Redbooks
ibm.com/redbooks

IBM Storage Virtualize and VMware: Integrations, Implementation and Best Practices

Vasfi Gucer

Federica Donald

Warren Hawkins

Markus Oscheka

Jared Pateman

Storage

IBM

Redbooks

IBM Redbooks

IBM Storage Virtualize and VMware: Integrations, Implementation and Best Practices

May 2024

SG24-8549-00

Note: Before using this information and the product it supports, read the information in “Notices” on page xi.

First Edition (May 2024)

This edition applies to IBM Storage Virtualize Version 8.6 and VMware vSphere Version 8.0.

Contents

Notices ix
Trademarks x

Preface xi
Authors xi
Now you can become a published author, too! xiii
Comments welcome xiii
Stay connected to IBM Redbooks xiii

Chapter 1. Introduction 1
1.1 IBM and VMware 2
1.2 Overview of IBM Storage Virtualize and IBM Storage FlashSystem 2
1.2.1 IBM Storage Virtualize 2
1.2.2 IBM Storage FlashSystem 3
1.2.3 Key IBM Storage Virtualize terminology 4
1.2.4 Key VMware terminology 5
1.3 Overview of IBM Storage FlashSystem with VMware 6

Chapter 2. Host and storage connectivity 7
2.1 Test environment implementation 8
2.1.1 IBM Storage Virtualize host clusters 8
2.1.2 Use cases for implementing throttles 10
2.1.3 Data reduction pools 11
2.2 Host connectivity protocols 12
2.2.1 iSCSI 13
2.2.2 iSER 13
2.2.3 NVMe over Fibre Channel 14
2.2.4 SCSI Fibre Channel 16
2.2.5 NVMe over Remote Direct Memory Access 17
2.2.6 NVMe over TCP 17
2.3 Multi-path considerations 18
2.3.1 Native multipathing path-selection policies 18
2.3.2 High-performance plug-in and path selection policies 20
2.4 Zoning considerations 22
2.5 Recommendations for tuning ESXi hosts 24

Chapter 3. VMware vSphere storage configurations 25
3.1 Datastore types 26
3.1.1 vSphere Virtual Machine File System 26
3.1.2 Raw Device Mappings 30
3.1.3 VMware vSphere Virtual Volume 31
3.2 VMware vSphere Storage APIs – Array Integration 33
3.2.1 Atomic Test and Set / SCSI Compare and Write 34
3.2.2 Extended copy 35
3.2.3 WRITE_SAME 36
3.2.4 SCSI UNMAP command 36

Chapter 4. Preparing for disaster recovery 41
4.1 Introduction 42

4.2 Volume groups 42
4.2.1 Policy-based replication 42
4.2.2 Volume group snapshots 43
4.2.3 Safeguarded Copy 43
4.3 Copy services overview 43
4.3.1 Volume group snapshots 44
4.3.2 Safeguarded Copy 44
4.3.3 Policy-based replication 45
4.3.4 FlashCopy 46
4.3.5 Metro Mirror 46
4.3.6 Global Mirror 46
4.3.7 Policy-based replication 47
4.3.8 Remote copy consistency groups 47
4.3.9 VMware Site Recovery Manager 47
4.3.10 Storage Replication Adapter 48
4.4 Storage Replication Adapter with VMware Site Recovery Manager 49
4.4.1 Storage replication adapter planning 50
4.4.2 Storage Replication Adapter for VMware installation 53
4.4.3 Storage Replication Adapter configuration and usage 55
4.5 IBM HyperSwap with VMware vSphere Metro Storage Cluster 70
4.5.1 IBM HyperSwap 71
4.5.2 VMware vSphere Metro Storage Cluster 75
4.5.3 IBM HyperSwap with VMware vSphere Metro Storage 77

Chapter 5. Embedded VASA Provider for Virtual Volumes (vVol) 83
5.1 Overview 84
5.1.1 Supported platforms for the Embedded VASA Provider 84
5.1.2 Feature comparison between the Embedded VASA Provider and IBM Spectrum Connect 85
5.2 System prerequisites 85
5.2.1 Preparing IBM Storage Virtualize for vVol 85
5.2.2 Configuring the NTP server 87
5.2.3 Configuring a storage system certificate 87
5.2.4 Exporting Root Certificate and adding to vCenter truststore 91
5.2.5 Preparing ESXi hosts for vVol connectivity 93
5.3 Enabling vVols by using an Embedded VASA Provider 99
5.3.1 Parent pool 100
5.3.2 Child pool (vVol-enabled Storage Container) 101
5.3.3 Provisioning policy 101
5.3.4 Storage credentials 101
5.3.5 Registering the Storage Provider in vSphere 102
5.3.6 Creating the vVol datastore 105
5.3.7 Provisioning additional vVol datastores 108
5.4 Migrating from existing IBM Spectrum Connect vVol configurations 111
5.4.1 Supported migration path 111
5.4.2 VM migrations by using Storage vMotion 111
5.4.3 Removing the vVol IBM Spectrum Connect configuration from vCenter 112
5.5 Decommissioning IBM Spectrum Connect 115
5.5.1 Identifying and removing the vVol child pools for IBM Spectrum Connect 115
5.5.2 Removing the user account that is used by IBM Spectrum Connect 117
5.5.3 Migrating virtual machines to the vVol datastore 118

Chapter 6. Overview of the IBM Storage plug-in for vSphere 125

6.1 Supported platforms for the IBM Storage plug-in for vSphere 126
6.2 Architecture of the IBM Storage plug-in for vSphere. 126
6.2.1 Required resources. 126
6.3 Downloading and deploying the OVA 127
6.3.1 First time boot 133
6.3.2 Registering and unregistering the plug-in 134
6.3.3 Unregistering the plug-in. 135
6.3.4 Checking the status of the plug-in. 136
6.4 Upgrading from a previous version 137
6.4.1 What you need to know before upgrading 137
6.4.2 Upgrade process. 137
6.4.3 Updating Photon OS packages. 138
6.5 Using the dashboard 138
6.5.1 Navigating to the dashboard 138
6.5.2 Adding storage systems 139
6.5.3 Refreshing the inventory of registered storage systems. 142
6.5.4 Editing storage systems 142
6.5.5 Deleting storage systems 144
6.5.6 Viewing more information about storage systems 145
6.6 Datastore actions and panels 146
6.6.1 Creating datastore(s) 146
6.6.2 Summary panel. 150
6.6.3 Expanding a datastore 151
6.6.4 Datastore snapshots 152
6.6.5 Creating a new datastore from a snapshot 153
6.6.6 Deleting a datastore 158
6.7 Host panels 159
6.7.1 Summary panel. 159
6.7.2 Configure panel. 160
6.7.3 Creating a new host 161
6.8 Cluster panels 162
6.8.1 Summary panel. 162
6.8.2 Configuration panel. 163
6.9 Enforcing practical usage behavior. 165
6.9.1 Child pools 165
6.9.2 Ownership groups. 165
6.9.3 Provisioning policies 165
6.9.4 Volume protection. 166
6.10 Troubleshooting 166
6.10.1 Collecting a snap 166
6.10.2 Copying a snap to an IBM storage system 166
6.10.3 Viewing the logs 166
6.10.4 vSphere task names being misreported 167
6.10.5 Restarting the vSphere Client Service in vCenter. 167
6.10.6 Pinging the appliance 167
6.10.7 Changing the network configuration 168

Chapter 7. IBM Storage Insights 169
7.1 IBM Storage Insights editions 170
7.2 IBM Storage Insights architecture. 173
7.3 IBM Storage Insights Monitoring. 174
7.4 IBM Storage Insights VMware integration. 174

Chapter 8. Integrating with VMware by using IBM Spectrum Connect 179
8.1 Overview of IBM Spectrum Connect 180
8.1.1 Supported cloud interfaces 180
8.1.2 Installation considerations. 180
8.1.3 Downloading and installing IBM Spectrum Connect 182
8.1.4 Initial configuration 183
8.1.5 Registering a Storage System into IBM Spectrum Connect 187
8.2 Understanding Storage Spaces and Storage Services 188
8.2.1 Creating Storage Services 189
8.2.2 Allocating capacity to Storage Services 191
8.2.3 Delegating Storage Services to vCenter 194
8.3 VMware vSphere Virtual Volumes 195
8.3.1 VMware vSphere Virtual Volumes overview 195
8.3.2 Configuring IBM Storage Virtualize to support vVols 197
8.3.3 Configuring IBM Spectrum Connect 202
8.3.4 Configuring VMware vSphere vCenter 204
8.3.5 Creating a vVol datastore 206
8.4 Best-practice considerations and troubleshooting 210
8.4.1 Protecting the IBM Spectrum Connect server. 210
8.4.2 Viewing the relationships between vVol and VM 211
8.4.3 Mirroring the utility volume 211
8.4.4 Performing an upgrade on a storage system with vVols enabled. 212
8.4.5 Understanding audit log entries 212
8.4.6 IBM Storage Virtualize GUI. 214
8.4.7 Metadata VDisk. 214
8.4.8 Enabling debugging in IBM Spectrum Connect 215
8.4.9 Certificates 215
8.4.10 Prerequisites, limitations, and restrictions. 217
8.5 IBM Storage Enhancements for VMware vSphere Web Client plug-in 218
8.5.1 Installing the vSphere plug-in 218
8.5.2 Provisioning storage from within vCenter 220
8.5.3 Using the IBM Storage Enhancements vSphere plug-in. 220
8.5.4 Viewing more storage information from within the vSphere Client 225
8.6 Performing more storage volume management tasks. 227
8.6.1 Considerations 227
8.7 IBM Storage Plug-in for VMware vRealize Orchestrator. 228
8.7.1 Configuring IBM Spectrum Connect for VMware vRealize Orchestrator 228
8.7.2 Using vRealize Automation and VMware vRealize Orchestrator 232
8.8 IBM Storage Management Pack for VMware vRealize Operations Manager 234
8.8.1 Configuring IBM Spectrum Connect for VMware vRealize Operations Manager 235
8.8.2 Installing Management Pack in VMware vRealize Operations Manager 236

Chapter 9. Troubleshooting 241
9.1 Collecting data for support 242
9.1.1 Data collection guidelines for SAN Volume Controller and IBM FlashSystem . . 242
9.1.2 Data collection guidelines for VMware ESXi. 243
9.1.3 Data collection guidelines for VMware Site Recovery Manager 243
9.1.4 Data collection guidelines for IBM Spectrum Connect (VASA or vVols). 244
9.2 Common support cases 245
9.2.1 Storage loss of access 245
9.2.2 VMware migration task failures. 247
9.2.3 Registration of vVol/VASA Storage Provider failures 247

9.2.4 vVol Metadata migration before upgrading to 8.6.1.x or newer 255

Related publications 259
IBM Redbooks 259
Online resources 259
Help from IBM 259

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at https://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX®
Easy Tier®
FlashCopy®
HyperSwap®
IBM®
IBM Cloud®
IBM FlashCore®
IBM FlashSystem®
IBM Spectrum®
Redbooks®
Redbooks (logo) ®
Storwize®

The following terms are trademarks of other companies:

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

ITIL is a Registered Trade Mark of AXELOS Limited.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware, VMware vSphere, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redbooks® publication details the configuration and best practices for using the IBM Storage FlashSystem family of storage products within a VMware environment.

Topics illustrate planning, configuring, operations, and preferred practices that include integration of IBM FlashSystem® storage systems with the VMware vCloud suite of applications:

- VMware vSphere Web Client (vWC)
- vSphere Storage APIs - Storage Awareness (VASA)
- vSphere Storage APIs – Array Integration (VAAI)
- VMware Site Recovery Manager (SRM)
- VMware vSphere Metro Storage Cluster (vMSC)
- Embedded VASA Provider for VMware vSphere Virtual Volumes (vVols)

This book is intended for presales consulting engineers, sales engineers, and IBM clients who want to deploy IBM Storage FlashSystem storage systems in virtualized data centers that are based on VMware vSphere.

Authors

This book was produced by a team of specialists from around the world.

Vasfi Gucer works as the Storage Team Leader on the IBM Redbooks Team. He has more than 30 years of experience in the areas of systems management, networking hardware, and software. He writes extensively and teaches IBM classes worldwide about IBM products. His focus has been primarily on storage, cloud computing, and cloud storage technologies for the last 10 years. Vasfi is also an IBM Certified Senior IT Specialist, Project Management Professional (PMP), IT Infrastructure Library (ITIL) V2 Manager, and ITIL V3 Expert.

Federica Donald joined IBM as a Platform Developer and graduated from university with an Electrical and Electronic Engineering degree. Later, she transitioned into UX/UI development for IBM storage. Federica is currently the Lead UI Developer for the IBM Storage Virtualize Plug-in for vSphere.

Warren Hawkins has been a member of the IBM Storage Virtualize development team in Hursley for 10 years, specializing in the testing of VMware vSphere and Windows Hyper-V integration and interoperability. Warren is a regular speaker at both IBM User Groups/Conferences and partner events such as VMware VMworld and Cisco LIVE! Warren has also co-authored numerous Redbooks and Redpapers and worked with Cisco to publish Cisco Validated Designs as part of Versastack. Before joining IBM, Warren worked for 10 years as a systems administrator in both the public and private sectors managing Windows, Citrix, and VMware environments.

Markus Oscheka is an IT Specialist for Proof of Concepts and Benchmarks in the Disk Solution Europe team in Kelsterbach, Germany. His areas of expertise include setup and demonstration of IBM System Storage solutions in various environments including IBM AIX®, Linux, Windows, VMware ESXi, and Solaris. He has performed many Proof of Concepts and Benchmarks on the DS8000/Spectrum Accelerate family/Storage Virtualize family. Furthermore, he has worked as a Technical Advisor for Storage. Currently he works in the Hosting and Tools Development Department, taking care of several vSphere Environments and helping clients with VMware-related services. He has co-authored various Redbooks and spoken at several System Technical Universities. He holds a degree in Electrical Engineering.

Jared Pateman joined IBM from the graduate scheme with a degree in Computer Science from the University of Derby. Jared works as part of the platform development team within IBM Storage Virtualize and has been responsible for the backend development and architecture of the IBM Storage Virtualize plug-in for vSphere.

Thanks to the following people for their contributions to this project:

Eddie Lin, Adrian Moldovan
IBM UK

Elias Luna, Marie Janiak, Bill Martinson
IBM USA

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on LinkedIn:

  https://www.linkedin.com/groups/2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/subscribe

- Stay current on recent Redbooks publications with RSS Feeds:

  https://www.redbooks.ibm.com/rss.html

1

Introduction

This IBM Redbooks publication describes the configuration and best practices for using IBM Storage Virtualize based storage systems within a VMware environment. This version of the book addresses IBM Storage Virtualize Version 8.6 with VMware vSphere 8.0.

This publication is intended for Storage and VMware administrators. The reader is expected to have a working knowledge of IBM Storage Virtualize and VMware. Initial storage and server setup is not covered.

This chapter includes the following sections:

- 1.1, “IBM and VMware” on page 2
- 1.2, “Overview of IBM Storage Virtualize and IBM Storage FlashSystem” on page 2
- 1.3, “Overview of IBM Storage FlashSystem with VMware” on page 6

1.1 IBM and VMware

IBM and VMware have a long record of collaboration. VMware was founded in 1998, and the beginning of IBM Storage Virtualize dates back to the early 2000s. Almost since inception, IBM and VMware have been technology partners.

IBM is a VMware Technology Alliance Partner. IBM storage is deployed in the VMware Reference Architectures Lab. Therefore, VMware products run well on IBM storage.

1.2 Overview of IBM Storage Virtualize and IBM Storage FlashSystem

IBM Storage Virtualize refers to the storage software. IBM Storage Virtualize systems are systems like IBM Storage FlashSystem and IBM SAN Volume Controller (SVC).

For this book, the focus is on the storage as IBM Storage FlashSystem. However, other IBM Storage Virtualize storage products work in similar fashion.

For more information, see the following IBM Redbooks publications:

- *Implementation Guide for IBM Storage FlashSystem and IBM SAN Volume Controller: Updated for IBM Storage Virtualize Version 8.6, SG24-8542*
- *Performance and Best Practices Guide for IBM Storage FlashSystem and IBM SAN Volume Controller: Updated for IBM Storage Virtualize Version 8.6, SG24-8543*

1.2.1 IBM Storage Virtualize

IBM Storage Virtualize refers to the software that runs on various IBM storage hardware. Its models include the IBM Storage FlashSystem 5000, IBM Storage FlashSystem 7000, IBM Storage FlashSystem 9000, and IBM SAN Volume Controller (SVC). The former IBM Storwize® family also uses IBM Storage Virtualize. Except for differences in hardware and licensing, all IBM Storage Virtualize products behave identically. Some features are supported only on specific code levels and hardware platforms.

The primary function of IBM Storage Virtualize is block-level storage virtualization. IBM defines storage virtualization as a technology that makes one set of resources resemble another set of resources, preferably with more desirable characteristics.

The storage that is presented to the host is virtual and does not correspond to a specific back-end storage resource so that IBM Storage Virtualize can perform many enterprise-class features without impacting the hosts.

IBM Storage Virtualize first came to market in 2003 in the form of the IBM SVC. In 2003, the SVC was a cluster of commodity servers attached to a storage area network (SAN). The SVC did not contain its own storage. Instead, SVC used back-end storage that was provided from other storage systems. At the time of writing, IBM Storage Virtualize supports up to 500+ different storage controllers.

IBM Storage Virtualize includes the following advantages:

- Data compression and deduplication
- Software and hardware encryption
- SafeGuarded Copy

- IBM Easy Tier® for workload balancing
- Multi-tenancy
- Thin-provisioning
- 2-site and 3-site replication and point-in-time copy
- Software-defined storage (SDS) capability to cloud service providers (CSPs)

These features combine to make a compelling suite of storage management tools.

IBM Storage Virtualize is software, so new features and functions are added regularly. IBM Storage Virtualize includes several technologies so that it integrates well with VMware.

Also, all IBM storage includes the following benefits:

- IBM Storage Insights, which provides a cloud-based dashboard to monitor all storage across the enterprise. It is useful for tracking both performance and capacity usage.
- Remote support and remote upgrades.
- Backed by various premium support offerings.

1.2.2 IBM Storage FlashSystem

Since 2011, IBM Storage Virtualize is also available in various canister and enclosure hardware architectures. Originally branded under the Storwize name, these products are now called IBM Storage FlashSystem. The lab environment that was used for this IBM Redbooks publication was built around an IBM Storage FlashSystem 5200. These models include internal storage that is virtualized the same as with SVC. IBM Storage FlashSystem products can also virtualize external storage, but the market has shifted focus toward using internal storage.

IBM Storage FlashSystem 5200 supports a range of storage media with an emphasis on high-performance Non-Volatile Memory Express (NVMe) drives. For most storage administrators, capacity and performance optimization include IBM FlashCore® Module (FCM) modules. FCMs are the next generation of IBM Storage FlashSystem Micro Latency Modules. They offer high throughput and built-in compression without a performance penalty.

On the high end is Storage Class Memory (SCM), which is built around Intel 3D-Xpoint and Samsung Z-NAND technologies. SCM offers high throughput and low latency, with limited capacities. The IBM Storage FlashSystem 5200 control enclosure supports NVMe SCM and FCM and solid-state drives (SSDs), and serial-attached SCSI (SAS) SSDs are supported only by using expansion enclosures.

Figure 1-1 shows the front of an IBM Storage FlashSystem 5200 enclosure. It is configured with 12 dual-ported NVMe drive slots.

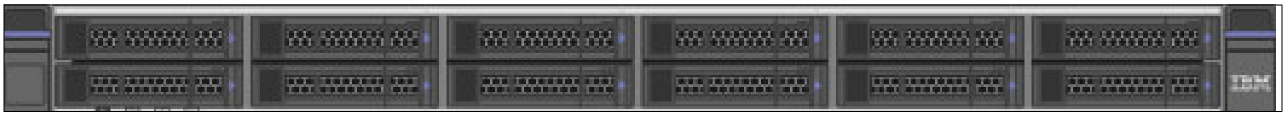


Figure 1-1 The front of an IBM Storage FlashSystem 5200

Each system can be scaled up to include addition control enclosures or scaled out to include more expansion enclosures.

Figure 1-2 shows the back of an IBM Storage FlashSystem 5200 enclosure. In the center are two canisters that run the IBM Storage Virtualize software and perform I/O. The canisters are identical. The far left and right sides contain redundant power supplies.

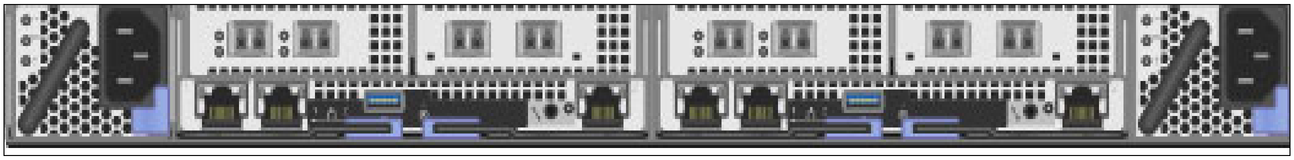


Figure 1-2 The back of an IBM Storage FlashSystem 5200

IBM Storage FlashSystem 5200 can be configured with various I/O ports that support various protocols. The most common configuration is 8 Fibre Channel (FC) ports. These ports can support the Fibre Channel Protocol (FCP) or Non-Volatile Memory Express over Fibre Channel (NVMe over FC).

1.2.3 Key IBM Storage Virtualize terminology

Table 1-1 lists the key IBM Storage Virtualize terminology.

Table 1-1 Key IBM Storage Virtualize terminology

Term	Definition
Canister	The IBM Storage FlashSystem hardware that runs the IBM Storage Virtualize software
Node	The software representation of the canister in the system
I/O group	A pair of nodes or canisters that work together to service I/O
Drive	FlashCore Module, Non-Volatile Memory Express (NVMe) SSD, or hard disk drive (HDD) storage hardware
Array	A RAID array of drives
Managed disk (MDisk)	Either an array of internal storage or a logical unit number (LUN) provided by an external storage controller
Pool	A collection of MDisks that provide a pool or storage for allocation to volumes
Volume or VDisk	The virtual LUN that is presented to the host
SafeGuarded Copy	Immutable copies of primary volumes
Host	The server that uses the storage. An ESXi server in this case
IBM HyperSwap®	A business continuity solution that copies data across two sites

1.2.4 Key VMware terminology

Table 1-2 lists the key VMware terminology.

Table 1-2 Key VMware terminology

Term	Definition
Host	An VMware ESXi server that is running on a physical server
Cluster	A group of ESXi servers
Data center	A group of ESXi host clusters
Datastore	SAN-based shared storage resources for ESXi clusters. Local disk-based datastores cannot be shared by multiple servers.
Native multipathing (NMP)	NMP plug-in. Most of the FC SAN-based storage systems are controlled by NMP.
High-performance plug-in (HPP)	NVMe-based storage systems are controlled by HPP.
Claim rules	Claim rules determine which multipathing module owns the paths to a storage device. They also define the type of multipathing support that the host provides to the device.
VAAI	VMware vSphere Storage APIs – Array Integration (VAAI), also referred to as hardware acceleration or hardware offload application programming interfaces (APIs), are a set of APIs to enable communication between VMware vSphere ESXi hosts and storage devices.
VMware vSphere Virtual Volumes (vVols)	vVols are virtual machine disk (VMDK) granular storage entities that are exported by storage arrays. vVols are exported to the ESXi host through a small set of Protocol Endpoints (PEs). PEs are part of the physical storage fabric, and they establish a data path from virtual machines (VMs) to their respective vVols on demand. Storage systems enable data services on vVols. The results of these data services are newer vVols. Data services configuration and management of virtual volume systems are exclusively done out-of-band regarding the data path.

1.3 Overview of IBM Storage FlashSystem with VMware

Figure 1-3 summarizes the various VMware and IBM software components that are discussed in this publication.

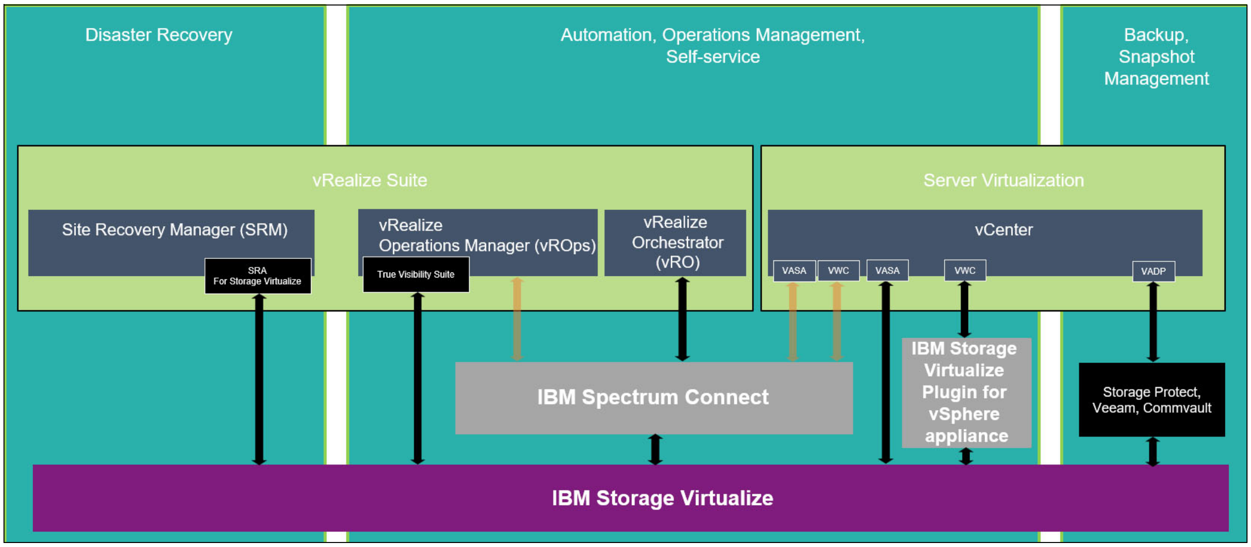

Disaster Recovery
Automation, Operations Management, Self-service
Backup, Snapshot Management
vRealize Suite
Server Virtualization
Site Recovery Manager (SRM)
SRA For Storage Virtualize
vRealize Operations Manager (vROps)
True Visibility Suite
vRealize Orchestrator (vRO)
vCenter
VASA
VWC
VASA
VWC
VADP
IBM Spectrum Connect
IBM Storage Virtualize Plugin for vSphere appliance
Storage Protect, Veeam, Commvault
IBM Storage Virtualize

Figure 1-3 Integrating IBM Storage with VMware

Integrating IBM Storage Virtualize with VMware includes the following key components:

- Integration with vSphere Client. For more information about the Integration with vSphere Client, see Chapter 6, “Overview of the IBM Storage plug-in for vSphere” on page 125.
- Integration with vVols. For more details about Integration with vVols, refer to Chapter 5, “Embedded VASA Provider for Virtual Volumes (vVol)” on page 83.
- Integration with VMware Site Recovery Manager. For more information about Integration with VMware Site Recovery Manager, see Chapter 4, “Preparing for disaster recovery” on page 41.
- IBM Spectrum® Connect, which is a no additional charge software solution that is available with all IBM storage but will be deprecated. Transparent orange arrows in Figure 1-3 depict non-preferred integrations through IBM Spectrum Connect. For more information about IBM Spectrum Connect, see Chapter 8, “Integrating with VMware by using IBM Spectrum Connect” on page 179.

2

Host and storage connectivity

This chapter describes the test environment setup that is used in this book. It also discusses options for host to storage connectivity, which includes host-cluster configuration, protocols such as Fibre Channel and Internet Small Computer System Interface (iSCSI), iSCSI Extensions for RDMA (iSER), NVMe over Fibre Channel, NVMe over RDMA, NVMe over TCP, and multipath configuration options.

This chapter includes the following sections:

- 2.1, “Test environment implementation” on page 8
- 2.2, “Host connectivity protocols” on page 12
- 2.3, “Multi-path considerations” on page 18
- 2.4, “Zoning considerations” on page 22
- 2.5, “Recommendations for tuning ESXi hosts” on page 24

2.1 Test environment implementation

Figure 2-1 depicts the configuration and connectivity for the test environment for host connectivity that is used in this book. Two IBM Storage FlashSystem 5200 are cabled to redundant IBM Fibre Channel switches. Each canister on each IBM Storage FlashSystem has two ports that are connected to each switch. Four VMware hosts, or servers, are used for this book.

Each host is connected to the switch:

- The hosts with the blue-colored connections are zoned to the FS9200-2 with blue-colored connections.
- The hosts with the green-colored connections are zoned to the FS9200-1 with green-colored connections.

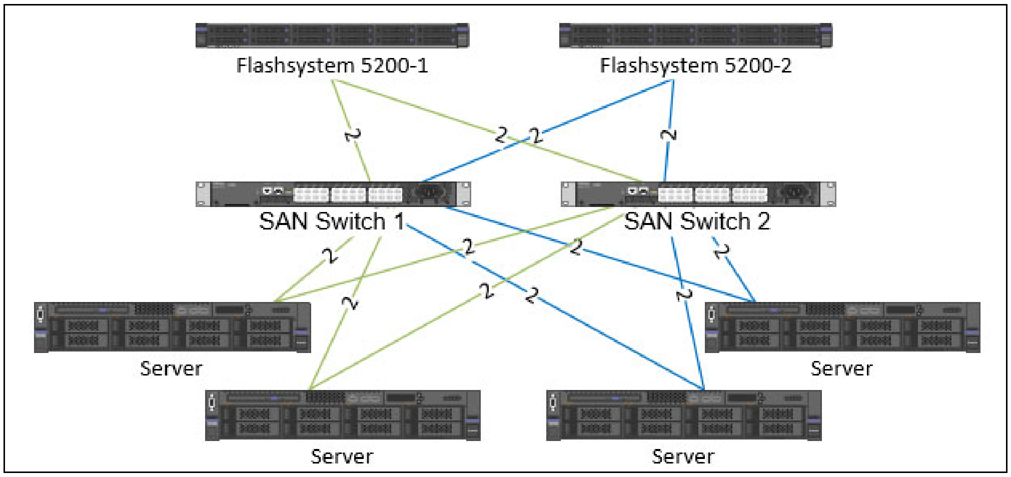


Figure 2-1 Configuration and connectivity for the test environment that is used in this book

2.1.1 IBM Storage Virtualize host clusters

IBM Storage Virtualize version 7.7.1 or later supports host clusters. With a host cluster, a user can create a group of hosts to form a cluster. A cluster is treated as a single entity, which allows multiple hosts to have access to the same set of volumes.

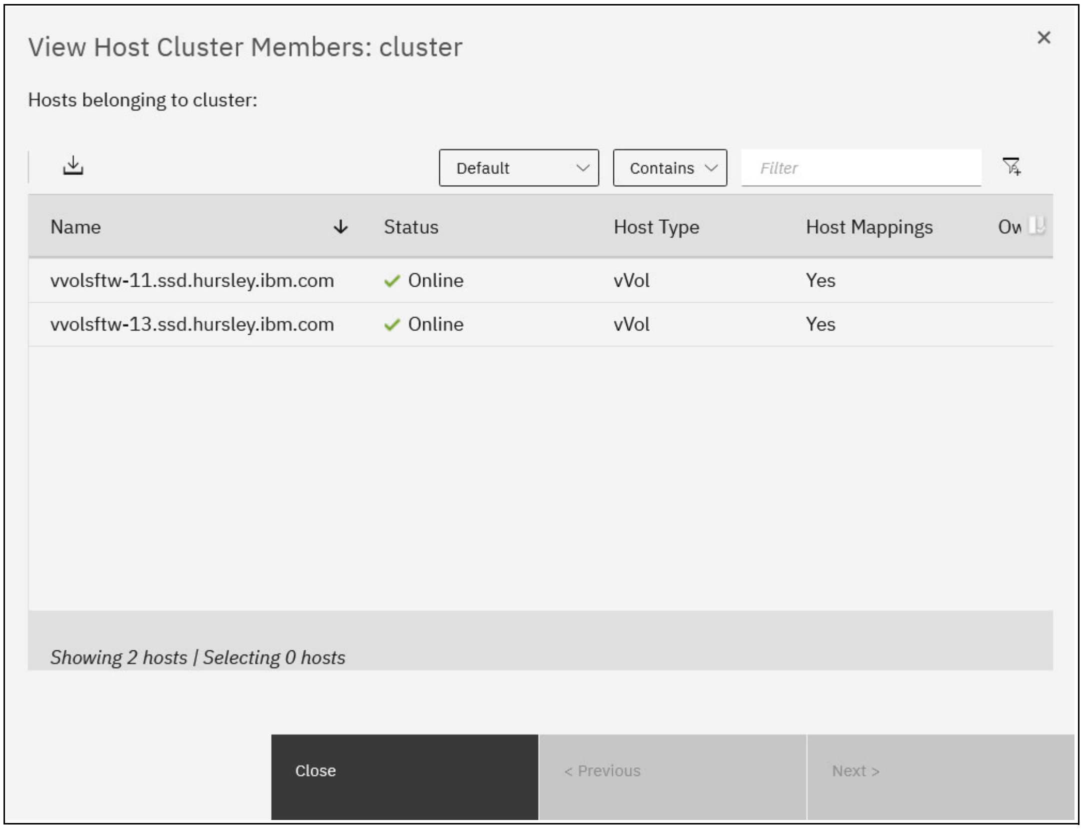
Volumes that are mapped to a host cluster are assigned to all members of the host cluster that use the same Small Computer System Interface (SCSI) ID. Before this feature was implemented in IBM Storage Virtualize, as an example, a VMware vSphere cluster would be created as a single host object, containing all the worldwide port names (WWPNs) for the hosts in the cluster, up to 32.

With host clusters, a storage administrator can define individual host objects for each ESXi host and add them to a host cluster object that represents each vSphere cluster. If hosts are later added to the host cluster, they automatically inherit shared host cluster volume mappings. Similarly, when removing a host from a host cluster, you have the option to either retain or remove any shared mappings. It also ensures that volumes are mapped with consistent SCSI IDs across all host cluster members. Because of these factors, it is recommended to use host clusters to simplify storage provisioning and management where possible. You can have up to 128 hosts in a single host cluster object. Host clusters are easier to manage than single host objects because the 32 worldwide port name (WWPN) limitation is removed.

The minimum size of a cluster is two nodes for vSphere high availability (HA) to protect workloads if one host stops functioning. However, in most use cases, a 3-node cluster is more appropriate because you have the option of using Distributed Resource Scheduler (DRS) and of running maintenance tasks on an ESXi server without having to disable HA.

Configuring large clusters has benefits, too. You typically have a higher consolidation ratio, but there might be a downside if you do not have enterprise-class or correctly sized storage in the infrastructure. If a datastore is presented to a 32-node or a 64-node cluster and the virtual machines (VMs) on that datastore are spread across the cluster, there is a chance of SCSI-locking contention issues. Using a VMware vSphere Storage APIs Array Integration (VAAI) aware array helps reduce this problem with Atomic Test and Set (ATS). However, if possible, consider starting small and gradually growing the cluster size to verify that your storage behavior is not impacted.

Figure 2-2 shows one of the VMware host clusters that was used in the test configuration for this book. There are two hosts that are defined in the VMware host cluster.


View Host Cluster Members: cluster

Hosts belonging to cluster:

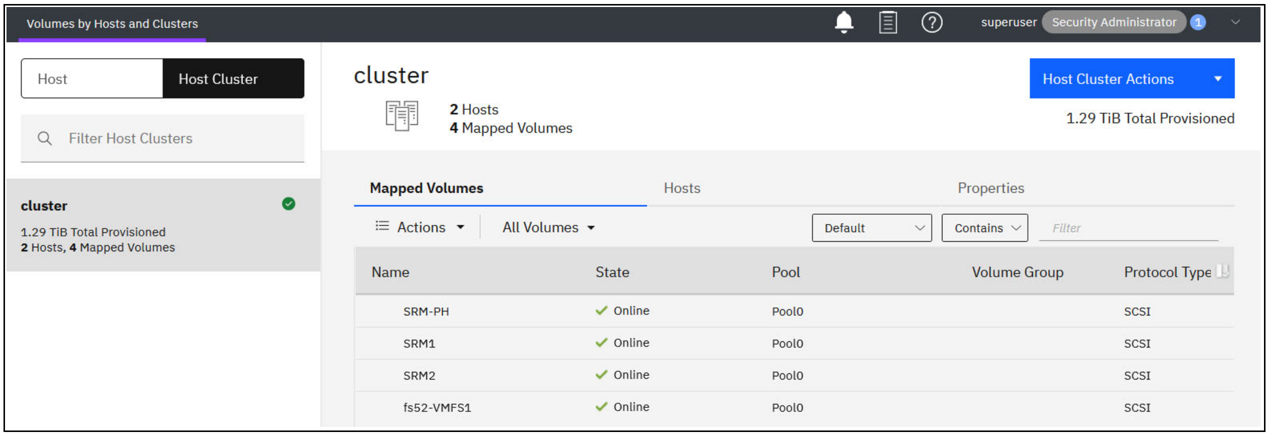
Name	Status	Host Type	Host Mappings	Ow
vvolsftw-11.ssd.hursley.ibm.com	✓ Online	vVol	Yes	
vvolsftw-13.ssd.hursley.ibm.com	✓ Online	vVol	Yes	

Showing 2 hosts | Selecting 0 hosts

Figure 2-2 VMware host clusters that were used in the test configuration

Note: Do not add Non-Volatile Memory Express (NVMe) hosts and SCSI hosts to the same host cluster.

Figure 2-3 shows the volumes that are assigned to the host cluster.



cluster

1.29 TiB Total Provisioned

2 Hosts, 4 Mapped Volumes

cluster

2 Hosts
4 Mapped Volumes

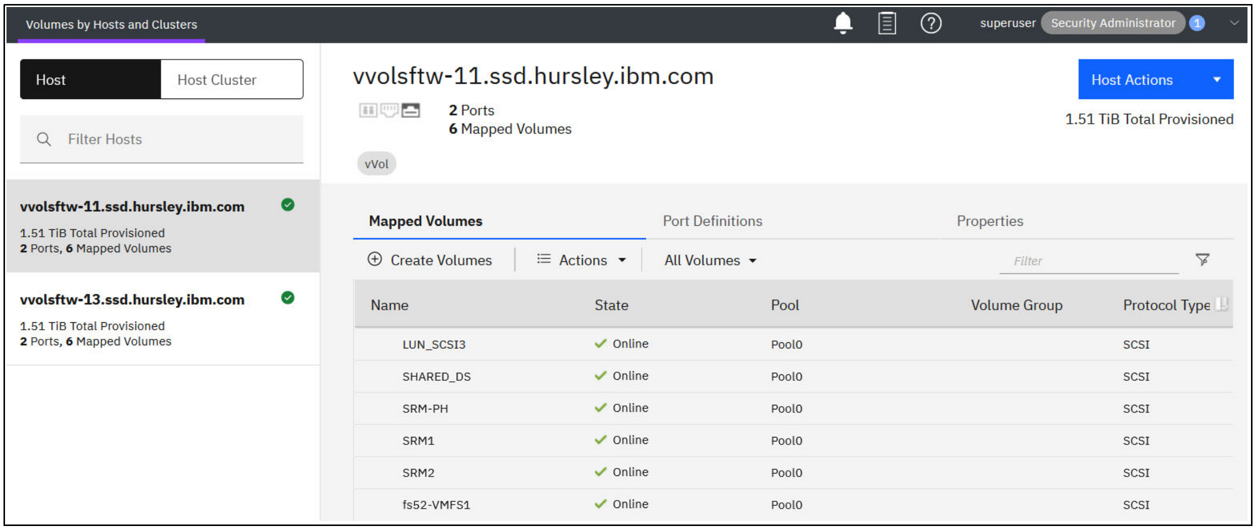
1.29 TiB Total Provisioned

Name	State	Pool	Volume Group	Protocol Type
SRM-PH	✓ Online	Pool0		SCSI
SRM1	✓ Online	Pool0		SCSI
SRM2	✓ Online	Pool0		SCSI
fs52-VMFS1	✓ Online	Pool0		SCSI

Figure 2-3 Volumes that are assigned to the host cluster

Figure 2-4 shows one of the hosts in the host cluster with the volumes that are connected to it. The volumes were assigned to the host cluster, and not directly to the host. Any hosts that are added to a host cluster have all of the volumes mapped to the host cluster automatically assigned to the hosts.

> **Note:** Private mappings can still be provisioned to individual hosts within a host cluster, for example for storage area network (SAN) Boot configurations.



vvolsftw-11.ssd.hursley.ibm.com

1.51 TiB Total Provisioned

2 Ports, 6 Mapped Volumes

vvolsftw-13.ssd.hursley.ibm.com

1.51 TiB Total Provisioned

2 Ports, 6 Mapped Volumes

vvolsftw-11.ssd.hursley.ibm.com

2 Ports
6 Mapped Volumes

1.51 TiB Total Provisioned

Name	State	Pool	Volume Group	Protocol Type
LUN_SCSI3	✓ Online	Pool0		SCSI
SHARED_DS	✓ Online	Pool0		SCSI
SRM-PH	✓ Online	Pool0		SCSI
SRM1	✓ Online	Pool0		SCSI
SRM2	✓ Online	Pool0		SCSI
fs52-VMFS1	✓ Online	Pool0		SCSI

Figure 2-4 One of the hosts in the host cluster with the volumes that are connected to it

2.1.2 Use cases for implementing throttles

With IBM Storage FlashSystem storage, you can configure throttles for the following items:

- Hosts
- Host clusters
- Volumes
- SCSI offload
- Storage pools

A common use case for throttles on hosts, host clusters, and volumes can be applied when test and production workloads are mixed on the same IBM Storage Virtualize system. Test-related workloads should not affect production, so you can throttle test hosts and volumes to give priority to production workloads.

IBM Storage Virtualize supports commands that are used for SCSI offload and VMware VAAI:

- SCSI offload enables the host to offload some data operations to the storage system.
- VAAI enables VMware hosts to also offload some operations to supported storage systems.

Both technologies reduce traffic on the storage network, and load on the host. Hosts use offload commands to perform tasks such as formatting new file systems or performing data copy operations without the need of a host to read and write data. Examples are the WRITE SAME and XCOPY commands. IBM Storage Virtualize 8.1.0.0 introduced support for WRITE SAME when UNMAP is enabled. WRITE SAME is a SCSI command that tells the storage system to write the same pattern to a volume or an area of a volume.

When SCSI UNMAP is enabled on IBM Storage FlashSystem storage, it advertises this situation to hosts. At versions 8.1.0.0 and later, some hosts respond to the UNMAP command by issuing a WRITE SAME command, which can generate large amounts of I/O. If the back-end storage system cannot handle the amount of I/O, volume performance can be impacted. IBM Storage Virtualize offload throttling can limit the concurrent I/O that is generated by the WRITE SAME or XCOPY commands.

When you enable offload throttling, the following bandwidth throttle values are recommended:

- For systems that manage any enterprise or nearline storage, the recommended value is 100 MBps.
- For systems managing *only* tier1 flash or tier0 flash, the recommended value is 1000 MBps.

Enable the offload throttle by using the following command line interface (CLI) command:

```
mkthrottle -type offload -bandwidth bandwidth_limit_in_MB
```

2.1.3 Data reduction pools

Data reduction can increase storage efficiency and reduce storage costs, especially for IBM Storage Virtualize systems. Data reduction reduces the amount of data that is stored on both the internal drives and the virtualized external storage systems by reclaiming previously used storage resources that are no longer needed by host systems.

IBM Storage Virtualize systems implement data reduction by using data reduction pools (DRPs). A DRP can contain thin-provisioned or compressed volumes. DRPs also provide more capacity to volumes in the pool by supporting data deduplication.

With a log-structured pool implementation, DRPs help to deliver more consistent performance from compressed volumes. DRPs also support compression of all volumes in a system, potentially extending the benefits of compression to all data in a system. Traditional storage pools have a fixed allocation unit of an extent, and that does not change with DRPs. However, features like thin provisioning and IBM Real-time Compression (RtC) use smaller allocation units and manage this allocation with their own metadata structures. These features are described as binary trees or Log Structured Arrays (LSAs).

For thin-provisioned volumes to stay thin, you must be able to reclaim capacity that is no longer used. For LSAs, where all writes go to new capacity, you must be able to garbage-collect the old overwritten data blocks. This action also needs to be done at the smaller allocation unit size in a DRP volume.

Figure 2-5 shows the types of volumes that can be created in a DRP.

- DRP fully allocated volumes provide the best performance for the IBM Storage FlashSystem products, but storage efficiency and space savings are not realized.
- Thin-compressed volumes provide storage-space efficiency with the best performance of the four options for space-efficient volumes.

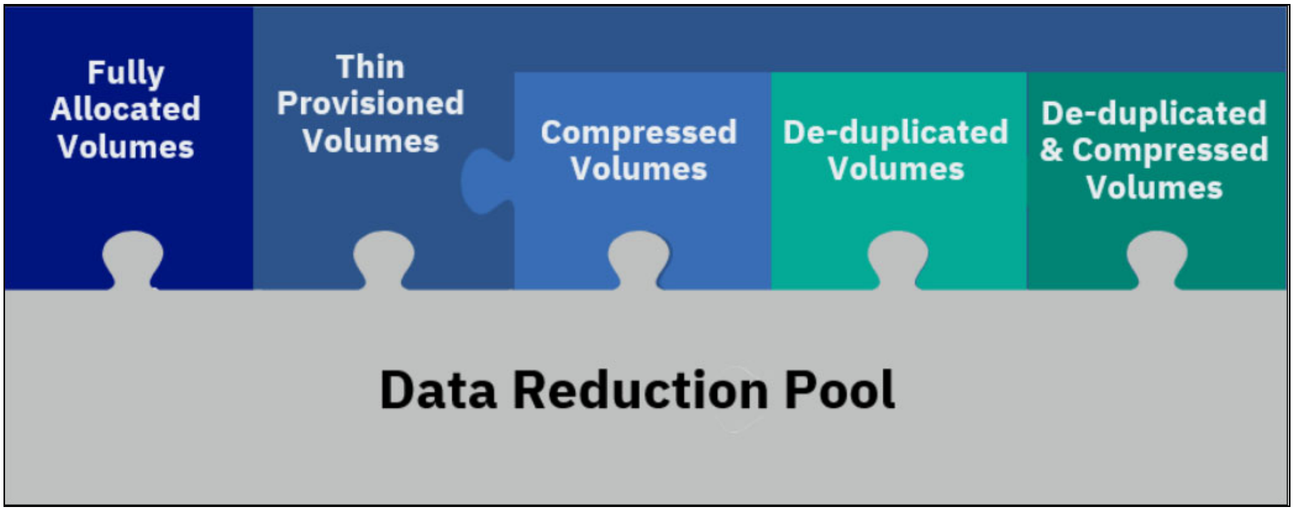


Figure 2-5 Types of volumes that can be created in a data reduction pool

> **Best practice:** DRPs are suitable for scenarios where capacity savings are prioritized at the cost of performance. For performance sensitive workloads, ensure that sufficient performance benchmarking has been validated before employing DRPs throughout your environment.

For more information about data reduction pools, see the Redbooks publication *Implementation Guide for IBM Storage FlashSystem and IBM SAN Volume Controller: Updated for IBM Storage Virtualize Version 8.6,* SG24-8542.

2.2 Host connectivity protocols

IBM Storage FlashSystem support both Ethernet-based and Fibre-Channel-based host-attachment protocols:

- Ethernet-based protocols include iSCSI, iSER, NVMe over RDMA, and NVMe over TCP. All of these protocols can be implemented over existing Ethernet networks and do not require a dedicated storage network.
- Fibre-Channel-based protocols include Non-Volatile Memory Express over Fibre Channel (NVMe over FC) and traditional SCSI Fibre Channel, which is most often referred to as Fibre Channel.

2.2.1 iSCSI

iSCSI connectivity is a software feature that is provided by the Storage Virtualize code. The iSCSI protocol is a block-level protocol that encapsulates SCSI commands into Transmission Control Protocol/Internet Protocol (TCP/IP) packets. Therefore, iSCSI uses an IP network rather than requiring the Fibre Channel (FC) infrastructure. For more information about the iSCSI standard, see Request for Comment (RFC) 3720.

