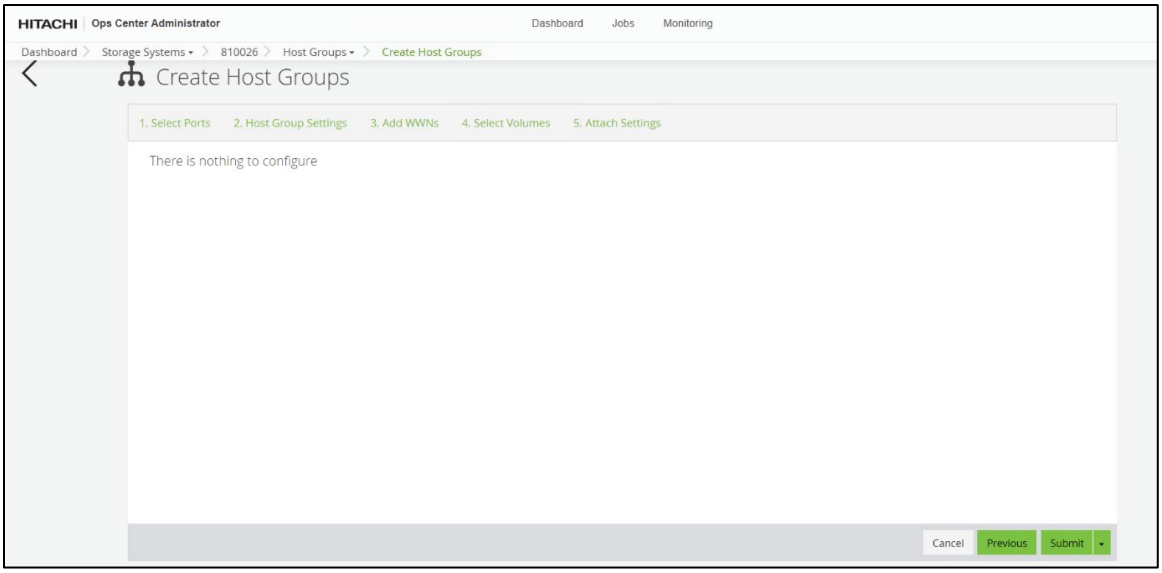




5. In the ‘Select Volumes’ page, click **Next**.



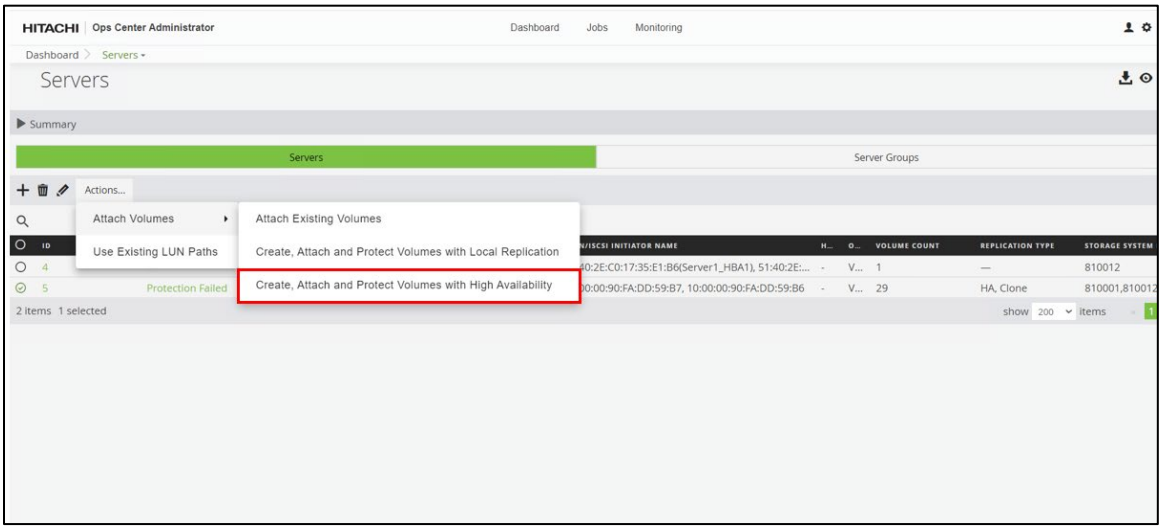
6. In the ‘Attach Settings’ page, click **Submit**.