An iSCSI client, which is known as an iSCSI initiator, sends SCSI commands over an IP network to an iSCSI target. A single iSCSI initiator or iSCSI target is called an iSCSI node.

You can use the following types of iSCSI initiators in host systems:

- Software initiator. Available for most operating systems (OSs), including IBM AIX, Linux, and Windows.
- Hardware initiator. Implemented as a network adapter with an integrated iSCSI processing unit, which is also known as an iSCSI host bus adapter (HBA).

Ensure that the iSCSI initiators and targets that you plan to use are supported. Use the following sites for reference:

- IBM Storage FlashSystem 8.6 Support Matrix
- IBM Storage FlashSystem 9x00 8.6
- IBM System Storage Interoperation Center (SSIC)

iSCSI qualified name

An IBM Storage FlashSystem cluster can provide up to eight iSCSI targets, one per canister. Each canister has its own iSCSI Qualified Name (IQN), which, by default, is in the following format:

```
iqn.1986-03.com.ibm:2145.<clustername>.<nodename>
```

An alias string can also be associated with an iSCSI node. The alias enables an organization to associate a string with the iSCSI name. However, the alias string is not a substitute for the iSCSI name.

> **Important:** The cluster name and node name form part of the IQN. Changing any of them might require reconfiguration of all iSCSI nodes that communicate with IBM Storage FlashSystem.

2.2.2 iSER

IBM Storage FlashSystems that run IBM Storage Virtualize v8.2.1 or later support iSER for host attachment, which is implemented by using RDMA over Converged Ethernet (RoCE) or Internet Wide-Area RDMA Protocol (iWARP). This feature supports a fully Ethernet-based infrastructure and not Fibre Channel in your data center:

- IBM Storage FlashSystem internode communication with 2 or more IBM Storage FlashSystem in a cluster.
- HyperSwap.

Using iSER requires that an Ethernet adapter is installed in each node, and that dedicated Remote Direct Memory Access (RDMA) ports are used for internode communication. RDMA enables the Ethernet adapter to transfer data directly between nodes. The direct transfer of data bypasses the central processing unit (CPU) and cache and makes transfers faster.

Requirements for RDMA connections:

- Either 25 Gbps or 100 Gbps Ethernet adapter is installed on each node.
- Ethernet cables between each node are connected correctly.
- Protocols on the source and destination adapters are the same.
- Local and remote IP addresses can be reached.
- Each IP address is unique.
- The local and remote port virtual LAN identifiers are the same.
- A minimum of two dedicated ports are required for node-to-node RDMA communications to ensure the best performance and reliability. These ports cannot be used for host attachment, external storage, or IP replication traffic.
- A maximum of four ports per node is allowed for node-to-node RDMA connections.

2.2.3 NVMe over Fibre Channel

The NVMe transport protocol provides enhanced performance on high-demand IBM Storage FlashSystem drives. NVMe is a logical device interface specification for accessing non-volatile storage media. Host hardware and software use NVMe to fully make use of the levels of parallelism possible in modern All Flash Arrays (AFAs).

Compared to SCSI, NVMe offers performance improvements in I/O operations and latency. This is achieved through features such as multiple, deep command queues and a streamlined architecture. SCSI can also support multiple queues with features like blk_mq, but NVMe provides a more efficient and robust approach. Additionally, NVMe's architecture is better optimized for using multi-core processors for further performance gains.

NVMe is designed to have up to 64 thousand queues. In turn, each of those queues can have up to 64 thousand commands that are processed simultaneously. This queue depth is much larger than what SCSI typically has. NVMe also streamlines the list of commands to only the basic commands that Flash technologies need.

IBM Storage FlashSystem implements NVMe by using the NVMe over Fibre Channel protocol. NVMe over Fibre Channel uses the Fibre Channel protocol as the transport so that data can be transferred from host memory to the target, which is similar to RDMA. For more information about NVMe, see *IBM Storage and the NVM Express Revolution*, REDP-5437.

Every physical FC port on IBM Storage FlashSystem storage supports four virtual ports: one for SCSI host connectivity, one for NVMe over Fibre Channel host connectivity, one for SCSI host failover, and one for NVMe over Fibre Channel host failover. Every NVMe virtual port supports the functions of NVMe discovery controllers and NVMe I/O controllers. Hosts create associations, NVMe logins, to the discovery controllers to discover volumes or to I/O controllers to complete I/O operations on NVMe volumes. Up to 128 discovery associations are allowed per node, and up to 128 I/O associations are allowed per node. An extra 128 discovery associations and 128 I/O associations per node are allowed during N_Port ID virtualization (NPIV) failover.

At the time of this writing, IBM Storage FlashSystem 9200 8.6 supports a maximum of 64 NVMe hosts in a four I/O group configuration. However, a single I/O group supports a maximum of 16 NVMe hosts. For more information, see V8.6.0.x Configuration Limits and Restrictions for IBM Storage FlashSystem 9100 and 9200.

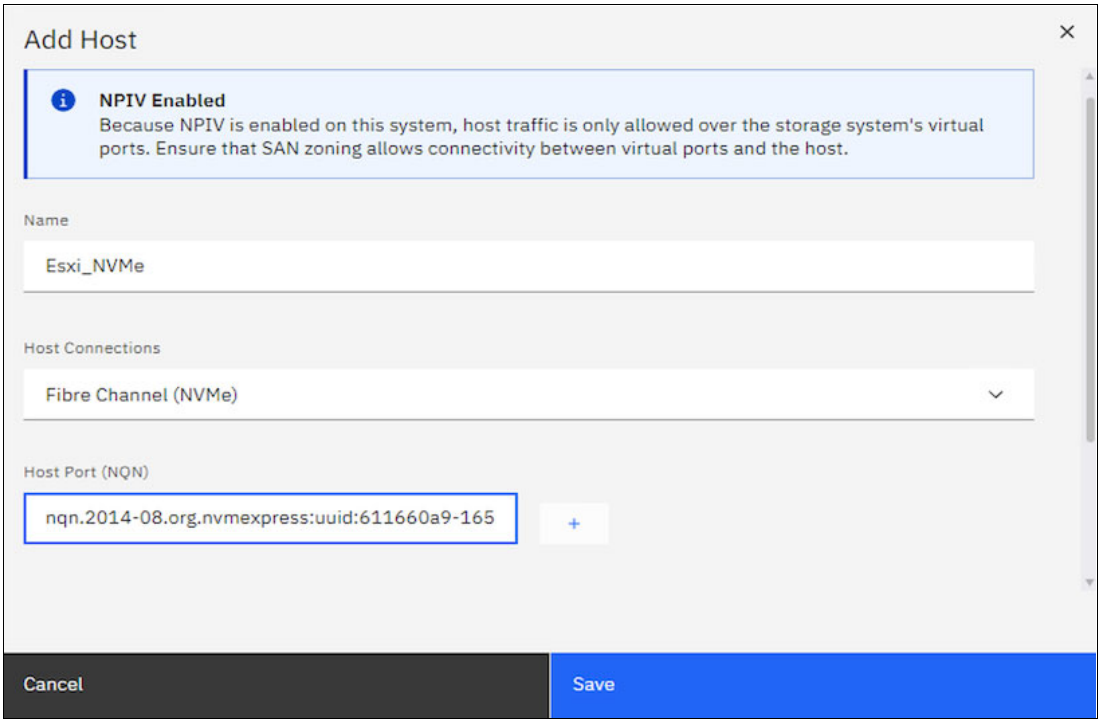
If NVMe over Fibre Channel is enabled on the IBM Storage FlashSystem, each physical WWPN reports up to four virtual WWPNs. Table 2-1 lists the NPIV ports and port usage when NVMe over Fibre Channel is enabled.

Table 2-1 NPIV ports and port usage when NVMe over Fibre Channel is enabled

NPIV port	Port description
Primary Port	The WWPN that communicates with other nodes in the cluster and with back-end storage, if the IBM Storage Virtualize system is virtualizing any external storage.
SCSI Host Attach Port	The virtual WWPN that is used for SCSI attachment to hosts. This WWPN is a target port only.
Failover SCSI Host Port	The standby WWPN that is brought online only if the partner node in an I/O group goes offline. This WWPN is the same WWPN as the primary host WWPN of the partner node.
NVMe Host Attach Port	The WWPN that communicates with hosts for NVMe over Fibre Channel. This WWPN is a target port only.
Failover NVMe Host Attach Port	The standby WWPN that is brought online only if the partner node in an I/O group goes offline. This WWPN is the same WWPN as the primary host WWPN of the partner node.

For more information about NVMe over Fibre Channel and configuring hosts to connect to IBM Storage FlashSystem storage systems by using NVMe over Fibre Channel, see VMware ESXi installation and configuration for NVMe over Fibre Channel hosts.

Figure 2-6 shows how to add an NVMe over Fibre Channel host to an IBM Storage FlashSystem from the Add Host window.



Add Host

NPIV Enabled

Because NPIV is enabled on this system, host traffic is only allowed over the storage system's virtual ports. Ensure that SAN zoning allows connectivity between virtual ports and the host.

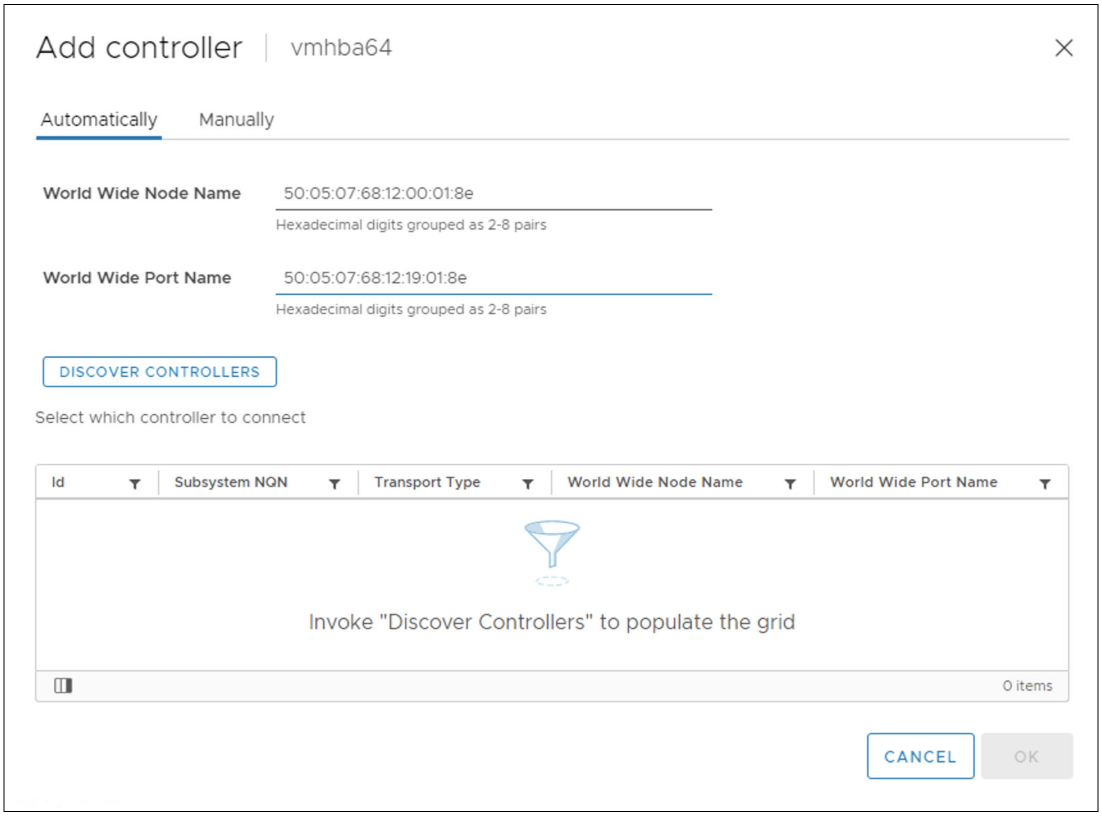
Name: Esxi_NVMe

Host Connections: Fibre Channel (NVMe)

Host Port (NQN): nqn.2014-08.org.nvmexpress:uuid:611660a9-165

Figure 2-6 Adding an NVMe over Fibre Channel host to IBM Storage FlashSystem

After adding a VMware NVMe over Fibre Channel host to an IBM Storage FlashSystem, you must discover the storage subsystem on the VMware ESXi host. You must discover both nodes for each adapter on the IBM Storage FlashSystem by using the NVMe WWPNs that are zoned with the ESXi host. To do so, click **DISCOVER CONTROLLERS** in the window that is shown in Figure 2-7.


Add controller | vmhba64

World Wide Node Name: 50:05:07:68:12:00:01:8e

World Wide Port Name: 50:05:07:68:12:19:01:8e

Invoke "Discover Controllers" to populate the grid

Figure 2-7 Discovering the IBM Storage FlashSystem NVMe controller on VMware

NVMe devices are managed by the VMware high-performance plug-in (HPP). To see the NVMe devices, run the **`esxcli storage hpp device list`** command by using ESXCLI.

2.2.4 SCSI Fibre Channel

FC is a storage networking transport that transports SCSI commands and data from hosts to storage. The Fibre Channel Protocol (FCP) is the transport layer that transmits the SCSI commands. Hosts and storage systems are connected to switches or directors to create a SAN. Figure 2-1 on page 8 is an example of two single-switch SANs that are used to create this book.

The IBM Storage Virtualize software that runs on IBM Storage FlashSystem uses the SCSI protocol to communicate with its clients, and presents storage space in the form of SCSI logical units (LUs) identified by SCSI logical unit numbers (LUNs).

> **Note:** In formal practice, LUs and LUNs are different entities. In practice, the term LUN is often used to refer to a logical disk or LU.

Most applications do not directly access storage but instead work with files or records. Therefore, the OS of a host must convert these abstractions to the language of storage, which are vectors of storage blocks that are identified by logical block addresses within an LU. In IBM Storage Virtualize, each of the externally visible LUs is internally represented by a volume, which is an amount of storage that is taken out of a storage pool. Hosts use the SCSI protocol to send I/O commands to IBM Storage FlashSystem storage to read and write data to these LUNs.

As with NVMe over Fibre Channel host attachment, if NPIV is enabled on the IBM Storage FlashSystem storage system, hosts attach to a virtual WWPN. Table 2-1 on page 15 lists the SCSI and Failover Host Attach Ports.

2.2.5 NVMe over Remote Direct Memory Access

IBM Storage Virtualize 8.5.0 or later can be attached to an NVMe host through NVMe over Remote Direct Memory Access (NVMe over RDMA). NVMe over RDMA uses RoCE v2 as the transport protocol. RoCE v2 is based on UDP. RDMA is a host-offload and host-bypass technology that allows an application, which includes storage, to make data transfers directly to and from another application's memory space. The RDMA-capable Ethernet network interface cards (RNICs), and not the host, manage reliable data transfers between source and destination.

VMware V7.0u2 and later supports RoCE v2 as host connectivity for IBM Storage Virtualize 8.5 storage systems.

RNICs can use RDMA over Ethernet through RoCE encapsulation. RoCE wraps standard InfiniBand payloads with Ethernet or IP over Ethernet frames, which is sometimes called InfiniBand over Ethernet. There are two main RoCE encapsulation types:

1. RoCE v1

   Uses dedicated Ethernet Protocol Encapsulation to send Ethernet packets between source and destination MAC addresses by using Ethertype 0x8915.

2. RoCE v2

   Uses dedicated UDP over Ethernet Protocol Encapsulation to send IP UDP packets by using port 4791 between source and destination IP addresses. UDP packets are sent over Ethernet by using source and destination MAC addresses.

   RoCE v2 is not compatible with other Ethernet options, such as RoCE v1.

Note: Unlike RoCE v1, RoCE v2 is routable.

For more information about configuring the VMware ESXi for NVMe over RDMA on IBM Storage FlashSystem storage systems, see NVMe over RDMA and NVMe over TCP host attachments.

2.2.6 NVMe over TCP

IBM Storage Virtualize 8.6.0 can be attached to an NVMe host through NVMe over TCP. In this first release, only FlashSystem and SVC platforms that are equipped with Mellanox CX-4 or CX-6 adapters are supported.

VMware vSphere V7.0u3 and later supports NVMe over TCP as host connectivity for IBM Storage Virtualize 8.6 storage systems.

For more information about configuring the VMware ESXi for NVMe over TCP on IBM Storage Virtualize systems, see Configuring the VMware ESXi operating system for NVMe over RDMA and NVMe over TCP hosts.

2.3 Multi-path considerations

This section describes multi-path considerations, such as path selection policies and zoning considerations.

2.3.1 Native multipathing path-selection policies

There are three general VMware native multipathing (NMP) plug-in path-selection policies or path-selection plug-ins (PSPs). A PSP is a VMware ESXi host setting that defines a path policy to an LUN. The three PSPs are Most Recently Used (MRU), Fixed, and Round-Robin (RR).

Most Recently Used

The policy selects the first working path, which is discovered at system start time. If this path becomes unavailable, the ESXi or ESX host switches to an alternative path and continues to use the new path while it is available. ESXi and ESX host switches do not return to the previous path if it returns, and the host switch remains on the working path until the working path fails.

> **Tip:** The VMware `preferred` flag can be set on a path. This flag is not applicable if the path selection policy is set to Most Recently Used.

Fixed

The Fixed policy uses the designated preferred path flag if it is configured. Otherwise, it uses the first working path that is discovered at system start time. If the ESXi host cannot use the preferred path or it becomes unavailable, the ESXi host selects an alternative available path. The host automatically returns to the previously defined preferred path when it becomes available. This policy is the default for LUNs that are presented from an active/active storage array.

Round-Robin

The Round-Robin policy is the recommended policy for IBM Storage Virtualize systems. This path selection policy uses a round-robin algorithm to load balance paths across all LUNs when connecting to a storage array. This policy is the default for VMware starting with ESXi 5.5.

Data can travel through only one path at a time for a single volume:

- For active/passive storage arrays, only the paths to the preferred storage controller are used.
- For an active/active storage array, all paths are used for transferring data, assuming that all paths are available.

With Asymmetric Logical Unit Access (ALUA) in an active/active storage array, such as the IBM Storage FlashSystem 9100, 9200 and 9500 systems, only the optimized paths to the preferred control enclosure node are used for transferring data. Round-Robin cycles through only those optimized paths. Configure pathing so that half the LUNs are preferred by one control enclosure node, and the other half are preferred by the other control enclosure node.

Latency Round-Robin is activated by default when Round-Robin is selected as the path selection policy. Latency Round-Robin considers I/O bandwidth and path latency when selecting an optimal path for I/O. When this latency mechanism is used, Round-Robin dynamically selects the best path for better load-balancing. For more information about Latency Round-Robin, see Change Default Parameters for Latency Round-Robin.

Round-Robin path selection limit

Round-Robin Path switching supports two limits:

1. Input/output operations per second (IOPS) limit: A new path is used after a specified number of IOPS are completed on the current path.
2. Bytes limit: A new path is used after a specified number of bytes are transferred on the current path.

The default path selection limit is IOPS, and the default value is 1000 IOPS before the path changes. In some cases, a host can experience latency to storage with no latency seen on the SAN. In these cases, the load of 1000 IOPS saturates the bandwidth of the path. Lowering this value can increase storage performance and help minimize the impact of path failure or node outages during firmware upgrade or hardware maintenance. The recommended path-selection limit setting for IBM Storage Virtualize systems is to use IOPS and set the value to 1. For more information about the IOPS limit, see Adjusting Round Robin IOPS limit from default 1000 to 1 (2069356).

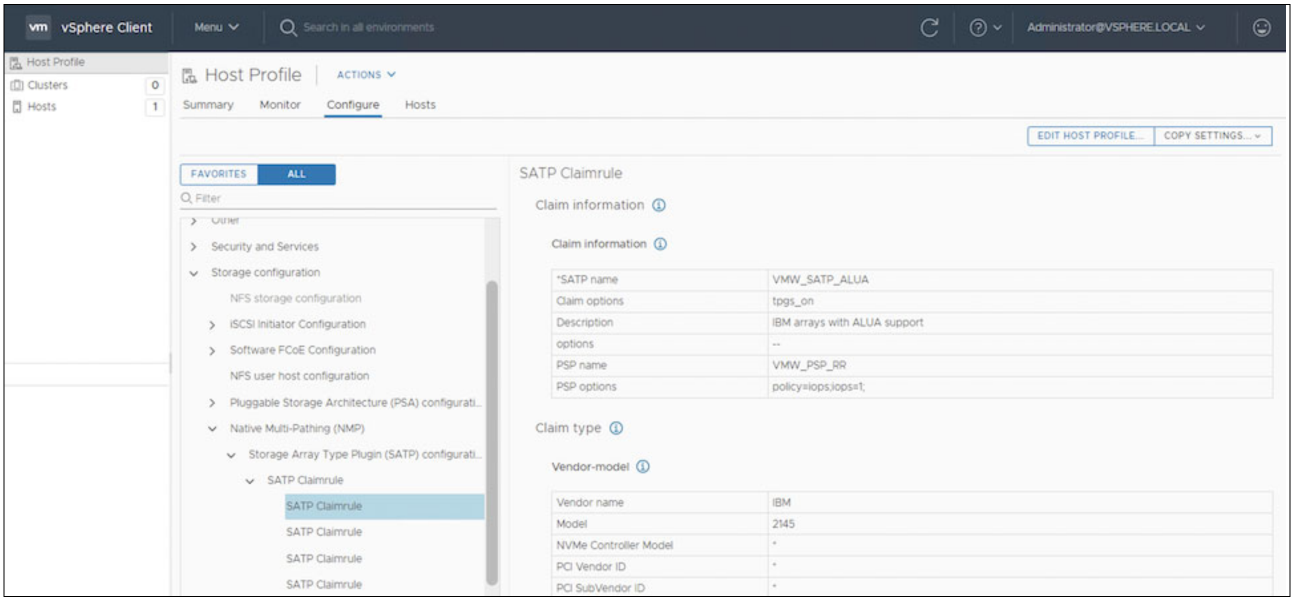
Path selection with claim rules

Claim rules help to set the path selection limit and path selection policy settings in new LUNs that are assigned to the ESXi host. Example 2-1 shows an example of creating a claim rule.

Example 2-1 Creating a claim rule for an IBM Storage Virtualize system to set the path selection limit to 1

```
esxcli storage nmp satp rule add -s VMW_SATP_ALUA -V IBM -M "2145" -c tpgs_on --psp="VMW_PSP_RR"
-e "IBM arrays with ALUA support" -O "iops=1"
```

To configure the claim rule, use the vSphere Host Profile window, as shown in Figure 2-8.


vm vSphere Client
Menu
Search in all environments
Administrator@VSPHERE.LOCAL
Host Profile
Clusters 0
Hosts 1
Host Profile
ACTIONS
Summary
Monitor
Configure
Hosts
EDIT HOST PROFILE...
COPY SETTINGS...
FAVORITES
ALL
Filter
Other
Security and Services
Storage configuration
NFS storage configuration
iSCSI Initiator Configuration
Software FCoE Configuration
NFS user host configuration
Pluggable Storage Architecture (PSA) configurati...
Native Multi-Pathing (NMP)
Storage Array Type Plugin (SATP) configurati...
SATP Claimrule
SATP Claimrule
SATP Claimrule
SATP Claimrule
SATP Claimrule

SATP Claimrule

Claim information

Claim information

*SATP name	VMW_SATP_ALUA
Claim options	tpgs_on
Description	IBM arrays with ALUA support
options	--
PSP name	VMW_PSP_RR
PSP options	policy=iops;iops=1;

Claim type

Vendor-model

Vendor name	IBM
Model	2145
NVMe Controller Model	*
PCI Vendor ID	*
PCI SubVendor ID	*

Figure 2-8 Configuring a claim rule by using the Host Profile window

> **Note:** Existing and previously presented devices must be manually set to Round-Robin with an IOPS limit of 1. Optionally, the ESXi host can be restarted so that it can inherit the multipathing configuration that is set by the new rule.

2.3.2 High-performance plug-in and path selection policies

For VMware 6.7 and later, there is a new multipath plug-in that is called the high-performance plug-in (HPP). The HPP replaces the NMP for high-speed devices, such as NVMe. The HPP is the default plug-in that claims NVMe over Fabrics (NVMe-oF) targets. Within ESXi, the NVMe-oF targets are emulated and presented to users as SCSI targets. The HPP supports only active/active and implicit ALUA targets.

In vSphere 7.0 Update 1 and earlier, NMP remains the default plug-in for local NVMe devices, but you can replace it with HPP. Starting with vSphere 7.0 Update 2, HPP becomes the default plug-in for local NVMe and SCSI devices, but you can replace it with NMP.

Consider the following configuration recommendations for HPP:

- Use the vSphere version that supports HPP.
- Use HPP for local NVMe and SCSI devices and for NVMe-oF devices.
- If you use NVMe-oF, do not mix transport types to access the same namespace.
- Configure your VMs to use VMware Paravirtual controllers.
- Set the latency sensitive threshold to bypass the I/O scheduler.
- If a single VM drives a significant share of the I/O workload of the device, consider spreading the I/O across multiple virtual disks. Attach the disks to separate virtual controllers in the VM.

By default, ESXi passes every I/O through the I/O scheduler. However, using the scheduler might create internal queuing, which is not efficient with the high-speed storage devices.

You can configure the latency sensitive threshold and enable the direct submission mechanism that helps I/O to bypass the scheduler. With this mechanism enabled, the I/O passes directly from Pluggable Storage Architecture (PSA) through the HPP to the device driver.

For the direct submission to work properly, the observed average I/O latency must be less than the latency threshold that you specify. If the I/O latency exceeds the latency threshold, the system stops the direct submission, and temporarily reverts to using the I/O scheduler. The direct submission is resumed when the average I/O latency drops below the latency threshold again.

Note: HPP does not benefit when the systems are not capable of 200,000 IOPS.

Example 2-2 shows how to list the devices that are controlled by the HPP.

Example 2-2 Output of using the esxcli storage hpp device list command

```
[root@localhost:~] esxcli storage hpp device list
eui.70000000000004b5005076081280000c
   Device Display Name: NVMe Fibre Channel Disk (eui.70000000000004b5005076081280000c)
   Path Selection Scheme: LB-RR
   Path Selection Scheme Config: {iops=1,bytes=10485760;}
   Current Path: vmhba64:C0:T0:L3
   Working Path Set: vmhba64:C0:T0:L3, vmhba65:C0:T0:L3
   Is SSD: true
   Is Local: false
   Paths: vmhba64:C0:T0:L3, vmhba65:C0:T1:L3, vmhba65:C0:T0:L3, vmhba64:C0:T1:L3
   Use ANO: false
```

To support multipathing, HPP uses the Path Selection Schemes (PSSs) when you select physical paths for I/O requests.

ESXi supports the following path selection mechanisms for HPP.

Load Balance - Round-Robin

Load Balance - Round-Robin (LB-RR) is the default scheme for the devices that are claimed by HPP. After transferring a specified number of bytes or I/Os on a current path, the scheme selects the path by using the Round-Robin algorithm.

Load Balance - Latency

To achieve better load-balancing results, Load Balance - Latency (LB-Latency) dynamically selects an optimal path by considering the following path characteristics:

- The **`latency evaluation`** `time` parameter indicates at what time interval, in milliseconds, that the latency of paths must be evaluated.
- The **`sampling I/Os per path`** parameter controls how many sample I/Os must be issued on each path to calculate the latency of the path.

Load Balance - IOPS

When using Load Balance - IOPS (LB-IOPS), after transferring a specified number of I/Os on a current path, the system selects an optimal path that has the least number of outstanding I/Os. The default number of I/Os is 1000.

Load Balance - Bytes

When using Load Balance - Bytes (LB-BYTES), after transferring a specified number of bytes on a current path, the system selects an optimal path that has the least number of outstanding bytes. The default number of bytes is 10 MB.

Fixed

With this scheme, a designated preferred path is used for I/O requests. If the preferred path is not assigned, the host selects the first working path that is discovered at start time. If the preferred path becomes unavailable, the host selects an alternative available path. The host returns to the previously defined preferred path when it becomes available again.

When you configure `FIXED` as a path selection mechanism, select the preferred path.

2.4 Zoning considerations

Modern SAN switches have three types of zoning available:

- Switch port zoning, also called port zoning and switch port-based zoning
- Worldwide node name (WWNN) zoning
- WWPN zoning

The preferred method is to use only WWPN zoning. Do not mix zoning types. WWPN zoning is more flexible than switch port zoning and is required if the IBM Storage Virtualize NPIV feature is enabled. Switch port zoning can cause failover of the NPIV ports to not work correctly, and in certain configurations can cause a host to be connected to the IBM Storage FlashSystem on both the physical and virtual WWPNs.

For more information about the NPIV feature and switch port zoning, see Using Switch Port-Based Zoning with the IBM Spectrum Virtualize NPIV Feature.

A common misconception is that WWPN zoning provides poorer security than port zoning. However, modern SAN switches enforce the zoning configuration directly in the switch hardware. Also, you can use port-binding functions on SAN switches so that a WWPN is connected to a particular SAN switch port. Port binding also prevents unauthorized devices from logging in to your fabric if they are connected to switch ports. Lastly, the default zone on each of your virtual fabrics should have a zone policy of deny, which means that any device in the default zone cannot communicate with any other device on the fabric. All unzoned devices (that are not in at least one named zone) are in the default zone.

Naming convention

When you create and maintain a Storage Network zoning configuration, you must have a defined naming convention and zoning scheme. If you do not define a naming convention and zoning scheme, your zoning configuration can be difficult to understand and maintain. Environments have different requirements, which means that the level of detailing in the zoning scheme varies among environments of various sizes. Therefore, ensure that you have an understandable scheme with an appropriate level of detailing for your environment. Then, use it consistently whenever you change the environment.

Aliases

Use aliases when you create your IBM Storage Virtualize system zones. Aliases make your zoning easier to configure and understand and minimize errors. Define aliases for the physical WWPNs, the SCSI-FC WWPNs, and the NVMe over Fibre Channel WWPNs if you have that feature enabled.

You should have the following zones:

- A zone containing all of the IBM Storage Virtualize system aliases for the physical WWPNs that are dedicated for internode use.
- A zone containing all of the IBM Storage Virtualize system aliases for both the local and remote IBM Storage Virtualize system physical WWPNs that are dedicated for partner use if replication is enabled.
- One zone for each host initiator containing the alias for the host initiator and either the IBM Storage Virtualize system SCSI-FC virtual WWPNs, or the NVMe over Fibre Channel virtual WWPNS, depending on which type of host attachment the host is using. For an alternative to this approach, see “Multi-inititiator zoning” on page 23.
- One zone per storage system containing the aliases for the storage system and the IBM Storage Virtualize system physical WWPNs if the IBM Storage FlashSystem is virtualizing storage.

Tip: If you have enough IBM Storage Virtualize system ports available and you have many hosts that you are connecting to an IBM Storage Virtualize system, you should use a scheme to balance the hosts across the ports on the IBM Storage Virtualize system. You can use a simple round-robin scheme, or you can use another scheme, such as numbering the hosts with the even-numbered hosts zoned to the even-numbered ports and the odd-numbered hosts zoned to the odd-numbered ports. Whichever load-balancing scheme that you choose to use, you should ensure that the maximum number of paths from each host to each volume is four paths. The maximum supported number is eight paths for volumes and sixteen paths for HyperSwap volumes. The recommended number is four paths per volume.

Important: Mixing different connectivity protocols in the same host cluster is not supported. *Avoid configuring vSphere clusters with a mixed storage connectivity.*
IBM Storage Virtualize volume mappings cannot be shared between, for example, a SCSI and NVMe hosts.

For SAN zoning best practices, see IBM Support SAN Zoning Best Practices.

Multi-inititiator zoning

For host clusters such as VMware, it is desirable to have all hosts in the cluster in the same zone because it makes administration and troubleshooting easier. This setup can cause issues where a malfunctioning host affects all other hosts in the zone. Traditional best-practice zoning is to have only one initiator (host) per zone.

In recent years, Brocade released the Peer Zoning feature. Cisco released a similar feature that is called Smart Zoning. Both features allow multiple initiators to be in the same zone, but prevent them from connecting to each other. They can connect only to target ports in the zone, which allows multiple hosts to be in the same zone, but prevents the issue of a malfunctioning host port from affecting the other ports.

For VMware clusters, the preferred zoning configuration is to have the ports for all of the hosts in the cluster in a zone with the IBM Storage FlashSystem virtual WWPN.

- Brocade Peer zoning must be enabled for this zone on Brocade fabrics. Brocade Peer Zoning was introduced in FOS v7.4.x.

For more information about Brocade Peer zoning, see *Brocade Fabric OS Administration Guide 9.1.x*.

- Cisco Smart Zoning must be enabled for this zone on Cisco fabrics. Cisco Smart Zoning was introduced in NX-OS v5.2.x.

  For more information about Cisco Smart Zoning, see “Configuring and Managing Zones” in *Cisco MDS Family 9000 NX-OS Fabric Configuration Guide*.

2.5 Recommendations for tuning ESXi hosts

This section describes tuning ESXi hosts for better storage performance.

Setting the Round-Robin IOPS limit to 1

The recommended option for configuring Round-Robin and the correct IOPS limit is to create a rule that sets any new device that is added to that host automatically as a Round-Robin PSP with an I/O Operation Limit value of 1.

VMware Paravirtual SCSI

Paravirtual SCSI (PVSCSI) adapters are high-performance storage adapters that can result in greater throughput and lower CPU usage. PVSCSI adapters are best for SAN environments, where hardware or applications drive a high amount of I/O throughput. The VMware PVSCSI adapter driver is also compatible with the Windows Storport storage driver. PVSCSI adapters are not suitable for direct-attached storage environments.

Large-scale workloads with intensive I/O patterns require adapter queue depths greater than the PVSCSI default values. At the time of writing, the PVSCSI queue depth default values are 64 for device and 254 for adapter. You can increase PVSCSI queue depths to 254 for device and 1024 for adapter inside a Windows or Linux VM.

Eager-zeroed thick virtual disks

An eager-zeroed thick disk has all space allocated and zeroed out at the time of creation. The process increases the time that it takes to create the disk but results in the best performance, even on the first write to each block.

Latency sensitive threshold on NVMe volumes

When you use the HPP for your storage devices, set the latency sensitive threshold for the device so that I/O can avoid the I/O scheduler. By default, ESXi passes every I/O through the I/O scheduler. However, using the scheduler might create internal queuing, which is not efficient with the high-speed storage devices. You can configure the latency sensitive threshold and enable the direct submission mechanism that helps I/O to bypass the scheduler. With this mechanism enabled, the I/O passes directly from PSA through the HPP to the device driver. If the I/O latency exceeds the latency threshold, the system stops the direct submission, and temporarily reverts to using the I/O scheduler. The direct submission is resumed when the average I/O latency is less than the latency threshold.

3

VMware vSphere storage configurations

This chapter describes storage-related configurations in VMware vSphere for IBM Storage FlashSystem storage systems.

This chapter includes the following sections:

- 3.1, “Datastore types” on page 26
- 3.2, “VMware vSphere Storage APIs – Array Integration” on page 33

3.1 Datastore types

Datastores are logical containers that provide a uniform model for storing virtual machine (VM) files, ISO images, and VM templates. The following sections describe the types of datastores that can be deployed with IBM Storage FlashSystem.

3.1.1 vSphere Virtual Machine File System

One type of datastore that you can deploy on IBM Storage FlashSystem storage systems uses the native vSphere Virtual Machine File System (VMFS) format. It is a special high-performance file system format that is optimized for storing VMs and allows shared access to multiple VMware vSphere hosts to concurrently read and write to the same storage. A VMFS datastore can span multiple volumes, which are also called logical unit numbers (LUNs), but this setup is not advisable. Instead, an implementation in a one-to-one type of relationship is recommended. Several versions of the VMFS file system have been released since its introduction. Currently, ESXi supports VMFS5 and VMFS6.

When you work with VMFS datastores, consider the following items:

- Datastore extents

  Do not span more than one extent in a datastore. The recommendation is to have a 1:1 ratio between the datastore and the volume.

- Block size

  The block size on a VMFS datastore defines the maximum file size and the amount of space a file occupies. VMFS5 and VMFS6 datastores support the block size of 1 MB.

- Storage vMotion

  Storage vMotion supports migration across VMFS, virtual storage area network (VSAN), and VMware vSphere Virtual Volume (vVol) datastores. A vCenter Server performs compatibility verification to validate Storage vMotion across different types of datastores.

- Storage Distributed Resource Scheduler (SDRS)

  VMFS5 and VMFS6 can coexist in the same datastore cluster. However, all datastores in the cluster must use homogeneous storage devices. Do not mix devices of different formats within the same datastore cluster.

- Device Partition Formats

  A new VMFS5 or VMFS6 datastore uses a globally unique identifier (GUID) partition table to format the storage device. You can use the GUID partition table (GPT) format to create datastores larger than 2 TB. If your VMFS5 datastore was upgraded from VMFS3, it continues to use the master boot record (MBR) partition format, which is characteristic for VMFS3. Conversion to GPT occurs only after you expand the datastore to a size larger than 2 TB.

Storage I/O Control

Storage I/O Control (SIOC) is a feature that provides I/O prioritization for virtual machine disks (VMDKs) that are on a shared datastore. When a latency threshold is crossed for a shared datastore, SIOC engages and starts prioritizing access to that datastore. By default, all VMs have the same number of shares and a fair access to the datastore. Therefore, SIOC prevents the *noisy neighbor* issue from occurring and ensures that one VM does not monopolize access to that datastore.

Starting with vSphere 6, VMware introduced I/O reservations with SIOC. When reservations are used, the same I/O injector that is used for checking latency also samples the I/O operations per second (IOPS) capabilities of a datastore. When the configured IOPS reservation that is set on the VMs exceeds the observed IOPS capabilities of that datastore, IOPS are distributed to the VMs proportionally to their percentage of the number of set reservations.

The lowest value that you can set is 5 milliseconds. The default is 30 ms. Typically, you cannot reach this value with IBM Storage FlashSystem because it runs IOPS in microseconds. However, if the specified latency is reached, SIOC acts to reduce latency to acceptable levels.

For critical systems, the usual recommendation is to not employ limits or throttling on the VMs resources. Even though SIOC falls into the throttling category, it also provides a fail-safe for unavoidable and unpredictable contention. This function might be helpful when there are multiple VMDKs that share a datastore for manageability reasons.

For more information, see Storage I/O control for critical apps is a great idea.

> **Note:** The goal of Distributed Resource Scheduler (DRS) I/O load-balancing is to fix long-term prolonged I/O imbalances, VMware vSphere SIOC addresses short-term burst and loads.

SIOC limitations and requirements

The following requirements and limitations apply to SIOC:

- Datastores that are SIOC-enabled must be managed by a single vCenter Server system.
- SIOC is supported on VMFS datastores only.
- SIOC does not support datastores with multiple extents.

Setting the Storage I/O Control threshold value

The congestion threshold value for a datastore is the upper limit of latency that is allowed for a datastore before SIOC assigns importance to the VM workloads according to their shares.

You do not need to adjust the threshold setting in most environments. If you change the congestion threshold setting, set the value based on the following considerations:

- A higher value typically results in higher aggregate throughput and weaker isolation. Throttling does not occur unless the overall average latency is higher than the threshold.
- If throughput is more critical than latency, do not set the value too low. For example, for Fibre Channel disks, a value below 20 ms might lower peak disk throughput. A high value of more than 50 ms might allow high latency without significant gain in overall throughput.
- A lower value results in lower device latency and stronger VM I/O performance isolation. Stronger isolation means that the shares controls are enforced more often. Less device latency translates into lower I/O latency for the VMs with the highest shares, at the cost of higher I/O latency experienced by the VMs with fewer shares.
- A low value of less than 20 ms results in lower device latency and isolation among I/Os at the potential cost of a decrease in aggregate datastore throughput.
- Setting the value high or low results in poor isolation.

Datastore clusters: Easy Tier versus SDRS

A datastore cluster is a collection of datastores with shared resources and a shared management interface. You can use vSphere SDRS to manage storage resources when you create a datastore cluster.

SDRS consists of features that can be used to balance storage space and load between datastores by using Storage vMotion to migrate VMs. Depending on your environment, you can automate these tasks or decide to be notified and implement actions yourself.

Easy Tier is an automated process running in IBM Storage Virtualize which constantly monitors the read/write activity on all volumes within a given storage pool. Typically, the system automatically and non-disruptively moves frequently accessed data, referred to as hot data, to a faster tier of storage. For example, the hot data is moved from lower-speed, high-capacity storage to flash-based storage MDisks. To accommodate this, rarely accessed data, cold data, is demoted to a lower tier thus optimizing the I/O flow of the system as a whole.

Note: When you use both Easy Tier and SDRS, the behavior of SDRS can adversely affect the Easy Tier algorithm, which is also called a heatmap, and can unexpectedly impact performance.

In an IBM Storage FlashSystem Easy Tier environment, disable I/O-related functions of SDRS so that Easy Tier can work properly.

SDRS I/O balancing

SDRS is load-balancing based on I/O latency and I/O metrics. I/O metrics build upon SIOC, which continuously monitors the I/O latency, which is the round-trip for I/O. SDRS captures this performance data over a period. The initial period is 16 hours, and after that, it is based on the advanced setting of checking for imbalance every defined period with a default of 8 hours.

If the latency for a datastore exceeds the threshold default of 15 ms over a percentage of time, SDRS migrates VMs to other datastores within the datastore cluster until the latency is below the threshold limit. SDRS might migrate a single VM or multiple VMs to reduce the latency for each datastore below the threshold limit. If SDRS is unsuccessful in reducing latency for a datastore, then at a minimum it tries to balance the latency among all datastores within a datastore cluster.

When I/O metrics are enabled, SIOC is enabled on all datastores in the datastore cluster.

Note: The I/O latency threshold for SDRS should be lower than or equal to the SIOC congestion threshold.

SDRS space balancing

VMware Storage DRS (SDRS) acts as an automated storage manager for your datastore clusters. It continuously monitors the space usage across all datastores in the cluster. When a datastore's used space exceeds a set threshold (default 80%), SDRS can intelligently migrate VMs to other datastores within the cluster. This helps optimize space utilization and maintain storage efficiency. However, it considers a utilization difference threshold (default 5%) between source and destination. If the difference is minimal, SDRS avoids unnecessary migrations. Additionally, it migrates VMs only when there's sufficient space available in the destination datastore.

Powered-on VMs with snapshots are not considered for space balancing.

Tip: As a general recommendation, consider using a datastore cluster or SDRS whenever possible. However, make sure to disable latency-based rules in the Easy Tier environment. SDRS simplifies VM placement when creating, deploying, or cloning VMs. SDRS provides recommendations for balancing on space and I/O. In manual mode, recommendations can be applied on a case-by-case basis.

For more information, see SDRS FAQ (2149938).

Capacity sizing and number of volumes

Table 3-1 summarizes the storage maximums for an ESXi host at the time of writing.

Table 3-1 ESXi host maximums: storage

Category	Description	Limit
Virtual Disks	Virtual Disks per Host	2048
Fibre Channel	LUNs per host	1024
Fibre Channel	LUN size	64 TB
Fibre Channel	LUN ID	0 - 16383
Fibre Channel	Number of paths to a LUN	32
Fibre Channel	Number of total paths on a server	4096
Fibre Channel	Number of host bus adapters (HBAs) of any type	8
Fibre Channel	HBA ports	16
Fibre Channel	Targets per HBA	256
iSCSI Physical	LUNs per server	1024
iSCSI Physical	10 Gb Internet Small Computer System Interface (iSCSI) HBA initiator ports per server	4
iSCSI Physical	Network interface cards (NICs) that can be associated or port-bound with the software iSCSI stack per server	8
iSCSI Physical	Number of total paths on a server	4096
iSCSI Physical	Number of paths to a LUN (software iSCSI and hardware iSCSI)	32
iSCSI Physical	10 Gb iSCSI HBA targets per adapter port	128
iSCSI Physical	Software iSCSI targets	256
Common VMFS	Volume size	64 TB
Common VMFS	Volumes per host	1024
Common VMFS	Hosts per volume	64
Common VMFS	Powered on VMs per VMFS volume	2048
Common VMFS	Concurrent vMotion operations per VMFS volume	128
VMFS5 / VMFS-6	Raw Device Mapping size (virtual compatibility)	62 TB
VMFS5 / VMFS-6	Raw Device Mapping size (physical compatibility)	64 TB

Category	Description	Limit
VMFS5 / VMFS-6	Block size	1 MB
VMFS5 / VMFS-6	File size	62 TB
VMFS5 / VMFS-6	Files per volume	~130690
RDMA NVMe	Namespaces per server	32
RDMA NVMe	Number of paths to a namespace	4
RDMA NVMe	Number of total paths on a server	128
RDMA NVMe	Initiator ports per server	2

3.1.2 Raw Device Mappings

Raw Device Mapping (RDM) is used with VMware ESXi hosts to provide a VM with access to an entire LUN. RDM can be seen as a mapping file in a separate Virtual Machine File System (VMFS) volume, which acts as a proxy to a raw physical storage device, which is a LUN. The RDM contains metadata for managing and redirecting disk access to the physical device.

With RDM, a VM can access and use a storage LUN directly, and it allows the use of VMFS manageability.

Figure 3-1 shows an illustration of the RDM. RDM is a symbolic link from a VMDK file on a VMFS to a raw LUN.

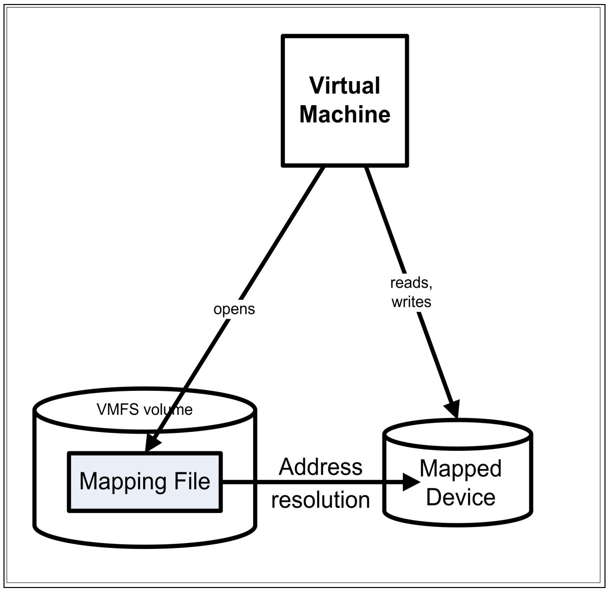


Figure 3-1 Illustrating Raw Device Mapping

An RDM offers several benefits, but it should not be used in every situation. In general, virtual-disk files are preferred over RDMs for manageability purpose.

The most common use case for RDM is Microsoft Cluster Server (MSCS). In an MSCS clustering scenario that spans multiple hosts, which can be a mix of virtual and physical clusters, the cluster data and quorum disk are to be configured as RDMs.

Use of storage area network management agents within a virtual machine

The are two possible RDM modes:

1. Virtual. With virtual mode, the RDM appears to be the same as a virtual disk in a VMFS and the VMKernel sends its reads and writes to the mapping file instead of accessing the physical device directly.
2. Physical. Physical mode provides more control over the physical LUN to access it directly, However, VMware snapshots are not supported. Also, in physical mode, you cannot convert the RDM disk to a VMFS virtual disk by using storage vMotion.

3.1.3 VMware vSphere Virtual Volume

Before VMware vSphere Virtual Volumes (vVols), a VMDK was presented to a VM in the form of a file. This file represents a disk to the VM, which is then accessed by the guest operating system in the same way as a physical disk is accessed on a physical server. This VMDK is stored on a VMware file system (VMFS) formatted datastore.

The VMFS datastore is hosted by a single volume on a storage system, such as the IBM Storage FlashSystem 9200. A single VMFS datastore can have hundreds or even thousands of VMDKs.

VMware vVols provide a one-to-one mapping between the VM's disks and the volumes that are hosted by the storage system. These vVols are wholly owned by the VM. Making the vVols available at the storage level enables storage system-based operations at the granular VM level. For example, capabilities such as compression and encryption can be applied to an individual VM. Similarly, IBM FlashCopy® can be used at the vVol level when you perform snapshot and clone operations.

The integration of vVols with IBM Storage Virtualize storage systems is dependent upon the vSphere application programming interfaces (APIs) for Storage Awareness (VASA). These APIs facilitate VM-related tasks that are initiated at the vSphere level to be communicated down to the storage system.

IBM support for VASA was originally provided by IBM Spectrum Connect, but for IBM Storage Virtualize 8.5.1.0 or later the VASA functionality is serviced by the new Embedded VASA Provider. IBM Spectrum Connect is an out-of-band VASA Provider, which enables the communication between vSphere and the storage system along the control plane.

Note: IBM Spectrum Connect is still required to use vVols on IBM FlashSystem 5015, 5035 or 5045 platforms.

IBM Storage FlashSystem manages vVols at the storage level and enables the flexible and dynamic provisioning of VM storage that is required of a truly software-defined storage environment.

For information about how to implement vVols with IBM Storage FlashSystem, see Chapter 8, "Integrating with VMware by using IBM Spectrum Connect" on page 179.

Storage system considerations

When you plan an implementation of vVols, the goal is to highlight the decisions that need to be made to maximize the potential of vVols and meet the needs of your environment.

Because the storage for vVols is allocated as a child pool, it is important to consider the structure of the parent pools from which these child pools are allocated. The following sections describe the two contrasting approaches to defining parent pools and a description of how their usage might influence the vVols environment.

Drive class based

You might want to define parent pools based on the underlying drive class. This approach enables the allocation of child pools from a specific tier of storage. At the vSphere level, these child pools serve as the backing-storage container for distinct vVols datastores. This approach enables you to determine the class of storage for individual vVols when provisioning VMs.

You can use vSphere policies, for example, Gold, Silver, and Bronze, to select the appropriate class of storage when you provision VMs.

Figure 3-2 shows an example of this configuration.

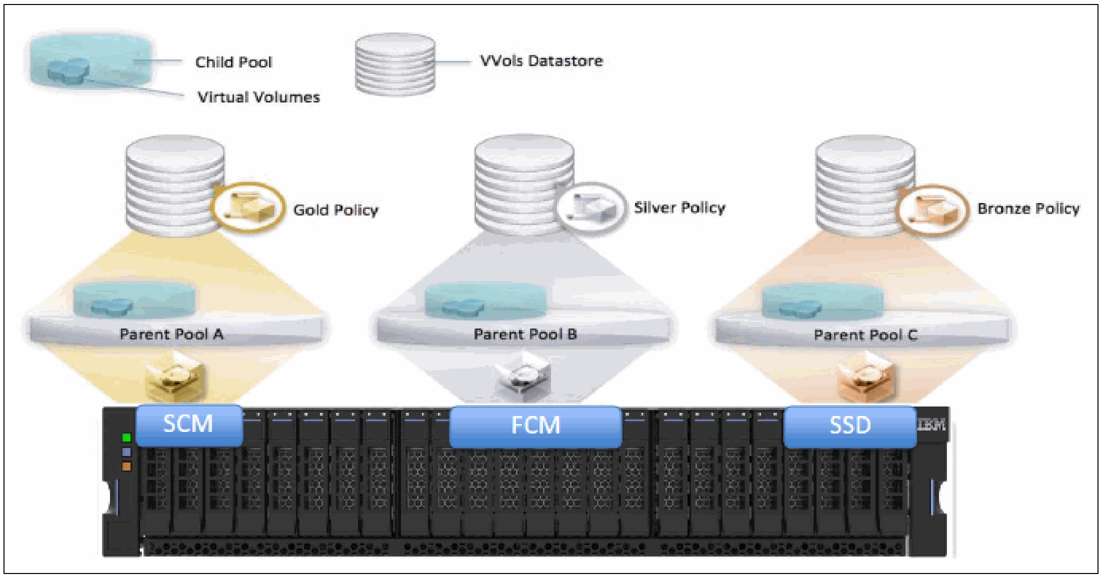


Figure 3-2 A vVols environment where parent and child pools are segregated by drive class

With the introduction of vVols, by defining a range of storage services on IBM Spectrum Connect, policies can become far more interesting and useful than the simple Gold, Silver, and Bronze model.

Each of the policies (gold, silver, and bronze) can be further subdivided. For example, the solid-state drive (SSD) parent pool can be divided into two distinct child pools. One child pool is linked to an encrypted storage service, and the other is associated with an unencrypted storage service. This approach provides the vSphere administrators with the flexibility to provision VMs on storage that matches the requirements of the application, on a per-VM basis.

IBM Easy Tier based

An alternative to the drive-class based parent pools would be to define parent pools with a combination of drive classes, and enable the IBM Easy Tier feature. By monitoring the heatmap of a volume's extents, Easy Tier can intelligently optimize the use of storage by automatically migrating these extents onto the most appropriate storage tier.

Because vVols are a special volume, Easy Tier can manage their extents in an identical fashion.

- A *hot* or frequently used extent of a vVol is promoted to faster storage, such as SSD.
- A *cold* or infrequently used extent of a vVol is moved onto slower drives.

A vVols implementation that takes advantage of Easy Tier can provide greater simplicity for the storage administrator. By defining a child pool within an Easy Tier enabled parent pool, the storage system is enabled to manage the extents of any vVols created therein.

This flexibility removes the requirement for a choice of storage class when the vSphere administrator initially provisions the VM. Such an approach can also minimize the need for Storage vMotion tasks because Easy Tier eliminates the requirement to manually migrate vVols onto faster or slower storage as the needs of an application change.

Figure 3-3 demonstrates a vVols configuration, based on a single parent pool, with Easy Tier enabled.

Note: Easy Tier also provides benefits within a single-tiered pool. When enabled, Easy Tier automatically balances the load between managed disks (MDisks) to optimize performance.

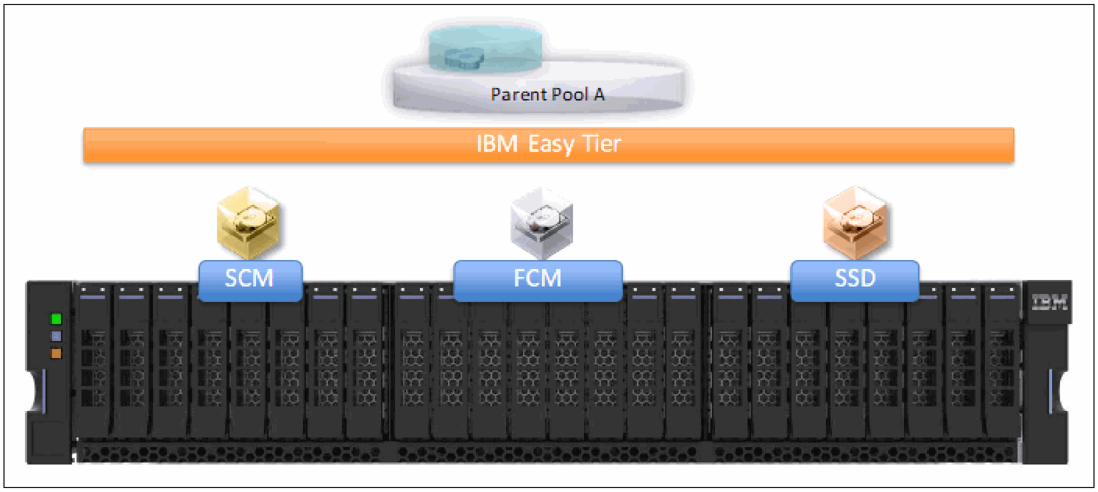


Figure 3-3 The simplified approach to vVols provisioning that can be implemented by enabling Easy Tier

3.2 VMware vSphere Storage APIs – Array Integration

VMware vSphere Storage APIs – Array Integration (VAAI), also known as hardware acceleration, is an API that allows the VMware vSphere host to offload resource-intensive I/O operations to the storage array, for example, by copying the VM files.

- Without VAAI, the VM files are copied by using the host.
- With VAAI, the data is copied within the same storage array.

VAAI helps the ESXi performance because the storage area network (SAN) fabric is not used and fewer central processing unit (CPU) cycles are needed because the copy does not need to be handled by the host.

In vSphere 5.x and later releases, these extensions, VAAI operations, are implemented as T10 SCSI commands. As a result, with the devices that support the T10 SCSI standard, such as the IBM Storage FlashSystem, your ESXi host can communicate directly and does not require the VAAI plug-ins.

The following types of operations are supported by the VAAI hardware acceleration for IBM Storage FlashSystem:

- Atomic Test and Set (ATS), which is used during the creation and locking of files on the VMFS volume
- Clone Blocks, Full Copy, and extended copy (XCOPY), which is used to copy or migrate data within the same physical array
- Zero Blocks/Write Same, which is used when creating VMDKs with an eager-zeroed thick provisioning profile
- SCSI UNMAP, which is used to reclaim storage space

3.2.1 Atomic Test and Set / SCSI Compare and Write

ATS, also known as hardware-assisted locking, relegates resource-access serialization at the granularity of the block-level during VMware metadata updates. ATS uses this approach rather than using a mature SCSI2 reservation, which serializes access to the adjacent ESXi hosts with a minimum scope of an entire LUN.

ATS is a standard T10 SCSI command with opcode 0x89, which is SCSI Compare and Write (CAW). The ATS primitive has the following advantages where LUNs are used by multiple applications or processes at one time:

- Significantly reduces SCSI reservation contentions by locking a range of blocks within a LUN rather than issuing a SCSI reservation on the entire LUN
- Enables parallel storage processing
- Reduces latency for multiple ESXi hosts accessing the same LUN during common operations
- Increases cluster scalability by greatly extending the number of ESXi hosts and VMs that can viably reside simultaneously on a VMFS datastore

Our recommendation is to enable ATS hardware-accelerated locking and set to **`ATS-only public`**. For more information, see Configuring the ESXi operating system.

> **Note:** All newly formatted VMFS5 and VMFS6 datastores use the ATS-only mechanism if the underlying storage supports it. SCSI reservations are never used.
>
> VMFS3 volumes that are upgraded to VMFS5 must be manually upgraded to ATS-only so that it is easier to redeploy the datastore and migrate the VMs to the datastore.

VMware ATS heartbeating

VMware ESXi uses the SCSI CAW command to heartbeat periodically to datastores. VMware refers to this command as ATS.

> **Note:** The use of ATS heartbeating is not supported on the following platforms:
>
> - ESXi hosts that run version 5.5 update 2 or later
> - ESXi version 6.0 before update 3

During high-latency events, ATS heartbeats might timeout, which results in ATS miscompare errors. If multiple heartbeat attempts fail, the ESXi host might lose access to the datastore in which timeouts are observed.

ATS heartbeating increases the load on the system and can lead to access issues on busy systems, particularly during maintenance procedures. To reduce this load, ATS heartbeats can be disabled.

- For VMware vSphere versions 5.5 and 6.0, the recommendation is to disable ATS heartbeating because of host-disconnect issues.

  To disable ATS heartbeats, run the following command:

  ```
  esxcli system settings advanced set -i 0 -o /VMFS3/UseATSForHBOnVMFS5
  ```

- For VMware vSphere versions 6.5, 6.7 and 7.0, the recommendation is to enable ATS heartbeating.

  To enable ATS heartbeats, run the following command-line interface (CLI) command:

  ```
  esxcli system settings advanced set -i 1 -o /VMFS3/UseATSForHBOnVMFS5
  ```

3.2.2 Extended copy

XCOPY, also known as a hardware-accelerated move, offloads copy operations from VMware ESXi to the IBM Storage FlashSystem. This process allows for rapid movement of data when performing copy or move operations within the IBM storage system. XCOPY reduces CPU cycles and host bus adapter (HBA) workload of the ESXi host.

Similarly, XCOPY reduces the volume of traffic that is moving through the SAN when a VM is deployed. It does so by synchronizing individual VM-level or file system operations, including clone and migration activities, with the physical storage-level operations at the granularity of individual blocks on the devices. The potential scope in the context of the storage is both within and across LUNs.

The **XCOPY** command has the following benefits:

- Expedites copy operations including the following tasks:
  - Cloning of VMs, including deploying from template
  - Migrating VMs from one datastore to another (storage vMotion)
- Minimizes host processing and resource allocation: Copies data from one LUN to another without reading and writing through the ESXi host and network.
- Reduces SAN traffic.

The SCSI opcode for XCOPY is **0x83**. As a best practice, set the XCOPY transfer size to **4096**, as shown in Example 3-1.

Example 3-1 XCOPY transfer size 4096

```
# Get-VMHost  | Get-AdvancedSetting -Name DataMover.MaxHWTransferSize | select Entity, name, value
Entity                         Name                        Value
------                         ----                        -----
vmlab11c2.ssd.hursley.ibm.com DataMover.MaxHWTransferSize  4096
```

3.2.3 WRITE_SAME

Block Zeroing, Write_Same (Zero), or hardware-accelerated initialization uses the **`WRITE_SAME 0x93`** SCSI command to issue a chain of identical write transactions to the storage system. This command almost eliminates server processor and memory use by eliminating the need for the host to run repetitive identical write transactions. It also reduces the volume of host HBA and SAN traffic when repetitive block-level write operations are performed within VM disks to the IBM Storage FlashSystem.

The **`WRITE_SAME 0x93`** SCSI command allows the IBM Storage FlashSystem to minimize internal bandwidth consumption. For example, when provisioning a VMDK file with the **`eagerzeroedthick`** specification, the Zero Block's primitive issues a single **`WRITE_SAME`** command. The single **`WRITE_SAME`** command replicates zeros across the capacity range that is represented by the difference between the provisioned capacity of the VMDK and the capacity that is consumed by actual data. The alternative to using the **`WRITE_SAME`** command requires the ESXi host to issue individual writes to fill the VMDK file with zeros. The same applies when cloning or running storage vMotion of a VM with eager-zeroed thick VMDKs.

The scope of the Zero Block's primitive is the VMDK creation within a VMFS datastore. Therefore, the scope of the primitive is generally within a single LUN on the storage subsystem, but it can potentially span LUNs backing multi-extent datastores.

Block Zeroing offers the following benefits:

- Offloads initial formatting of Eager Zero Thick (EZT) VMDKs to the storage array
- Assigns zeros to large areas of storage without writing zeros from the ESXi host
- Speeds up creation of new VMs
- Reduces elapsed time, server workload, and network workload

> **Note:** In thin-provisioned volumes, IBM Storage FlashSystem further augments this benefit by flagging the capacity as `zeroed` in metadata without the requirement to physically write zeros to the cache and the disk, which implies even faster provisioning of the eager-zeroed VMDKs.

3.2.4 SCSI UNMAP command

IBM Storage FlashSystem that is built with IBM Storage Virtualize software supports the SCSI UNMAP command since Version 8.1.0, which enables hosts to notify the storage controller of capacity that is no longer required, which might improve savings. Reclaiming storage space can provide higher host-to-flash I/O throughput and improve flash endurance.

When an IBM Storage FlashSystem receives a SCSI UNMAP command, it overwrites the relevant region of the volume with all-zero data, which allows thin-provisioned storage controllers, such as the IBM Storage FlashSystem, to reclaim physical capacity through garbage collection.

The main benefit is that this action helps prevent a thin-provisioning storage controller from running out of free capacity for write I/O requests. When thin-provisioned storage controllers are used, SCSI UNMAP should normally be left enabled.

With lower-performing storage, such as nearline arrays, extra I/O workload can be generated, which can increase response times.

To enable SCSI UNMAP, run the following command on IBM Storage FlashSystem:

```
chsystem -hostunmap on
```

Enabling SCSI UNMAP does not affect data on older volumes that are created before using this command. Create datastores on newly created volumes, migrate data through storage vMotion, and delete old volumes.

SCSI UNMAP effects on standard storage pool and on data reduction pool

Hosting UNMAP commands in a standard storage pool results in data being zeroed, but does not increase the free capacity that is reported by the storage pool. When an array is composed of IBM FlashCore Module (FCM) modules, the UNMAP command increases the free physical capacity on that array.

Host UNMAP commands can increase the free capacity that is reported by the data reduction pool (DRP) when received by thin-provisioned or compressed volumes. SCSI UNMAP commands are also sent to internal FlashCore Modules (FCMs) to free physical capacity.

For more information, see SCSI Unmap support in IBM Spectrum Virtualize systems.

For more information about DRPs, see *Introduction and Implementation of Data Reduction Pools and Deduplication*, SG24-8430.

Storage space reclamation

ESXi supports the SCSI UNMAP command, also known as the space reclamation command, that originates from a VMFS datastore or a VM guest operating system.

Inside the VM, storage space is freed when you delete files on the thin virtual disk. Storage space that is left by deleting or removing files from a VMFS datastore can be freed up within the file system. This free space is allocated to a storage device until the file system releases or unmaps it. This operation helps the storage array to reclaim unused free space.

Space reclamation requests from VMFS datastores

VMFS5 and earlier file systems do not unmap free space automatically, but you can use the **`esxcli storage vmfs unmap`** command to reclaim space manually. When you use the command, be aware that it might send many unmap requests simultaneously. This action can lock some of the resources during the operation.

On VMFS6 datastores, ESXi supports the automatic asynchronous reclamation of free space. VMFS6 can run the UNMAP command to release free storage space in the background on thin-provisioned storage arrays that support unmap operations. Asynchronous unmap processing has several advantages:

- Unmap requests are sent at a rate that can be throttled in vSphere, which helps to avoid any instant load on the backing array.
- Freed regions are batched and unmapped together.
- I/O performance of other workloads is not impacted by the UNMAP command.

For information about the space-reclamation parameters for VMFS6 datastores, see Space Reclamation Requests from VMFS Datastores.

Space reclamation requests from guest operating systems

ESXi supports the UNMAP commands that are issued directly from a guest operating system to reclaim storage space. The level of support and requirements depend on the type of datastore in which your VM resides.

The guest operating system notifies VMFS about freed space by sending the UNMAP command. The UNMAP command that is sent from the guest operating system releases space within the VMFS datastore. The command proceeds to the array so that the array can reclaim the freed blocks of space.

VMs that use VMFS5 typically cannot pass the UNMAP command directly to the array. You must run the **esxcli storage vmfs unmap** command to trigger unmaps from the IBM Storage FlashSystem. However, for a limited number of the guest operating systems, VMFS5 supports the automatic space reclamation requests.

To send the unmap requests from the guest operating system to the array, the VM must meet the following prerequisites:

- The virtual disk must be thin-provisioned.
- VM hardware must be version 11 (ESXi 6.0) or later.
- The advanced **EnableBlockDelete** setting must be set to 1.
- The guest operating system must be able to identify the virtual disk as thin.

VMFS6 generally supports automatic space-reclamation requests that generate from the guest operating systems, and passes these requests to the array. Many guest operating systems can send the UNMAP command and do not require any additional configuration. The guest operating systems that do not support automatic unmaps might require user intervention.

The following considerations apply when you use space reclamation with VMFS6:

- VMFS6 processes the unmap request from the guest operating system (OS) only when the space to reclaim equals 1 MB or is a multiple of 1 MB. If the space is less than 1 MB or is not aligned to 1 MB, the unmap requests are not processed.
- For VMs with snapshots in the default SEsparse format, VMFS6 supports the automatic space reclamation only on ESXi hosts version 6.7 or later.

Space reclamation affects only the top snapshot and works when the VM is powered on.

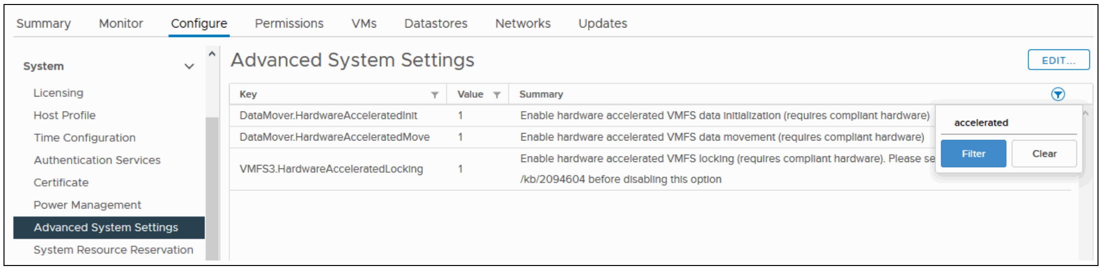
IBM Storage FlashSystem and VAAI

To verify which VAAI operations are supported by your storage device, issue a command as shown in Example 3-2.

Example 3-2 Verifying device VAAI support where "naa.xxx" stands for device identifier

```
[root@ESX1-ITSO:~] esxcli storage core device vaai status get -d naa.xxx
naa.xxx
   VAAI Plugin Name:
   ATS Status: supported
   Clone Status: supported
   Zero Status: supported
   Delete Status: unsupported
```

You can verify and change your VAAI settings in the host Advanced System Settings (Figure 3-4 on page 39). A value of 1 means that the feature is enabled. If the setting is host-wide, it is enabled if the connected storage supports it.



Advanced System Settings

Key	Value	Summary
DataMover.HardwareAcceleratedInit	1	Enable hardware accelerated VMFS data initialization (requires compliant hardware)
DataMover.HardwareAcceleratedMove	1	Enable hardware accelerated VMFS data movement (requires compliant hardware)
VMFS3.HardwareAcceleratedLocking	1	Enable hardware accelerated VMFS locking (requires compliant hardware). Please se /kb/2094604 before disabling this option

Figure 3-4 VAAI settings

Table 3-2 lists the VAAI settings and parameter descriptions.

Table 3-2 Parameters description

Parameter name	Description
DataMover.HardwareAcceleratedInit	Zero Blocks/Write Same
DataMover.HardwareAcceleratedMove	Clone Blocks/XCOPY
VMFS3.HardwareAcceleratedLocking	Atomic Test and Set (ATS)

It is advisable to keep all VAAI operations enabled when using IBM Storage FlashSystem storage systems so that as much work as possible is offloaded to storage.

Example 3-3 shows how to evaluate the VAAI status by using the PowerCLI command.

Example 3-3 PowerCLI command that is used to evaluate the VAAI status

```
# Get-VMHost  | Get-AdvancedSetting -name *HardwareAccelerated* | select Name, value
Name                                  Value
----                                  -----
DataMover.HardwareAcceleratedMove         1
VMFS3.HardwareAcceleratedLocking          1
DataMover.HardwareAcceleratedInit         1
```

Hardware offloading is not used if the following conditions occur:

- The source and destination VMFS datastores have different block sizes. This situation can happen when you use existing VMFS3 datastores.
- The source disk is RDM and the destination is a non-RDM, regular VMDK.
- The source VMDK type is `eagerzeroedthick` but the destination VMDK type is thin.
- The source or destination VMDK is in a sparse or hosted format.
- The source VM has a snapshot.
- The logical address and transfer length in the requested operation are not aligned to the minimum alignment required by the storage device. All datastores created with the vSphere Web Client are aligned automatically.
- The VMFS has multiple LUNs or extents, and they are on different arrays.
- Hardware cloning between arrays, even within the same VMFS datastore, does not work. This situation is not the case if arrays are managed by IBM Storage FlashSystem by using external virtualization.

Note: You might decide to increase a block size (`MaxHWTransferSize` for XCOPY), which is processed by storage globally. Although changing default values is not recommended, you might notice a small improvement, typically around 10%, in the performance during Data Mover operations. This change is global and affects all your VAAI-enabled storage devices that are connected to the ESXi. Therefore, changing the default values can have an unpredictable impact on different storage arrays.

4

Preparing for disaster recovery

This chapter describes some of the solutions that can help you prepare your environment to recover from a disruption by using VMware and IBM Storage Virtualize Data Protection and Disaster Recovery, which includes the following sections:

- 4.1, “Introduction” on page 42
- 4.2, “Volume groups” on page 42
- 4.3, “Copy services overview” on page 43
- 4.4, “Storage Replication Adapter with VMware Site Recovery Manager” on page 49
- 4.5, “IBM HyperSwap with VMware vSphere Metro Storage Cluster” on page 70

4.1 Introduction

The term disaster recovery (DR) is normally used regarding a large, significant, and disruptive event, such as an earthquake or flood. But DR can also be valuable for smaller events, such as power-loss or a localized network failure.

Companies prepare for DR by implementing business continuity solutions to maintain and restore operations if a disruption or disaster occurs, but they do not always test those solutions regularly. The ability to recover the systems needs to be tested regularly to make sure that procedures work, rather than waiting until a disruption happens. Flaws might be detected each time you test because perfection is impossible to achieve when the environment changes every day.

As cyberattacks increase in both frequency and sophistication, storage data protection is an important consideration for everyone from corporate executives to IT managers. However, even with protections in place, 100% data loss prevention is not possible. And, increasingly, cyberattacks that use ransomware and malware are targeting backup copies of data to make recovery and replication even harder. IBM Storage Virtualize incorporates several different Data Protection techniques to help mitigate risk in the event of a security breach.

Copy services are a collection of functions that provide capabilities for business continuity, disaster recovery, data migration, and data duplication solutions. This chapter provides an overview and the preferred best practices guide for VMware and IBM Storage Virtualize using Data Protection techniques.

For replication capabilities including support for VMware Site Recovery Manager (SRM) and by using the IBM Storage Replication Adapter (SRA), the following mechanisms are supported:

- Policy-based replication
- HyperSwap
- Metro Mirror
- Global Mirror

The following copy services techniques are implemented in IBM Storage Virtualize to help protect against unexpected data loss:

- Volume group snapshots
- SafeGuarded Copy
- FlashCopy

4.2 Volume groups

A volume group is, as the name suggests a group of volumes. More importantly, it is a container for managing a set of related volumes as a single object with the goal of simplifying the process of provisioning, managing, replicating, and protecting data.

The volume group provides consistency across all volumes in the group and can be used with the following functions.

4.2.1 Policy-based replication

You can use volume groups for policy-based replication. Policy-based replication is configured on all volumes in a volume group by assigning a replication policy to that volume group. The system automatically replicates the data and configuration for volumes in the group based on the values and settings in the replication policy. As part of policy-based replication, a recovery volume group is created automatically on the recovery system. Recovery volume groups cannot be created, changed, or deleted other than by the policy-based replication. A single replication policy can be assigned to multiple volume groups to simplify replication management. When additional volumes are added to the group, replication is automatically configured for these new volumes. Policy-based replication supports configuration changes while the partnership is disconnected. After the partnership is reconnected, the system automatically reconfigures the recovery system.

4.2.2 Volume group snapshots

Snapshots are the read-only point-in-time copies of a volume group that cannot be directly accessed from the hosts. To access the snapshot contents, you can create a clone or thin clone of a volume group snapshot. You can use the command-line interface or management GUI to configure volume groups to use snapshot policies for multiple volumes for consistent management. Snapshots are always in the same pool as the parent volume, and the I/O group of the snapshot is same as the parent volume.

4.2.3 Safeguarded Copy

One implementation of volume groups is to group volumes to be configured as Safeguarded. The Safeguarded copy function is a cyber-resiliency feature that creates immutable copies of data that cannot be changed or manipulated.

A Safeguarded volume group describes a set of source volumes that can span different pools and are backed up collectively with the Safeguarded Copy function. Safeguarded snapshots are created either manually, or through an internal scheduler that is defined in the snapshot policy. Alternatively, Safeguarded snapshots can be configured with an external snapshot scheduling application such as IBM Copy Services Manager.

4.3 Copy services overview

IBM Storage Virtualize system offers a complete set of copy services functions to VMware that provide capabilities for business continuity, disaster recovery, data movement, and data duplication solutions. The IBM Storage Virtualize Family Storage Replication Adapter (SRA) is a software add-on that integrates with the VMware Site Recovery Manager (SRM) solution and enables SRM to perform failovers together with supported IBM Storage FlashSystem storage. You can make mirror images of part or all of your data between two sites, which is advantageous in DR scenarios with the capabilities of copying data from production environments to another site for resilience.

The following copy services relationships are supported by IBM Storage Virtualize system:

- Policy-based replication
- Volume group snapshots
- SafeGuarded Copy
- FlashCopy, for point-in-time copy
- Metro Mirror, for synchronous remote copy
- Global Mirror, for asynchronous remote copy
- Global Mirror with change volumes (GMCV), for asynchronous remote copy for a low-bandwidth connection

Replication relationships can be created between a maximum of four independent IBM Storage Virtualize systems. Partnerships can be a mix of any of the IBM Storage Virtualize systems. For example, an IBM Storage FlashSystem storage array can replicate to a SAN Volume Controller (SVC) storage system and vice versa. For more information about these services, see Chapter 10, “Advanced Copy Services” in the IBM Redbooks publication titled *Implementation Guide for IBM Storage FlashSystem and IBM SAN Volume Controller: Updated for IBM Storage Virtualize Version 8.6,* SG24-8542.

Note: All these copy services, except Snapshot, are supported by VMware SRM when using IBM Storage Virtualize Family SRA 4.1.0.

4.3.1 Volume group snapshots

Volume group snapshots are the next generation of copy services for IBM FlashSystem and Storage Virtualize. This point-in-time copy solution builds upon the robustness and versatility of existing IBM FlashCopy technology and streamlines it for ease of use and simplicity. Volume group snapshots can be triggered manually, or by an internal scheduler that runs within the storage system in accordance with pre-defined snapshot policies.

Snapshot policies

A snapshot policy is a set of rules that controls the creation, retention, and expiration of snapshots.

With snapshot policies, administrators can schedule the creation of snapshots for volumes in a volume group at specific intervals and retain based on their security and recovery point objectives (RPO). A snapshot policy has the following properties:

- It can be assigned to one or more volume groups.
- Only one snapshot policy can be scheduled to one volume group.
- The system supports a maximum number of 32 snapshot policies.

The system supports an internal scheduler to manage and create snapshot policies on the system. The management GUI supports selecting either a user-defined policy or a predefined policy, and the user-defined policies can be created by using the management GUI or by using the **mksnapshotpolicy** command. Predefined policies contain specific retention and frequency values for common use-cases. Both predefined and user-defined policies are managed on the IBM Storage Virtualize system.

4.3.2 Safeguarded Copy

The Safeguarded Copy function supports the ability to create cyber-resilient point-in-time copies of volumes that cannot be changed or deleted through user errors, malicious actions, or ransomware attacks.

Safeguarded snapshots are supported on the system through an internal scheduler that is defined in the snapshot policy. When the policy is assigned to a volume group, you can select the Safeguarded option. The policy creates immutable snapshots of all volumes in the volume group. The system supports internal and external snapshot scheduling applications such as IBM Copy Services Manager and IBM Storage Copy Data Management. For Safeguarded snapshots with internal scheduler, refer to Managing snapshots.

After you configure Safeguarded Copy function on your system, regularly test the configuration to ensure that Safeguarded backups are ready in the event of a cyberattack. In addition to testing and recovering, you can also manage objects that are related to the

Safeguarded Copy function on the system. These tasks include adding source volumes to Safeguarded volume groups, managing Safeguarded backups after expiration, and other actions. Some administrative actions are completed on the system, and others are completed on the management interface for the external scheduling application, such as IBM Storage Copy Data Management or IBM Copy Services Manager.

4.3.3 Policy-based replication

Policy-based replication uses volume groups and replication policies to automatically deploy and manage replication. Policy-based replication can simplify configuring, managing, and monitoring replication between two systems.

A replication policy is a key concept in policy-based replication. Replication policies are assigned to volume groups and define how replication is applied to all volumes within that volume group. A replication policy can be assigned to multiple volume groups, but a volume group can be assigned to only a single replication policy.

Volume groups used with policy-based replication require that all volumes in the volume group have the same caching I/O group.

Policy-based replication supports the following three replication modes.

Production

In a volume group where the volumes in the group are accessible for host I/O, configuration changes are allowed. This system acts as the source for replication to any recovery copies. By definition, a production volume group always contains an up-to-date copy of application data for host access.

Recovery

On the system where the volumes in the group are able to only receive replication I/O, they act as a target for replication and cannot be used for host I/O. Configuration changes are not allowed on the recovery copy, but changes made to the production copy are replicated to the recovery copy.

Independent

If independent access is enabled for the volume group, such as during a disaster, each copy of the volume group is accessible for host I/O, and configuration changes are allowed. Replication is suspended in this state and configuration changes are allowed on both the copies.

Replication policies do not define the direction for replication. Direction for replication is determined when a replication policy is associated with a volume group, or a volume group is created specifying a replication policy. The system where replication policy is configured is the production system.

An important concept is that the configuration and the data on the volumes are coupled, and the recovery point is formed from both the configuration and volume data. Adding, creating, removing, or deleting volumes from a volume group is reflected on the recovery system at the equivalent point-in time as they did on the production system. If independent access is enabled on a recovery volume group during a disaster, then volumes on the production system are from a previous point-in-time. When independent access is enabled on the recovery system, any partially synchronized volumes are deleted.

If a volume group is independent, configuration changes that are made from either system are not applied to the other copy of the volume group. When replication is restarted, the system automatically changes the configuration on the recovery volume group to match the production volume group.

When you delete volumes from the production volume group, the copy of the volume on the recovery volume group is deleted. The volume is deleted when the recovery volume group has a recovery point that does not include the deleted volume.

Removing a replication policy from a volume group causes the recovery volume group and its volumes to be deleted. To keep the recovery copy, independent access must be enabled on the recovery copy first and then the replication policy must be removed from the volume group in both locations.

The replication policy assigned to a volume group can be changed to a compatible policy without requiring a full resynchronization. A compatible policy that is associated is defined as having the same locations. With the compatible policy, the existing replication policy gets removed, and the new policy is applied. Attempts to change the policy to an incompatible policy is rejected by the system.

4.3.4 FlashCopy

FlashCopy is known as a point-in-time copy. It makes a copy of the blocks from a source volume and duplicates them to the target volumes.

When you initiate a FlashCopy operation, a FlashCopy relationship is created between a source volume and a target volume. A FlashCopy relationship is a mapping of the FlashCopy source volume and a FlashCopy target volume. This mapping allows a point-in-time copy of that source volume to be copied to the associated target volume. If it is a persistent FlashCopy, the FlashCopy relationship exists between this volume pair from the time that you initiate a FlashCopy operation until the storage unit copies all data from the source volume to the target volume or until you delete the FlashCopy relationship.

4.3.5 Metro Mirror

Metro Mirror is a type of remote copying that creates a synchronous copy of data from a primary volume to a secondary volume that is read only. A secondary volume can be located either on the same system or on another system. The maximum distance that is allowed between systems in Metro Mirror relationships is 300 km. When a host issues a `write` command to a volume, the data is replicated to the remote cluster before the host is notified that the I/O is finished.

Tip: Metro Mirror can increase write latency. For best performance, use shorter distances and create Metro Mirror relationships only between systems with similar performance.

4.3.6 Global Mirror

The Global Mirror function provides an asynchronous copy process. When a host writes to the primary volume, confirmation of I/O completion is received before the write operation completes for the copy on the secondary volume. The maximum acceptable distance between systems in Global Mirror relationships is 25,000 km or 250 ms latency.

Global Mirror change volumes

Global Mirror *change volumes* are copies of data from a primary volume or secondary volume that are used in Global Mirror relationships. Using change volumes lowers bandwidth requirements by addressing only the average throughput, not the peak.

4.3.7 Policy-based replication

Policy-based replication is the successor to asynchronous Remote Copy for providing replication services for IBM Storage FlashSystem, IBM SAN Volume Controller, and IBM Storage Virtualize for version 8.5.2 and later. This management model uses volume groups and replication policies to enable the system to automatically deploy and manage replication. This can simplify the tasks that are associated with configuring, managing, and monitoring replication.

Compared to Remote Copy, policy-based replication replicates data between systems with minimal overhead, significantly higher throughput, and reduced latency characteristics.

4.3.8 Remote copy consistency groups

You can group Metro Mirror or Global Mirror relationships into a consistency group so that they can be updated at the same time. A command is then simultaneously applied to all of the relationships in the consistency group.

> **Note:** Volume groups provide the same consistency capability to policy-based replication configurations.

4.3.9 VMware Site Recovery Manager

VMware SRM is known in the virtualization world for providing simple, affordable, and reliable business continuity and disaster recovery management.

The use of SRM with IBM Storage Virtualize system can help you protect your virtual environment.

SRM automates the failover processes and the ability to test failover processes or DR without having a negative impact on the live environment, which helps you meet your recovery time objectives (RTOs).

VMware SRM supports three forms of replication:

1. Array-based replication (ABR), where the storage system manages the virtual machine (VM) replication with the following attributes:
   - Compatible storage is required, such as systems powered by IBM Storage Virtualize.
   - Storage arrays are configured with an SRA.
2. Host-based replication, which is known as vSphere Replication (VR), where vSphere manages the VM replication with the following attributes:
   - Does not depend on storage array compatibility.
   - Increased network efficiency by replicating only the most recent data in the changed disk areas.
   - Minimum RPO = 5 minutes.

3. vVol-based replication:
   - Compatible Storage is required.
   - At the time of writing, it is *not* supported by Storage Virtualize systems.

Figure 4-1 shows an overview of the VMware SRM.

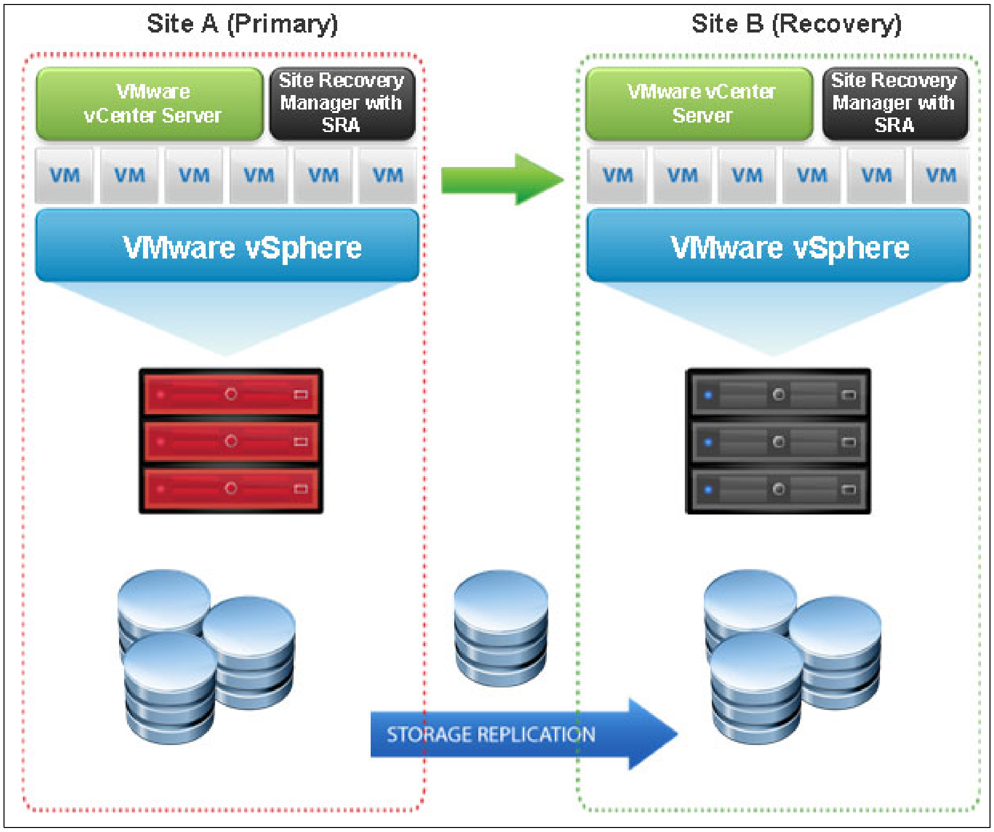


Figure 4-1 VMware SRM

VMware SRM requires one vCenter server in each site with the respective licenses. Also, if you are using SRM with IBM Storage FlashSystem storage, you are required to use an IBM Storage Virtualize SRA, which is described in 4.3.10, “Storage Replication Adapter” on page 48.

For more information about SRM, see VMware Site Recovery Manager Documentation.

4.3.10 Storage Replication Adapter

Storage Replication Adapter (SRA) is a storage vendor plug-in that is developed by IBM. SRA is required for the correct functioning of SRM when it is used with IBM Storage Virtualize systems.

The adapter is used to enable the management of Advanced Copy Services (ACS) on IBM FlashSystem Storage, such as policy-based replication, Metro Mirror, Global Mirror and Global Mirror with change volumes.

The combination of SRM and SRA enables the automated failover of VMs from one location to another, connected by either replication method.

By using the IBM Storage Virtualize Family Storage Replication Adapter, VMware administrators can automate the failover of an IBM Storage FlashSystem 9500 at the primary SRM site to a compatible system at a recovery (secondary) SRM site. Compatible systems include another IBM Storage FlashSystem 9500, 9200, 9100, 7300, 7200, or IBM SAN Volume Controller.

In a failover, the ESXi servers at the secondary SRM site mount the replicated datastores on the mirrored volumes of the auxiliary storage system. When the primary site is back online, run a failback from the recovery site to the primary site by clicking **Reprotect** in the SRM.

For more information, see the IBM Storage Virtualize Family Storage Replication Adapter documentation.

4.4 Storage Replication Adapter with VMware Site Recovery Manager

Figure 4-2 shows how an IBM Storage Virtualize system is integrated in a typical VMware SRM DR solution.

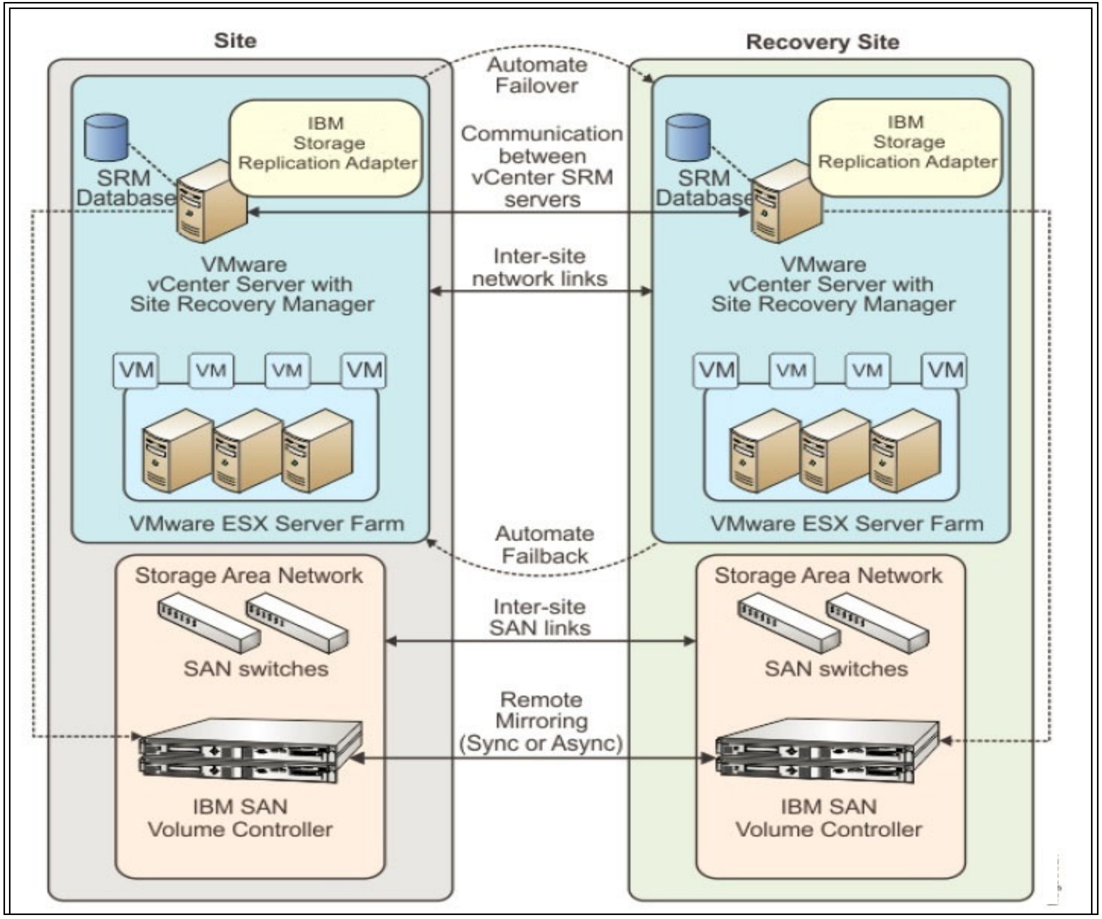

Site
Recovery Site
Automate Failover
IBM Storage Replication Adapter
SRM Database
Communication between vCenter SRM servers
IBM Storage Replication Adapter
SRM Database
VMware vCenter Server with Site Recovery Manager
Inter-site network links
VMware vCenter Server with Site Recovery Manager
VM
VM
VM
VM
VM
VM
VM
VM
VMware ESX Server Farm
Automate Failback
VMware ESX Server Farm
Storage Area Network
SAN switches
Inter-site SAN links
Storage Area Network
SAN switches
Remote Mirroring (Sync or Async)
IBM SAN Volume Controller
IBM SAN Volume Controller

Figure 4-2 SRA and VMware SRM with IBM Storage Virtualize integrated solution

SRA configuration might vary depending on the specific site configuration. Consider the following preparatory steps and configuration when using SRA with SRM.

4.4.1 Storage replication adapter planning

This section describes storage replication adapter planning.

Preparing the SRA environment

To prepare the SRA environment, complete the following steps:

1. Ensure that the supported storage systems firmware version is used.
2. Provision appropriate-sized target volumes on the storage system at the recovery (secondary) site. Create Metro Mirror, Global Mirror, or Policy-based Replication relationships between the source and target volumes and add the relationships to consistency groups, as needed.
3. Create a dedicated user on both source and target storage systems with the right privileges for the SRA:
   - For SRA non-preconfigured settings, a user with Administrator or higher privilege is needed.
   - For SRA preconfigured settings, a user with CopyOperator or higher privilege is needed.
4. Use the same username and password on both the protected (primary) and the recovery site.

Verifying the mirroring configuration

Consider the following points for verifying the mirroring configuration:

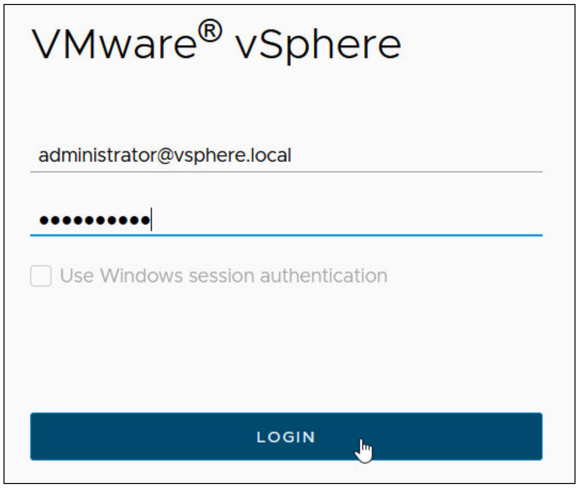
- Ensure that all VMware ESXi hosts, IBM Storage Virtualize systems, and volumes at both sites are properly connected to their remote counterparts and configured for site mirroring.
- Establish mirror-connectivity between the local IBM Storage Virtualize storage system at the protected, primary site and the IBM Storage Virtualize system at the recovery, secondary site. For IBM SVC Stretched Cluster, stretched volumes are created, and both copies of a stretched volume are online. For IBM HyperSwap, HyperSwap volumes are created, and both the primary volume and secondary volume of a HyperSwap volume are online.
- Use a unique name for each IBM Storage Virtualize system at both the protected and the recovery sites.
- Verify that the storage pools that contain the replicated volumes at both sites have sufficient available capacity for creating the snapshots of all replicated volumes concurrently.
- For non-pre-configured environments, extra space for Test Failover and Failover is necessary. Ensure that enough space is available in the pool.
- Ensure that protected volumes are mapped to the protected VMware ESX hosts:
  - For Stretched Cluster, the stretched volumes are mapped to both the protected and recovery VMware ESX hosts.
  - For IBM HyperSwap, the primary volume of a HyperSwap is mapped to both the protected and recovery VMware ESX hosts.
- Ensure that remote copy relationships exist for all volumes:
  - For IBM Stretched Cluster, stretched volumes are created, and both copies of a stretched volume are online.
  - For IBM HyperSwap, HyperSwap volumes are created, and both the primary volume and secondary volume of a HyperSwap volume are online.

- Ensure that for non-preconfigured environments, the recovery volumes remain unmapped.
- Make sure that the recovery VMware ESXi hosts are defined as hosts at the recovery site and report as online.