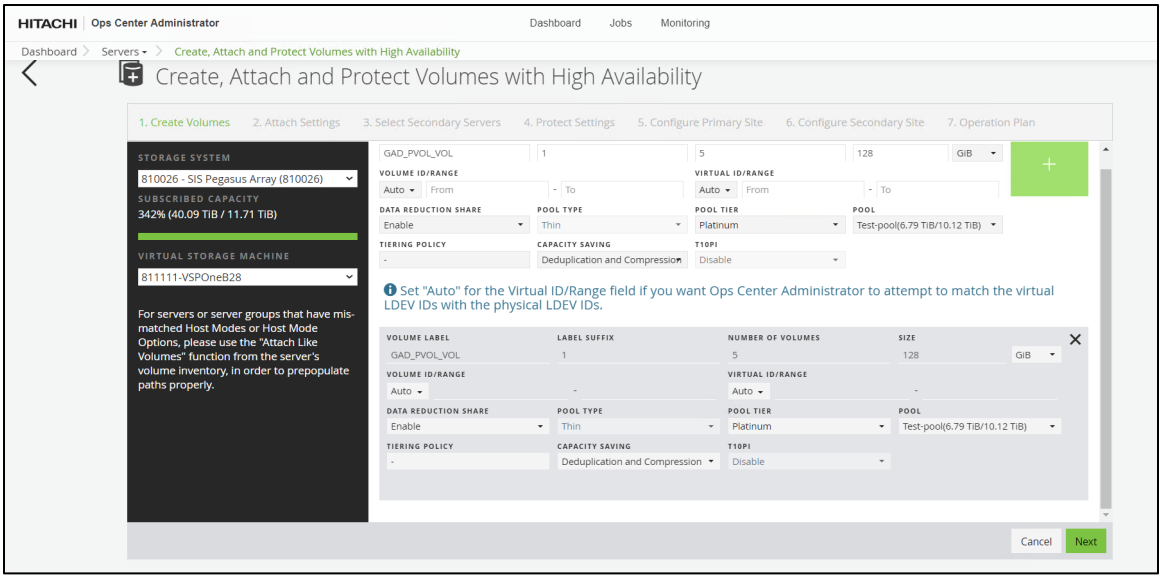
Similarly, create a GAD host group on the secondary storage system by following the same steps.

Creating a GAD Pair using High Availability

1. From the Ops Center Administrator dashboard, navigate to **Servers** > **Actions** menu, and then click **Create, Attach and Protect Volumes with High Availability**.

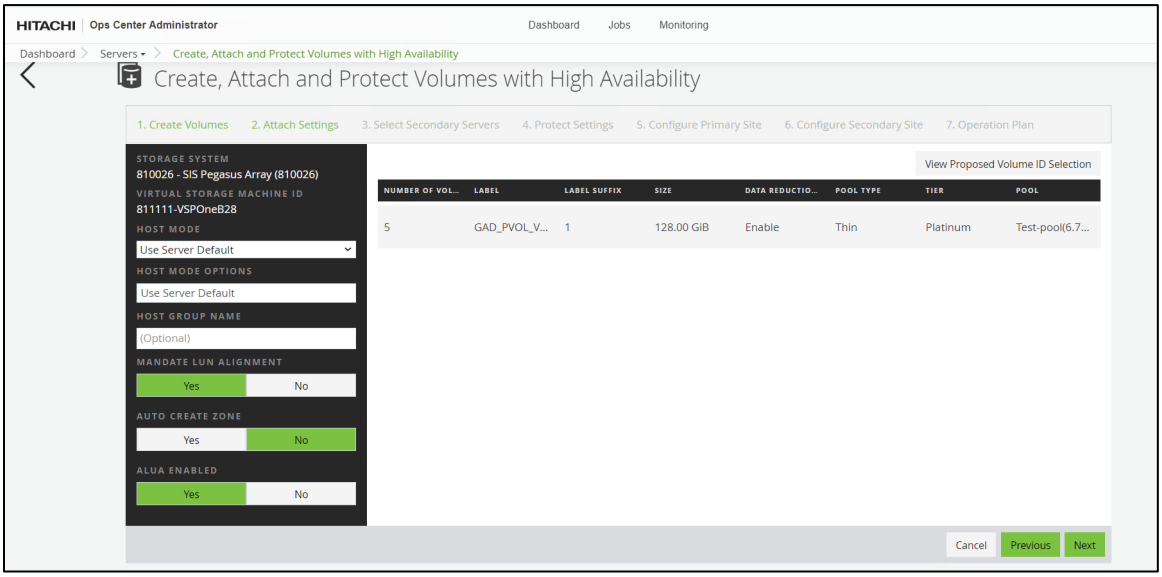


2. In the ‘Create, Attach and Protect Volumes with High Availability’ page, enter the information as shown in the following screenshot, and then click **Next**.