Verifying the VMware Site Recovery Manager installation

Before you embark with the installation of IBM Storage Virtualize system SRA container, verify that the VMware SRM is already installed and accessible at both the protected, primary site and the recovery, secondary site, and both sites are paired, by following these steps:

1. Log in to the VMware vSphere Client (Figure 4-3).



administrator@vsphere.local

●●●●●●●●●●●

□ Use Windows session authentication

Figure 4-3 VMware vSphere Client login

2. Select **Menu** → **Site Recovery** (Figure 4-4 on page 52).
3. The local SRM instance is shown, click **OPEN Site Recovery** (Figure 4-5 on page 52).
4. The paired SRM instances are shown in Figure 4-6 on page 53.

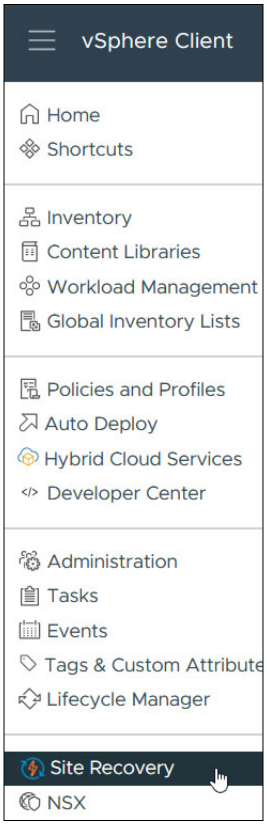
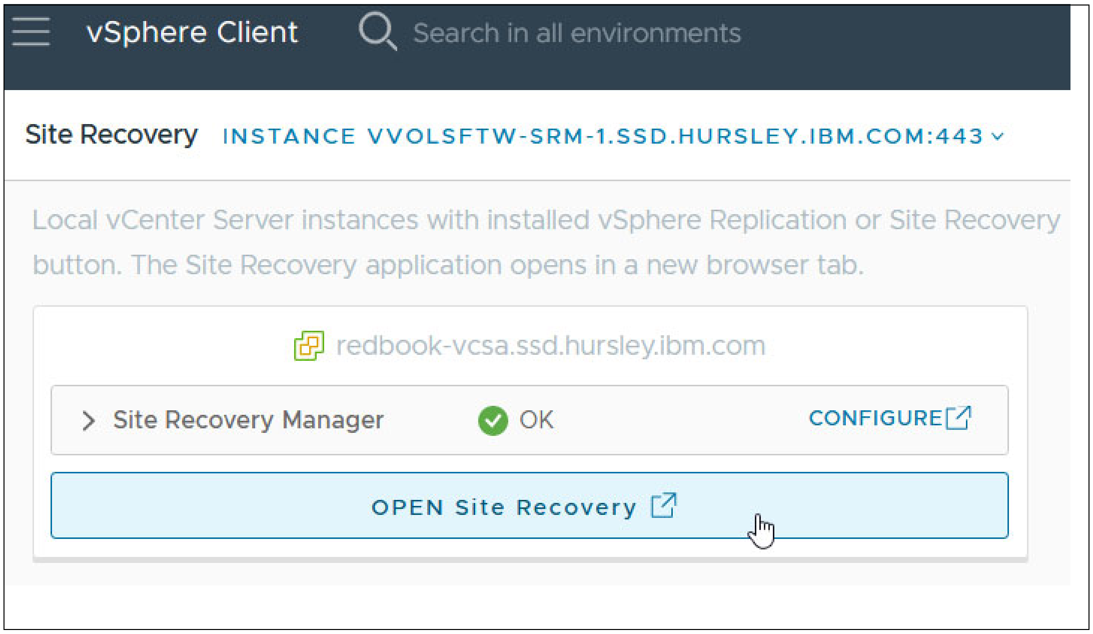


Figure 4-4 Site Recovery Icon


vSphere Client
Search in all environments
Site Recovery
INSTANCE VVOLSFTW-SRM-1.SSD.HURSLEY.IBM.COM:443

Local vCenter Server instances with installed vSphere Replication or Site Recovery button. The Site Recovery application opens in a new browser tab.

redbook-vcsa.ssd.hursley.ibm.com
Site Recovery Manager
OK
CONFIGURE
OPEN Site Recovery

Figure 4-5 Site Recovery Pane in vSphere Client

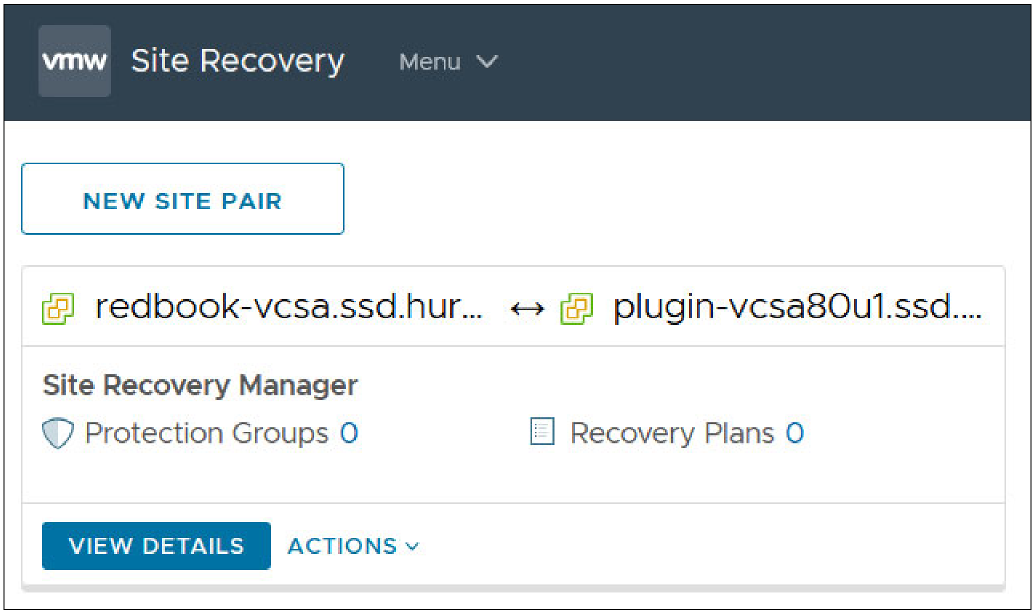


Figure 4-6 Site Recovery: Paired Sites

4.4.2 Storage Replication Adapter for VMware installation

For more information about how to download the IBM Storage Virtualize Family Storage Replication Adapter for VMware, see Downloading the SRA.

As a best practice, stop your currently installed version of the SRA container before running a different version. Ensure that you satisfy all of the prerequisites that are listed in before you run the SRA container. Follow the steps to run the IBM Storage Virtualize system SRA container on the SRM server.

1. Log in to the VMware SRM Appliance Management interface as admin, as shown in Figure 4-7.

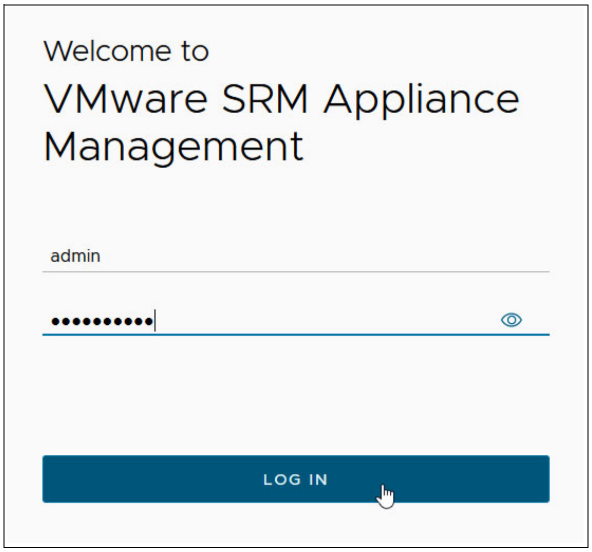
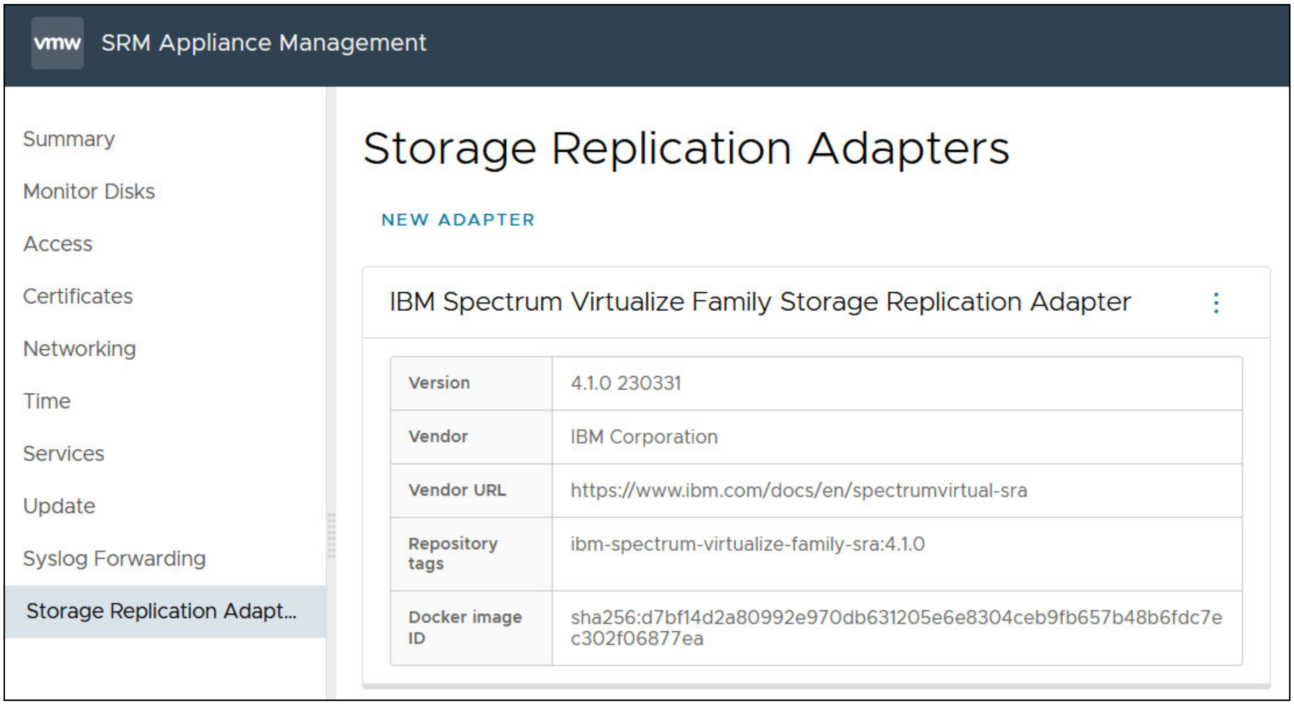


Figure 4-7 SRM Appliance Management interface login

2. In the SRM Appliance Management interface, select **Storage Replication Adapters** → **NEW ADAPTER**. Click **Upload**. Go to the directory where you saved the SRA file, and double-click it. The SRA upload process begins.
3. When the upload process finishes, click **Close**. The SRA card is displayed on the Storage Replication Adapters view (Figure 4-8). Repeat this step on the other site to install the SRA on the other SRM instance on the other site.



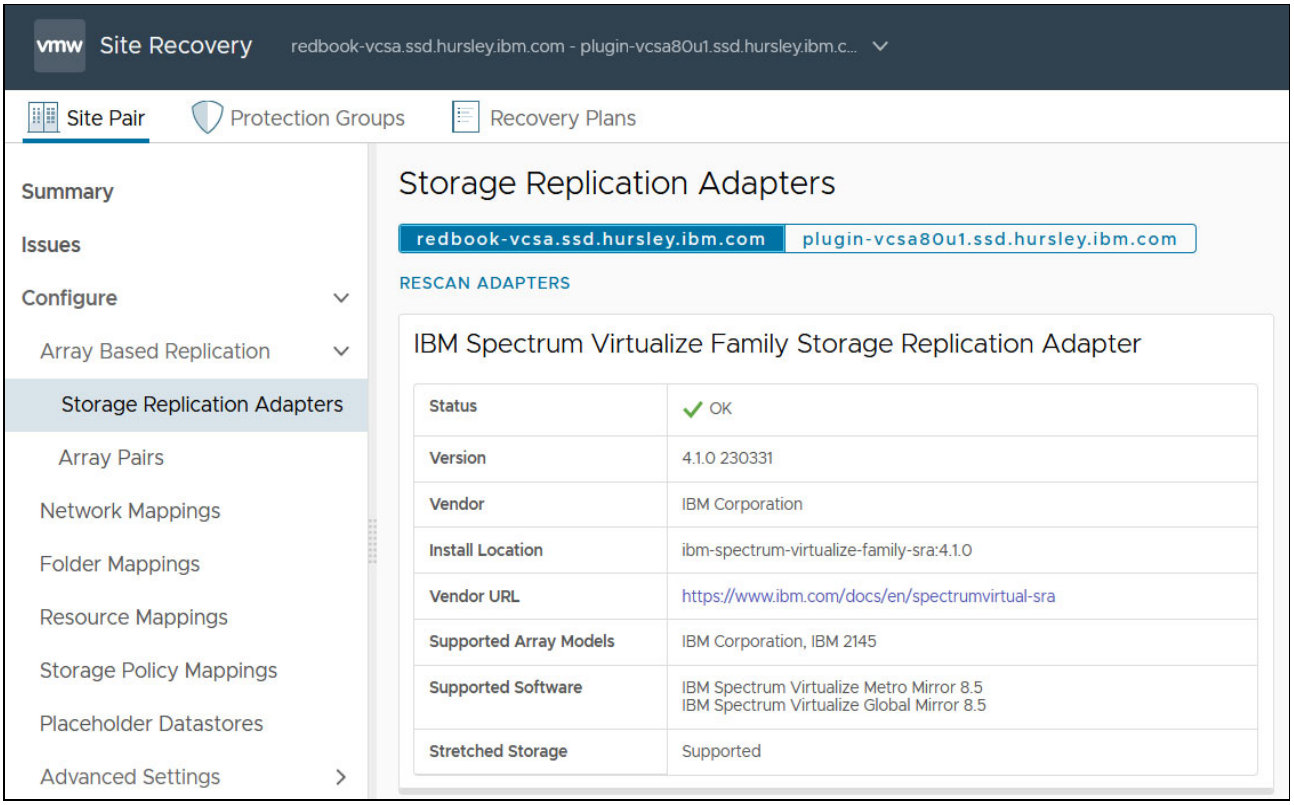
Storage Replication Adapters

IBM Spectrum Virtualize Family Storage Replication Adapter

Version	4.1.0 230331
Vendor	IBM Corporation
Vendor URL	https://www.ibm.com/docs/en/spectrumvirtual-sra
Repository tags	ibm-spectrum-virtualize-family-sra:4.1.0
Docker image ID	sha256:d7bf14d2a80992e970db631205e6e8304ceb9fb657b48b6fdc7ec302f06877ea

Figure 4-8 Storage Replication Adapters view

4. Log in to the vSphere Client.
5. Select **Site Recovery** → **Open Site Recovery**, select a site pair, and click **View Details**.
6. On the **Site Pair** tab, select **Configure** → **Array Based Replication** → **Storage Replication Adapters** → **RESCAN ADAPTERS**. After the rescan is complete, the Status field value is updated to `OK` (Figure 4-9 on page 55).



IBM Spectrum Virtualize Family Storage Replication Adapter

Status	✓ OK
Version	4.1.0 230331
Vendor	IBM Corporation
Install Location	ibm-spectrum-virtualize-family-sra:4.1.0
Vendor URL	https://www.ibm.com/docs/en/spectrumvirtual-sra
Supported Array Models	IBM Corporation, IBM 2145
Supported Software	IBM Spectrum Virtualize Metro Mirror 8.5 IBM Spectrum Virtualize Global Mirror 8.5
Stretched Storage	Supported

Figure 4-9 Site Recovery view

4.4.3 Storage Replication Adapter configuration and usage

When the storage replication adapter installation is complete, see Configuration. To check the SRA settings and if they match the environment, login through an ssh connection to the SRM appliance on both sites with the admin user and list the containers. Then check the SRA settings with the following command:

```
docker exec <Container_ID> cat
/srm/sra/conf/IBMSpectrumVirtualizeFamilySRA/sra.settings on the SRA container
```

The command and output are shown in Example 4-1.

Example 4-1 Check SRA settings

```
admin@vvolsftw-srm-1 [ ~ ]$ docker container list
CONTAINER ID   IMAGE          COMMAND              CREATED        STATUS
PORTS     NAMES
3d45117fd5c2   d7bf14d2a809   "tail -f /dev/null"   40 hours ago   Up 40 hours
unruffled_lederberg
19b979085cdd   d7bf14d2a809   "tail -f /dev/null"   13 days ago    Up 13 days
elegant_raman
admin@vvolsftw-srm-1 [ ~ ]$ docker exec 3d45117fd5c2 cat
/srm/sra/conf/IBMSpectrumVirtualizeFamilySRA/sra.settings
# SRA configuration file
# Pre-configured Env: True, Non-preconfigured Env: False
preconfiguredEnv=False
```

```
# Choose the mdisk group which have enough free capacity from storage side, SRA
would create the test volumes on this mdisk group
testMDiskGroupID=0

# Standard Volume: 0, Thin Provisioned: 1, Compressed Volume: 2, Thin-Provisioned
with Deduplicated Volume: 3, Compressed with Deduplicated Volume: 4
volumeType=1

# Protect source volume: True/False
protectSource=False

# If protectSource is true, please set the appropriate MDisk group IDs
sourceMDiskGroupID=0

# Protect target volume: True/False
protectTarget=False

# If protectTarget is true, please set the appropriate MDisk group IDs
recoveryMDiskGroupID=0

# If SaveExportInformation is true, SRA will save host lun mapping to reuse in
failback
SaveExportInformation=False

# If force is true, SRA will forcefully discard switch step in recovery operation
if any failure: True/False
# Note: Not recommended to enable this param in normal scenario.
force=False
```

If changes to the configuration file are needed, determine the SRA configuration volume directory by using the following command:

```
docker inspect <Container_ID>|grep volume
```

As root user, edit the SRA configuration file as needed as shown in Example 4-2.

Example 4-2 Edit SRA configuration file

```
admin@vvolsftw-srm-1 [ ~ ]$ docker inspect 3d45117fd5c2|grep volume
                "Type": "volume",
                "Source":
"/var/lib/docker/volumes/d7bf14d2a80992e970db631205e6e8304ceb9fb657b48b6fdc7ec302f
06877ea-v/_data",
admin@vvolsftw-srm-1 [ ~ ]$ su - root
Password:
Last login: Wed Jul 12 05:22:54 UTC 2023 on pts/0
root@vvolsftw-srm-1 [ ~ ]# vi
/var/lib/docker/volumes/d7bf14d2a80992e970db631205e6e8304ceb9fb657b48b6fdc7ec302f0
6877ea-v/_data/IBMSpectrumVirtualizeFamilySRA/sra.settings
```

Before you configure and use the Array Based Replication make sure Network Mappings, Folder Mappings, Resource Mappings, Storage Mappings and Placeholder Data Stores are configured according to the VMware documentation. See Configuring Mappings.

Account for the following practices when working with SRA and VMware SRM:

- Create Metro Mirror, Global Mirror, or Policy-based Replication relationships between the source and target VDisks and add them to consistency groups, as explained in "Preparing the SRA environment" on page 50.
- Before you use the SRA, make sure that the relationships and consistency groups are in a consistent synchronized state.
- For Stretched Cluster, make sure that the two copies of a stretched volume are at different sites and that both copies are online.
- For IBM HyperSwap, make sure that the primary volume and secondary volume of a HyperSwap volume are online.
- All volumes that participate in SRM and belong to the same remote copy consistency group are shown under a single local consistency group. To avoid data inconsistencies when adding replicated VDisks to the same VM or datastore, all VDisks used by a single VM or application must be added to the same consistency group.

  If you plan to use VMware SRM to manage replicated volumes, use the Name Filter by using prefixes for the volume name. The volume names can be different for each site, but prefixes must be paired with the remote site array manager. For example, if the local site volume name is Pri_Win2019, and if it is mapped to Rec_Win2019 on the remote site, then you might enter the prefix `Pri` in the Name Filter field for the local site and the prefix `Rec` on the remote site. To use the Name Filter for the consistency group, enter the same names and prefixes at both the local and remote sites. For more information, see Filtering different consistency groups and volumes.
- Consider the following items for managing datastores and consistency groups:
  - The datastores of one VM should be in the same consistency group.
  - The datastore of the VM and the raw disk in the VM should be in the same consistency group.
  - You must have administrator privileges to install SRM.
  - Set the appropriate timeout and rescan values in SRM for recovery of many VMs.

Add an array pair

To be able to use SRM with Storage Virtualize system, you need to create an array pair in SRM.

1. On the Site Pair tab, select **Configure** → **Array Based Replication** → **Array Pairs** and click **ADD** as shown in Figure 4-10 on page 58. For more information, see Adding an array pair to the VMware Site Recovery Manager.

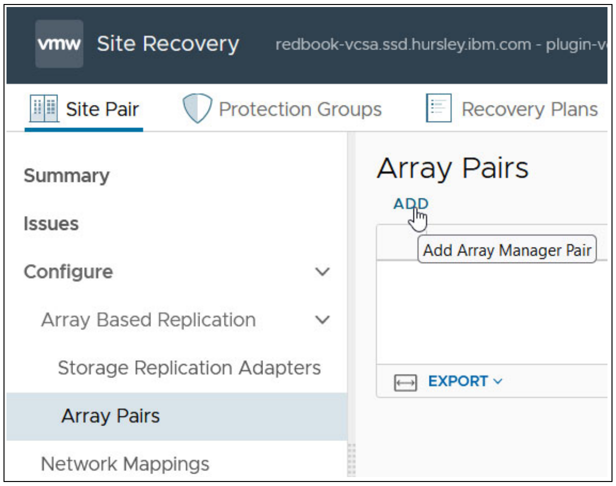
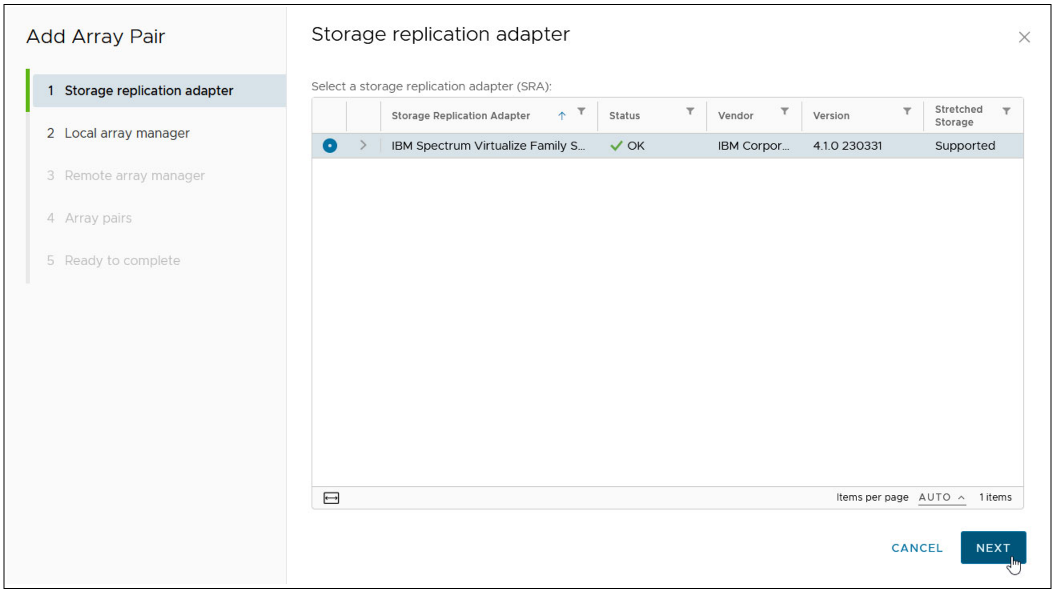


Figure 4-10 SRM Array Pairs

2. Select the SRA and click **NEXT** (Figure 4-11).



Storage replication adapter

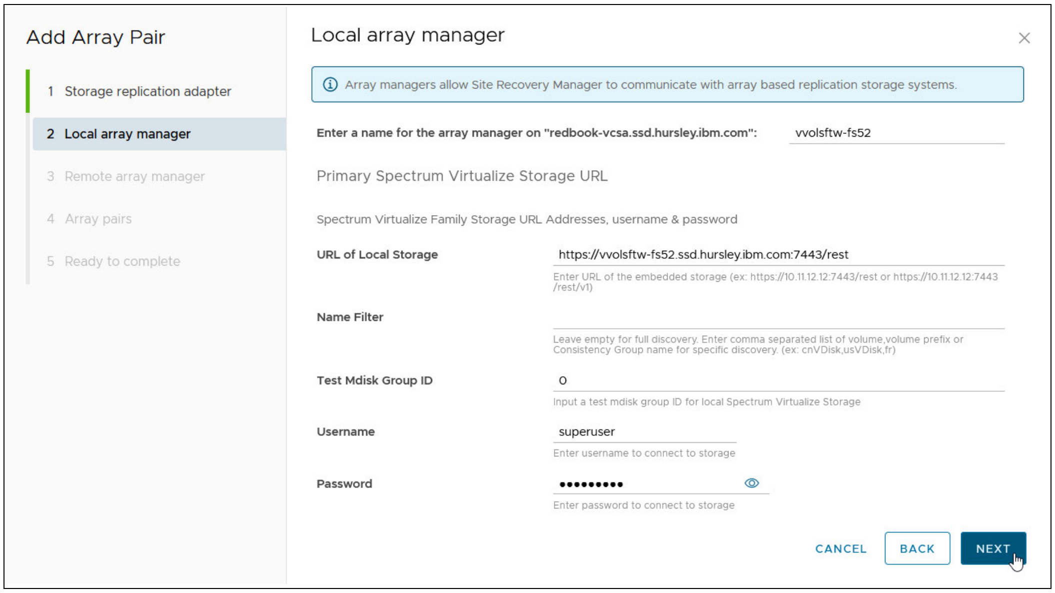
Select a storage replication adapter (SRA):

		Storage Replication Adapter	Status	Vendor	Version	Stretched Storage
●	>	IBM Spectrum Virtualize Family S...	✓ OK	IBM Corpor...	4.1.0 230331	Supported

Items per page AUTO 1 items

Figure 4-11 SRM Add Array Pair select SRA

3. Enter the name of the local FlashSystem. Enter the URL with either `/rest` or `/rest/v1` at the end. Enter the user and password and which pool will be used for Test. A pool is also called an MDisk Group. Select **NEXT**, as shown in Figure 4-12 on page 59.



Add Array Pair

1 Storage replication adapter
2 Local array manager
3 Remote array manager
4 Array pairs
5 Ready to complete

Local array manager

ⓘ Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "redbook-vcsa.ssd.hursley.ibm.com": vvolsftw-fs52

Primary Spectrum Virtualize Storage URL

Spectrum Virtualize Family Storage URL Addresses, username & password

URL of Local Storage: https://vvolsftw-fs52.ssd.hursley.ibm.com:7443/rest
Enter URL of the embedded storage (ex: https://10.11.12.12:7443/rest or https://10.11.12.12:7443/rest/v1)

Name Filter:
Leave empty for full discovery. Enter comma separated list of volume,volume prefix or Consistency Group name for specific discovery. (ex: cnVDisk,usVDisk,fr)

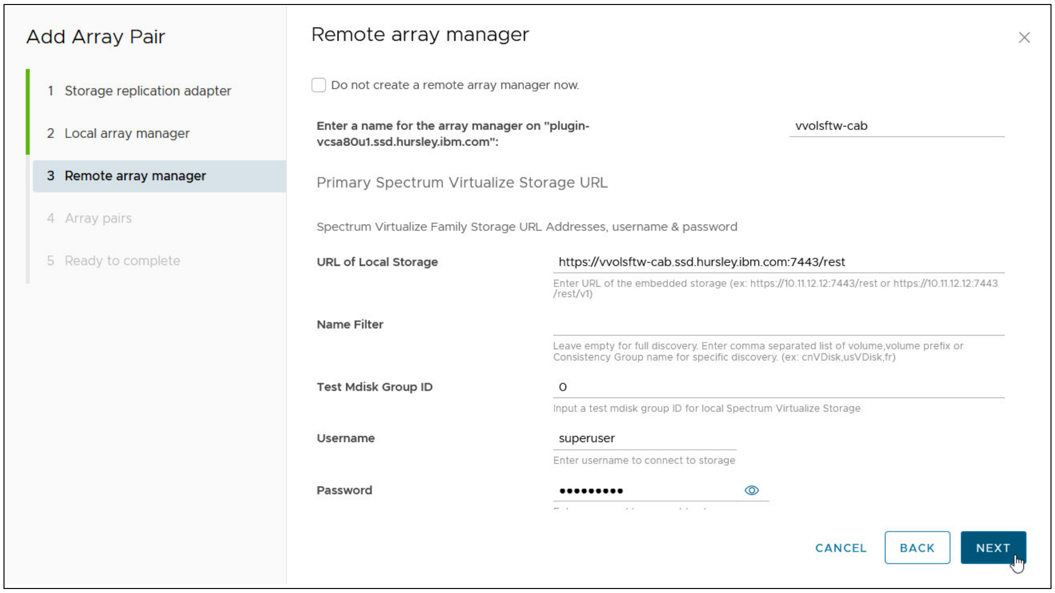
Test Mdisk Group ID: 0
Input a test mdisk group ID for local Spectrum Virtualize Storage

Username: superuser
Enter username to connect to storage

Password: •••••••••
Enter password to connect to storage

Figure 4-12 SRM Add Array Pair Define Local Array Manager

4. Enter the name of the remote FlashSystem. Enter the URL with either `/rest` or `/rest/v1` at the end. Enter the user ID and password and which pool to use for Test. Select **NEXT**, as shown in Figure 4-13.



Add Array Pair

1 Storage replication adapter
2 Local array manager
3 Remote array manager
4 Array pairs
5 Ready to complete

Remote array manager

☐ Do not create a remote array manager now.

Enter a name for the array manager on "plugin-vcsa80u1.ssd.hursley.ibm.com": vvolsftw-cab

Primary Spectrum Virtualize Storage URL

Spectrum Virtualize Family Storage URL Addresses, username & password

URL of Local Storage: https://vvolsftw-cab.ssd.hursley.ibm.com:7443/rest
Enter URL of the embedded storage (ex: https://10.11.12.12:7443/rest or https://10.11.12.12:7443/rest/v1)

Name Filter:
Leave empty for full discovery. Enter comma separated list of volume,volume prefix or Consistency Group name for specific discovery. (ex: cnVDisk,usVDisk,fr)

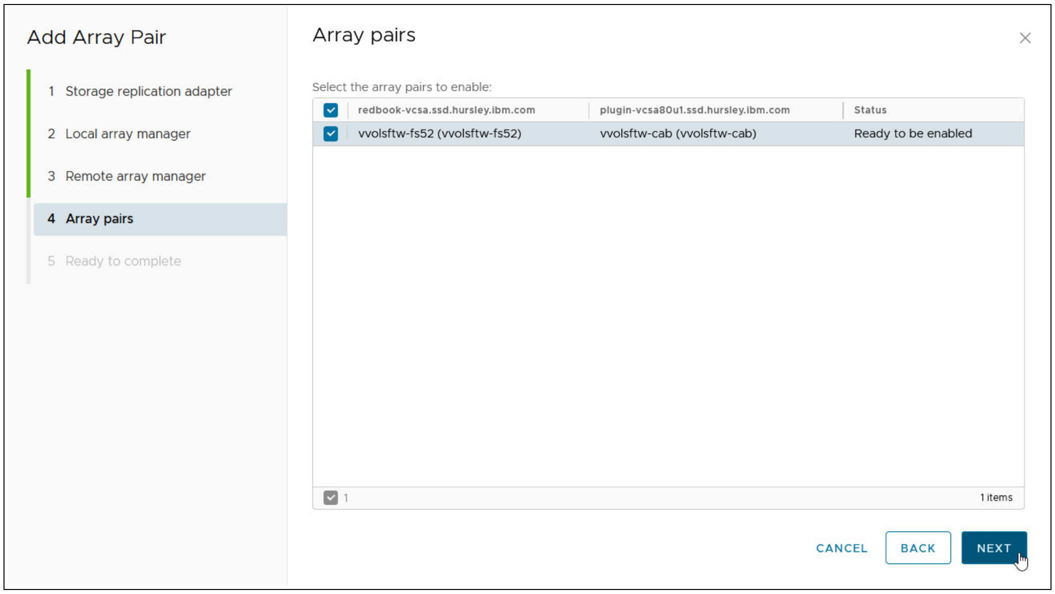
Test Mdisk Group ID: 0
Input a test mdisk group ID for local Spectrum Virtualize Storage

Username: superuser
Enter username to connect to storage

Password: •••••••••

Figure 4-13 SRM Add Array Pair Define Remote Array Manager

5. Select the array pair and click **NEXT**, as depicted in Figure 4-14.



Array pairs

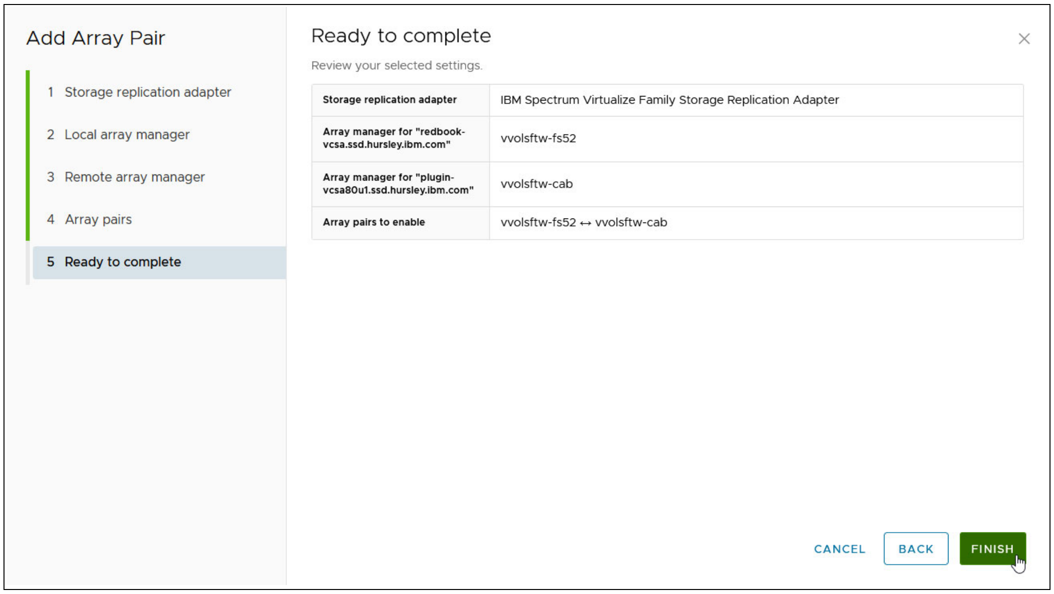
Select the array pairs to enable:

☑	redbook-vcsa.ssd.hursley.ibm.com	plugin-vcsa80u1.ssd.hursley.ibm.com	Status
☑	vvolsftw-fs52 (vvolsftw-fs52)	vvolsftw-cab (vvolsftw-cab)	Ready to be enabled

☑ 1 1 items

Figure 4-14 SRM Add Array Pair: Select Array Pair

6. Review the summary and click **FINISH** to create the array pair, as shown in Figure 4-15.



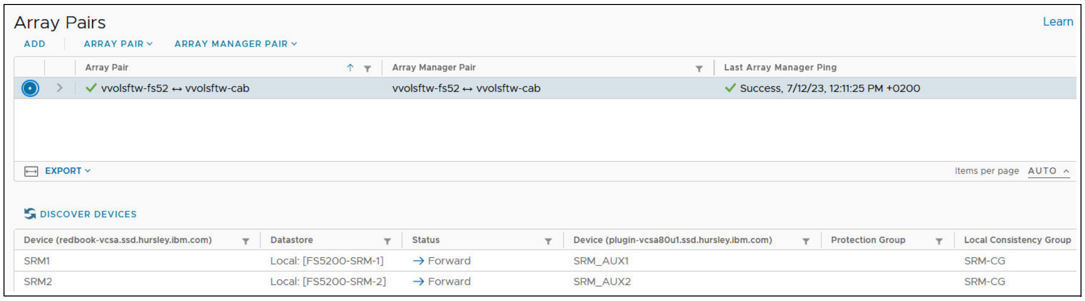
Ready to complete

Review your selected settings.

Storage replication adapter	IBM Spectrum Virtualize Family Storage Replication Adapter
Array manager for "redbook-vcsa.ssd.hursley.ibm.com"	vvolsftw-fs52
Array manager for "plugin-vcsa80u1.ssd.hursley.ibm.com"	vvolsftw-cab
Array pairs to enable	vvolsftw-fs52 ↔ vvolsftw-cab

Figure 4-15 SRM Add Array Pair Summary

7. Select the array pair and the Storage Virtualize systems replicated devices with their consistency group are shown, as illustrated in Figure 4-16 on page 61.



	Array Pair	Array Manager Pair	Last Array Manager Ping
●	✓ vvolsftw-fs52 ↔ vvolsftw-cab	vvolsftw-fs52 ↔ vvolsftw-cab	✓ Success, 7/12/23, 12:11:25 PM +0200

Device (redbook-vcsa.ssd.hursley.ibm.com)	Datastore	Status	Device (plugin-vcsa80u1.ssd.hursley.ibm.com)	Protection Group	Local Consistency Group
SRM1	Local: [FS5200-SRM-1]	→ Forward	SRM_AUX1		SRM-CG
SRM2	Local: [FS5200-SRM-2]	→ Forward	SRM_AUX2		SRM-CG

Figure 4-16 SRM Array Pairs and Replicated Devices

Add a Protection Group and Recovery Plan

A Protection Group is a bundle of Virtual Machines, which belong and will be protected together.

1. To add a Protection Group, click the Protection Groups Tab and select **NEW PROTECTION GROUP** as shown in Figure 4-17.

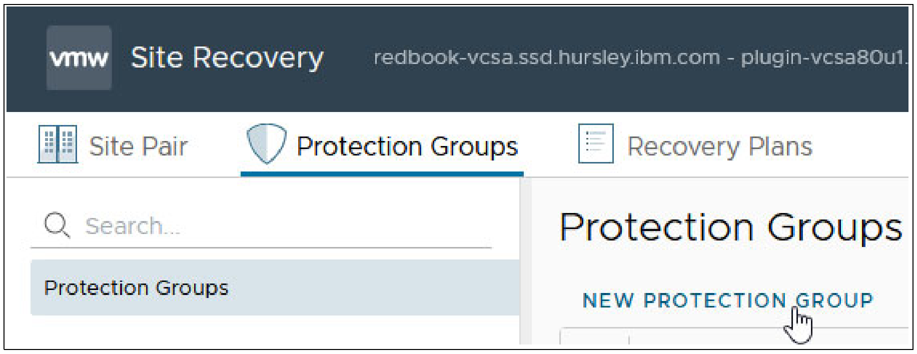
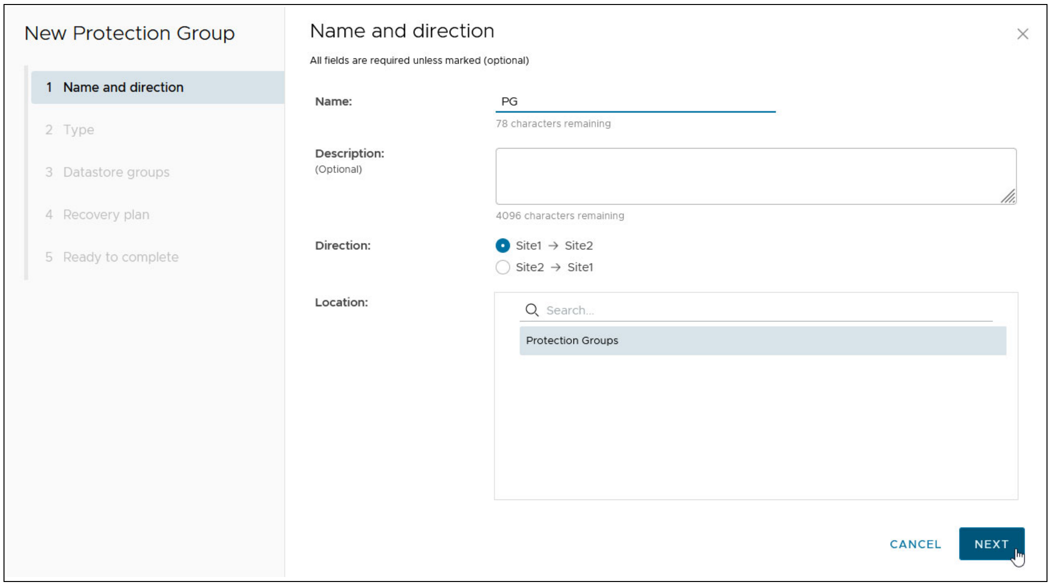


Figure 4-17 SRM New Protection Group

2. Choose a name for the Protection Group, select the protection direction and click **NEXT**, as shown in Figure 4-18.



Name and direction

All fields are required unless marked (optional)

Name: PG

78 characters remaining

Description:
(Optional)

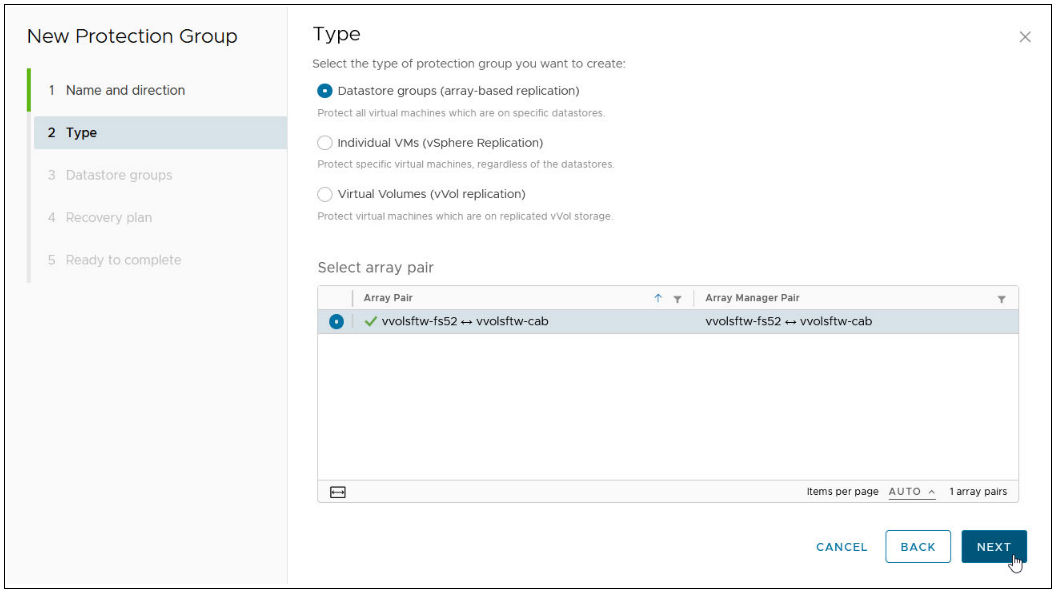
4096 characters remaining

Direction:
● Site1 → Site2
○ Site2 → Site1

Location:

Figure 4-18 SRM New Protection Group Name and Direction

3. For the Type, select Database groups (array-based replication) and click **NEXT**, as depicted in Figure 4-19.



New Protection Group

1 Name and direction
2 Type
3 Datastore groups
4 Recovery plan
5 Ready to complete

Type

Select the type of protection group you want to create:

● Datastore groups (array-based replication)
Protect all virtual machines which are on specific datastores.

○ Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.

○ Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

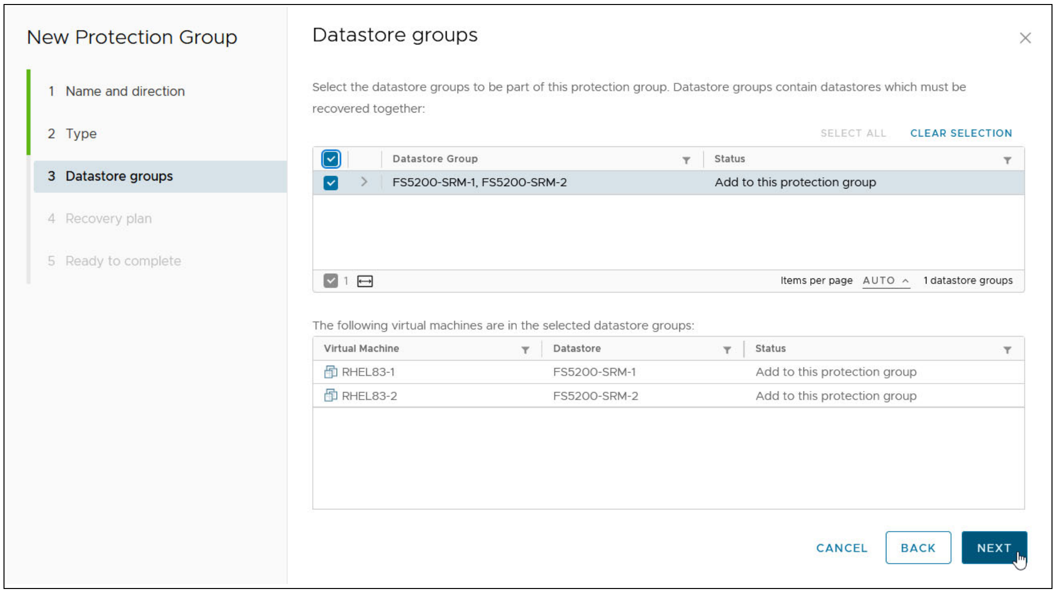
Select array pair

	Array Pair	Array Manager Pair
●	✓ vvolsftw-fs52 ↔ vvolsftw-cab	vvolsftw-fs52 ↔ vvolsftw-cab

Items per page AUTO 1 array pairs

Figure 4-19 SRM New Protection Group Type

4. Select the Data Store Group and verify the protected VMs, click **NEXT**, as shown in Figure 4-20.



New Protection Group

1 Name and direction
2 Type
3 Datastore groups
4 Recovery plan
5 Ready to complete

Datastore groups

Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together:

☑	Datastore Group	Status
☑	FS5200-SRM-1, FS5200-SRM-2	Add to this protection group

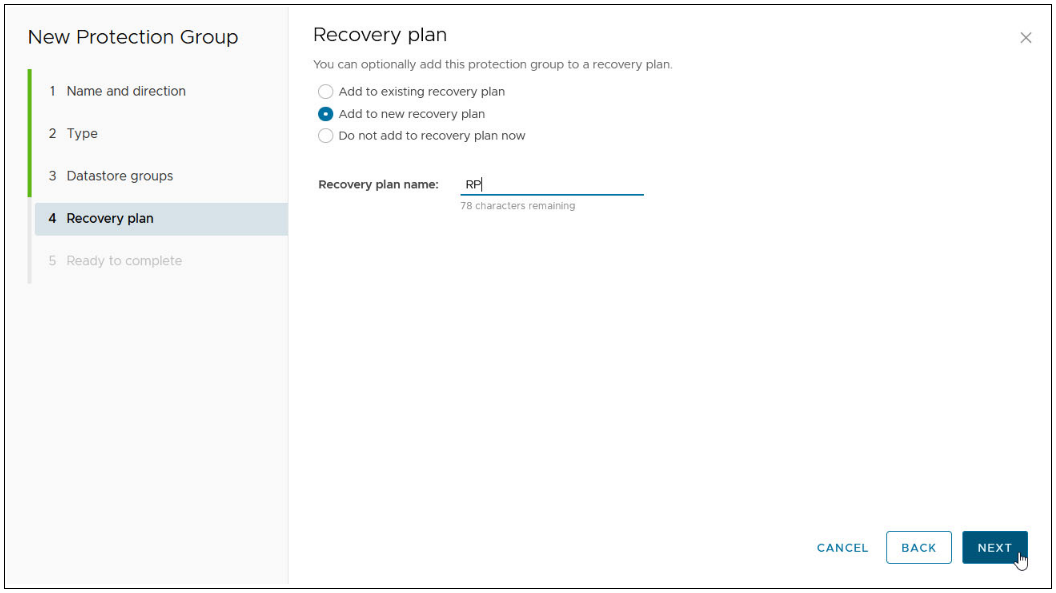
☑ 1 Items per page AUTO 1 datastore groups

The following virtual machines are in the selected datastore groups:

Virtual Machine	Datastore	Status
RHEL83-1	FS5200-SRM-1	Add to this protection group
RHEL83-2	FS5200-SRM-2	Add to this protection group

Figure 4-20 SRM New Protection Group Datastore groups

5. Select **Add to new recovery plan**, choose a name for the Recovery Plan and click **NEXT**, as illustrated in Figure 4-21**.**



Recovery plan

You can optionally add this protection group to a recovery plan.

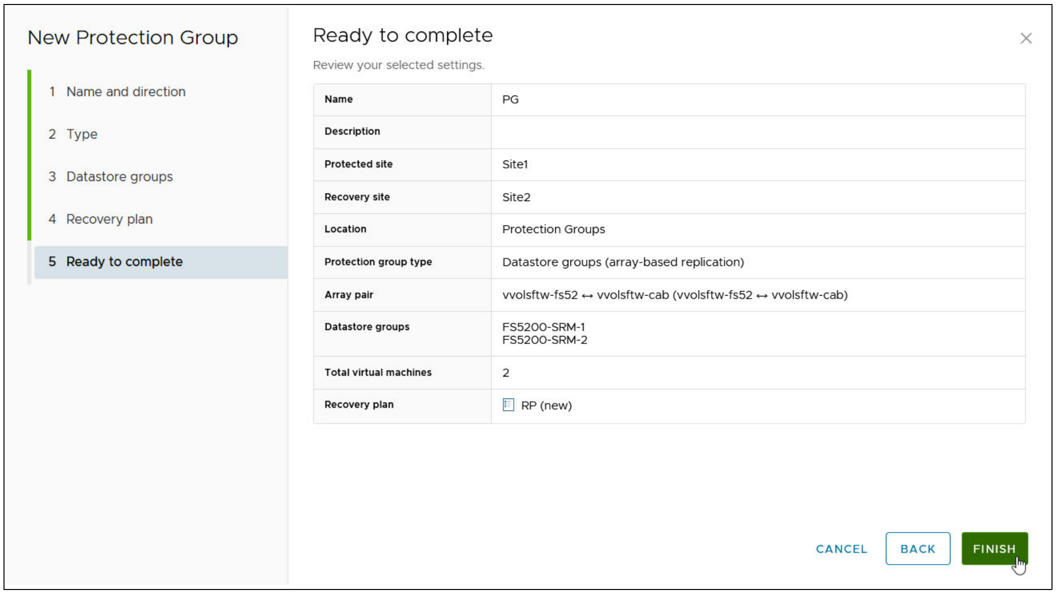
○ Add to existing recovery plan
● Add to new recovery plan
○ Do not add to recovery plan now

Recovery plan name: RP

78 characters remaining

Figure 4-21 SRM New Protection Group Recovery Plan

6. Review the summary and click **FINISH**, as depicted in Figure 4-22.



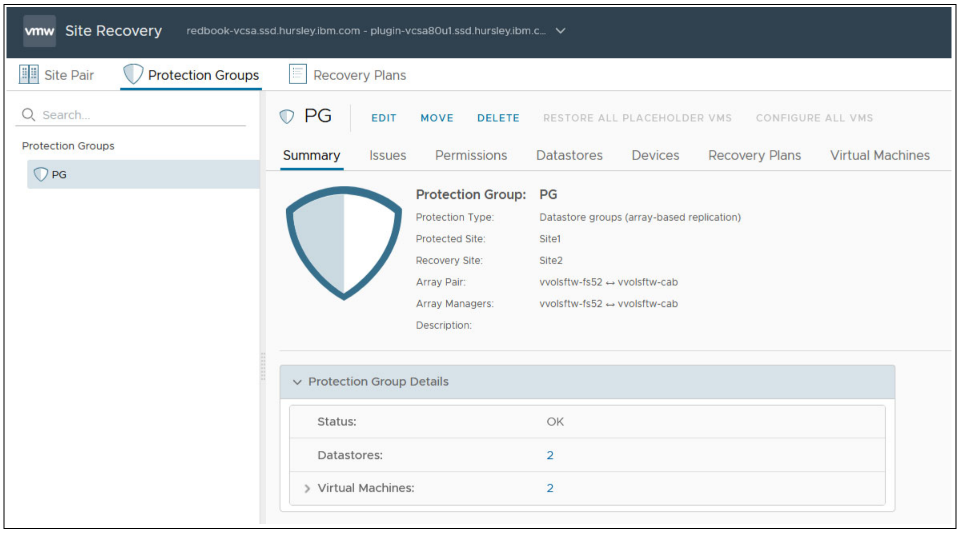
Ready to complete

Review your selected settings.

Name	PG
Description	
Protected site	Site1
Recovery site	Site2
Location	Protection Groups
Protection group type	Datastore groups (array-based replication)
Array pair	vvolsftw-fs52 ↔ vvolsftw-cab (vvolsftw-fs52 ↔ vvolsftw-cab)
Datastore groups	FS5200-SRM-1 FS5200-SRM-2
Total virtual machines	2
Recovery plan	RP (new)

Figure 4-22 SRM New Protection Group Summary

7. Select the Protection Group and check the status, number of VMs and number of datastores of the Protection Group, as shown in Figure 4-23.



Protection Groups: PG

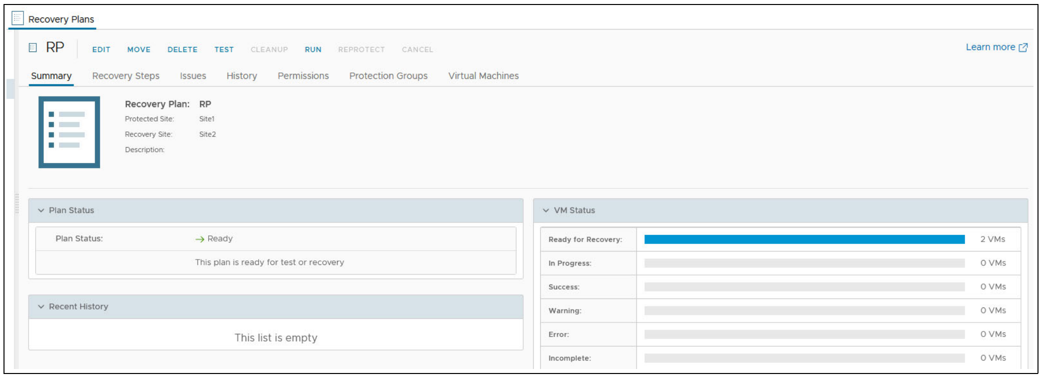
Protection Group: PG
Protection Type: Datastore groups (array-based replication)
Protected Site: Site1
Recovery Site: Site2
Array Pair: vvolsftw-fs52 ↔ vvolsftw-cab
Array Managers: vvolsftw-fs52 ↔ vvolsftw-cab
Description:

Protection Group Details

Status:	OK
Datastores:	2
Virtual Machines:	2

Figure 4-23 SRM Protection Group

8. To verify the Recovery Plan select the **Recovery Plans** tab and select the Recovery Plan, check the status and the number of VMs which are ready for recovery, as illustrated in Figure 4-24.



Recovery Plan: RP
Protected Site: Site1
Recovery Site: Site2
Description:

Plan Status

Plan Status: → Ready

This plan is ready for test or recovery

Recent History

This list is empty

VM Status

Ready for Recovery:	2 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs

Figure 4-24 SRM Recovery Plan

Test Recovery Plan

For more information about Recovery Plans, see Creating, Testing, and Running Recovery Plans

1. To start the Test of the Recovery Plan, which creates a snapshot on the recovery site, maps it to the ESXi hosts, mount the datastores, and starts the VMs in an isolated network environment, select **TEST**, as shown in Figure 4-25.

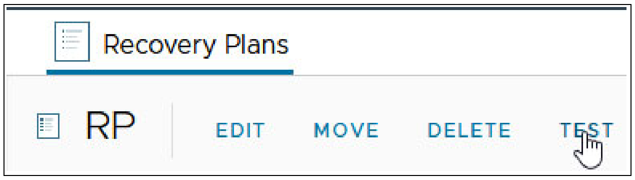
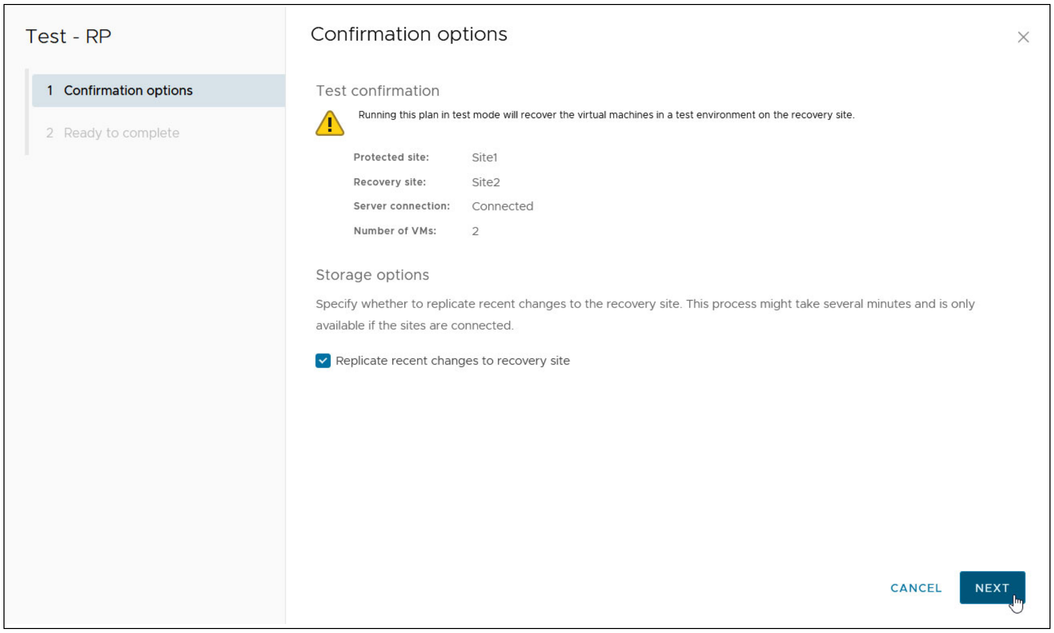


Figure 4-25 SRM Recovery Plan Test

2. Confirm the Test and click **NEXT**, as illustrated in Figure 4-26.



Test - RP

1 Confirmation options

2 Ready to complete

Confirmation options

Test confirmation

Running this plan in test mode will recover the virtual machines in a test environment on the recovery site.

Protected site:	Site1
Recovery site:	Site2
Server connection:	Connected
Number of VMs:	2

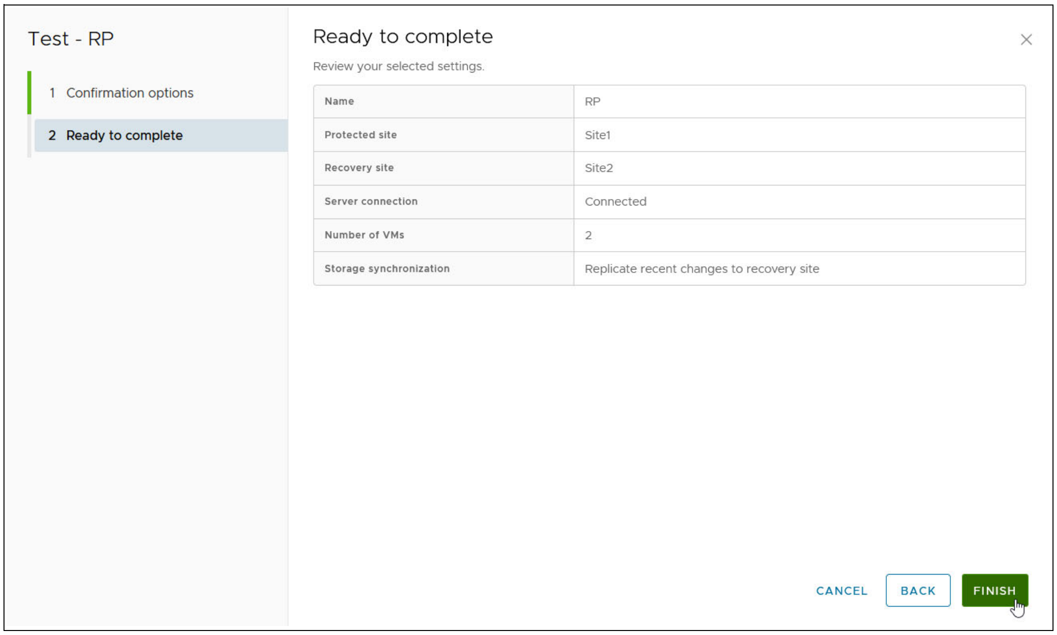
Storage options

Specify whether to replicate recent changes to the recovery site. This process might take several minutes and is only available if the sites are connected.

☑ Replicate recent changes to recovery site

Figure 4-26   SRM Recovery Plan Test options

3. Review the summary and click **FINISH**, as depicted in Figure 4-27.



Test - RP

1 Confirmation options

2 Ready to complete

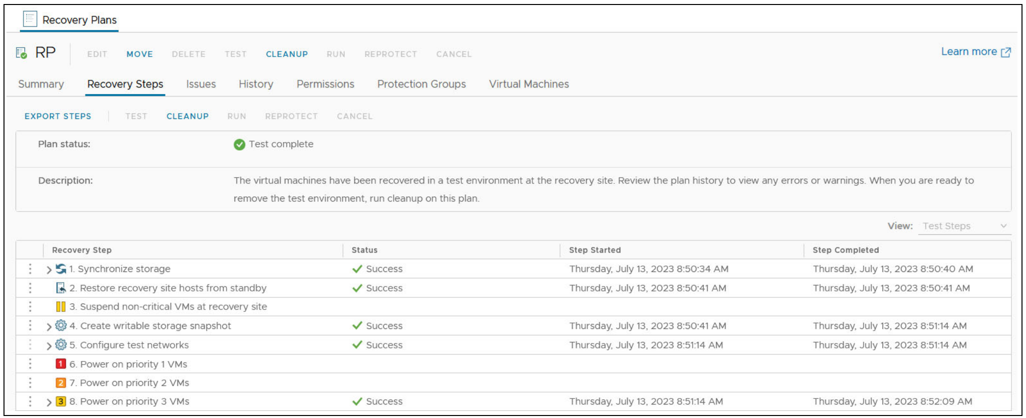
Ready to complete

Review your selected settings.

Name	RP
Protected site	Site1
Recovery site	Site2
Server connection	Connected
Number of VMs	2
Storage synchronization	Replicate recent changes to recovery site

Figure 4-27   SRM Recovery Plan Test summary

4. The Test starts and the results are visible in the tab Recovery Steps, as shown in Figure 4-28.



Plan status: Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

View: Test Steps

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Thursday, July 13, 2023 8:50:34 AM	Thursday, July 13, 2023 8:50:40 AM
2. Restore recovery site hosts from standby	✓ Success	Thursday, July 13, 2023 8:50:41 AM	Thursday, July 13, 2023 8:50:41 AM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Thursday, July 13, 2023 8:50:41 AM	Thursday, July 13, 2023 8:51:14 AM
5. Configure test networks	✓ Success	Thursday, July 13, 2023 8:51:14 AM	Thursday, July 13, 2023 8:51:14 AM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	✓ Success	Thursday, July 13, 2023 8:51:14 AM	Thursday, July 13, 2023 8:52:09 AM

Figure 4-28 SRM Recovery Plan Test Recovery Steps

Cleanup Recovery Plan

Perform the following steps to cleanup a Recovery Plan.

1. To clean up from the previous Test select **CLEANUP**, as shown in Figure 4-29.

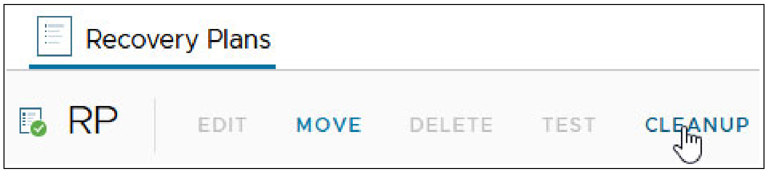
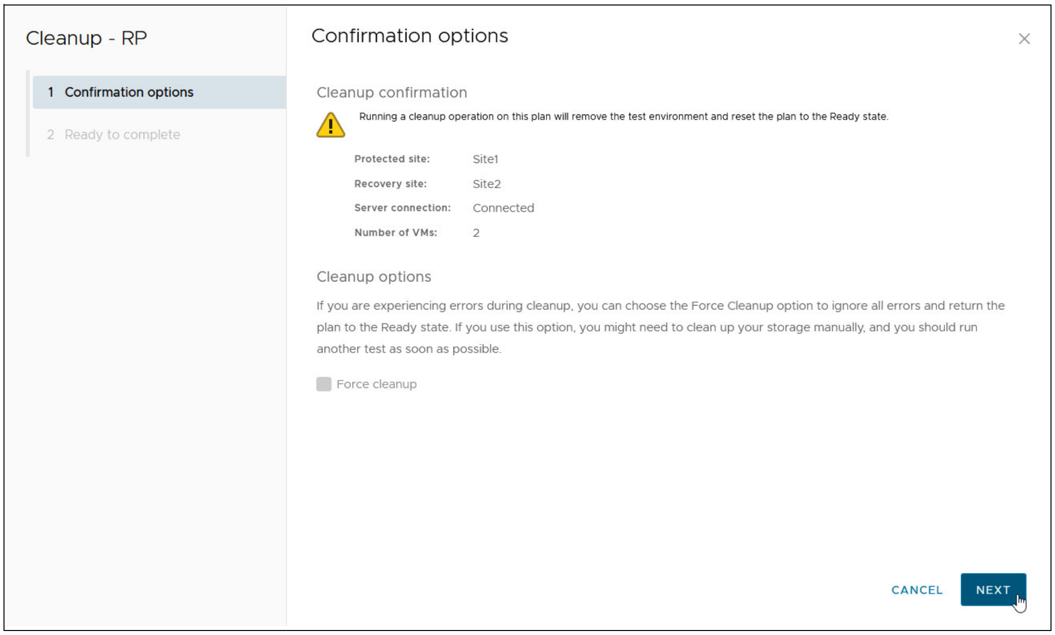


Figure 4-29 SRM Recovery Plan Cleanup

2. Confirm the cleanup and click **NEXT**, as illustrated in Figure 4-30.



Cleanup confirmation

Running a cleanup operation on this plan will remove the test environment and reset the plan to the Ready state.

Protected site:	Site1
Recovery site:	Site2
Server connection:	Connected
Number of VMs:	2

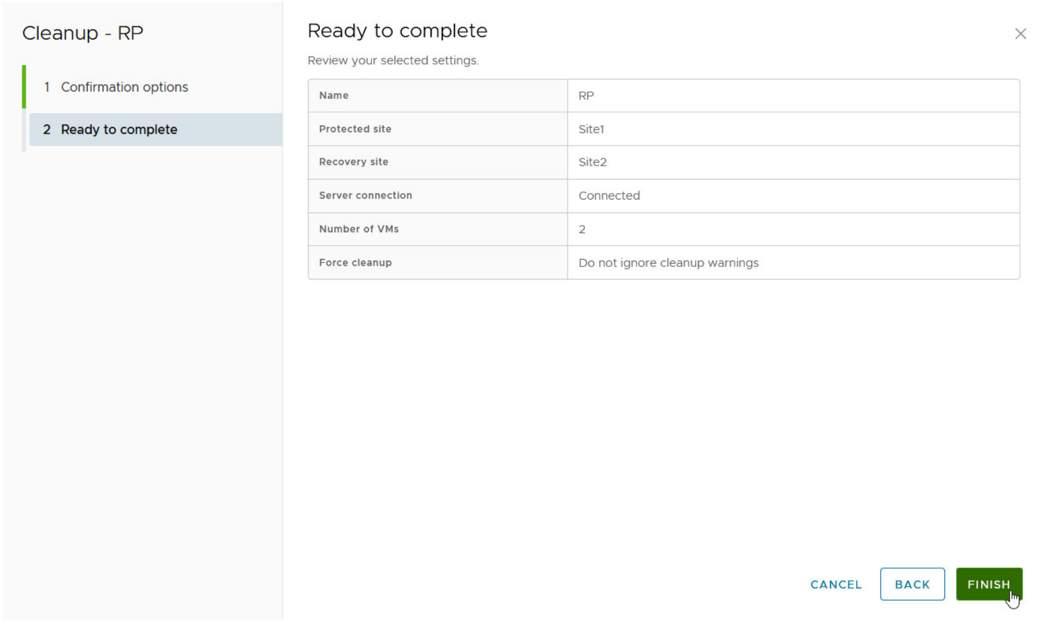
Cleanup options

If you are experiencing errors during cleanup, you can choose the Force Cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you might need to clean up your storage manually, and you should run another test as soon as possible.

□ Force cleanup

Figure 4-30 SRM Recovery Plan Cleanup Options

3. Review the summary and click **FINISH**, as depicted in Figure 4-31.



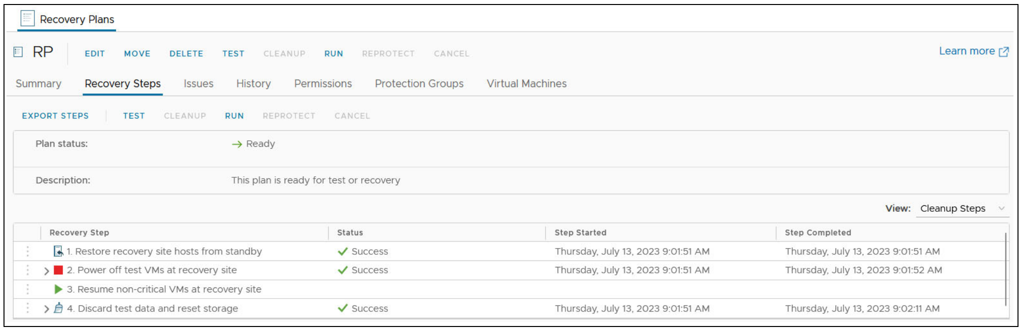
Ready to complete

Review your selected settings.

Name	RP
Protected site	Site1
Recovery site	Site2
Server connection	Connected
Number of VMs	2
Force cleanup	Do not ignore cleanup warnings

Figure 4-31 SRM Recovery Plan Cleanup Summary

4. The Cleanup starts and the results are visible in the tab Recovery Steps, as shown in Figure 4-32.



Plan status: → Ready

Description: This plan is ready for test or recovery

View: Cleanup Steps

Recovery Step	Status	Step Started	Step Completed
1. Restore recovery site hosts from standby	✓ Success	Thursday, July 13, 2023 9:01:51 AM	Thursday, July 13, 2023 9:01:51 AM
2. Power off test VMs at recovery site	✓ Success	Thursday, July 13, 2023 9:01:51 AM	Thursday, July 13, 2023 9:01:52 AM
3. Resume non-critical VMs at recovery site			
4. Discard test data and reset storage	✓ Success	Thursday, July 13, 2023 9:01:51 AM	Thursday, July 13, 2023 9:02:11 AM

Figure 4-32 SRM Recovery Plan Cleanup Recovery Steps

Run Recovery Plan

A Recovery Plan can run under planned or unplanned circumstances, if it is planned it is called Planned Migration. A Planned Migration shuts down the VMs on the Protected Site, stops the mirrors, changes the Recovery Site volumes to source volumes, maps those volumes, brings the datastores online, and starts the VMs on the Recovery Site

1. To run a Planned Migration, select **RUN**, as shown in Figure 4-33.

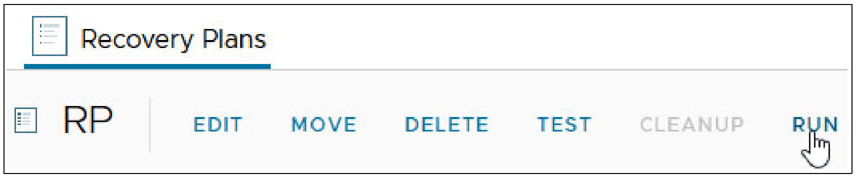
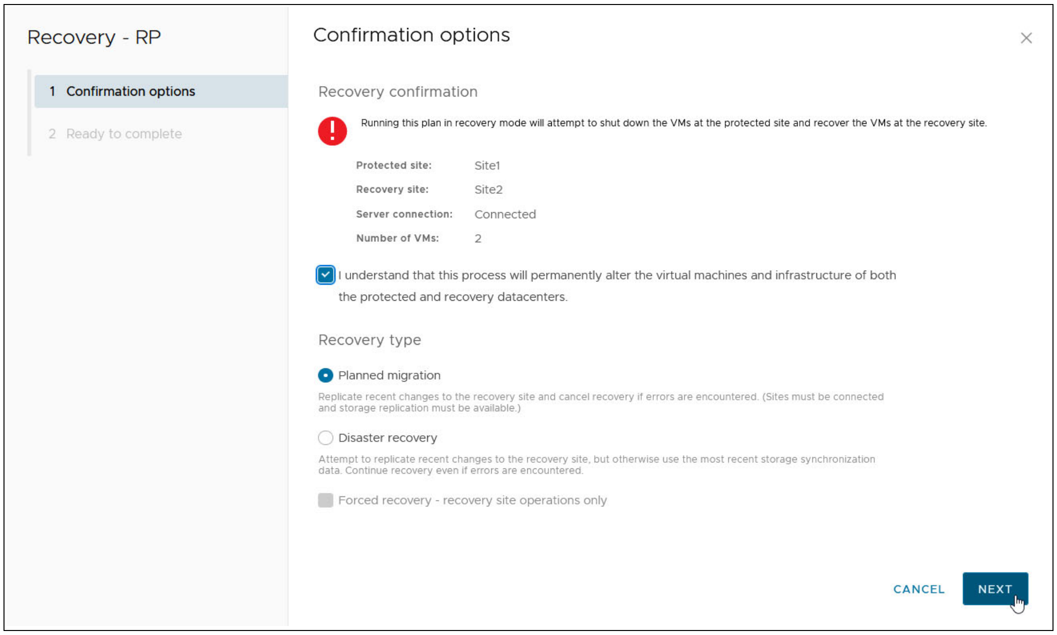


Figure 4-33 SRM Recovery Plan Run

2. Select that you understand the risks and confirm the recovery, and click **NEXT**, as illustrated in Figure 4-34.



Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site:	Site1
Recovery site:	Site2
Server connection:	Connected
Number of VMs:	2

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

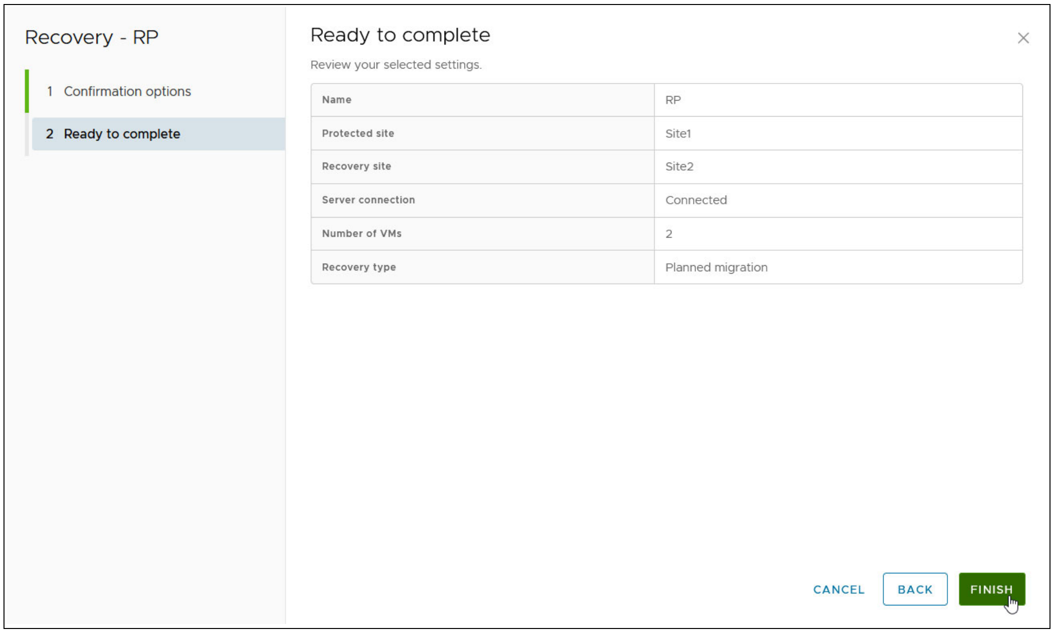
○ Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

□ Forced recovery - recovery site operations only

Figure 4-34 SRM Recovery Plan Run options

3. Review the summary and click **FINISH**, as depicted in Figure 4-35.



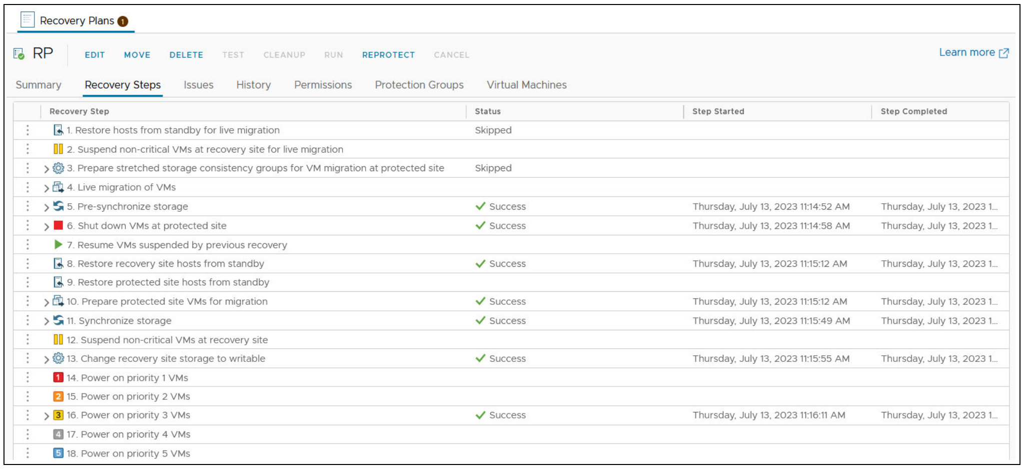
Ready to complete

Review your selected settings.

Name	RP
Protected site	Site1
Recovery site	Site2
Server connection	Connected
Number of VMs	2
Recovery type	Planned migration

Figure 4-35 SRM Recovery Plan Run summary

4. The Recovery starts and the results are visible in the tab Recovery Steps, as shown in Figure 4-32 on page 67.



Recovery Step	Status	Step Started	Step Completed
1. Restore hosts from standby for live migration	Skipped		
2. Suspend non-critical VMs at recovery site for live migration			
3. Prepare stretched storage consistency groups for VM migration at protected site	Skipped		
4. Live migration of VMs			
5. Pre-synchronize storage	✓ Success	Thursday, July 13, 2023 11:14:52 AM	Thursday, July 13, 2023 1...
6. Shut down VMs at protected site	✓ Success	Thursday, July 13, 2023 11:14:58 AM	Thursday, July 13, 2023 1...
7. Resume VMs suspended by previous recovery			
8. Restore recovery site hosts from standby	✓ Success	Thursday, July 13, 2023 11:15:12 AM	Thursday, July 13, 2023 1...
9. Restore protected site hosts from standby			
10. Prepare protected site VMs for migration	✓ Success	Thursday, July 13, 2023 11:15:12 AM	Thursday, July 13, 2023 1...
11. Synchronize storage	✓ Success	Thursday, July 13, 2023 11:15:49 AM	Thursday, July 13, 2023 1...
12. Suspend non-critical VMs at recovery site			
13. Change recovery site storage to writable	✓ Success	Thursday, July 13, 2023 11:15:55 AM	Thursday, July 13, 2023 1...
14. Power on priority 1 VMs			
15. Power on priority 2 VMs			
16. Power on priority 3 VMs	✓ Success	Thursday, July 13, 2023 11:16:11 AM	Thursday, July 13, 2023 1...
17. Power on priority 4 VMs			
18. Power on priority 5 VMs			

Figure 4-36 SRM Recovery Plan Run Recovery Steps

Reprotect Recovery Plan

A reprotect of the Recovery Plan changes the former Protected Site volumes to target volumes and activates the mirrors from the former Recovery Site, now the Protected Site, to the former Protected Site, now Recovery Site. Perform the following steps to reprotect a Recovery Plan:

1. To reprotect the Recovery Plan, select **REPROTECT**, as shown in Figure 4-37.

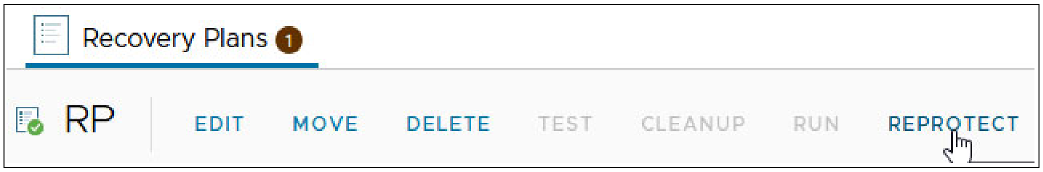
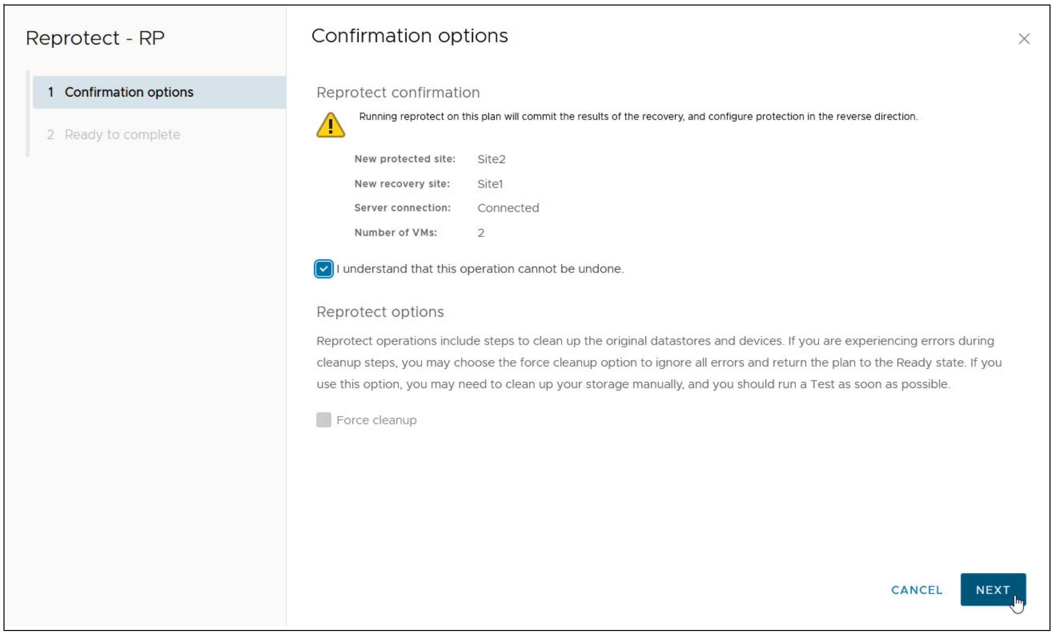


Figure 4-37 SRM Recovery Plan Reprotect

2. Select that you understand the risks and confirm the recovery **(**Figure 4-38). Click **NEXT.**



Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: Site2
New recovery site: Site1
Server connection: Connected
Number of VMs: 2

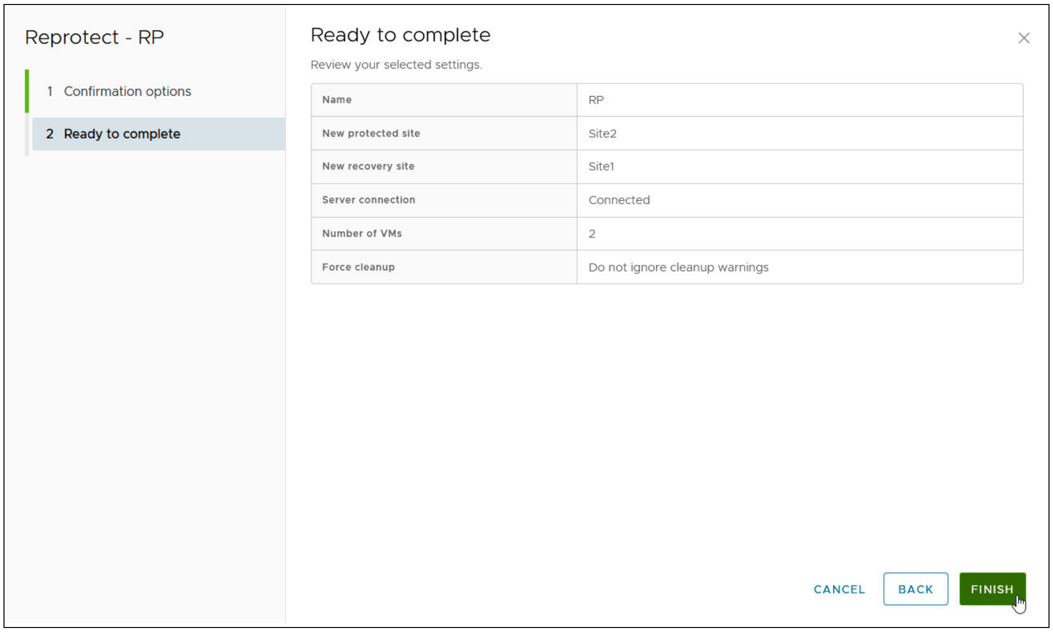
☑ I understand that this operation cannot be undone.

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Figure 4-38 SRM Recovery Plan Reprotect Options

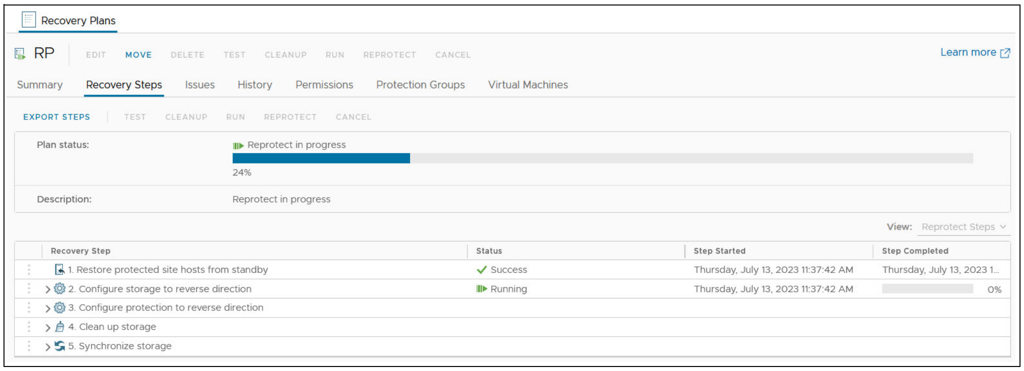
3. Review the summary and click **FINISH**, as depicted in Figure 4-39.



Name	RP
New protected site	Site2
New recovery site	Site1
Server connection	Connected
Number of VMs	2
Force cleanup	Do not ignore cleanup warnings

Figure 4-39 SRM Recovery Plan Reprotect Summary

4. The Reprotect starts and the results are visible in the tab Recovery Steps (Figure 4-40).



Plan status: Reprotect in progress 24%

Description: Reprotect in progress

Recovery Step	Status	Step Started	Step Completed
1. Restore protected site hosts from standby	✓ Success	Thursday, July 13, 2023 11:37:42 AM	Thursday, July 13, 2023 1...
2. Configure storage to reverse direction	Running	Thursday, July 13, 2023 11:37:42 AM	0%
3. Configure protection to reverse direction			
4. Clean up storage			
5. Synchronize storage			

Figure 4-40 SRM Recovery Plan Reprotect Recovery Steps

5. To failback to the original Protected Site another Planned Migration and Reprotect is necessary.

4.5 IBM HyperSwap with VMware vSphere Metro Storage Cluster

The IBM Storage Virtualize system supports multiple VMware vSphere stretched-storage cluster solutions with HyperSwap to provide the following benefits:

- Highly available active-active vSphere datastores
- Workload mobility
- Cross-site automated load-balancing
- Enhanced downtime avoidance
- Disaster avoidance

In this document, the focus is on solutions that rely both on VMware vSphere Metro Storage Cluster (vMSC) and VMware SRM in relation to IBM Storage Virtualize.

4.5.1 IBM HyperSwap

IBM Storage Virtualize HyperSwap is a dual-site solution that provides continuous availability of data during planned and unplanned outages. If storage at either site goes offline, HyperSwap automatically fails over storage access to the system at the surviving site.

When you configure a system with a HyperSwap topology, the system is split between two sites for data recovery, migration, or high availability use cases. When a HyperSwap topology is configured, each node or enclosure, external storage system, and host in the system configuration must be assigned to one of the sites in the topology. Both node canisters of an I/O group must be at the same site. This site must be the same site of any external storage systems that provide the managed disks to that I/O group. When managed disks are added to storage pools, their site attributes must match. This requirement ensures that each copy in a HyperSwap volume is fully independent and spans multiple failure domains (Figure 4-41).

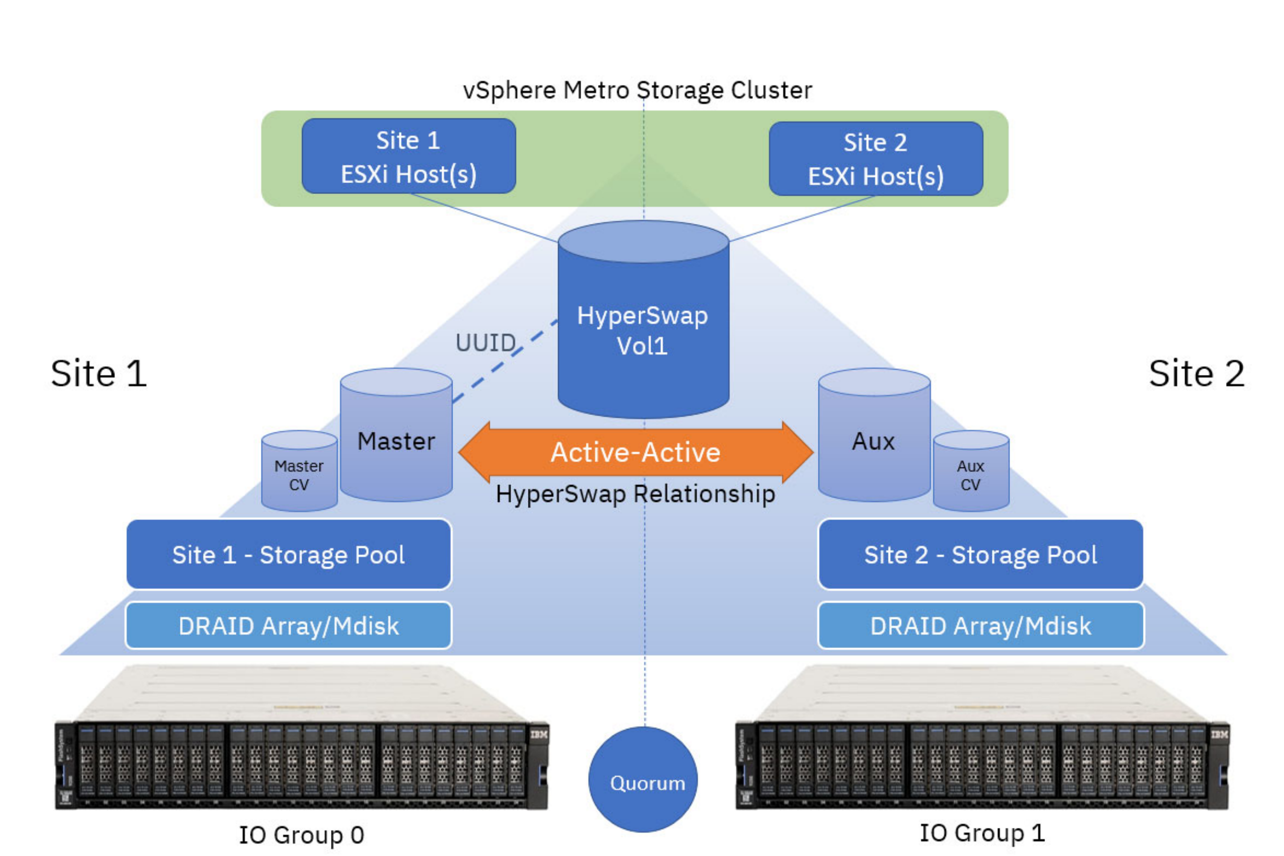


Figure 4-41 IBM HyperSwap

HyperSwap Volume is a group of volumes and remote copy relationships all working together to provide the active-active solution, and ensure that data is synchronized between sites.

A single HyperSwap Volume consists of the following items:

- A Master Volume and a Master Change Volume (CV) in one system site
- An Auxiliary Volume and an Auxiliary CV in the other system site

An active-active HyperSwap relationship exists between the Master and Auxiliary volumes to facilitate the data synchronization and replication between sites.

However, when you create a HyperSwap volume, the necessary components are created automatically, and the HyperSwap Volume can be managed as a single object.

Like a traditional Metro Mirror relationship, the active-active relationship attempts to keep the Master Volume and Auxiliary Volume synchronized while also servicing application I/O requests. The relationship uses the CVs as journaling volumes during the resynchronization process (Figure 4-42).

The HyperSwap Volume always uses the unique identifier (UID) of the Master Volume. The HyperSwap Volume is assigned to the host by mapping only the Master Volume even though access to the Auxiliary Volume is ensured by the HyperSwap function. For each HyperSwap volume, hosts across both sites see a single volume that is presented from the storage system with the UID of the Master Volume.

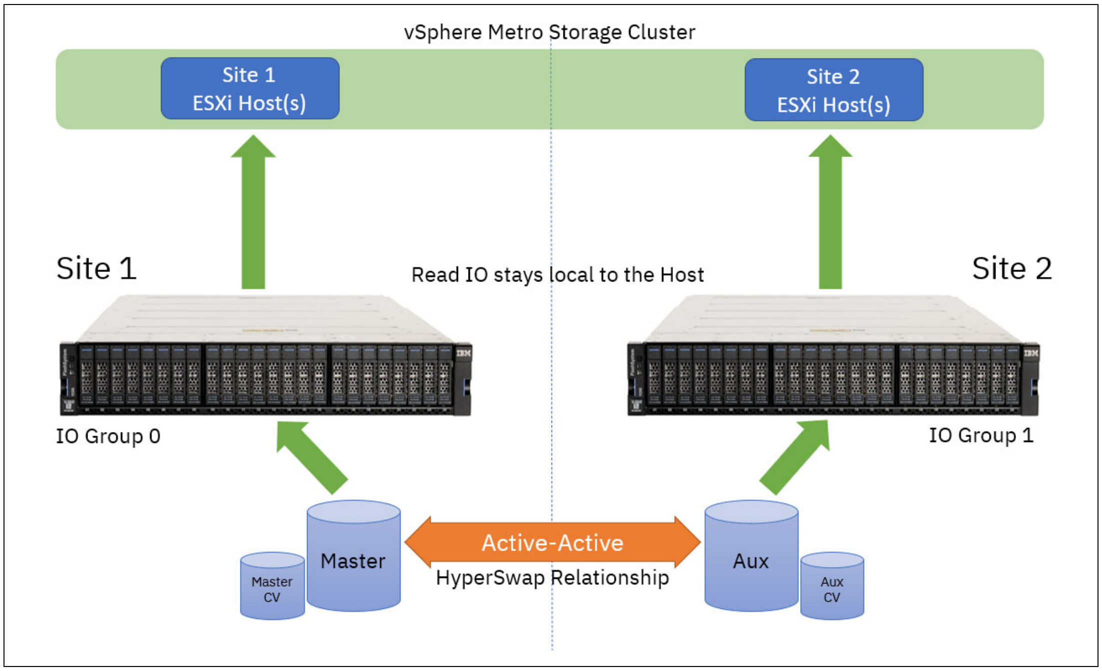


Figure 4-42 Read operations from hosts on either site are serviced by the local I/O group

To preserve application consistency when spanning multiple volumes, Consistency Groups can be created to keep a group of HyperSwap volumes consistent.