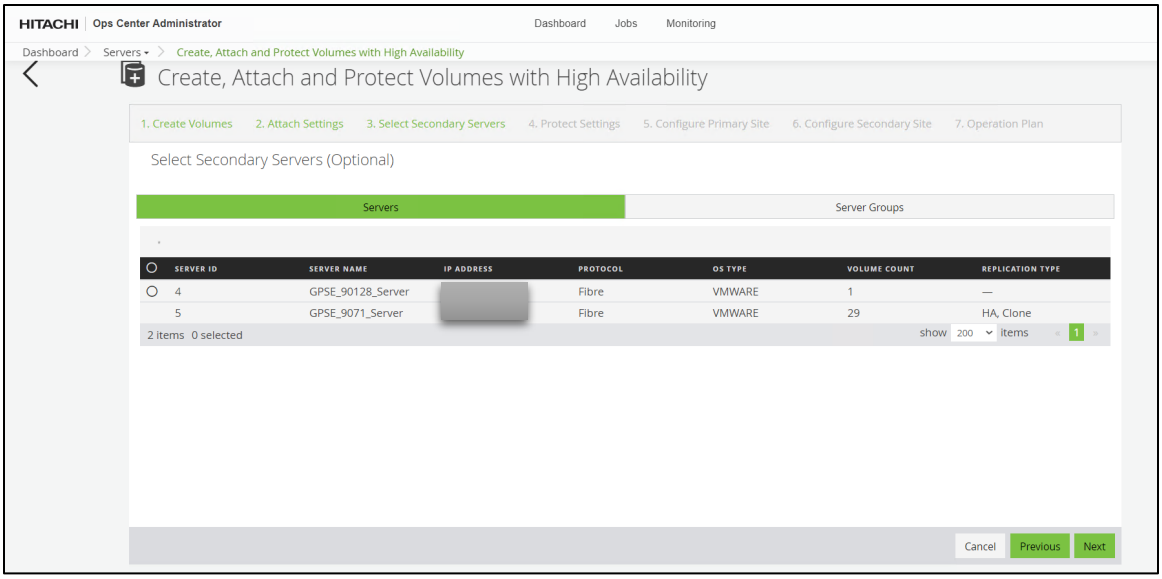
Note: By not specifying the **Volume ID/Range** manually, Ops Center Administrator will automatically assign the volumes.