Cluster considerations

Consider the following tips when you work with HyperSwap and VMware vSphere Metro Storage Cluster (vMSC):

- One IBM Storage Virtualize-based storage system, which consists of at least two I/O groups. Each I/O group is at a different site. Both nodes of an I/O group are at the same site.
- HyperSwap-protected hosts on IBM Storage Virtualize must be connected to both storage nodes by using Internet Small Computer System Interface (iSCSI) or Fibre Channel.
- In addition to the two sites that are defined as failure domain, a third site is needed to house a quorum disk or IP quorum application.

- More system resources are used to support a fully independent cache on each site. This allows full performance even if one site is lost.

HyperSwap relationships

One site is considered as the Primary for each HyperSwap Volume or Consistency Group. This site is dynamically chosen according to the site that writes more data (more than 75% of write I/Os) to the volume or consistency group over a 20-minute period.

This role can change after a period of 20 minutes, if an I/O majority is detected in nodes on the non-Primary site, or it can change immediately, if a Primary-site outage occurs.

> **Note:** Low write-throughput rates do not trigger a direction switch to protect against unnecessary direction changes when experiencing a trivial workload.

Although the I/O group on each site processes all reads from the hosts on that local site, any write requests must be replicated across the inter-site link, which incurs added latency. Writes to the primary site experience a latency of 1x the round-trip time (RTT) between the sites. However, due to the initial forwarding process, writes to the non-primary site experience 2x the RTT. Consider this additional performance impact when you provision storage for latency-sensitive applications.

These relationships automatically run and switch direction according to which copy or copies are online and up-to-date.

Relationships can be grouped into consistency groups, in the same way as other types of remote-copy relationships. The consistency groups fail over consistently as a group based on the state of all copies in the group. An image that can be used for disaster recovery is maintained at each site.

HyperSwap I/O flow

This section contains examples of the HyperSwap I/O flow. In the following examples, Site 1 is considered as Primary.

Read operations from ESXi Hosts at either site

Figure 4-43 on page 74 illustrates the flow of read I/O requests from hosts at either site in the VMware vSphere Metro Storage Cluster.

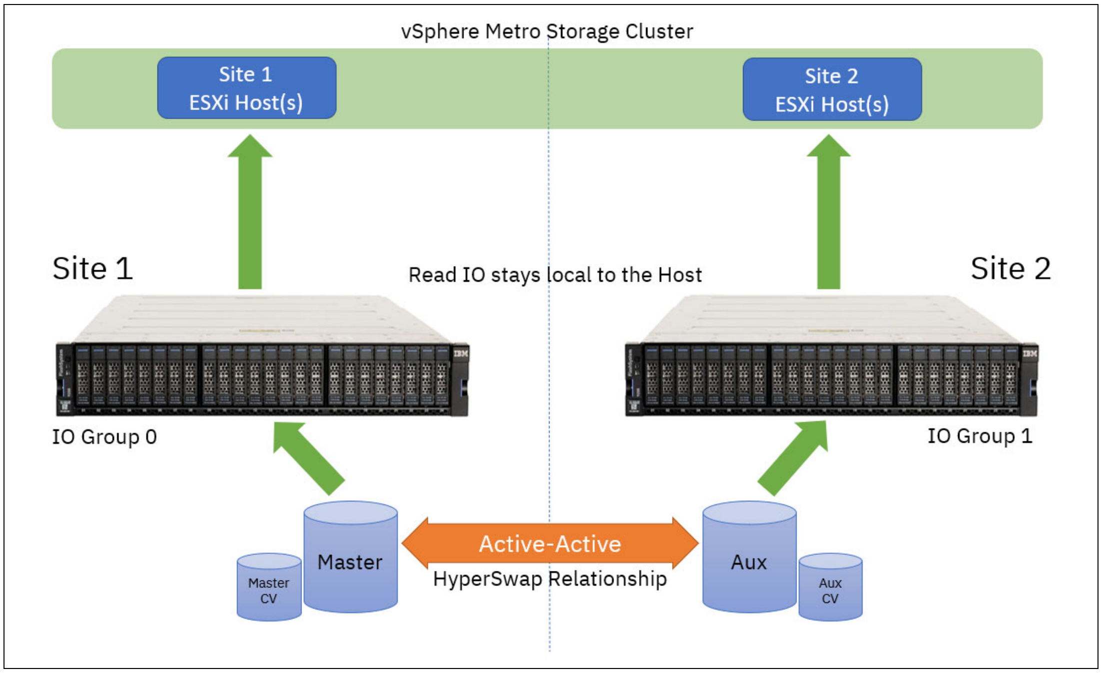


Figure 4-43 Read operations from hosts on either site are serviced by the local I/O group

Read I/O is facilitated by the I/O group that is local to the requesting host, which prevents the need for the I/O to transfer over the long-distance link and incur unnecessary latency.

Write operations from ESXi hosts at the local site

When hosts write on the Primary site, and the host, node, controller, and managed disk (MDisk) site awareness is correctly configured, the write I/Os go directly to the Primary site volume and I/O Group. The write I/Os are then replicated to the Secondary site volume and I/O Group (Figure 4-44).

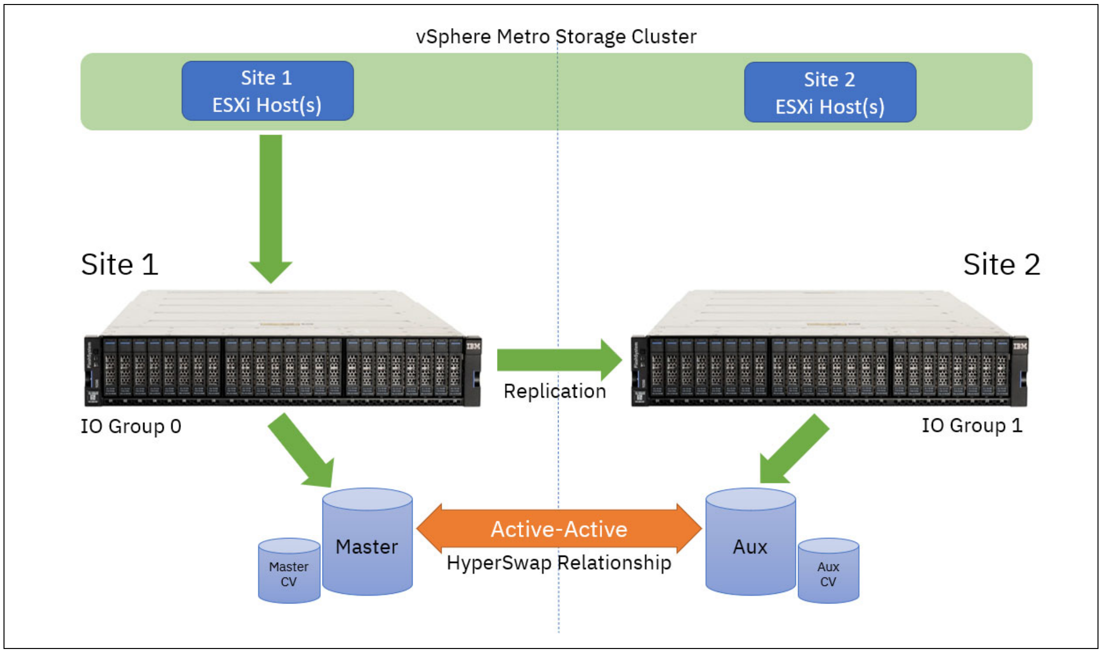


Figure 4-44 Write operations from hosts on primary are replicated

Write operations from ESXi hosts at the remote site

In this scenario, a write to I/O Group 1 must be applied to both copies, but the replication code cannot handle that task on I/O Group 0 because I/O Group 0 currently holds the Primary copy. The write data is initially transferred from the host into a data buffer on a node in I/O Group 1. The node in I/O Group 1 sends the write, both metadata and customer data, to a node in I/O Group 0 (Figure 4-45).

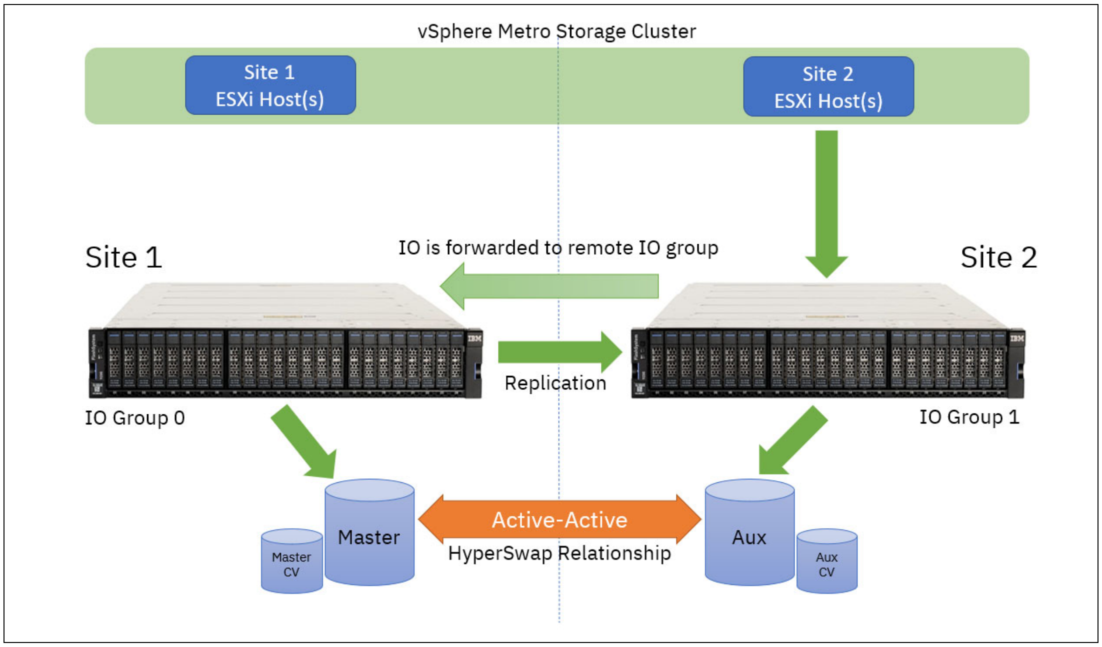


Figure 4-45 Write operations from hosts on Secondary are forwarded and replicated

On the node in I/O Group 0, the write is handled as though it were written directly to that I/O Group by a host. The replication code applies the write to the I/O Group 0 cache, and replicates it to I/O Group 1 to apply to the cache there, which means that writes to the secondary site have increased latency and use more bandwidth between the sites. However, sustained writes mainly to the secondary site over a 20-minute period switches the direction of the HyperSwap relationship, which eliminates this impact.

Note: Whenever the direction of a HyperSwap relationship changes, there is a brief pause to all I/O requests to that volume. In most situations, this pause is less than 1 second. Where possible, consider how application workload to a single HyperSwap volume (or HyperSwap consistency group) across sites can reduce the likelihood of repeated direction changes.

4.5.2 VMware vSphere Metro Storage Cluster

VMware vMSC is a storage-related feature and configuration that combines replication with array-based clustering that allows a single cluster to operate across geographically separate data centers. This capability allows two separated data centers to operate as a single cluster that provides significant benefits when maintaining data availability during both planned and unplanned downtimes.

IBM Storage Virtualize facilitates vMSC with the ability to create a single storage cluster that spans both sites, such that a datastore must be accessible in both locations. In other words, the datastore must be able to read and be written to simultaneously from both sites by using the HyperSwap feature of IBM Storage Virtualize. In a failure, the vSphere hosts are able to continue read and write access to the datastore from either location seamlessly and with no impact on ongoing storage operations.

Uniform versus Non-Uniform vMSC configurations

There are two ways in which a vMSC can be configured. The following terms refer to the different configurations of host connectivity across sites:

Non-Uniform host access configuration

An ESXi host has storage connectivity to only the storage system local to that site.

Uniform host access configuration

An ESXi host has storage connectivity to both local and remote storage systems.

For every volume presented from the IBM Storage FlashSystem, a preferred node is automatically elected. To evenly distribute the workload across the IBM Storage FlashSystem upon volume creation, the preferred node usually alternates between each node in the I/O group.

When you map a volume to a host object and rescan the host bus adapter (HBA) on the ESXi host, ESXi automatically identifies the available paths to both nodes in the I/O group. The paths to the preferred node for each volume are identified as the Active/Optimized paths. The paths to the non-preferred node are identified as Active/Non-Optimized paths.

By default, ESXi uses the Round-Robin path selection policy (PSP) to distribute I/O over any available Active/Optimized paths to the preferred node. A failover to Active/Non-Optimized paths occurs only if available paths to the preferred node do not exist.

Non-Uniform configuration

In Non-Uniform vMSC implementations, ESXi hosts use SCSI Asymmetric Logical Unit Access (ALUA) states to identify Active/Optimized paths to the preferred node in the local I/O group and Active/Non-Optimized paths to the partner node. The host has no visibility of the storage system at the remote site (Figure 4-46).

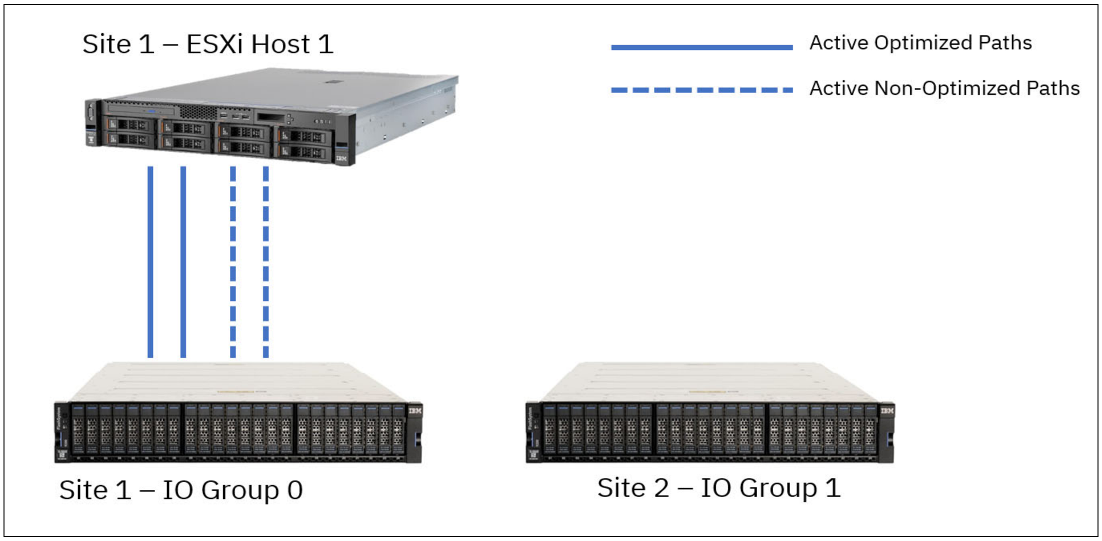


Figure 4-46 Non-Uniform host access vMSC

With Non-Uniform vMSC environments, if a storage failure occurs at the local site, the ESXi hosts lose access to the storage because paths are not available to the storage system at the remote site. However, this architecture might be useful when you run clustered applications like Microsoft SQL or Microsoft Exchange with servers that are at each site. It might be preferable to have a clustered application fail over so that an application can continue to run with locally available storage.

Uniform configuration

In Uniform vMSC implementation, ESXi hosts also uses SCSI ALUA states to identify Active/Optimized paths to the preferred node and Active/Non-Optimized paths to the partner node in the local I/O group. Extra paths to the remote I/O group are automatically detected as Active/Non-Optimized. ESXi uses the Optimized paths to the local preferred node where possible, and fails over to the Non-Optimized paths only if there are no available paths to the preferred node (Figure 4-47).

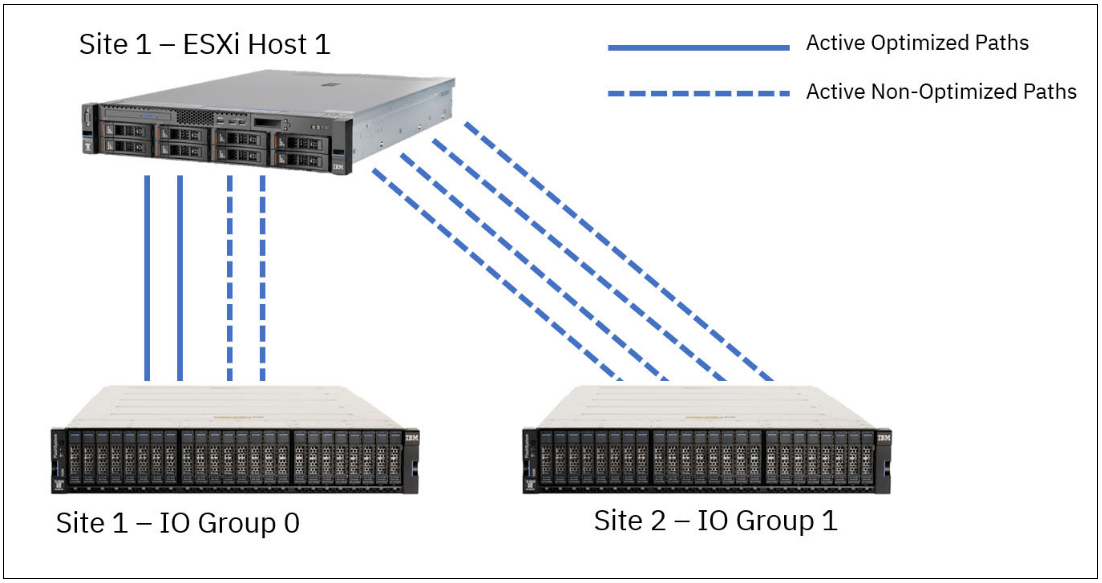


Figure 4-47 Uniform host access vMSC

4.5.3 IBM HyperSwap with VMware vSphere Metro Storage

Given the performance characteristics of a HyperSwap topology, it might be beneficial to review how HyperSwap volumes can be used by ESXi hosts to ensure optimal performance, data continuity, and reliability.

Virtual Machine File System datastore provisioning

As shown in Figure 4-48 on page 78, the following three different datastore architectures can be considered when provisioning and when using Virtual Machine File System (VMFS) datastores in a HyperSwap vMSC environment:

- Traditional Disaster Recovery
- Mixed access
- Alternating access

Each of these models applies at a single datastore level. Therefore, it is possible to incorporate all three methods in an IBM Storage FlashSystem HyperSwap architecture.

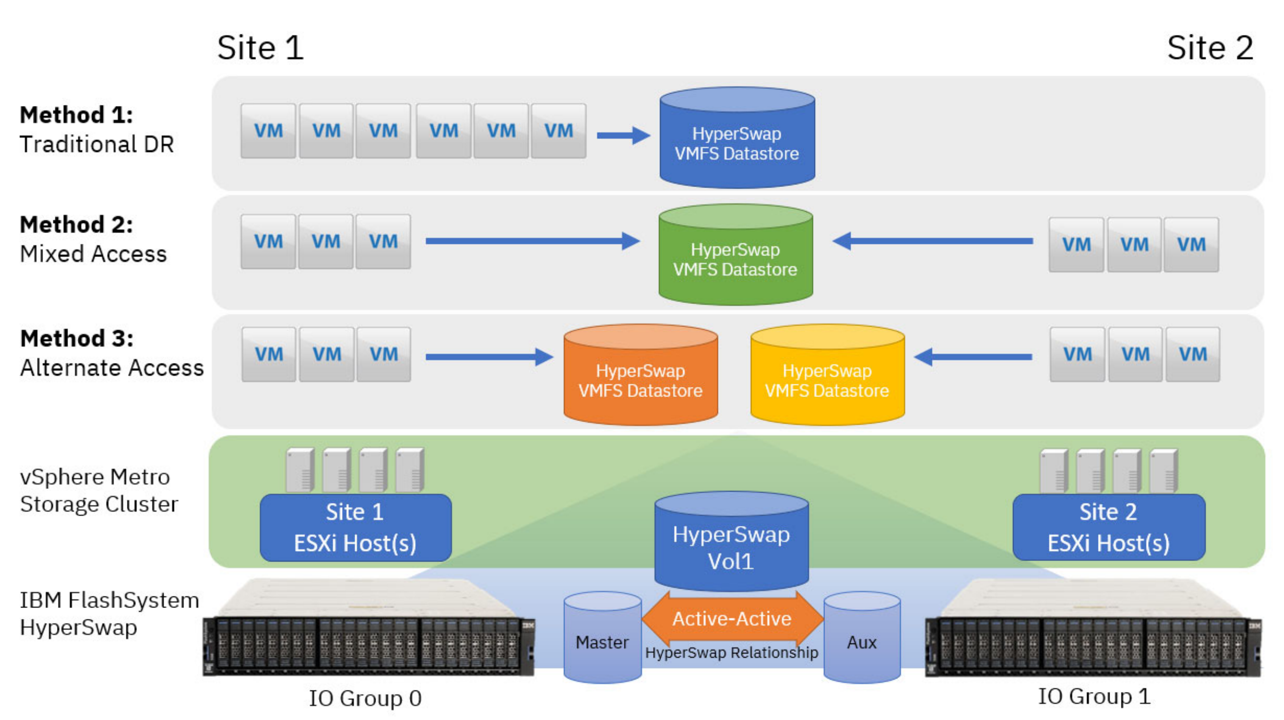


Figure 4-48 Three datastore architectures

Method 1: Traditional Disaster Recovery

This model can be conceptualized as a traditional DR configuration. In normal operating conditions, all VMs are running from a single site, and they fail over to ESXi hosts at the remote site only in a system or storage outage at Site 1. In this scenario, the direction of the HyperSwap relationship for the VMFS datastore is static because I/O is not running at Site 2. In a site outage, all the VMs are running on the ESXi hosts at Site 2 without requiring intervention on the storage system to enable access to the volumes.

The negative aspect of this configuration is that there can be many ESXi servers and storage resource at Site 2 that are idle.

Method 2: Mixed Access

In this scenario, the number of VMs for a datastore is split between both sites. ESXi servers at both sites are used, which maximizes compute resources at both sites. However, as discussed in “HyperSwap I/O flow” on page 73, any writes being performed at the non-primary site incur more latency when traversing the inter-site link. Potentially, half of the vSphere infrastructure can then experience additional latency.

In addition, if the workload is unregulated, the direction of the HyperSwap relationship can be swapped repeatedly, which generates more I/O pauses for each change of direction.

Method 3: Alternative Access

This scenario requires some minor, additional management to provision storage and maintain the vSphere environment. However, this scenario likely enables optimal storage performance and maximum realization of available compute resources.

Consider creating multiple VMFS datastores where the primary associated site alternates between Site 1 and Site 2, and keep VM-storage resources local to hosts that are running the VMs.

An example might include the following configuration:

- When you create datastores, use odd-numbered datastores to have a site preference of Site 1, and even-numbered datastores designated to Site 2.
- Migrate the compute resources for half of the VMs over to ESXi hosts on Site 2 to create an even distribution of workload between the two sites.
- For VMs running on ESXi hosts at Site 1, ensure the VMDKs are provisioned on odd-numbered datastores.

  For VMs running on ESXi hosts at Site 2, ensure the VMDKs are provisioned on the even-numbered datastores.
- Create Host/VM Groups and Host/VM Rules in vSphere to ensure that the Distributed Resource Scheduler (DRS) can function correctly to redistribute VMs across hosts within a site if required but can still enable failover in an outage.

As detailed in "Write operations from ESXi hosts at the remote site" on page 75, Alternative Access Method ensures that instead of any write I/Os at either site having to be forwarded over the inter-site link before being replicated to the remote site, they are serviced by the I/O group at the site where the I/O originated. This method reduces the overall latency and increases the performance and throughput.

The intention is for a given HyperSwap volume or consistency group to keep VM I/O workloads local to the host running the VM, which minimizes the workloads being driven from a host at the non-primary site.

In a site outage at either site, vSphere high availability (HA) automatically recovers the VMs on the surviving site.

For more information about DRS Host/VM groups and rules, see Create a VM-Host Group.

VMware Distributed Resource Scheduler

VMware DRS capabilities bring efficiency in the management of workloads through grouping VMware ESXi hosts into resource clusters to separate computing requests to different sites or failure domains. Employing VMware DRS in an active-active storage solution (such as HyperSwap) provides highly available resources to your workloads.

In an ideal HyperSwap environment, you do not want VMs to move to the other site. Instead, you want VMs to move to the other site only in a site failure, or intentionally balance workloads and achieve optimal performance.

ESXi hostnames

Create a logical naming convention so you can quickly identify which site a host is in. For example, the site can be included in the chosen naming convention or you can choose a numbering system that reflects the location (for example odd hosts are in site one). The naming convention makes the designing and the day-to-day running of your system easier.

Data locality and host affinity rules

Ideally, hosts should access data from their local storage array to improve response time. To ensure that this situation is the case, use VMware affinity rules to define the preferred site for VMs to run from a local logical unit number (LUN).

Logically name the LUNs with their home sites

This task is *not* a must and some want the flexibility to move LUNs between data centers, but it makes it easier for business as usual (BAU) staff to track which are local datastores.

VMware vSphere host multipathing ensures that VMs that are running continue to operate during various failure scenarios. Table 4-1 outlines the tested and supported failure scenarios when using SVC or IBM Storage FlashSystem family HyperSwap function, and VMware vSphere Metro Storage Cluster (vMSC).

Table 4-1 IBM Storage Virtualize HyperSwap and VMware vSphere Metro Storage Cluster supported failure scenarios

Failure scenario	HyperSwap behavior	VMware HA impact
Path failure: SVC or IBM Storage FlashSystem Family Back-End (BE) Port	Single path failure between SVC or IBM Storage FlashSystem Family control enclosure and flash enclosure. No impact on HyperSwap.	No impact.
Path failure: SVC or IBM Storage FlashSystem Family Front-End (FE) Port	Single path failure between SVC or IBM Storage FlashSystem Family control enclosure and vSphere host. vSphere host uses alternative paths.	No impact.
BE flash enclosure failure at Site-1	SVC or IBM Storage FlashSystem Family continues to operate from the volume copy at Site-2. When the flash enclosure at Site-1 is available, HyperSwap synchronizes the copies.	No impact.
BE flash enclosure failure at Site-2	Same behavior as failure at Site-1.	No impact.
SVC or IBM Storage FlashSystem Family control enclosure failure	SVC or IBM Storage FlashSystem Family continues to provide access to all volumes through the other control enclosures.	No impact.
Complete Site-1 failure (The failure includes all vSphere hosts and SVC or IBM Storage FlashSystem Family controllers at Site-1)	SVC or IBM Storage FlashSystem Family continues to provide access to all volumes through the control enclosures at Site 2. When the control enclosures at Site-1 are restored, the volume copies are synchronized.	VMs running on vSphere hosts at the failed site are impacted. VMware HA automatically restarts them on vSphere hosts at Site-2.
Complete site 2 failure	Same behavior as a failure of Site-1.	Same behavior as a failure of Site-1.
Multiple vSphere host failures Power Off	No impact.	VMware HA automatically restarts the VMs on available ESXi hosts in the VMware HA cluster.
Multiple vSphere host failures, network disconnect	No impact.	VMware HA continues to use the datastore heartbeat to exchange cluster heartbeats. No impact.
SVC or IBM Storage FlashSystem Family inter-site link failure, vSphere cluster management network failure	SVC or IBM Storage FlashSystem Family active quorum is used to prevent a split-brain scenario by coordinating one I/O group to remain servicing I/O to the volumes. The other I/O group goes offline.	vSphere hosts continue to access volumes through the remaining I/O group. No impact.
Active SVC or IBM Storage FlashSystem Family quorum disk failure	No impact to volume access. A secondary quorum disk is assigned upon failure of the active quorum.	No impact.

Failure scenario	HyperSwap behavior	VMware HA impact
vSphere host isolation	No impact.	HA event dependent upon isolation response rules configured for the vSphere cluster. VMs can be left running, or rules can dictate for VMs to shut down and restart on other hosts in the cluster.
vCenter server failure	No impact.	No impact to running VMs or VMware HA. VMware DRS function is affected until vCenter access is restored.

5

Embedded VASA Provider for Virtual Volumes (vVol)

This chapter describes the implementation of the Embedded VASA Provider feature and includes the following sections:

- 5.1, “Overview” on page 84
- 5.2, “System prerequisites” on page 85
- 5.3, “Enabling vVols by using an Embedded VASA Provider” on page 99
- 5.4, “Migrating from existing IBM Spectrum Connect vVol configurations” on page 111
- 5.5, “Decommissioning IBM Spectrum Connect” on page 115

5.1 Overview

VMware vSphere Virtual Volumes require the vSphere APIs for Storage Awareness (VASA) APIs to function, which are facilitated by a VASA Provider, also known as a storage provider. Historically, IBM storage systems that are powered by IBM Storage Virtualize required a separate, external application to fulfill the VASA provider role, that is, IBM Spectrum Connect. This application was installed in a Linux environment and required TCP/IP connectivity between the VMware vSphere environment and the management interface of the IBM Storage Virtualize storage system.

However, this external IBM Spectrum Connect component introduces an additional administrative burden in VMware vSphere Virtual Volume (vVol) environments because it requires the following items:

- Dedicated virtual machines (VMs)
- Installation of a supported Linux distribution to host the application
- Installation of several prerequisite packages and services
- On-going support to secure, update, and back up the VM or application
- A separate management interface
- Additional complexity in configuring and maintaining the environment

Starting with IBM Storage Virtualize firmware 8.5.1.0 or later, the VASA Provider function has been incorporated natively in to the configuration node of the cluster to simplify the overall architecture of a vVol environment. This feature is referred to as the Embedded VASA Provider.

5.1.1 Supported platforms for the Embedded VASA Provider

Of the hardware platforms that support the 8.5.1.0 firmware, Table 5-1 shows the ones that support the Embedded VASA Provider feature of IBM Storage Virtualize.

Table 5-1 Supported platforms for the Embedded VASA Provider

Platform name	Supports Embedded VASA Provider
IBM FlashSystem 5015	No
IBM FlashSystem 5035	No
IBM FlashSystem 5045	No
IBM FlashSystem 5100	Yes
IBM FlashSystem 5200	Yes (memory upgrade required)
IBM Storwize V7000	Yes (Gen3 only)
IBM FlashSystem 7200	Yes
IBM FlashSystem 7300	Yes
IBM FlashSystem 9110	Yes
IBM FlashSystem 9150	Yes
IBM FlashSystem 9200	Yes
IBM FlashSystem 9500	Yes

Platform name	Supports Embedded VASA Provider
IBM SAN Volume Controller - 2145-SV2	Yes
IBM SAN Volume Controller - 2145-SV3	Yes
IBM SAN Volume Controller - 2145-SA2	Yes

5.1.2 Feature comparison between the Embedded VASA Provider and IBM Spectrum Connect

In the initial release of the Embedded VASA Provider, there are several limitations that might restrict functions when compared to existing vVol support that uses IBM Spectrum Connect. Evaluate the requirements of your environment before selecting a VASA Provider.

Table 5-2 shows the feature comparison.

Table 5-2 Feature comparison between the Embedded VASA Provider and IBM Spectrum Connect

Item	IBM Spectrum Connect	Embedded VASA Provider
Enhanced Stretched Cluster	Yes	No
vVol mirroring	Yes	No
Multiple vCenter connectivity	Yes, with multiple IBM Spectrum Connect instances	No
Multiple vVol datastores	Yes	Yes

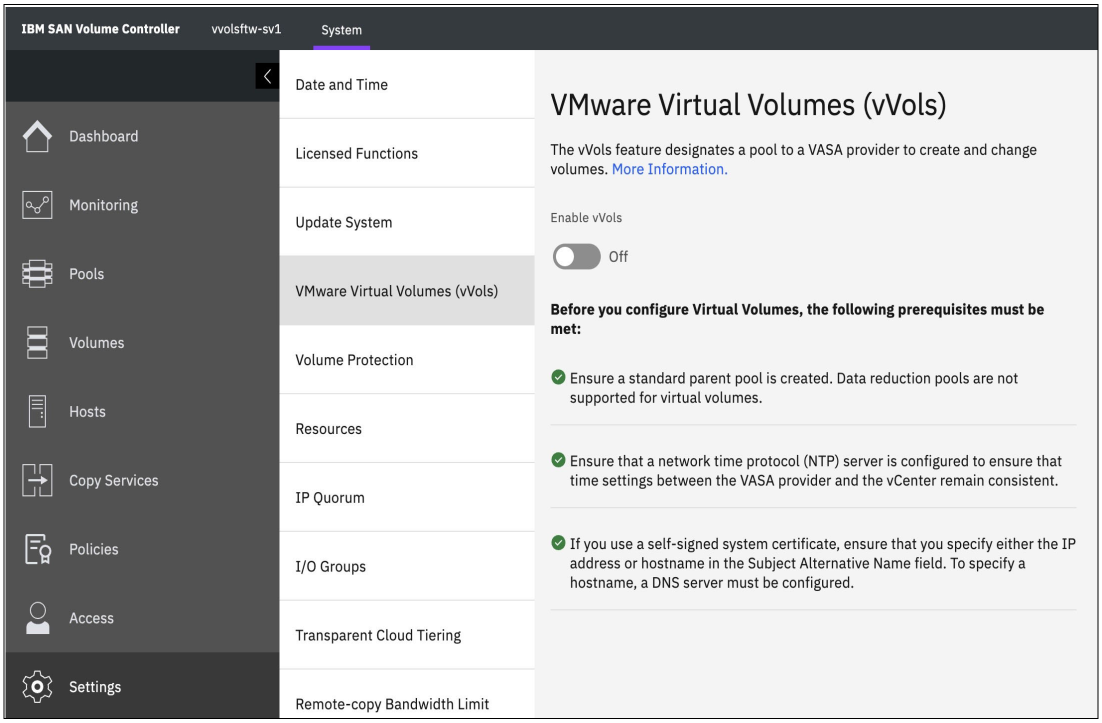
5.2 System prerequisites

This section includes a description of the system prerequisites for implementing the Embedded VASA Provider feature.

5.2.1 Preparing IBM Storage Virtualize for vVol

Before vVols can be enabled in the GUI, there are several prerequisites that must be completed. When you select **Settings** → **vVols GUI** and the window opens, you see that there are many checks that are being evaluated.

The Enable vVols toggle switch is disabled until the following tasks are completed, as shown in Figure 5-1.



VMware Virtual Volumes (vVols)

The vVols feature designates a pool to a VASA provider to create and change volumes. More Information.

Enable vVols

Off

Before you configure Virtual Volumes, the following prerequisites must be met:

✓ Ensure a standard parent pool is created. Data reduction pools are not supported for virtual volumes.

✓ Ensure that a network time protocol (NTP) server is configured to ensure that time settings between the VASA provider and the vCenter remain consistent.

✓ If you use a self-signed system certificate, ensure that you specify either the IP address or hostname in the Subject Alternative Name field. To specify a hostname, a DNS server must be configured.

Figure 5-1 vVols prerequisites

Configure the system with the following prerequisites:

- The system must have a standard pool with storage capacity that is allocated.

> **Note:** Data reduction pools (DRPs) are not supported for either the metadata volume disk (VDisk) or individual vVols.

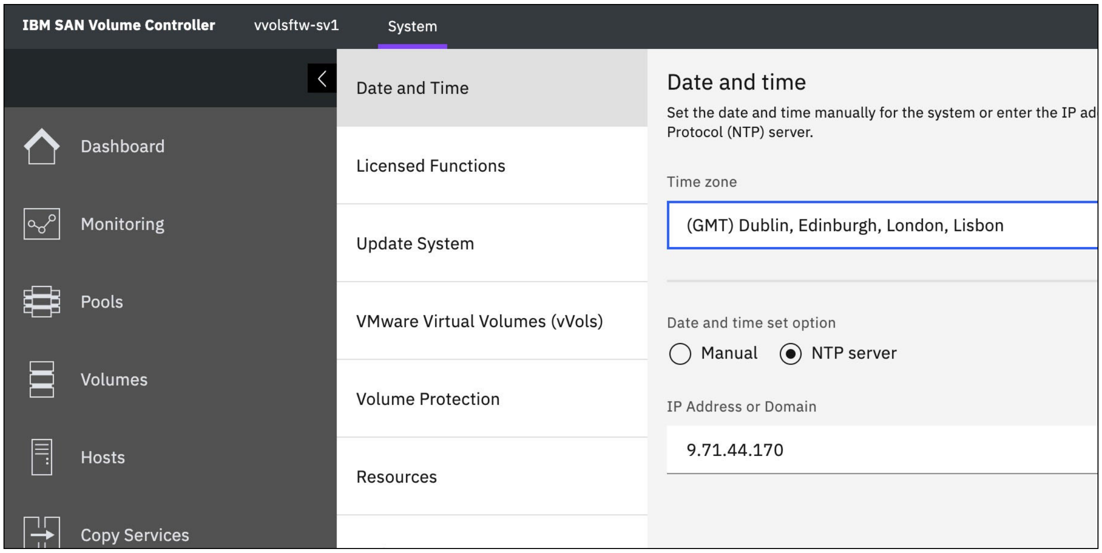
- The system must be configured with a Network Time Protocol (NTP) server to ensure that the date and time are consistent with the VMware infrastructure.
- The system must be configured with a certificate with a defined Subject Alternative Name value.

> **Note:** Additionally, all hosts that require access to the vVol datastore must be configured with the vVol host type.

5.2.2 Configuring the NTP server

To configure the NTP server on the system, complete the following steps:

1. Go to the **Settings** → **System** window in the GUI, and select **Date and time**, as shown in Figure 5-2.



Date and time

Set the date and time manually for the system or enter the IP ad
Protocol (NTP) server.

Time zone: (GMT) Dublin, Edinburgh, London, Lisbon

Date and time set option: ○ Manual ● NTP server

IP Address or Domain: 9.71.44.170

Figure 5-2 NTP time zone

2. Select the time zone.
3. Select **NTP server** and enter the IP address or fully qualified domain name (FQDN) for the NTP server within your environment.

> **Note:** If you use an FQDN or DNS name for the NTP server, you must ensure that a DNS server is configured in the system. To configure DNS servers, select **Settings** → **Network** and select **DNS**.

4. Click **Save** to complete the change.

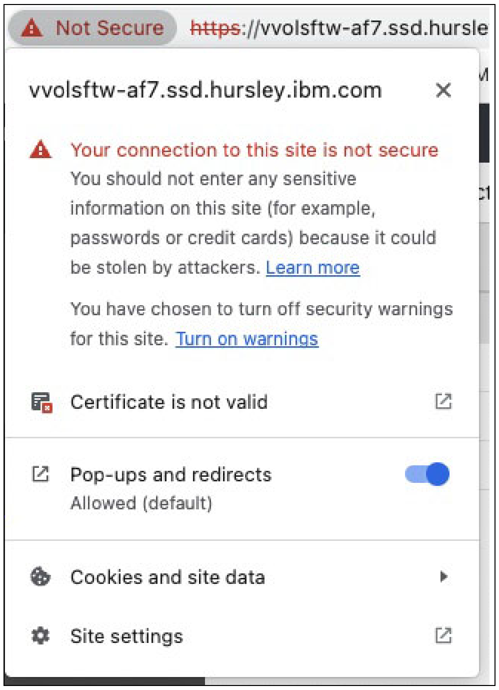
5.2.3 Configuring a storage system certificate

Instead of using simple username and password credentials, the Embedded VASA Provider uses SSL certificates for secured communication between vSphere and the IBM Storage Virtualize storage system.

When you use a self-signed certificate, you must update the Subject Alternative Name field in the certificate before registering the Embedded VASA Provider within vCenter. When you use a signed certificate, this value is likely defined.

To configure a storage system certificate, complete the following steps:

1. Confirm whether this value is defined on the system certificate by connecting to the web user interface for the storage system and inspecting the certificate information in the browser window. Review the certificate information in the browser window, as shown in Figure 5-3 on page 88.



Not Secure ~~https~~://vvolsftw-af7.ssd.hursle

vvolsftw-af7.ssd.hursley.ibm.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards) because it could be stolen by attackers. Learn more

You have chosen to turn off security warnings for this site. Turn on warnings

Certificate is not valid

Pop-ups and redirects

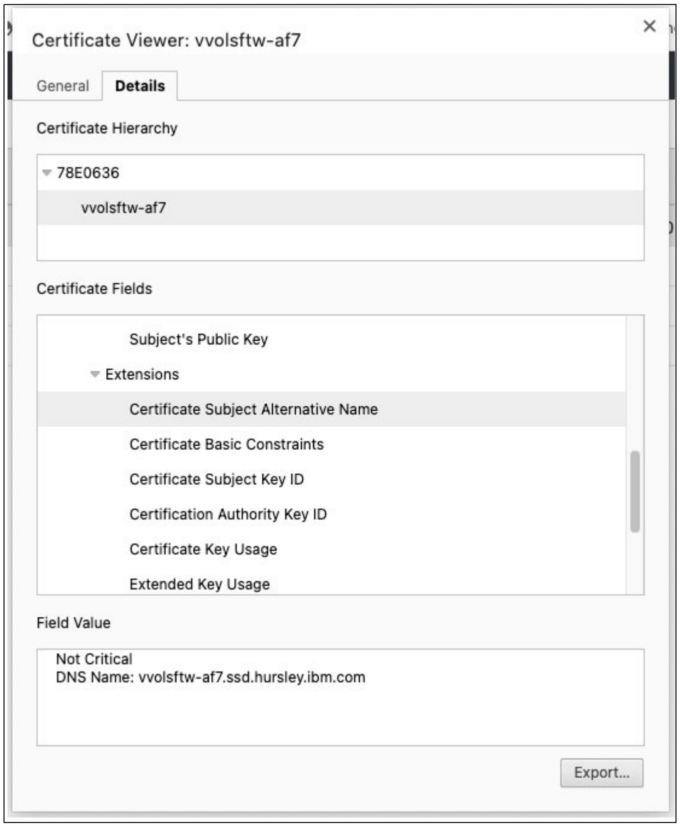
Allowed (default)

Cookies and site data

Site settings

Figure 5-3 Reviewing the certificate information

2. Expand the details and review the Subject Alternative Name value, as shown in Figure 5-4.



Certificate Viewer: vvolsftw-af7

General | **Details**

Certificate Hierarchy

- 78E0636
  - vvolsftw-af7

Certificate Fields

- Subject's Public Key
- Extensions
  - Certificate Subject Alternative Name
  - Certificate Basic Constraints
  - Certificate Subject Key ID
  - Certification Authority Key ID
  - Certificate Key Usage
  - Extended Key Usage

Field Value

```
Not Critical
DNS Name: vvolsftw-af7.ssd.hursley.ibm.com
```

Export...

Figure 5-4 Reviewing the Subject Alternative Name value

3. Alternatively, run the **lssystemcert** command, which shows the following output, as shown in Example 5-1.

Example 5-1 lssystemcert command

```
IBM_2145:vvolsftw-sv1:superuser>lssystemcert | grep -A 1 "Subject Alternative
Name"
X509v3 Subject Alternative Name: IP Address:9.71.20.20
```

4. If no Subject Alternative Name field is defined, update the self-signed certificate. To do this task, select **Settings** → **Security** and select **Secure Communications**, as shown in Figure 5-5.

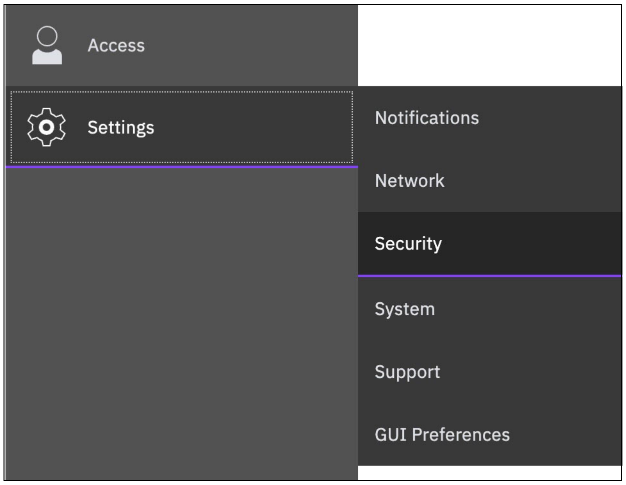
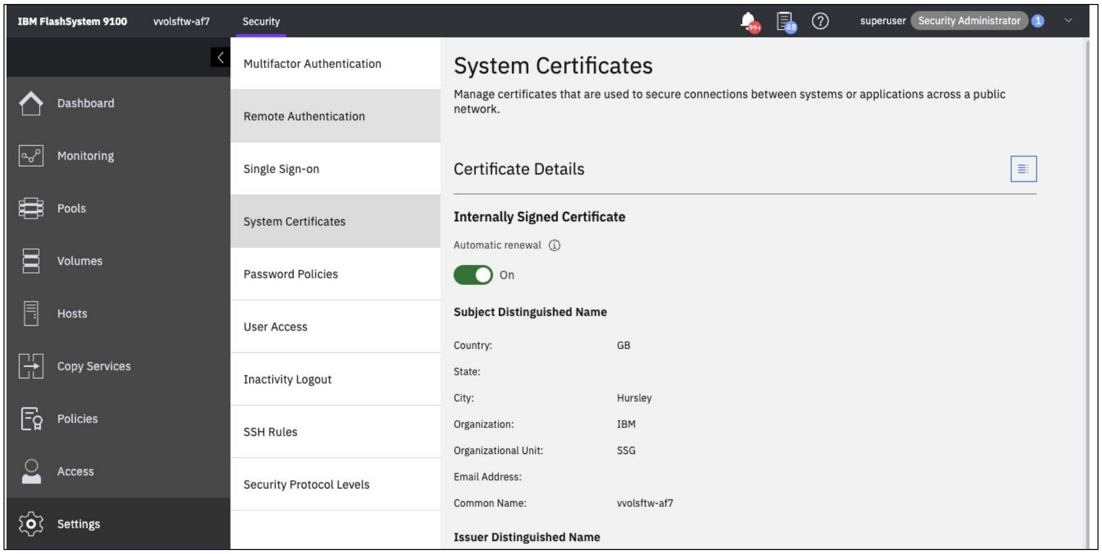


Figure 5-5 Secure Communications

5. Click **Update Certificate**, as shown in Figure 5-6.



System Certificates

Manage certificates that are used to secure connections between systems or applications across a public network.