8. In the ‘Attach Settings’ page, enter the information as shown in the following screenshot, and then click **Next**.

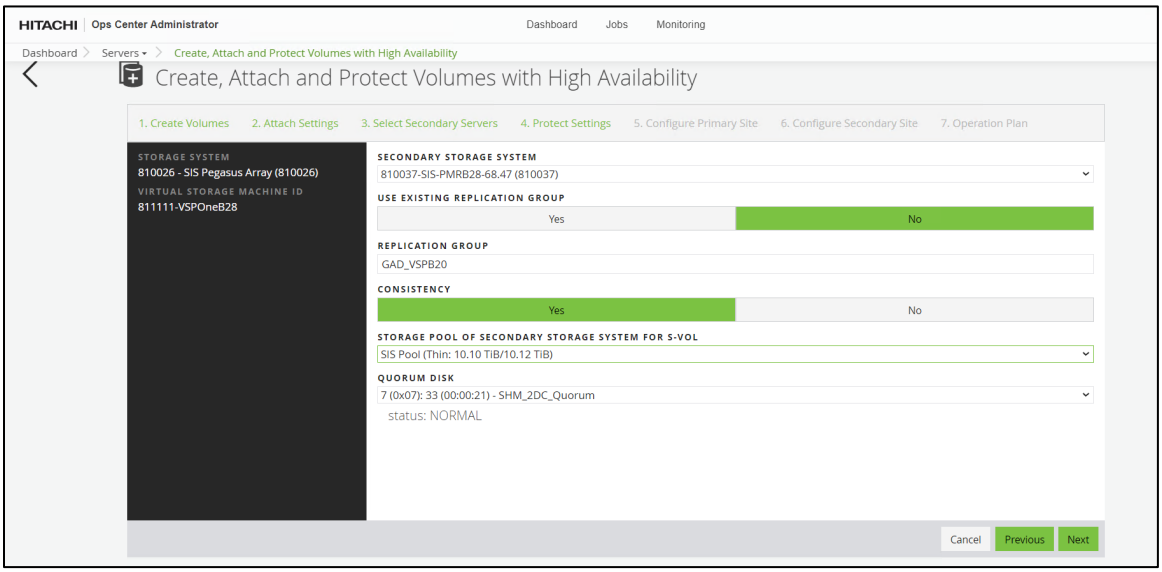


Note: This test was conducted in our lab environment using a single server. For production environments, you can add a secondary server based on the requirements.

9. In the ‘Select Secondary Servers’ page, select the secondary server and click **Next**.

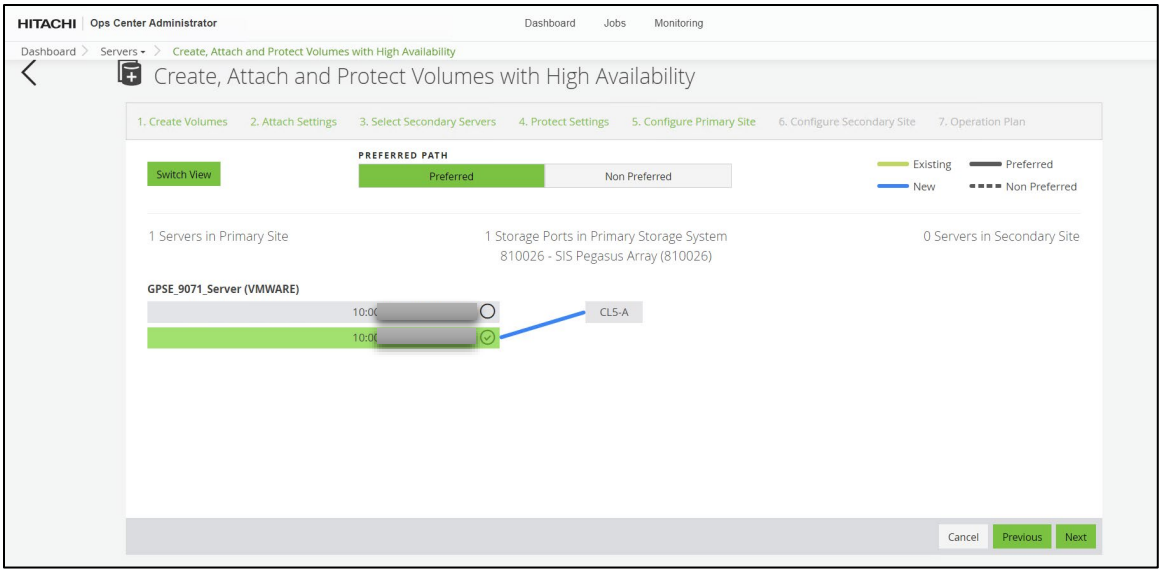


10. In the ‘Protect Settings’ page, select the **Secondary Storage System**, select the **Use Existing Replication Group** and **Consistency** options, select the **Storage Pool Of Secondary Storage System For S-VOL** where the S-VOL will reside, and the **Quorum Disk** as shown in the following screenshot, and then click **Next**.