Certificate Details

Internally Signed Certificate

Automatic renewal: On

Subject Distinguished Name

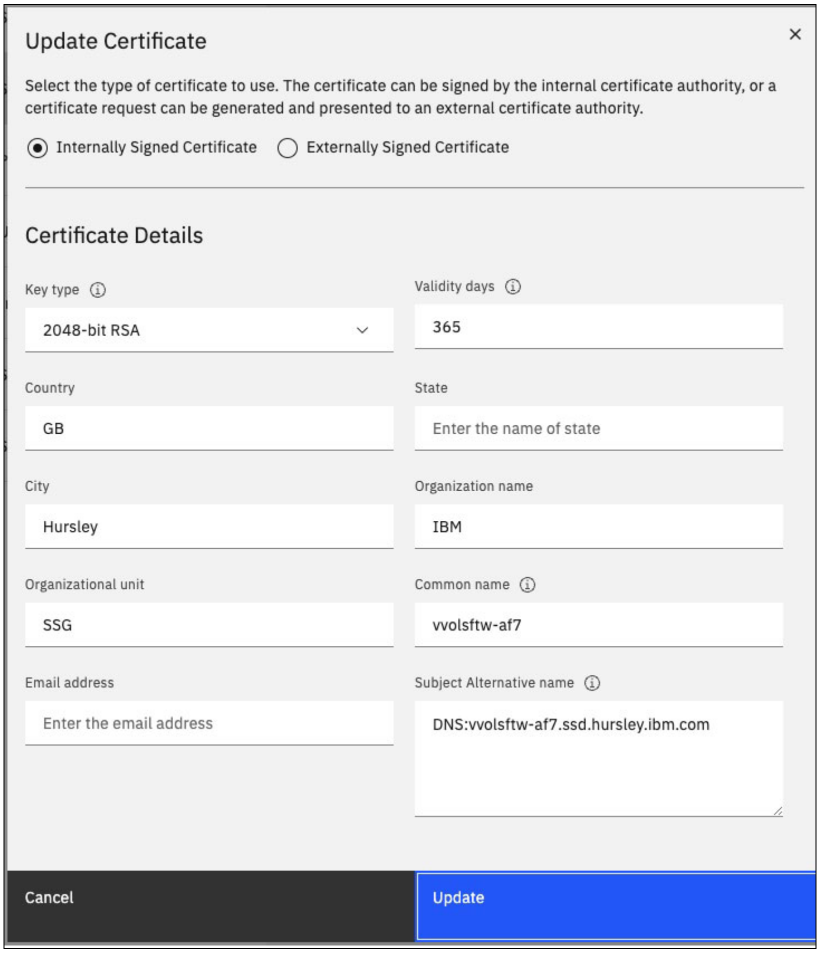
Country: GB
State:
City: Hursley
Organization: IBM
Organizational Unit: SSG
Email Address:
Common Name: vvolsftw-af7

Issuer Distinguished Name

Figure 5-6 Update Certificate

6. Complete the certificate notification and ensure that a Subject Alternative Name value is defined. This value can either be an IP address, DNS name, or FQDN. However, the specified Subject Alternative Name extension must resolve to the same host as the VASA provider's advertised IP address, hostname, or FQDN, as shown in Figure 5-7 on page 90.

Note: If you use an FQDN or DNS name, you must ensure that a DNS server is configured in the system. To configure DNS servers, select **Settings** → **Network** and select **DNS**.



Update Certificate

Select the type of certificate to use. The certificate can be signed by the internal certificate authority, or a certificate request can be generated and presented to an external certificate authority.

● Internally Signed Certificate ○ Externally Signed Certificate

Certificate Details

Key type: 2048-bit RSA	Validity days: 365
Country: GB	State: Enter the name of state
City: Hursley	Organization name: IBM
Organizational unit: SSG	Common name: vvolsftw-af7
Email address: Enter the email address	Subject Alternative name: DNS:vvolsftw-af7.ssd.hursley.ibm.com

Figure 5-7 Update Certificate

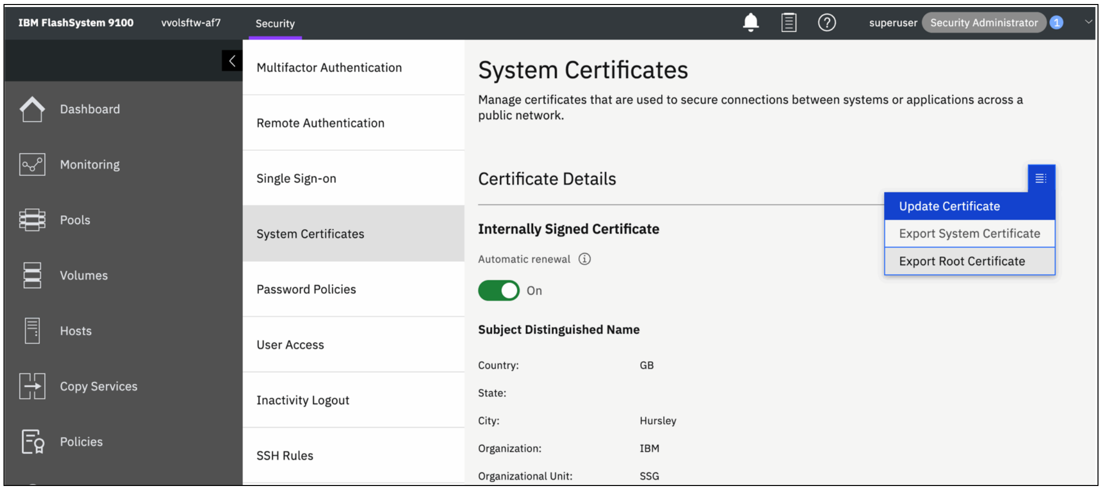
Note: In some versions of firmware, the GUI automatically populates some values for the **Subject Alternative Name** field, so do *not* user this page to view or verify the existing certificate values. Instead, check the certificate as reported by your web browser as mentioned previously in steps 1 and 2.

After updating the values in this window, clicking **Update** generates a new system-signed certificate for the storage system. During this time, the cluster IP is unavailable for a few minutes while the new security settings are applied. After a few minutes, you might need to refresh your browser window, and then you are prompted to accept the new self-signed certificate. Any I/O being processed by the system is unaffected by this process.

5.2.4 Exporting Root Certificate and adding to vCenter truststore

You are now required to export the root certificate from the storage system and upload it into the vCenter truststore.

1. To do this, navigate to **Settings** → **Security** and select **System Certificates**.
2. Locate the Action menu on the right side of the page, and select **Export Root Certificate**. See Figure 5-8.



System Certificates

Manage certificates that are used to secure connections between systems or applications across a public network.

Certificate Details

Internally Signed Certificate

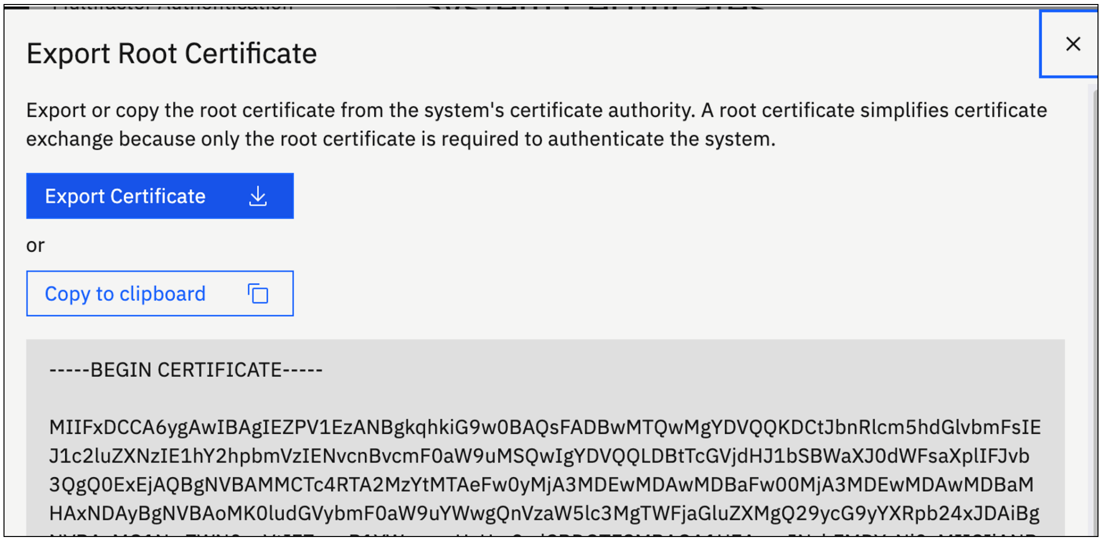
Automatic renewal: On

Subject Distinguished Name

Country: GB
State:
City: Hursley
Organization: IBM
Organizational Unit: SSG

Figure 5-8 Select Export Root Certificate

3. Select **Export Certificate** in the following dialog box (Figure 5-9).



Export Root Certificate

Export or copy the root certificate from the system's certificate authority. A root certificate simplifies certificate exchange because only the root certificate is required to authenticate the system.

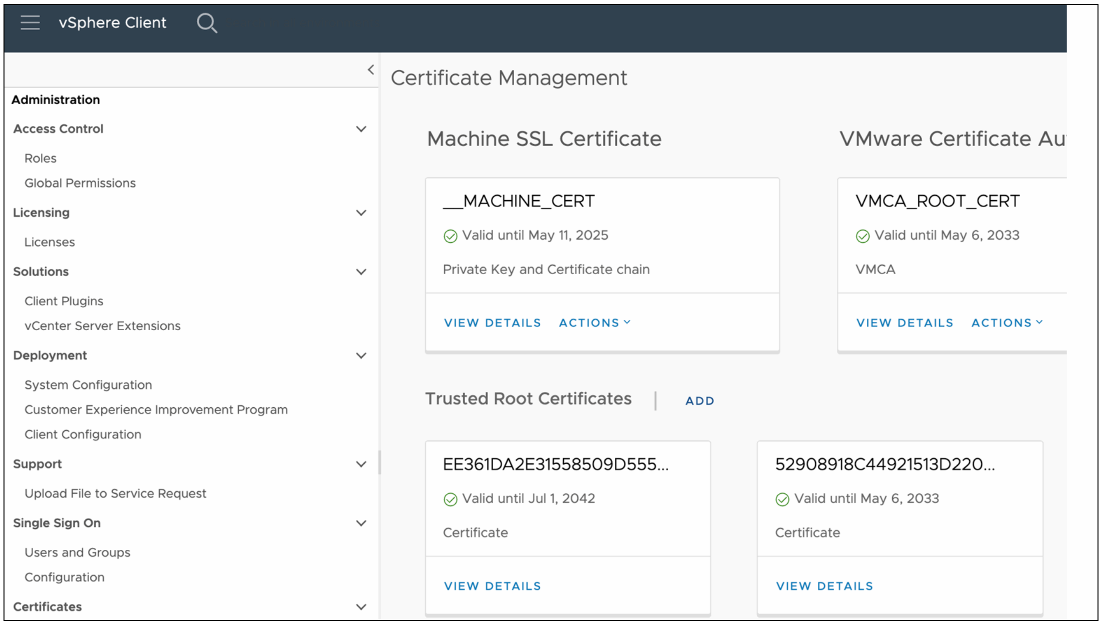
```
-----BEGIN CERTIFICATE-----

MIIFxDCCA6ygAwIBAgIEZPV1EzANBgkqhkiG9w0BAQsFADBwMTQwMgYDVQQKDCtJbnRlcm5hdGlvbmFsIE
J1c2luZXNzIE1hY2hpbmVzIENvcnBvcmF0aW9uMSQwIgYDVQQLDBtTcGVjdHJ1bSBWaXJ0dWFsaXplIFJvb
3QgQ0ExEjAQBgNVBAMMCTc4RTA2MzYtMTAeFw0yMjA3MDEwMDAwMDBaFw00MjA3MDEwMDAwMDBaM
HAxNDAyBgNVBAoMK0ludGVybmF0aW9uYWwgQnVzaW5lc3MgTWFjaGluZXMgQ29ycG9yYXRpb24xJDAiBg
```

Figure 5-9 Select Export Certificate

This downloads the storage system root certificate with a file name of `root_certificate.pem` through your browser session.

4. Navigate to the vSphere Client, and from the main navigation menu, select **Administration** → **Certificate Management**. See Figure 5-10 on page 92.



Machine SSL Certificate: __MACHINE_CERT, Valid until May 11, 2025, Private Key and Certificate chain

VMware Certificate Au: VMCA_ROOT_CERT, Valid until May 6, 2033, VMCA

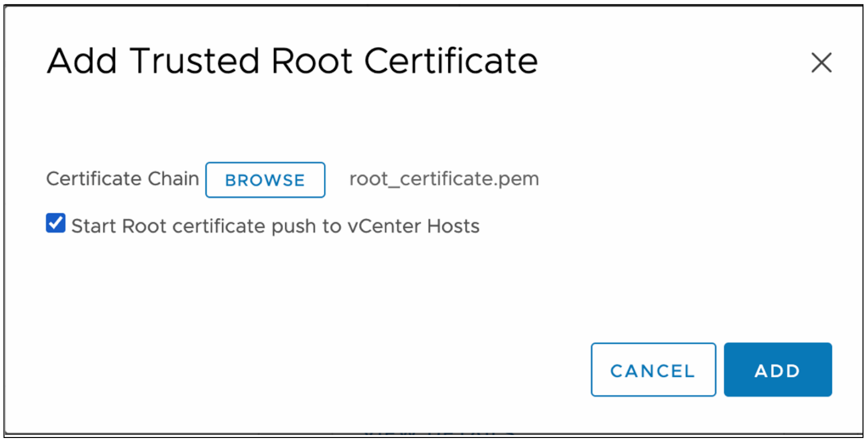
Trusted Root Certificates:

EE361DA2E31558509D555..., Valid until Jul 1, 2042, Certificate

52908918C44921513D220..., Valid until May 6, 2033, Certificate

Figure 5-10 Certificate Management

5. Locate Trusted Root Certificates and select **ADD**.
6. In the next window, browse to the `root_certificate.pem` file exported from the storage system, and check the box to **Start Root certificate push to vCenter Hosts**. Click **ADD**. See Figure 5-11.



Certificate Chain: root_certificate.pem

☑ Start Root certificate push to vCenter Hosts

Figure 5-11 Add Trusted Root Certificate

The new certificate is registered in the truststore, and a message stating “*CA certificates refresh on host successful!*”

5.2.5 Preparing ESXi hosts for vVol connectivity

Any ESXi hosts that require access to a vVol datastore must be defined as a vVol host type in the storage system.

> **Note:** As a best practice, create a single host object in IBM Storage Virtualize to represent each physical ESXi server in the configuration. When you use clustered host environments, for example, when multiple ESXi hosts are part of a vSphere cluster, use IBM Storage Virtualize Host Cluster objects to represent the vSphere cluster.

Complete the following steps:

1. To create a Host Cluster, select **Hosts** → **Host Clusters** in the management GUI, and select **Create Host Cluster**, as shown in Figure 5-12.

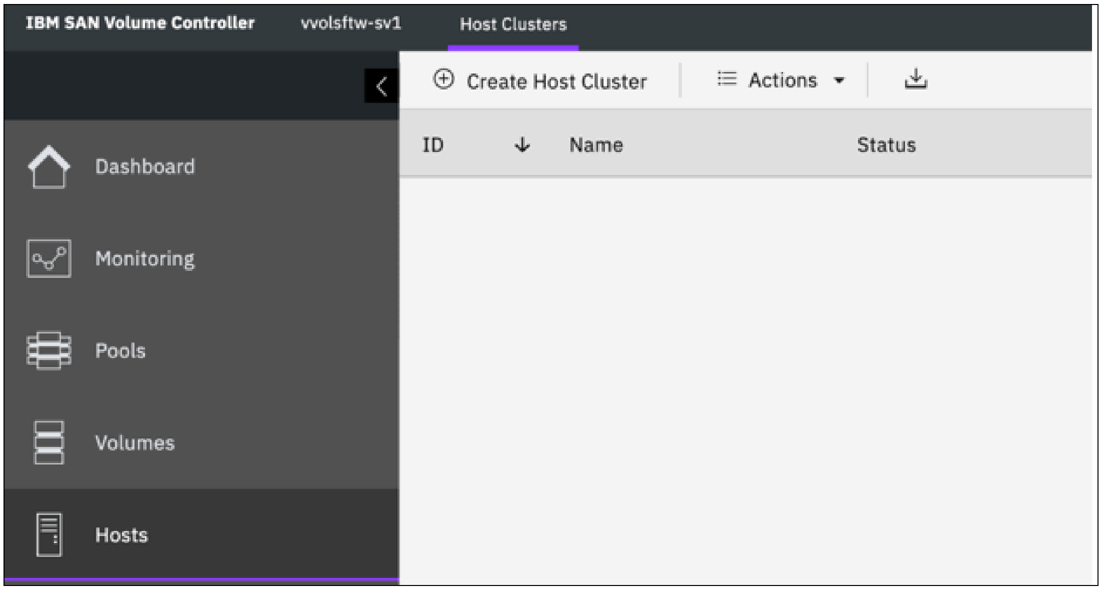
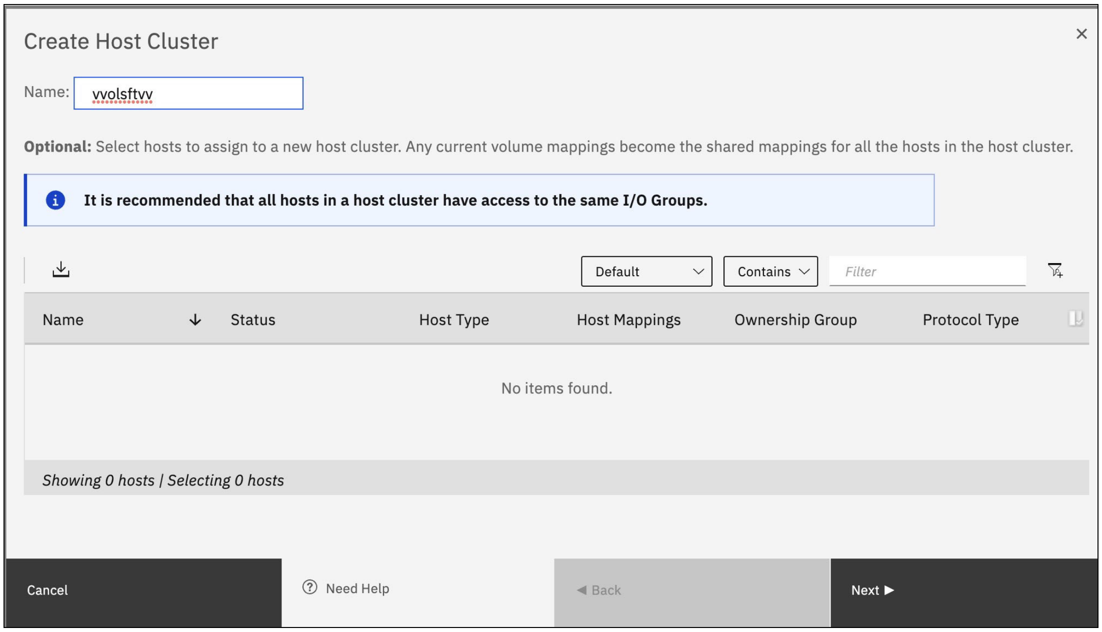


Figure 5-12 Create Host Cluster

2. Specify a name for the host cluster object and click **Next**. To simplify troubleshooting, consider using the same name for the Host Cluster object as is defined on the vSphere Cluster within vCenter, as shown in Figure 5-13 on page 94.
3. Review the summary window, and click **Make Host Cluster**, as shown in Figure 5-14 on page 94.



Create Host Cluster

Name: vvolsftvv

Optional: Select hosts to assign to a new host cluster. Any current volume mappings become the shared mappings for all the hosts in the host cluster.

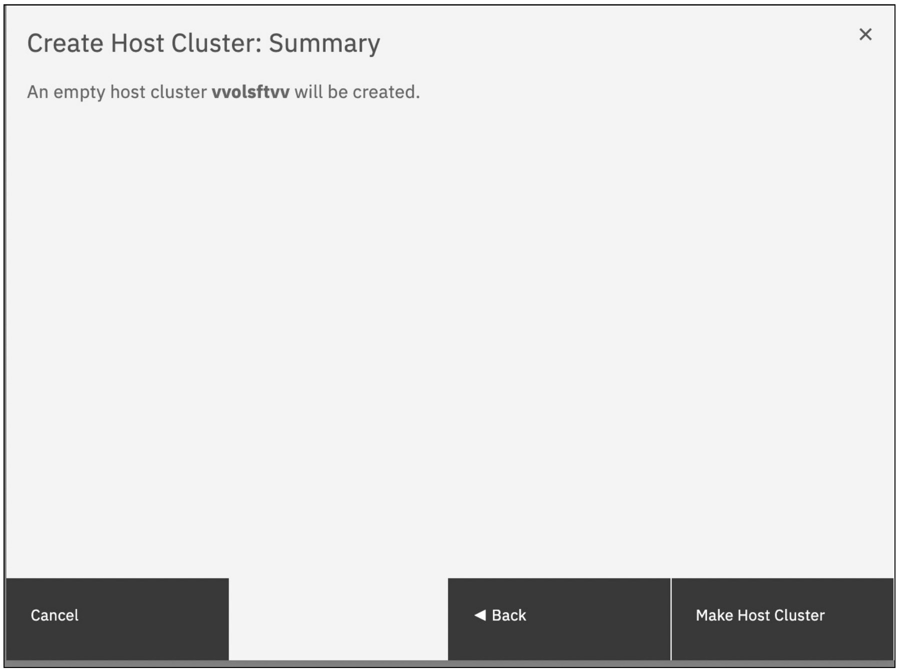
It is recommended that all hosts in a host cluster have access to the same I/O Groups.

Name	Status	Host Type	Host Mappings	Ownership Group	Protocol Type

No items found.

Showing 0 hosts | Selecting 0 hosts

Figure 5-13 Create Host Cluster



Create Host Cluster: Summary

An empty host cluster **vvolsftvv** will be created.

Figure 5-14 Make Host Cluster

4. When creating a host object, ensure that it is defined with the Host Type of vVol. To do this task, access the Hosts view in the GUI by selecting **Hosts** → **Hosts**, and clicking **Add Host**, as shown in Figure 5-15.

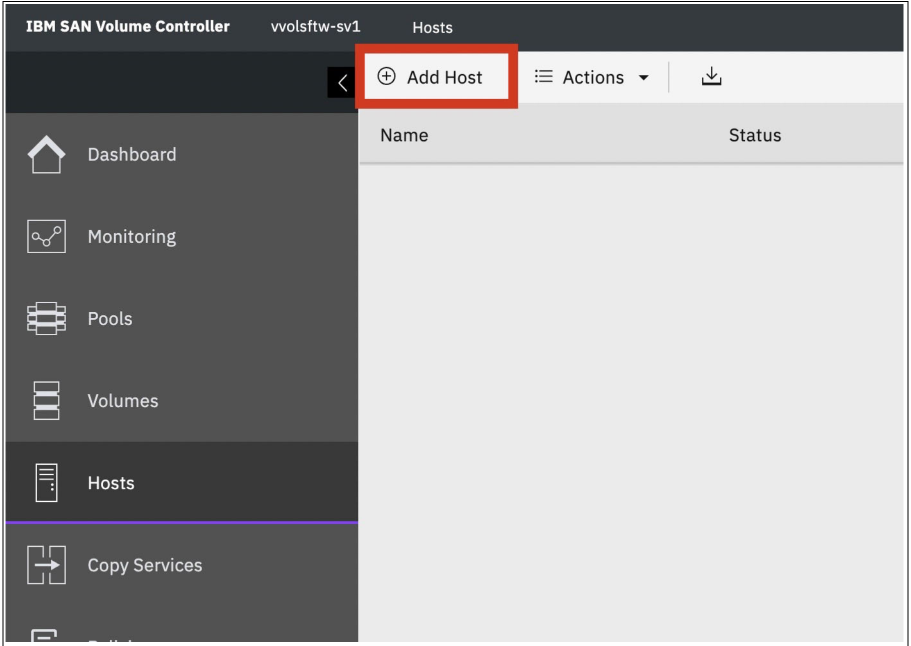
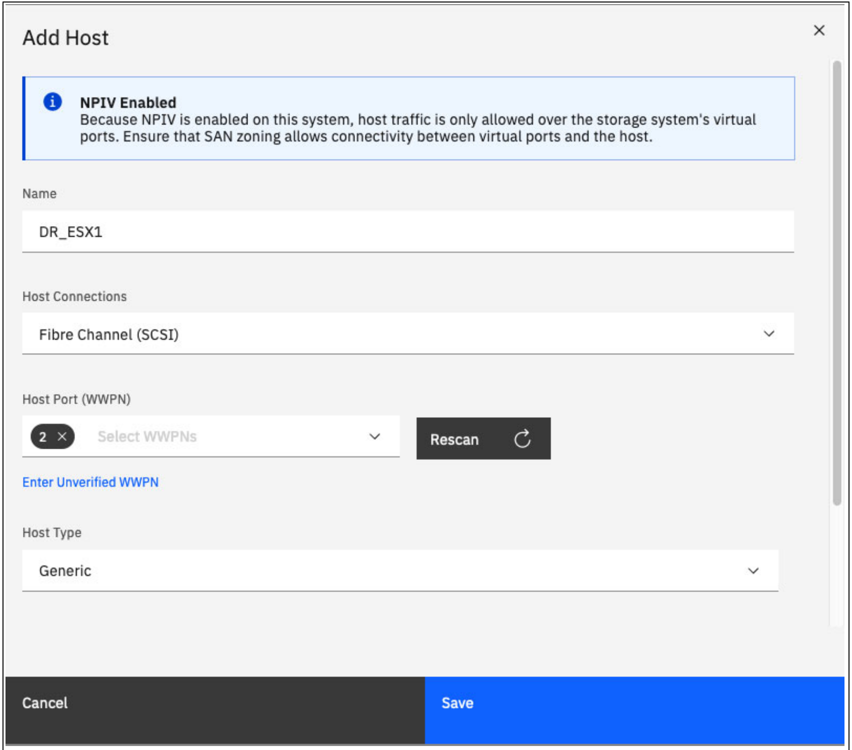


Figure 5-15 Add Host

5. Enter a descriptive name, select the **Host Port** definitions, and define the Host Type as **vVol**. Consider naming the host object in IBM Storage Virtualize with the same name as the one that the ESXi host uses in vCenter, as shown in Figure 5-16.


Add Host

NPIV Enabled
Because NPIV is enabled on this system, host traffic is only allowed over the storage system's virtual ports. Ensure that SAN zoning allows connectivity between virtual ports and the host.

Name: DR_ESX1

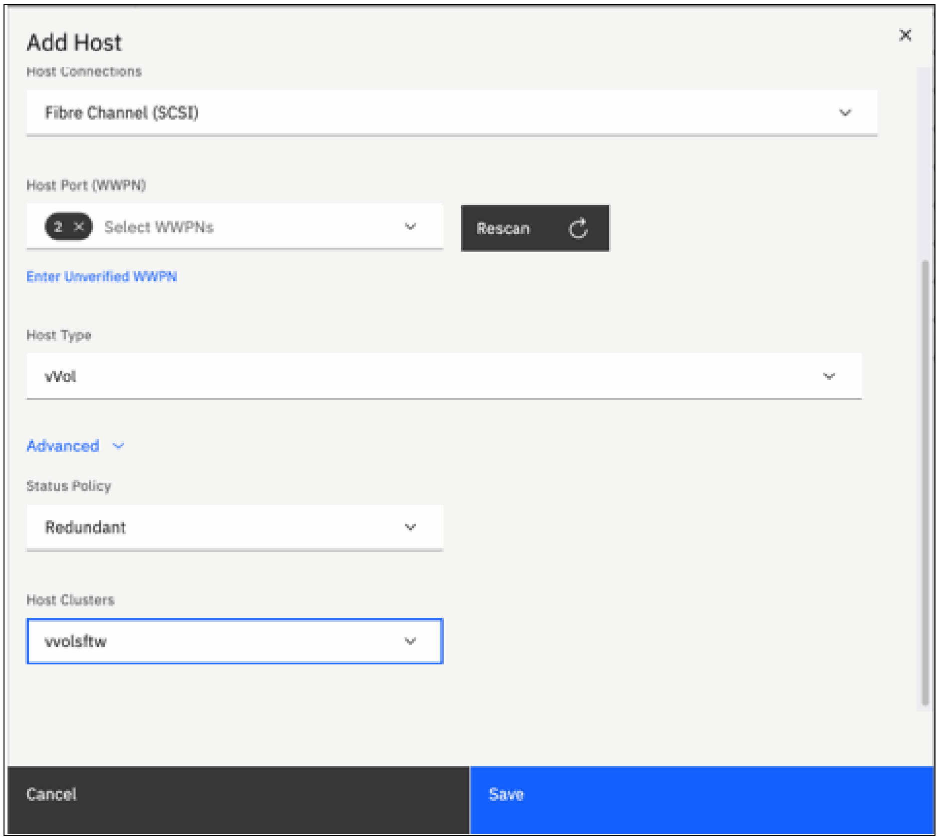
Host Connections: Fibre Channel (SCSI)

Host Port (WWPN): 2 Select WWPNs

Host Type: Generic

Figure 5-16 Entering the details

6. If the host object is a member of a Host Cluster, expand the advanced view and select the Host Cluster from the list, as shown in Figure 5-17.



Add Host

Host Connections: Fibre Channel (SCSI)

Host Port (WWPN): 2 Select WWPNs

Host Type: vVol

Status Policy: Redundant

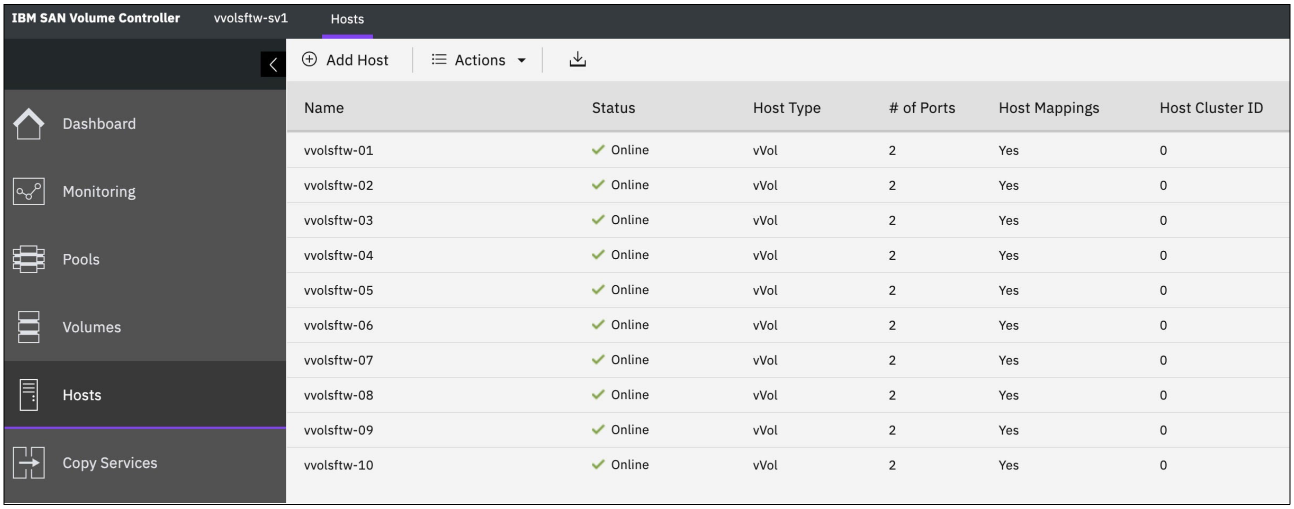
Host Clusters: vvolsftw

Figure 5-17 Selecting the Host Cluster

> **Note:** When creating the host object by using the CLI, use the host type **`adminlun`**:
>
> ```
> IBM_2145:vvolsftw-sv1:superuser>mkhost -fcwwpn
> 2100000E1EC249F8:2100000E1EC249F9 -name vvolsftw-02 -hostcluster vvolsftw -type
> adminlun
> ```

7. Repeat the process for each additional host that you want to create.

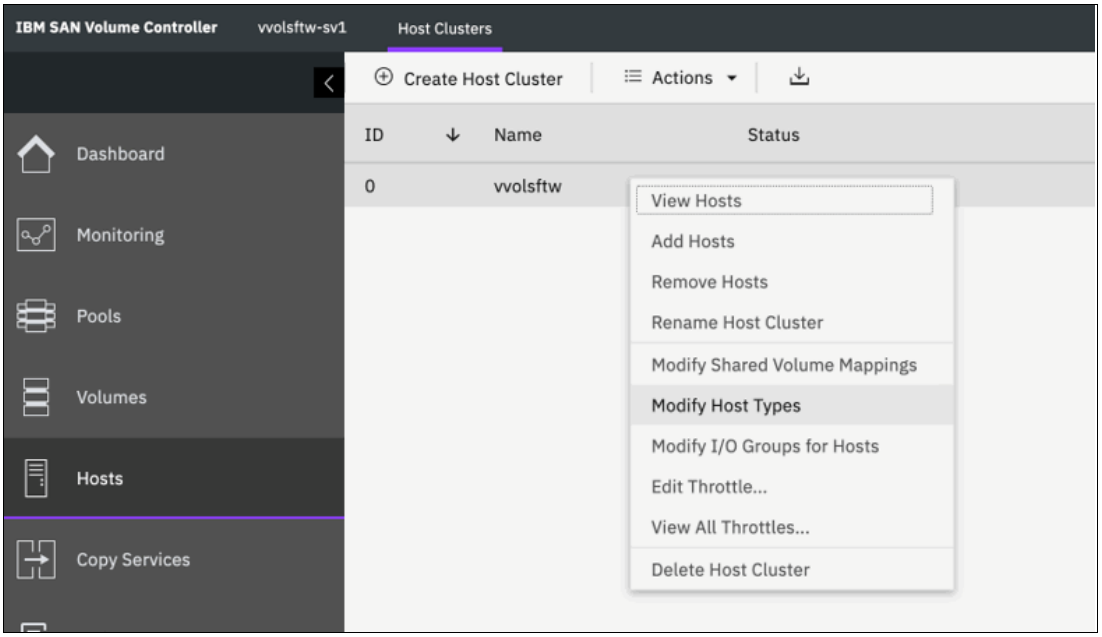
8. Verify that all hosts are correctly defined as vVol host types by selecting **Hosts** → **Hosts** in the storage system GUI, as shown in Figure 5-18.



Name	Status	Host Type	# of Ports	Host Mappings	Host Cluster ID
vvolsftw-01	✓ Online	vVol	2	Yes	0
vvolsftw-02	✓ Online	vVol	2	Yes	0
vvolsftw-03	✓ Online	vVol	2	Yes	0
vvolsftw-04	✓ Online	vVol	2	Yes	0
vvolsftw-05	✓ Online	vVol	2	Yes	0
vvolsftw-06	✓ Online	vVol	2	Yes	0
vvolsftw-07	✓ Online	vVol	2	Yes	0
vvolsftw-08	✓ Online	vVol	2	Yes	0
vvolsftw-09	✓ Online	vVol	2	Yes	0
vvolsftw-10	✓ Online	vVol	2	Yes	0

Figure 5-18 Hosts

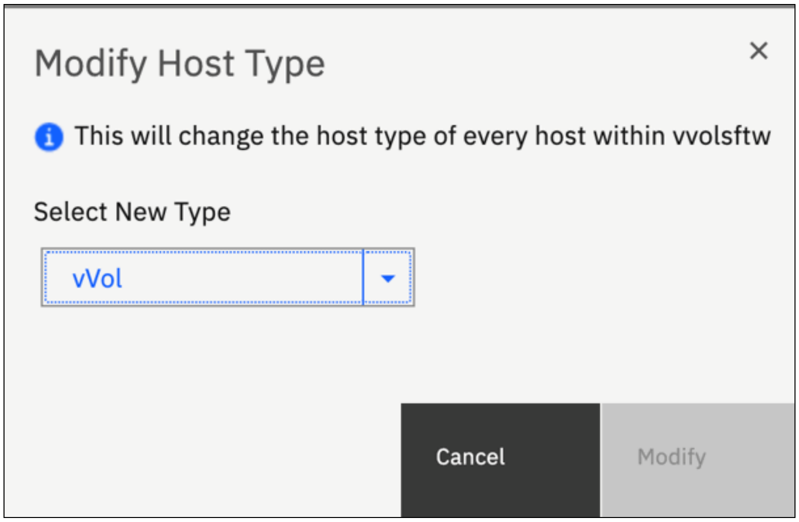
9. You can ensure consistency across all members of the host cluster by defining the host type at the host cluster level. To do this task, select **Hosts** → **Host Clusters**. Right-click the host cluster and select **Modify Host Types**, as shown in Figure 5-19.



ID	Name	Status
0	vvolsftw	

Figure 5-19 Selecting Modify Host Types

10. Select the vVol host type and click **Modify**, as shown in Figure 5-20 on page 98.


Modify Host Type

This will change the host type of every host within vvolsftw

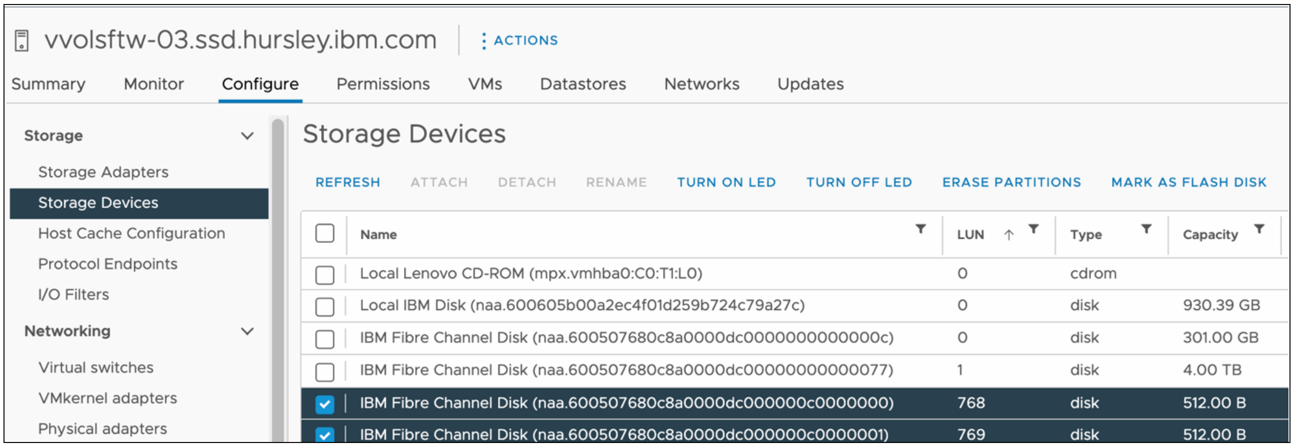
Select New Type

vVol

Figure 5-20 Clicking Modify

By configuring the vVol host type on the host or host cluster object, the system automatically presents the Protocol Endpoints to the ESXi hosts.

11. Before continuing with the Embedded VASA Provider configuration, verify that all hosts in the vSphere cluster correctly detected the Protocol Endpoints from the storage system. To do this task, rescan the storage adapters on each ESXi host and verify that there is a storage device with SCSI ID 768 and 769, as shown in Figure 5-21.


vvolsftw-03.ssd.hursley.ibm.com

Storage Devices

□	Name	LUN	Type	Capacity
□	Local Lenovo CD-ROM (mpx.vmhba0:C0:T1:L0)	0	cdrom	
□	Local IBM Disk (naa.600605b00a2ec4f01d259b724c79a27c)	0	disk	930.39 GB
□	IBM Fibre Channel Disk (naa.600507680c8a0000dc0000000000000c)	0	disk	301.00 GB
□	IBM Fibre Channel Disk (naa.600507680c8a0000dc00000000000077)	1	disk	4.00 TB
☑	IBM Fibre Channel Disk (naa.600507680c8a0000dc000000c0000000)	768	disk	512.00 B
☑	IBM Fibre Channel Disk (naa.600507680c8a0000dc000000c0000001)	769	disk	512.00 B

Figure 5-21 Rescanning the storage adapters

Protocol endpoints

A Protocol endpoint (PE) is presented from each node in the IBM Storage Virtualize cluster. When you use a storage system with multiple IO-groups, you might see a maximum of 8 PEs. Ensure that all ESXi hosts correctly identified all PEs before continuing.

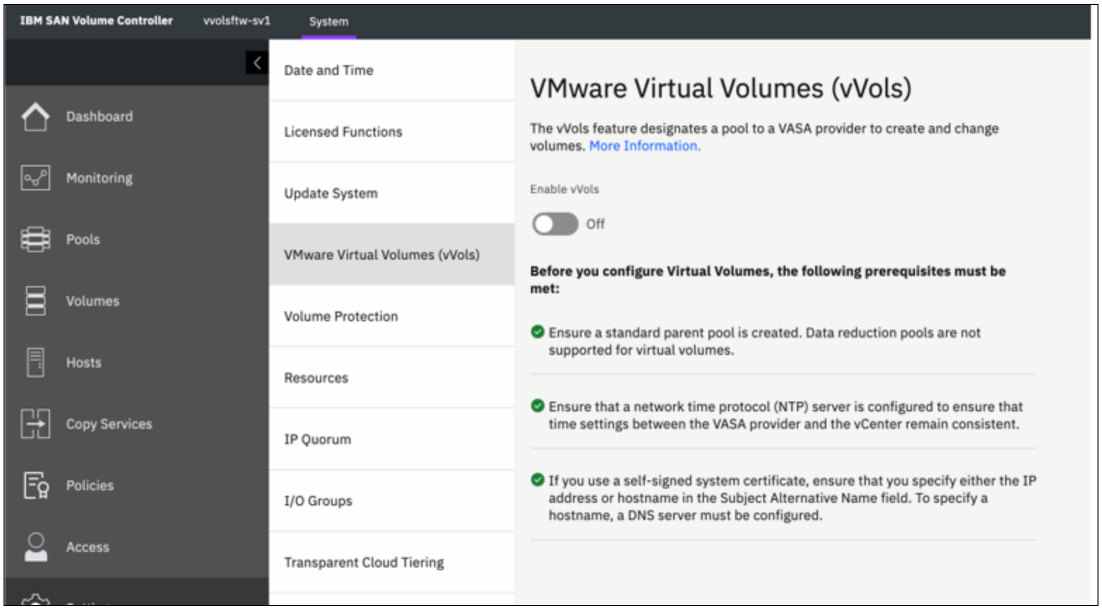
If PEs are not being detected by the ESXi host, review the VMware Hardware Compatibility Guide and ensure that your HBA driver and firmware level supports the Secondary LUNID. For more information, see Troubleshooting LUN connectivity issues on ESXi hosts (1003955).

Cisco UCS environments

Special consideration should be given to Cisco UCS environments where Cisco UCS manager employs a `Max LUNs Per Target` field that defaults to 256. This value masks any device that is mapped to the ESXi host with a SCSI ID higher than 255, which includes Protocol Endpoints presented from IBM storage systems. VMware recommends that this value be defined as 1024.

5.3 Enabling vVols by using an Embedded VASA Provider

After the three system prerequisites are met, the Enable vVol toggle becomes available, as shown in Figure 5-22.



VMware Virtual Volumes (vVols)

The vVols feature designates a pool to a VASA provider to create and change volumes. More Information.

Before you configure Virtual Volumes, the following prerequisites must be met:

✓ Ensure a standard parent pool is created. Data reduction pools are not supported for virtual volumes.

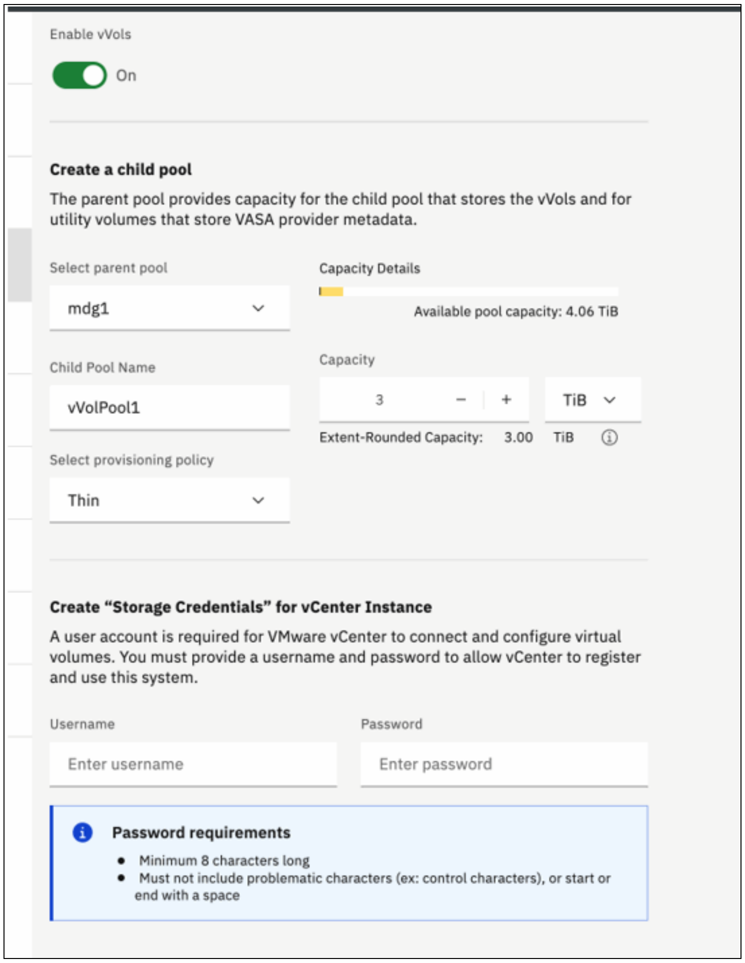
✓ Ensure that a network time protocol (NTP) server is configured to ensure that time settings between the VASA provider and the vCenter remain consistent.

✓ If you use a self-signed system certificate, ensure that you specify either the IP address or hostname in the Subject Alternative Name field. To specify a hostname, a DNS server must be configured.

Figure 5-22 Enable vVol toggle becomes available

Click **Enable vVol** to start the process.

After all the values are defined, the GUI creates all the necessary objects within IBM Storage Virtualize to facilitate vVol support, as shown in Figure 5-23 on page 100.



Enable vVols

On

Create a child pool

The parent pool provides capacity for the child pool that stores the vVols and for utility volumes that store VASA provider metadata.

Select parent pool: mdg1

Capacity Details

Available pool capacity: 4.06 TiB

Child Pool Name: vVolPool1

Capacity: 3 TiB

Extent-Rounded Capacity: 3.00 TiB

Select provisioning policy: Thin

Create "Storage Credentials" for vCenter Instance

A user account is required for VMware vCenter to connect and configure virtual volumes. You must provide a username and password to allow vCenter to register and use this system.

Username: Enter username

Password: Enter password

Password requirements

- Minimum 8 characters long
- Must not include problematic characters (ex: control characters), or start or end with a space

Figure 5-23 Required objects for vVol support are created

5.3.1 Parent pool

You are required to select a parent pool in which to store both the metadata vdisk and the associated child pool. The child pool is presented to vSphere as a vVol-enabled storage container.

A *metadata volume* (utility volume) is created as a thin-provisioned volume mounted internally on the configuration node and is used to store associated metadata for the vVol configuration. This metadata can include metadata for storage containers, virtual volumes storage policies and other objects that are required to facilitate the vVol infrastructure.

For versions 8.6.0.0 or later, the metadatavdisk is created as a 4 TB space efficient volume. For systems that are running versions earlier than 8.6.0.0, the metadatavdisk is a 2 TB space efficient volume.

Note: Although it is allocated a maximum capacity of 4 TB, this volume is intended to store only system metadata It is likely that the used capacity will never grow beyond a few gigabytes in size. Account for approximately 1 MB of consumed capacity per Virtual Volume.

5.3.2 Child pool (vVol-enabled Storage Container)

When you define a new child pool, enter a name and capacity for the child pool. This pool is presented to the vSphere environment as a vVol-enabled storage container, so the specified capacity of the pool dictates the size of the vVol datastore within vSphere. The capacity can be increased or decreased later, so there is flexibility for expansion and scale as the infrastructure matures.

Storage systems that are running firmware 8.6.0.0 or later support the creation of additional vVol child pools by using the GUI. For more information, see 5.3.7, “Provisioning additional vVol datastores” on page 108.

For storage systems running firmware that is earlier than version 8.6.0.0, the initial vVol configuration allows for the creation of only a single child pool. Additional vVol-enabled child pools can be created by using the storage system CLI if required.

5.3.3 Provisioning policy

The provisioning policy dictates how vVols are created within the IBM Storage Virtualize storage system. Each vVol child pool is associated with a specific provisioning policy, which means that, where possible, all vVols that are created in a vVol datastore are provisioned in the same way.

> **Note:** Swap vVols are always created as fully allocated volumes within IBM Storage Virtualize regardless of the specified provisioning policy.

There are two available provisioning policies to select:

- Standard. The Standard provisioning policy uses fully allocated volumes. All vVols that are created in pools with this policy are created as fully allocated volumes within IBM Storage Virtualize.
- Thin-provisioning. The Thin-provisioning policy uses space-efficient, thin-provisioned volumes. All vVols are created as space-efficient, thin-provisioned volumes within IBM Storage Virtualize.

5.3.4 Storage credentials

To register the VASA Provider within vCenter, you must enter the following information:

- Name
- URL
- Username
- Password

The system automatically creates a user group that is assigned with a specific role within IBM Storage Virtualize. A user account is created that uses the defined username and password and is configured as a member of this group and is granted specific access rights that allow manipulation of vVol objects within the storage system.