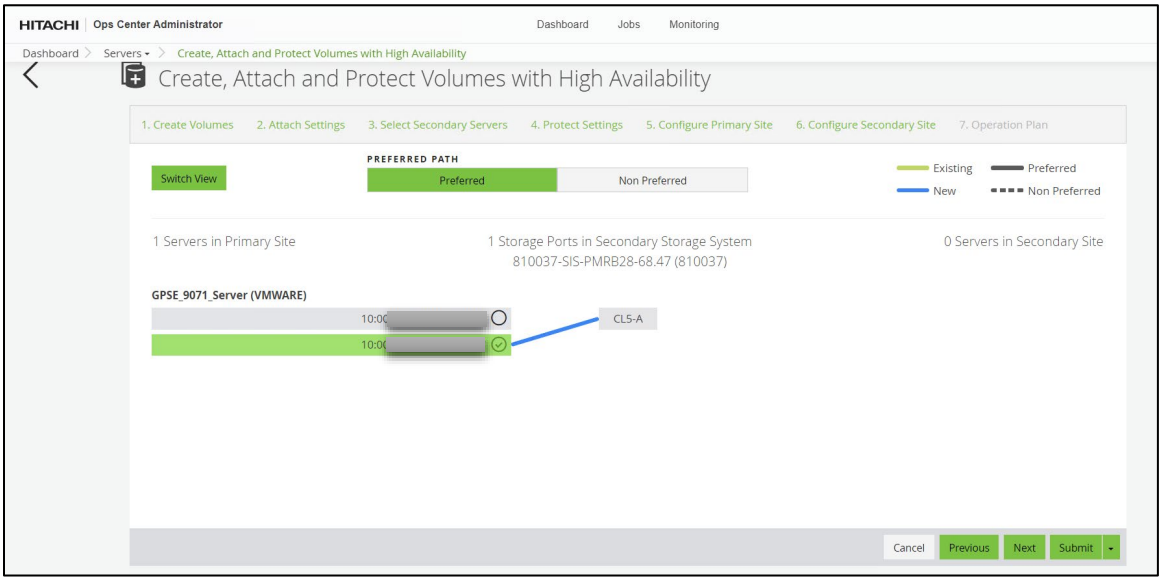


Note: Single or multiple paths can be created between the servers and the port reserved for GAD on the primary storage system. For a production environment, it is recommended to have multiple paths.

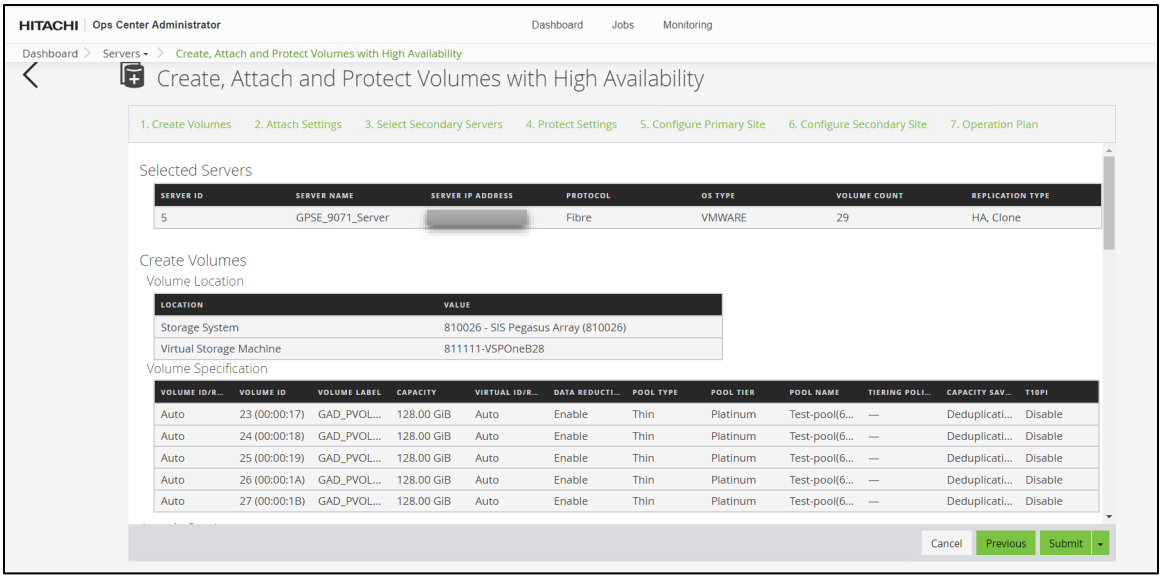
11. In the ‘Configure Primary Site’ page, select the server, select the storage port, and then click **Next**.



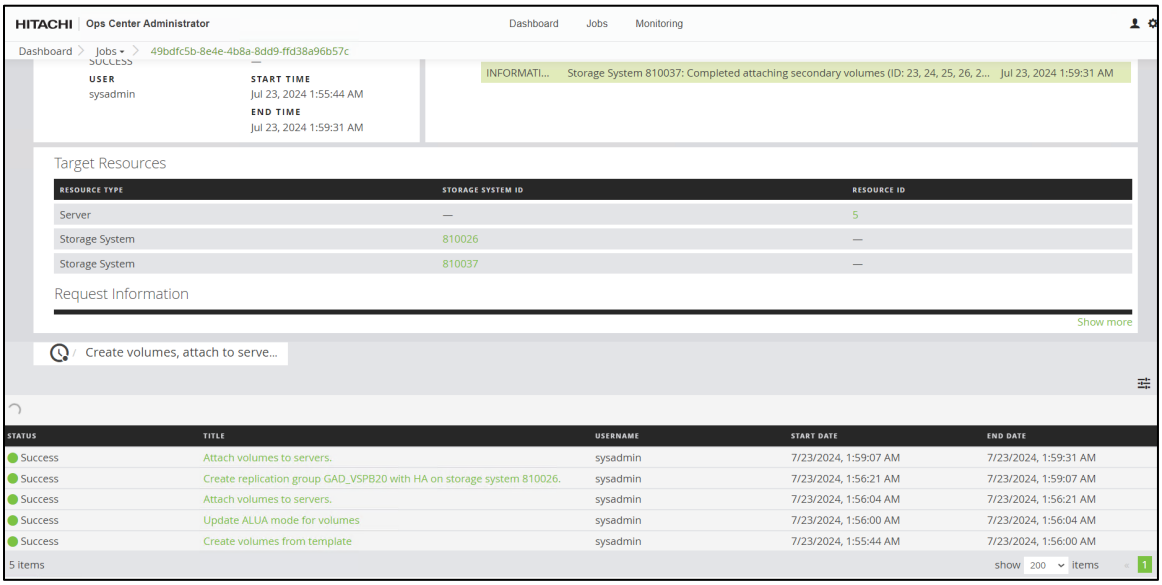
12. In the ‘Configure Secondary Site’ page, select the server, select the storage port, and then click **Next**.
    Note: Click **Submit** to proceed without verifying the details.

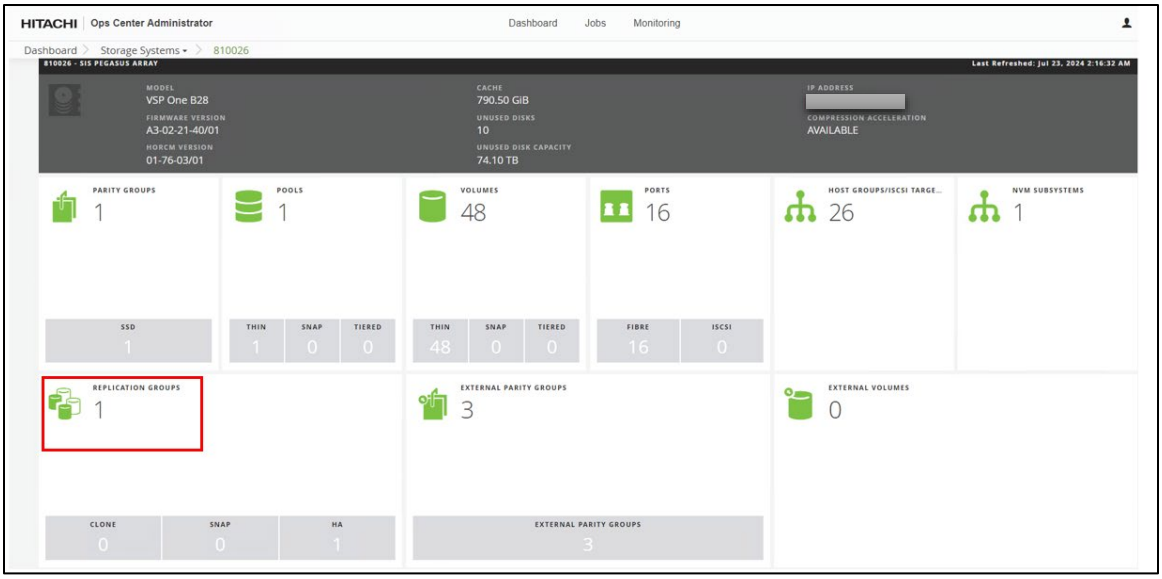


13. In the ‘Operation Plan’ page, verify the details and click **Submit**.

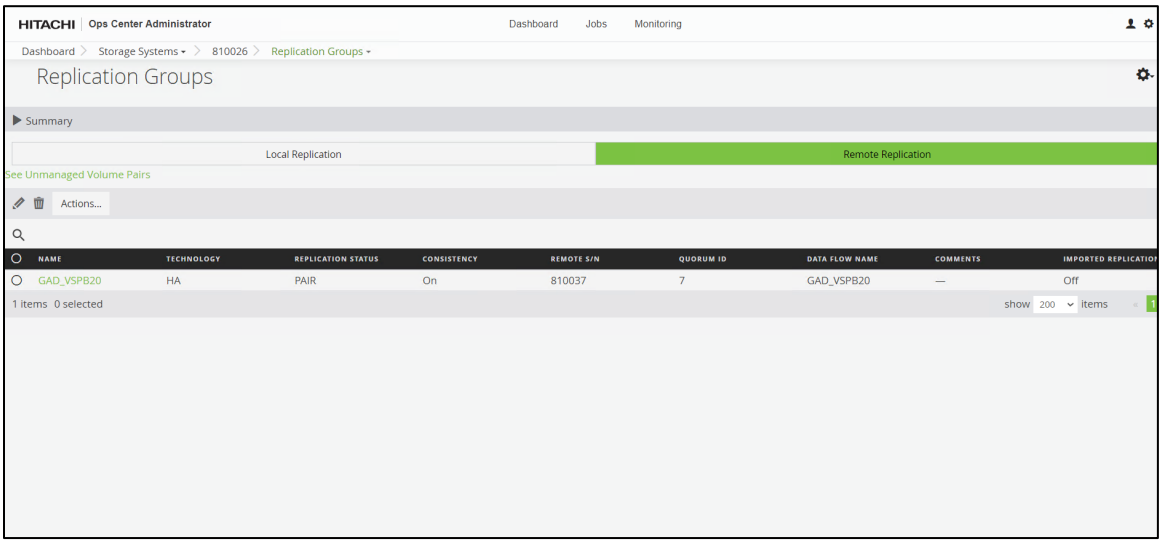


14. To verify pair status, from the dashboard navigate to **Jobs** > **Storage System** and click **Replication Groups**.

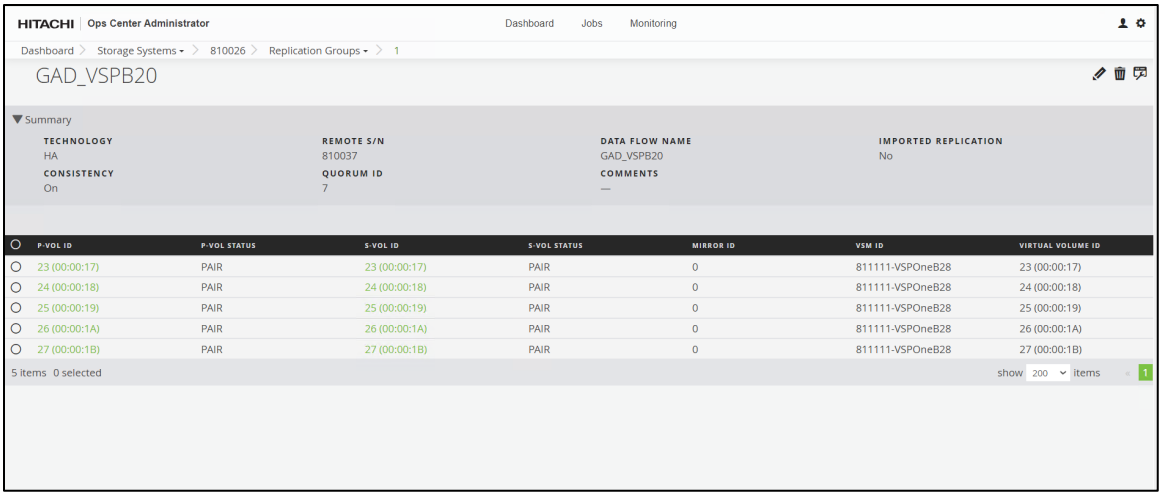


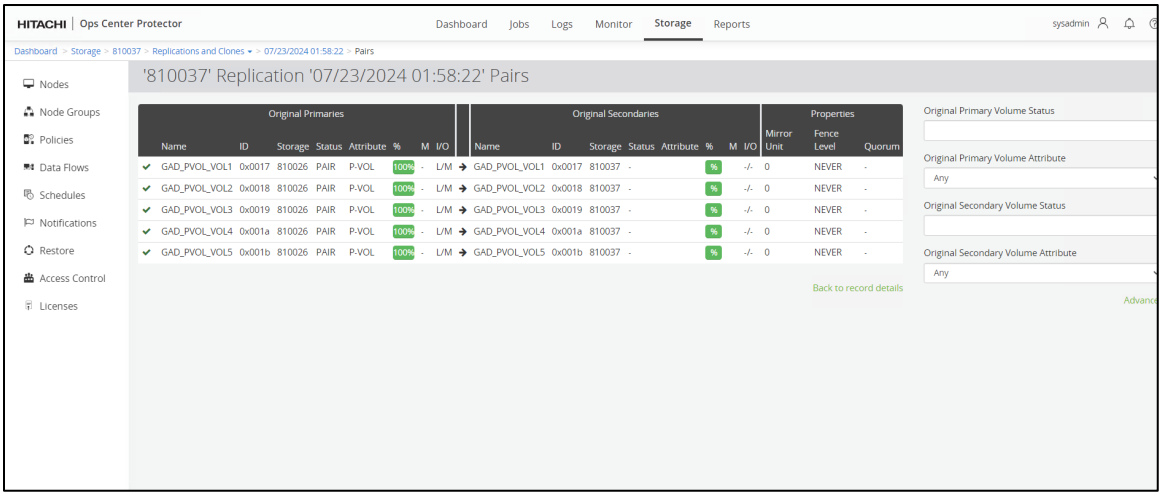


15. In the Remote Replication tab, select the replication group.



You can view the pair status between the P-VOL and S-VOL.


HITACHI | Ops Center Administrator
Dashboard
Jobs
Monitoring
Dashboard > Storage Systems > 810026 > Replication Groups > 1
GAD_VSPB20
Summary
TECHNOLOGY
HA
REMOTE S/N
810037
DATA FLOW NAME
GAD_VSPB20
IMPORTED REPLICATION
No
CONSISTENCY
On
QUORUM ID
7
COMMENTS
—
P-VOL ID
P-VOL STATUS
S-VOL ID
S-VOL STATUS
MIRROR ID
VSM ID
VIRTUAL VOLUME ID
23 (00:00:17) PAIR 23 (00:00:17) PAIR 0 811111-VSPOneB28 23 (00:00:17)
24 (00:00:18) PAIR 24 (00:00:18) PAIR 0 811111-VSPOneB28 24 (00:00:18)
25 (00:00:19) PAIR 25 (00:00:19) PAIR 0 811111-VSPOneB28 25 (00:00:19)
26 (00:00:1A) PAIR 26 (00:00:1A) PAIR 0 811111-VSPOneB28 26 (00:00:1A)
27 (00:00:1B) PAIR 27 (00:00:1B) PAIR 0 811111-VSPOneB28 27 (00:00:1B)
5 items 0 selected
show 200 items


HITACHI | Ops Center Protector
Dashboard
Jobs
Logs
Monitor
Storage
Reports
sysadmin
Dashboard > Storage > 810037 > Replications and Clones > 07/23/2024 01:58:22 > Pairs
'810037' Replication '07/23/2024 01:58:22' Pairs
Nodes
Node Groups
Policies
Data Flows
Schedules
Notifications
Restore
Access Control
Licenses
Original Primaries
Original Secondaries
Properties
Name ID Storage Status Attribute % M I/O
Mirror Unit
Fence Level
Quorum
GAD_PVOL_VOL1 0x0017 810026 PAIR P-VOL 100% L/M GAD_PVOL_VOL1 0x0017 810037 100% -/- 0 NEVER
GAD_PVOL_VOL2 0x0018 810026 PAIR P-VOL 100% L/M GAD_PVOL_VOL2 0x0018 810037 100% -/- 0 NEVER
GAD_PVOL_VOL3 0x0019 810026 PAIR P-VOL 100% L/M GAD_PVOL_VOL3 0x0019 810037 100% -/- 0 NEVER
GAD_PVOL_VOL4 0x001a 810026 PAIR P-VOL 100% L/M GAD_PVOL_VOL4 0x001a 810037 100% -/- 0 NEVER
GAD_PVOL_VOL5 0x001b 810026 PAIR P-VOL 100% L/M GAD_PVOL_VOL5 0x001b 810037 100% -/- 0 NEVER
Back to record details
Original Primary Volume Status
Original Primary Volume Attribute
Any
Original Secondary Volume Status
Original Secondary Volume Attribute
Any

Conclusion

This document enables you to effectively onboard VSP One Block 20 storage systems and manage them using Ops Center Administrator. In addition, this document provides detailed instructions for performing essential tasks such as provisioning the storage system and securing data with GAD using Ops Center Administrator, ensuring a streamlined and reliable management process.

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com