The storage credentials that are defined in this window are required when registering the Storage Provider within vSphere, and they are initially used to authenticate the vSphere environment against the IBM Storage Virtualize storage system.

However, after successful registration of the storage provider within vCenter, the password authentication mechanism is removed from the user account within IBM Storage Virtualize, and instead the vSphere certificate is used to authenticate the user account.

> **Note:** The password that is defined in the window is used once, and it is required only in the initial Storage Provider registration process.

After a successful registration, if it is necessary to reregister the storage provider in vCenter, the defined user account must be reconfigured with a new password and the certificate authentication must be removed. To do this task, connect to the storage system CLI and run the following commands:

1. To list all users that are configured on the system, run the following command:

   ```
   lsuser
   ```

2. Identify the user account that requires reconfiguration, and run the following command,:

   ```
   chuser -nocertuid -password <new password> <user_id or name>
   ```

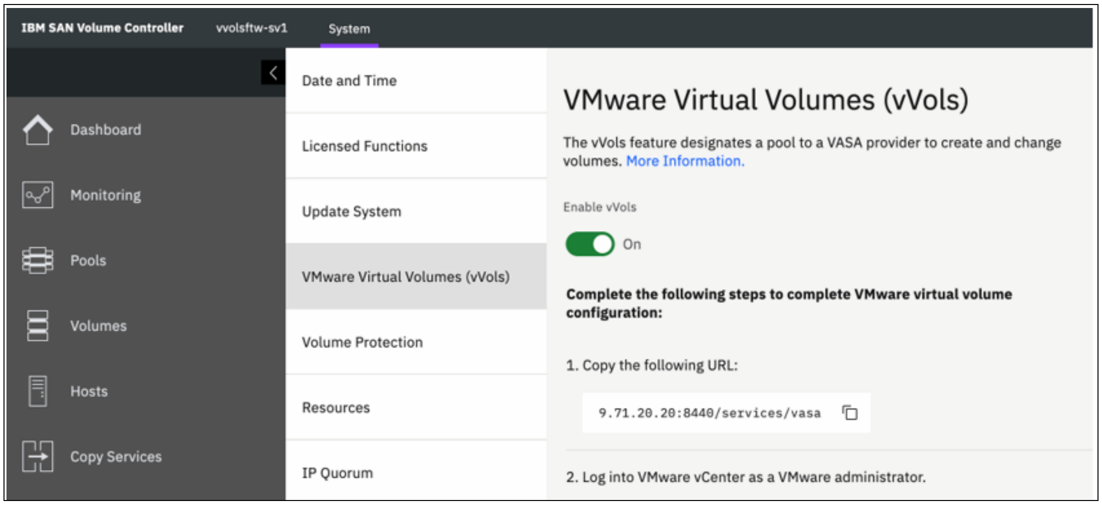
   For example, **`chuser -nocertuid -password C0mpl3xP@ss vmware`**

After the account has been reconfigured, the Storage Provider can be reregistered in vCenter by using the new password.

5.3.5 Registering the Storage Provider in vSphere

The field **Copy the following URL** is shown in Figure 5-24. This string is the URL that is required when you register the storage provider within vCenter in the following format:

```
https:// <FQDN/IP address> + :8440 + /services/vasa
```



VMware Virtual Volumes (vVols)

The vVols feature designates a pool to a VASA provider to create and change volumes. More Information.

Enable vVols

On

Complete the following steps to complete VMware virtual volume configuration:

1. Copy the following URL:

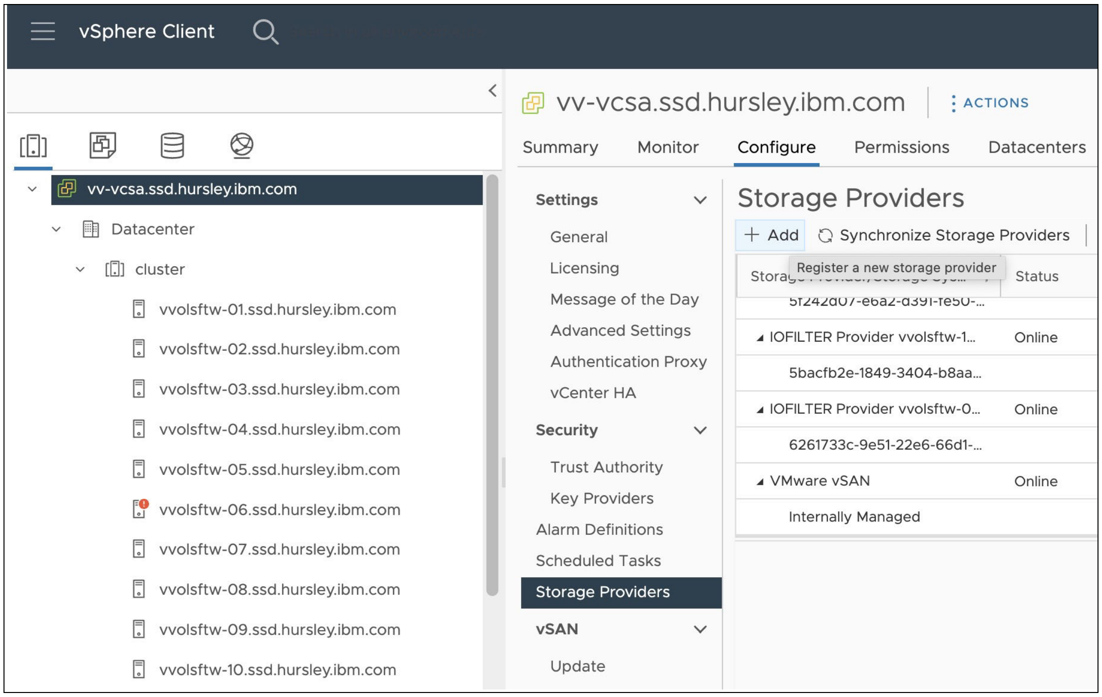
```
9.71.20.20:8440/services/vasa
```

2. Log into VMware vCenter as a VMware administrator.

Figure 5-24 Copy the following URL: option

To register the Storage Provider in vSphere, complete the following steps:

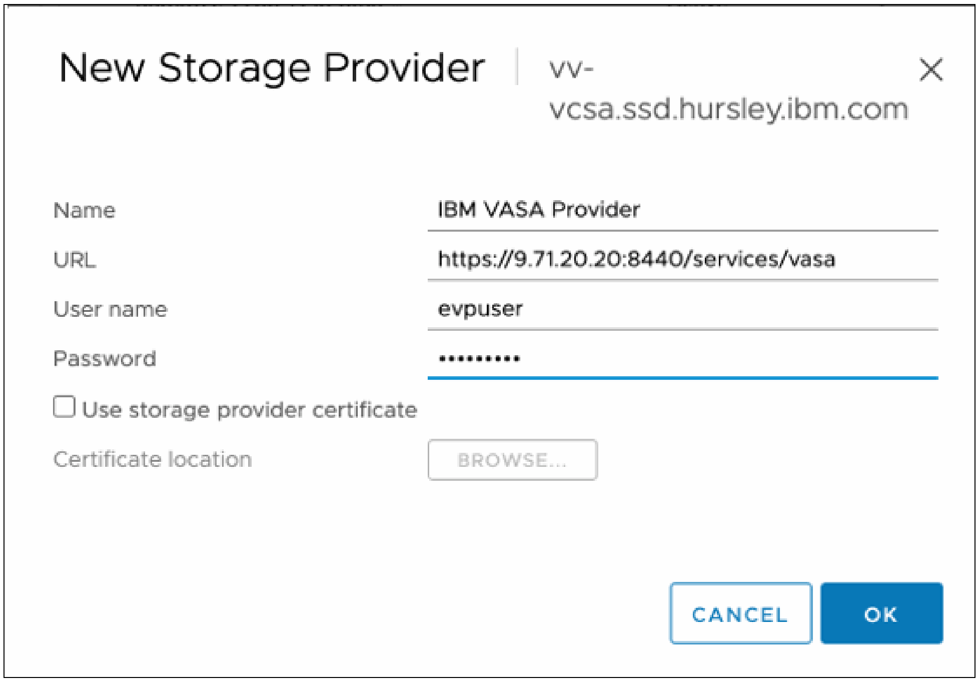
1. Click the copy icon in **Copy the following URL** field to copy the string to your clipboard.
2. Open the vCenter web interface and find the vCenter server in the inventory tree. Select **Configure** → **Storage Providers**, and then click **Add**, as shown in Figure 5-25.


vSphere Client
vv-vcsa.ssd.hursley.ibm.com
Datacenter
cluster
vvolsftw-01.ssd.hursley.ibm.com
vvolsftw-02.ssd.hursley.ibm.com
vvolsftw-03.ssd.hursley.ibm.com
vvolsftw-04.ssd.hursley.ibm.com
vvolsftw-05.ssd.hursley.ibm.com
vvolsftw-06.ssd.hursley.ibm.com
vvolsftw-07.ssd.hursley.ibm.com
vvolsftw-08.ssd.hursley.ibm.com
vvolsftw-09.ssd.hursley.ibm.com
vvolsftw-10.ssd.hursley.ibm.com
vv-vcsa.ssd.hursley.ibm.com
ACTIONS
Summary
Monitor
Configure
Permissions
Datacenters
Settings
General
Licensing
Message of the Day
Advanced Settings
Authentication Proxy
vCenter HA
Security
Trust Authority
Key Providers
Alarm Definitions
Scheduled Tasks
Storage Providers
vSAN
Update
Storage Providers
+ Add
Synchronize Storage Providers
Register a new storage provider

Storage Provider/Storage Sys...	Status
5f242d07-e6a2-d391-fe50-...	
IOFILTER Provider vvolsftw-1...	Online
5bacfb2e-1849-3404-b8aa...	
IOFILTER Provider vvolsftw-0...	Online
6261733c-9e51-22e6-66d1-...	
VMware vSAN	Online
Internally Managed	

Figure 5-25 Selecting Storage Providers

3. Enter an identifiable name, and paste the URL into the URL field. Add the user credentials that were defined earlier and click **OK**, as shown in Figure 5-26.



Name: IBM VASA Provider

URL: https://9.71.20.20:8440/services/vasa

User name: evpuser

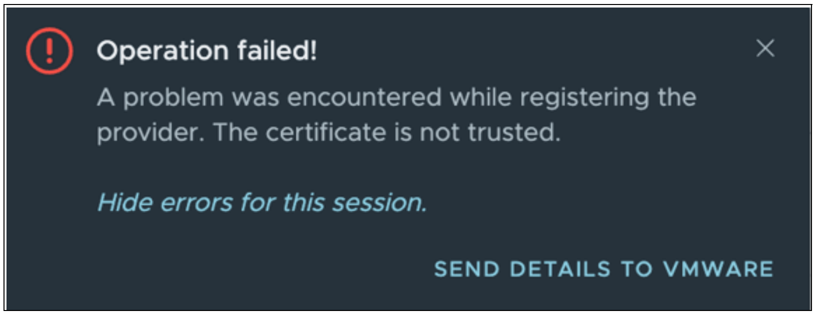
Password: ••••••••••

□ Use storage provider certificate

Certificate location

Figure 5-26 New Storage Provider

4. You might see an error or warning that says the operation failed. This message is related to the initial certificate thumbprint warning only, so it can be ignored (Figure 5-27).



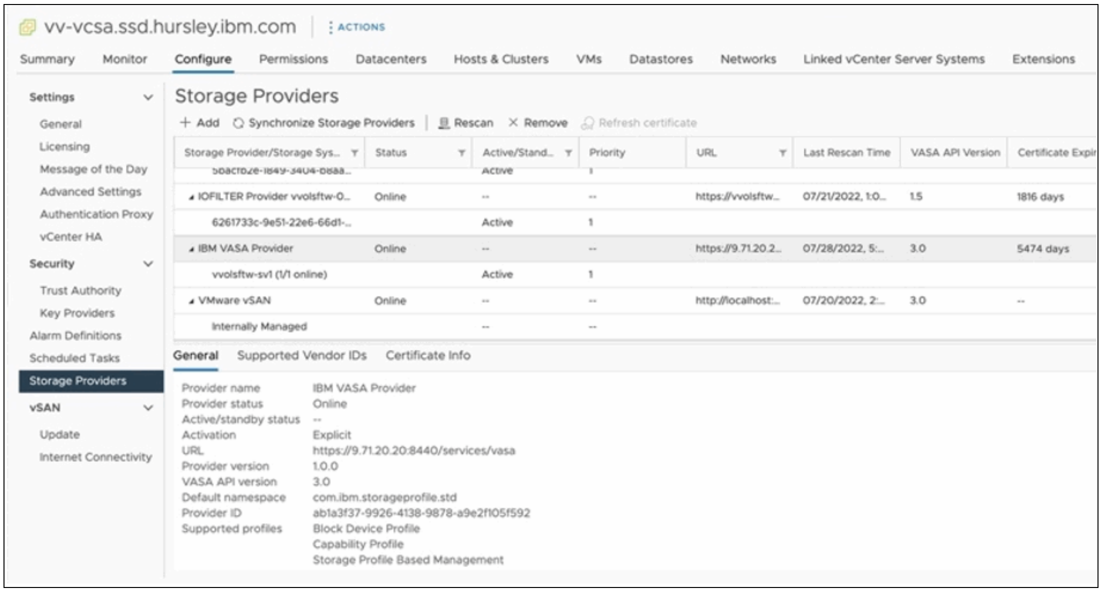
Operation failed!

A problem was encountered while registering the provider. The certificate is not trusted.

Figure 5-27 Operation failed message

If the registration of the Storage Provider has failed for any reason, see Chapter 9, “Troubleshooting” on page 241.

5. Verify that the newly added Storage Provider is showing online and active in the Storage Providers list (Figure 5-28).



Storage Providers

Storage Provider/Storage Sys...	Status	Active/Stand...	Priority	URL	Last Rescan Time	VASA API Version	Certificate Expir
5bacfb2e-1849-3404-b8aa...		Active	1				
IOFILTER Provider vvolsftw-0...	Online	--	--	https://vvolsftw...	07/21/2022, 1:0...	1.5	1816 days
6261733c-9e51-22e6-66d1-...		Active	1				
IBM VASA Provider	Online	--	--	https://9.71.20.2...	07/28/2022, 5:...	3.0	5474 days
vvolsftw-sv1 (1/1 online)		Active	1				
VMware vSAN	Online	--	--	http://localhost:...	07/20/2022, 2:...	3.0	--
Internally Managed		--	--				

Provider name	IBM VASA Provider
Provider status	Online
Active/standby status	--
Activation	Explicit
URL	https://9.71.20.20:8440/services/vasa
Provider version	1.0.0
VASA API version	3.0
Default namespace	com.ibm.storageprofile.std
Provider ID	ab1a3f37-9926-4138-9878-a9e2f105f592
Supported profiles	Block Device Profile Capability Profile Storage Profile Based Management

Figure 5-28 Newly added Storage Provider is showing online and active

5.3.6 Creating the vVol datastore

Review the vCenter inventory and identify the cluster or host that you want to mount on the vVol datastore by completing the following steps:

1. Right-click the cluster and select **Storage** → **New Datastore**, as shown in Figure 5-29.

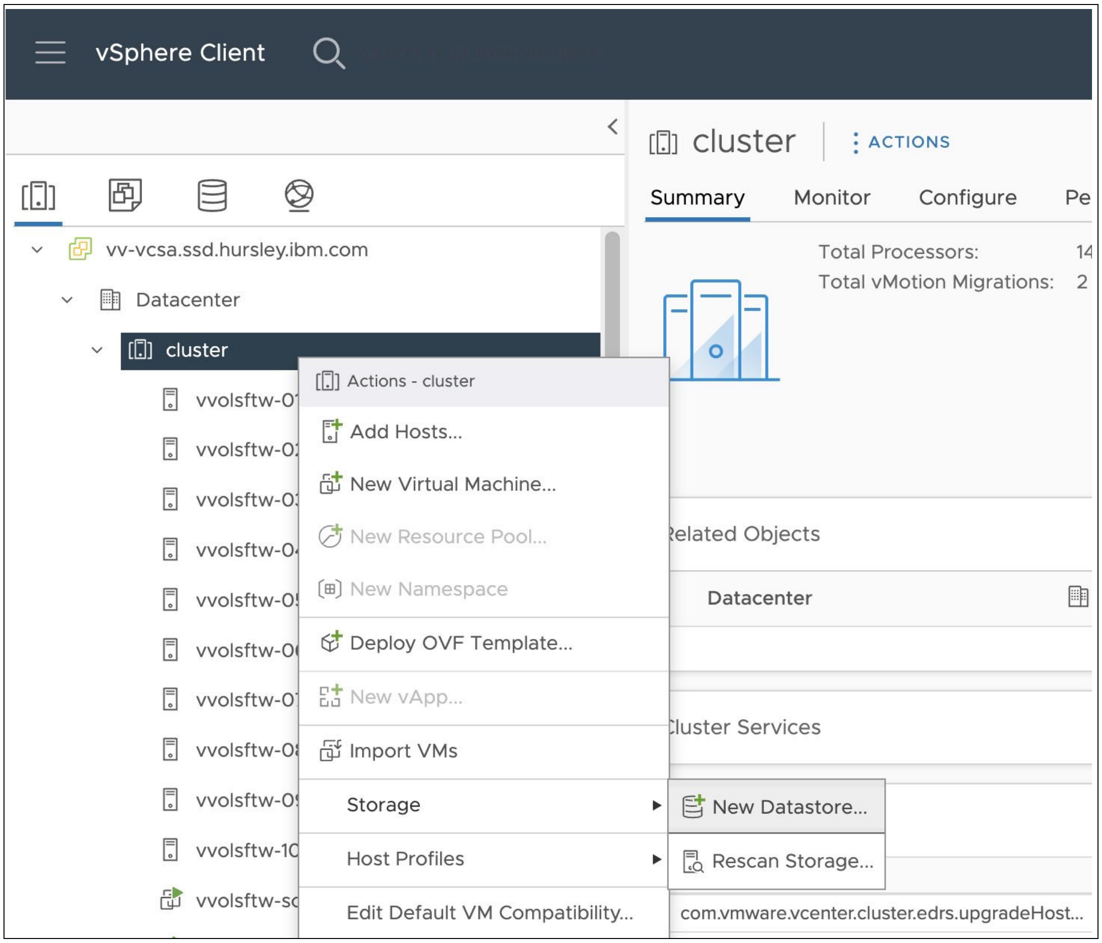
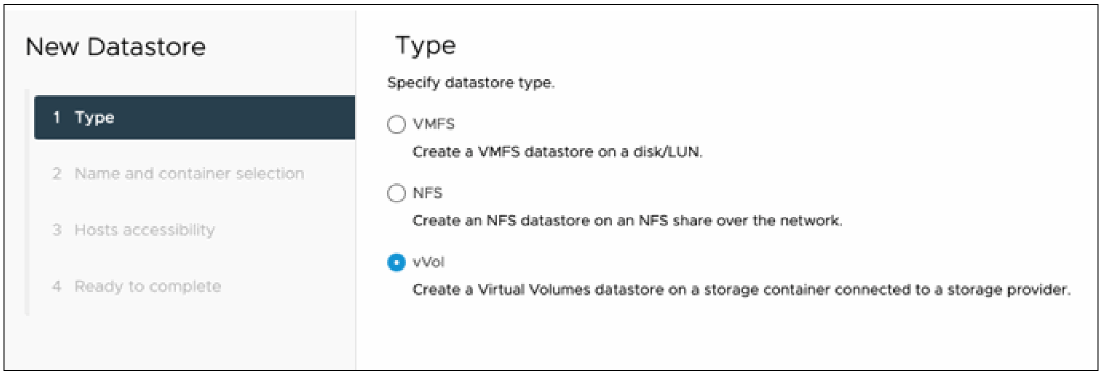


Figure 5-29 Selecting a New Datastore

2. Select **vVol** and select **NEXT** (Figure 5-30).



Specify datastore type.

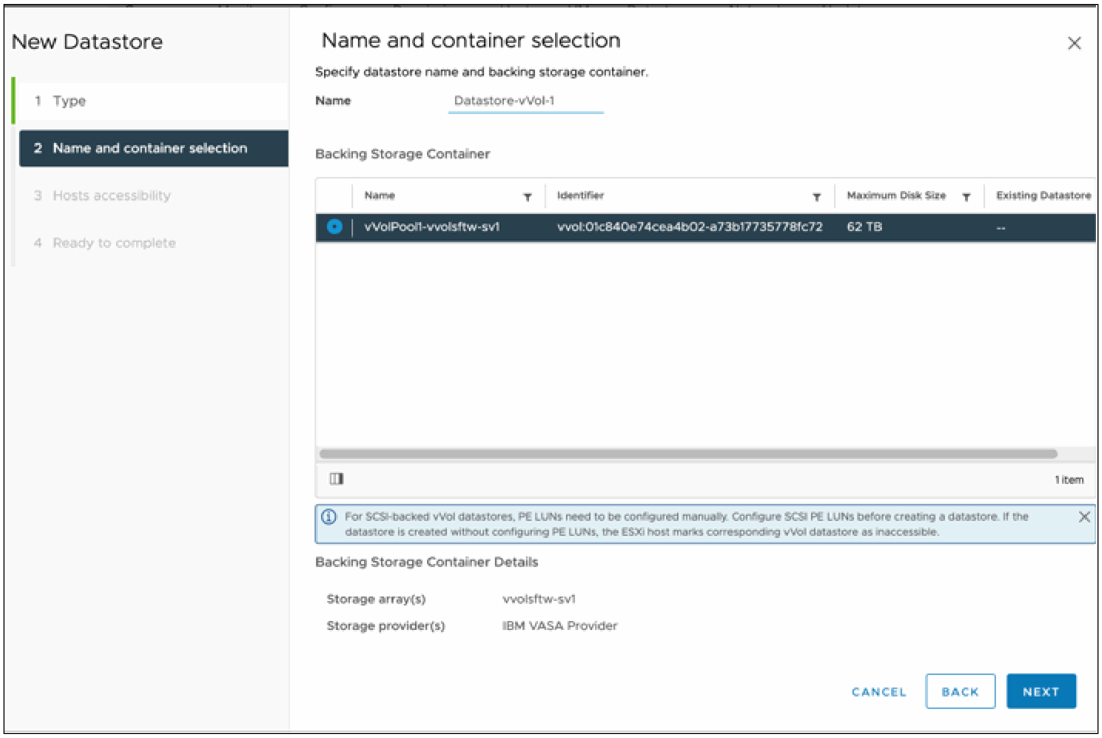
○ VMFS
Create a VMFS datastore on a disk/LUN.

○ NFS
Create an NFS datastore on an NFS share over the network.

● vVol
Create a Virtual Volumes datastore on a storage container connected to a storage provider.

Figure 5-30 Selecting vVol

3. Select the backing storage container in the list and define the name of the new vVol datastore. Click **NEXT** (Figure 5-31).



New Datastore

1 Type

2 Name and container selection

3 Hosts accessibility

4 Ready to complete

Name and container selection

Specify datastore name and backing storage container.

Name: Datastore-vVol-1

Backing Storage Container

	Name	Identifier	Maximum Disk Size	Existing Datastore
●	vVolPool1-vvolsftw-sv1	vvol:01c840e74cea4b02-a73b17735778fc72	62 TB	--

1 item

For SCSI-backed vVol datastores, PE LUNs need to be configured manually. Configure SCSI PE LUNs before creating a datastore. If the datastore is created without configuring PE LUNs, the ESXi host marks corresponding vVol datastore as inaccessible.

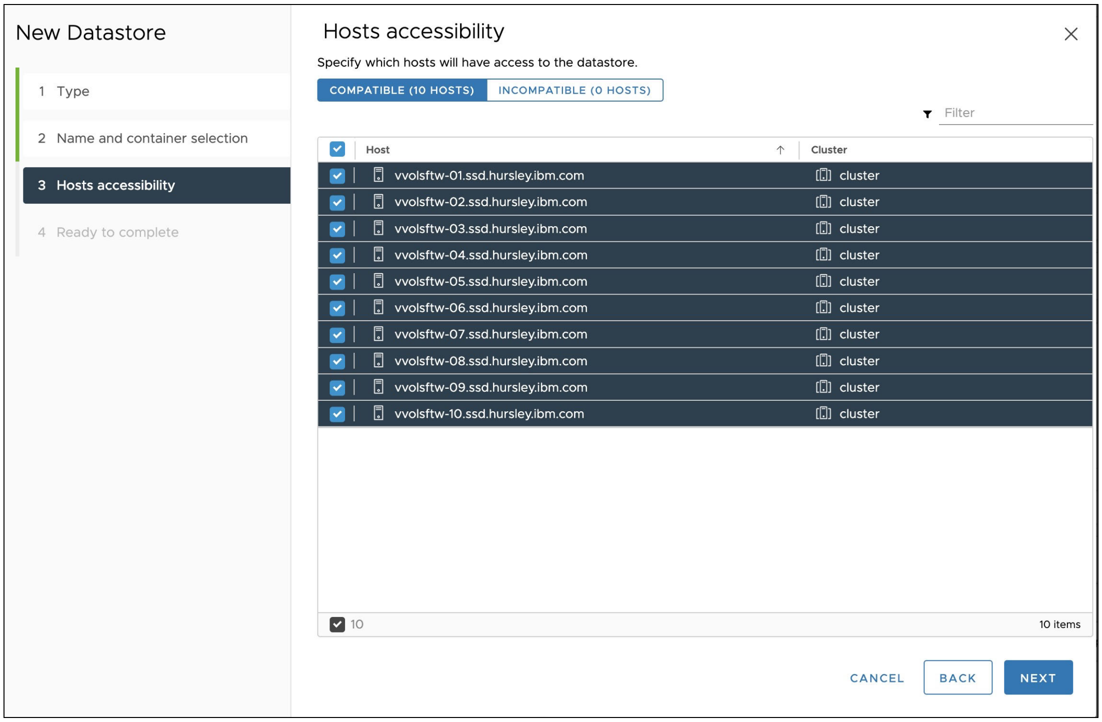
Backing Storage Container Details

Storage array(s): vvolsftw-sv1

Storage provider(s): IBM VASA Provider

Figure 5-31 Defining the name of the new vVol datastore

4. Select the hosts that will access the vVol datastore and click **NEXT** (Figure 5-32).



New Datastore

1 Type

2 Name and container selection

3 Hosts accessibility

4 Ready to complete

Hosts accessibility

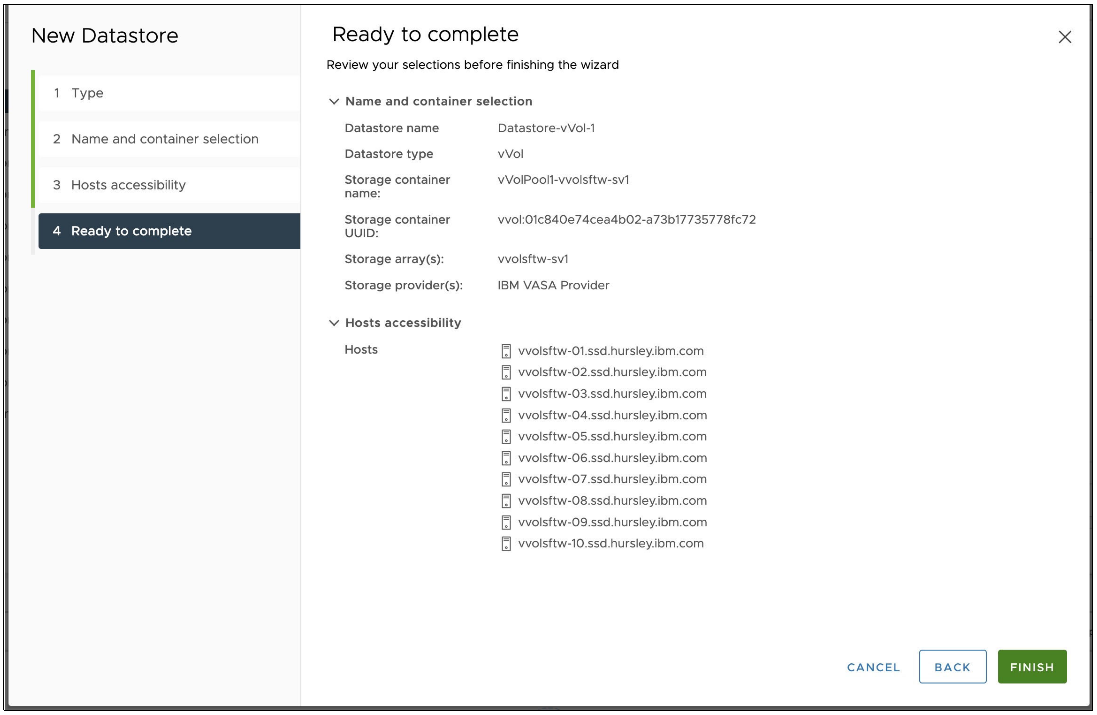
Specify which hosts will have access to the datastore.

☑	Host	Cluster
☑	vvolsftw-01.ssd.hursley.ibm.com	cluster
☑	vvolsftw-02.ssd.hursley.ibm.com	cluster
☑	vvolsftw-03.ssd.hursley.ibm.com	cluster
☑	vvolsftw-04.ssd.hursley.ibm.com	cluster
☑	vvolsftw-05.ssd.hursley.ibm.com	cluster
☑	vvolsftw-06.ssd.hursley.ibm.com	cluster
☑	vvolsftw-07.ssd.hursley.ibm.com	cluster
☑	vvolsftw-08.ssd.hursley.ibm.com	cluster
☑	vvolsftw-09.ssd.hursley.ibm.com	cluster
☑	vvolsftw-10.ssd.hursley.ibm.com	cluster

☑ 10 — 10 items

Figure 5-32 Selecting the hosts

5. Review the summary window and click **FINISH**, as shown in Figure 5-33.



Ready to complete

Review your selections before finishing the wizard

Name and container selection

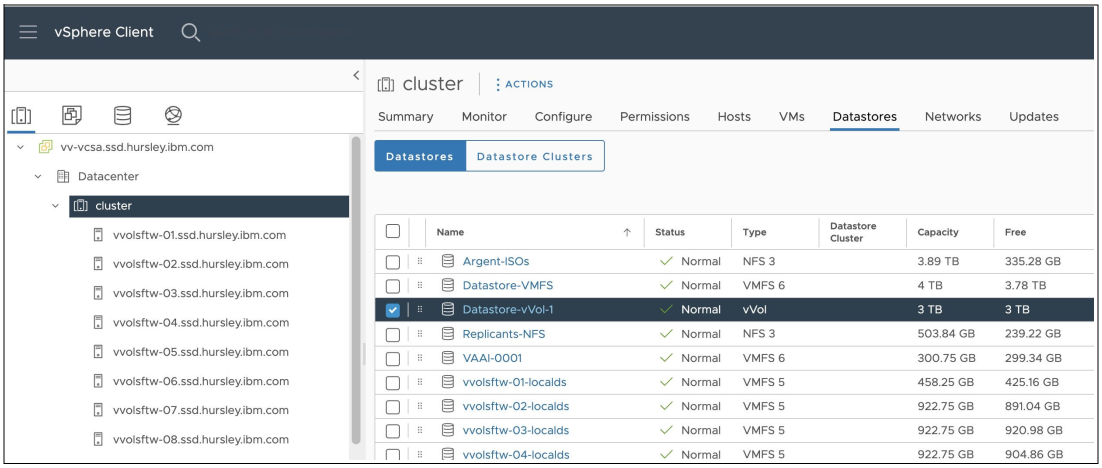
Datastore name	Datastore-vVol-1
Datastore type	vVol
Storage container name:	vVolPool1-vvolsftw-sv1
Storage container UUID:	vvol:01c840e74cea4b02-a73b17735778fc72
Storage array(s):	vvolsftw-sv1
Storage provider(s):	IBM VASA Provider

Hosts accessibility

Hosts
- vvolsftw-01.ssd.hursley.ibm.com
- vvolsftw-02.ssd.hursley.ibm.com
- vvolsftw-03.ssd.hursley.ibm.com
- vvolsftw-04.ssd.hursley.ibm.com
- vvolsftw-05.ssd.hursley.ibm.com
- vvolsftw-06.ssd.hursley.ibm.com
- vvolsftw-07.ssd.hursley.ibm.com
- vvolsftw-08.ssd.hursley.ibm.com
- vvolsftw-09.ssd.hursley.ibm.com
- vvolsftw-10.ssd.hursley.ibm.com

Figure 5-33 Summary window

6. Review the **Datastores** tab and ensure that the capacity and accessibility are correctly reported, as shown in Figure 5-34.


vSphere Client
vv-vcsa.ssd.hursley.ibm.com
Datacenter
cluster
vvolsftw-01.ssd.hursley.ibm.com
vvolsftw-02.ssd.hursley.ibm.com
vvolsftw-03.ssd.hursley.ibm.com
vvolsftw-04.ssd.hursley.ibm.com
vvolsftw-05.ssd.hursley.ibm.com
vvolsftw-06.ssd.hursley.ibm.com
vvolsftw-07.ssd.hursley.ibm.com
vvolsftw-08.ssd.hursley.ibm.com
cluster
ACTIONS
Summary
Monitor
Configure
Permissions
Hosts
VMs
Datastores
Networks
Updates
Datastores
Datastore Clusters

□	Name ↑	Status	Type	Datastore Cluster	Capacity	Free
□	Argent-ISOs	✓ Normal	NFS 3		3.89 TB	335.28 GB
□	Datastore-VMFS	✓ Normal	VMFS 6		4 TB	3.78 TB
☑	Datastore-vVol-1	✓ Normal	vVol		3 TB	3 TB
□	Replicants-NFS	✓ Normal	NFS 3		503.84 GB	239.22 GB
□	VAAI-0001	✓ Normal	VMFS 6		300.75 GB	299.34 GB
□	vvolsftw-01-localds	✓ Normal	VMFS 5		458.25 GB	425.16 GB
□	vvolsftw-02-localds	✓ Normal	VMFS 5		922.75 GB	891.04 GB
□	vvolsftw-03-localds	✓ Normal	VMFS 5		922.75 GB	920.98 GB
□	vvolsftw-04-localds	✓ Normal	VMFS 5		922.75 GB	904.86 GB

Figure 5-34 Reviewing the Datastores tab

5.3.7 Provisioning additional vVol datastores

This section provides the steps for provisioning more vVol datastores by using both the CLI and GUI of the storage system.

Creating additional vVol-enabled child pools by using the GUI

Only IBM storage systems running firmware 8.6.0.0 or later support the ability to create more vVol-enabled child pools from the GUI.

Navigate to the Pools view in the GUI, and then:

1. Identify the parent pool in which to create the vVol child pool. See Figure 5-35.

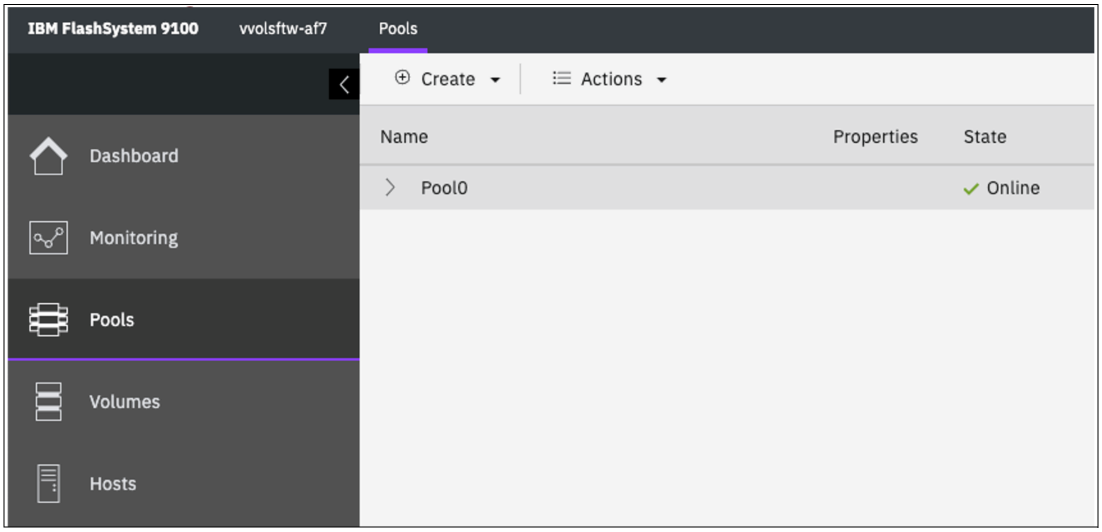


Figure 5-35 Identify the parent pool

2. Right click (or from the Actions menu), select **Create Child Pool**. See Figure 5-36.

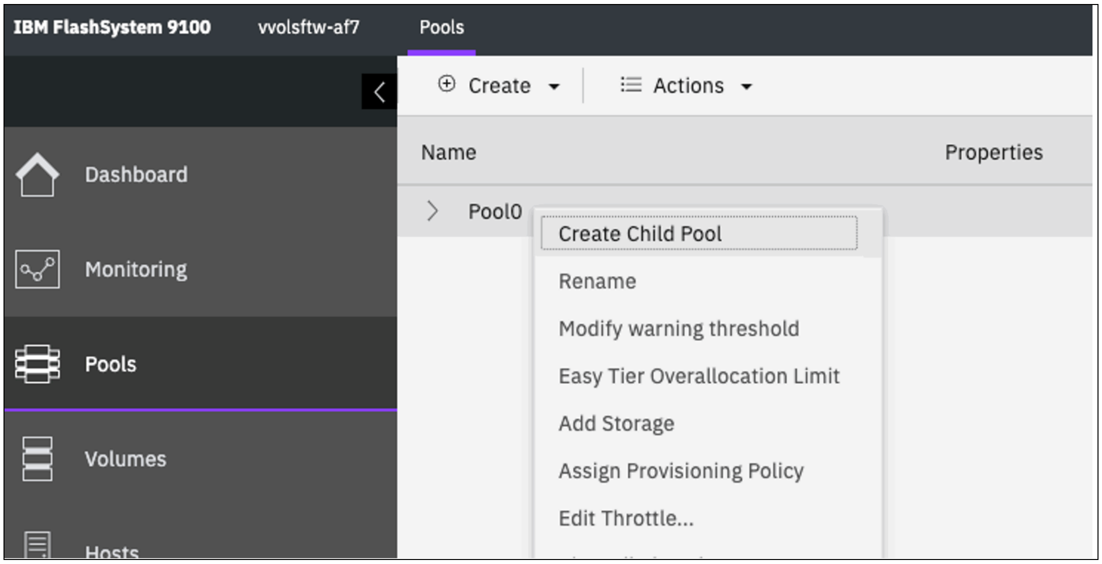
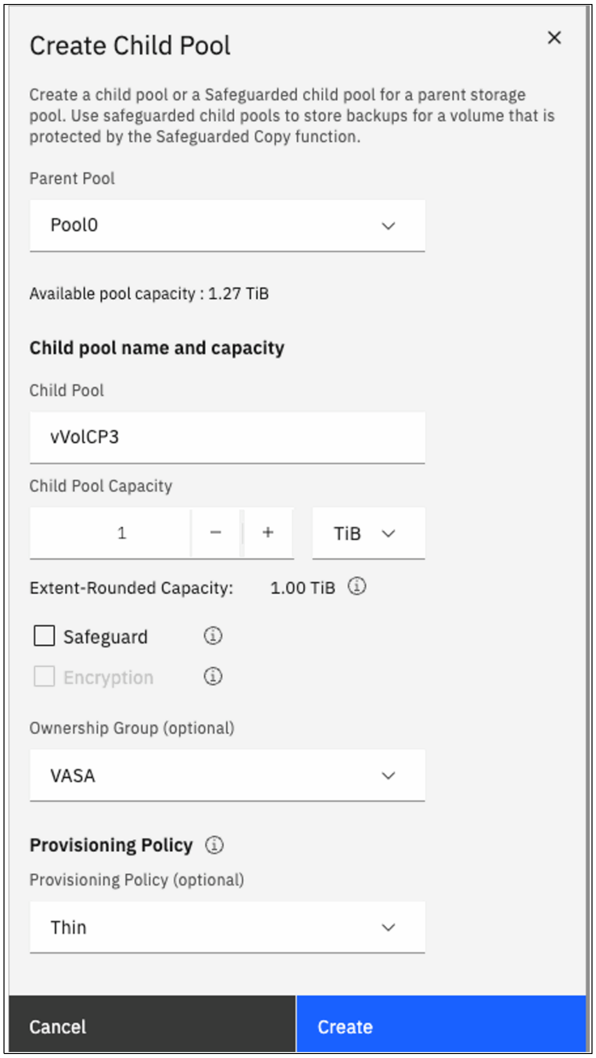


Figure 5-36 Create Child Pool

3. Define the name and capacity.



Create Child Pool

Create a child pool or a Safeguarded child pool for a parent storage pool. Use safeguarded child pools to store backups for a volume that is protected by the Safeguarded Copy function.

Parent Pool: Pool0

Available pool capacity : 1.27 TiB

Child pool name and capacity

Child Pool: vVolCP3

Child Pool Capacity: 1 TiB

Extent-Rounded Capacity: 1.00 TiB

□ Safeguard

□ Encryption

Ownership Group (optional): VASA

Provisioning Policy

Provisioning Policy (optional): Thin

Figure 5-37 Define an appropriate name, and capacity

4. Ensure the vVol/VASA Ownership Group and a Provisioning Policy are defined.
5. Click **Create**.
6. Follow the steps defined in “Creating the vVol enabled child pool” on page 110 to complete the process.

> **Note:** In some circumstances, it can take a few minutes for vSphere to detect the presence of a new vVol storage container.

Creating additional vVol-enabled child pools by using the CLI

Perform the following steps to create additional vVol-enabled child pools by using the CLI.

Identifying the parent pool

To create more child pools, use secure shell (ssh) to connect to the CLI of the IBM Storage Virtualize management interface. List the available parent pools by running the following command:

```
lsmdiskgrp -filtervalue type=parent
```

Identify the target parent pool in which to create the child pool and note the **`mdiskgrp`** ID or name.

Identifying the ownership group

Identify the ownership group that is assigned to the VASA provider by running the command in Example 5-2.

Example 5-2 The lsownershipgroup command

```
IBM_2145:vvolsftw-sv1:superuser>lsownershipgroup
id name
0  VASA
```

By default, the name that is associated with the VASA ownership group is `VASA`.

Identifying the provisioning policy

When vVol was enabled in IBM Storage Virtualize, the requested provisioning policy was created with the other required objects. If both provisioning policies are not listed, you might need to create them manually.

Identify the provisioning policy that is required for the new vVol child pool by running the **`lsprovisioningpolicy`** command, as shown in Example 5-3.

Example 5-3 The lsprovisioningpolicy command

```
IBM_2145:vvolsftw-sv1:superuser>lsprovisioningpolicy
id name     capacity_saving deduplicated in_use
0  Thin     thin            no           yes
1  Standard none            no           no
```

Creating the vVol enabled child pool

To create a vVol-enabled child pool by using the values that are identified in the earlier sections, run the command that is shown in Example 5-4.

Example 5-4 The mkmdiskgrp command

```
svctask mkmdiskgrp -name <name> -owner vvol_child_pool -ownershipgroup <VASA
ownershipgrp_id or name> -parentmdiskgrp <mdiskgrp id or name> -provisioningpolicy
<Thin or Standard> -size <capacity> -unit tb
```

5.4 Migrating from existing IBM Spectrum Connect vVol configurations

This section provides a description of the process of migrating from existing IBM Spectrum Connect vVol configurations.

5.4.1 Supported migration path

In the initial release of the Embedded VASA Provider, it is not possible to use both external and embedded VASA providers from the same vCenter to the same storage system. Therefore, there is no direct method of migrating between vVol datastores that are presented through IBM Spectrum Connect and vVol datastores that are provided by the Embedded VASA Provider.

To perform a migration between vVol solutions, you must complete the following steps:

1. Provision Virtual Machine File System (VMFS) datastores with sufficient capacity to store all VMs that are on the vVol storage.
2. Use Storage vMotion to migrate existing VMs or templates from vVol storage to VMFS datastores.
3. Remove the vVol IBM Spectrum Connect configuration from vCenter.
4. Disable or decommission the vVol function on the storage system.
5. Enable vVol using Embedded VASA Provider, register the storage provider and create vVol datastores.
6. Use Storage vMotion to migrate VMs and templates from VMFS storage to the new vVol datastores.
7. Remove the temporary VMFS datastores if they are no longer needed.

5.4.2 VM migrations by using Storage vMotion

Temporary storage is required to store the VMs during the decommissioning of IBM Spectrum Connect. If required, create volumes of suitable capacity to store all the VMs or templates while the IBM Spectrum Connect vVol storage is being decommissioned.

After the new volumes are created and mapped to the appropriate hosts or host cluster in the storage system, create the VMFS datastores.

Identify the VMs that are on the vVol datastores that are presented by IBM Spectrum Connect and run a storage migration to move them to the new VMFS datastores. Depending on the number of VMs, consider using, for example, PowerCLI to automate bulk VM migrations.

Note: VM templates might exist on the vVol datastores that require conversion into a VM before they can be migrated. After the migration completes, they can be converted back into a VM template.

5.4.3 Removing the vVol IBM Spectrum Connect configuration from vCenter

Removing the vVol IBM Spectrum Connect configuration from vCenter includes removing or unmounting the vVol datastores, removing storage policies, and removing the IBM Spectrum Storage Provider.

Removing or unmounting the vVol datastores

After all VMs and templates are migrated away from the IBM Spectrum Connect vVol datastores, it is safe to unmount and remove them from vCenter. Complete the following steps:

1. Select the vVol datastore to be removed and click **ACTIONS**, as shown in Figure 5-38.

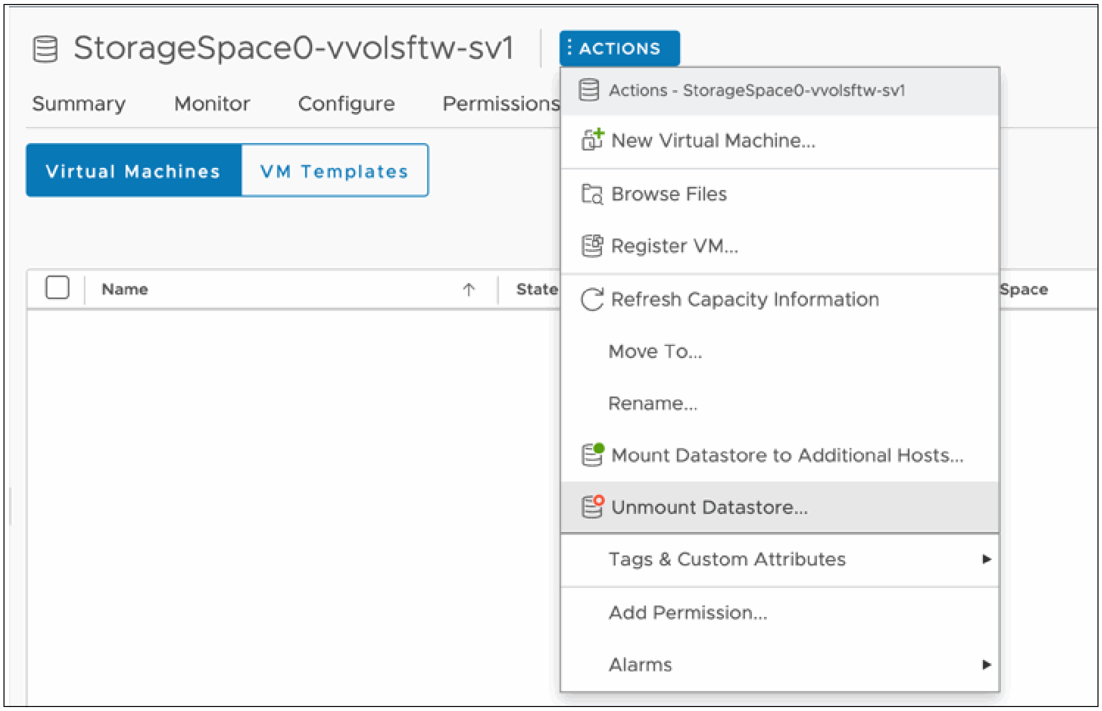
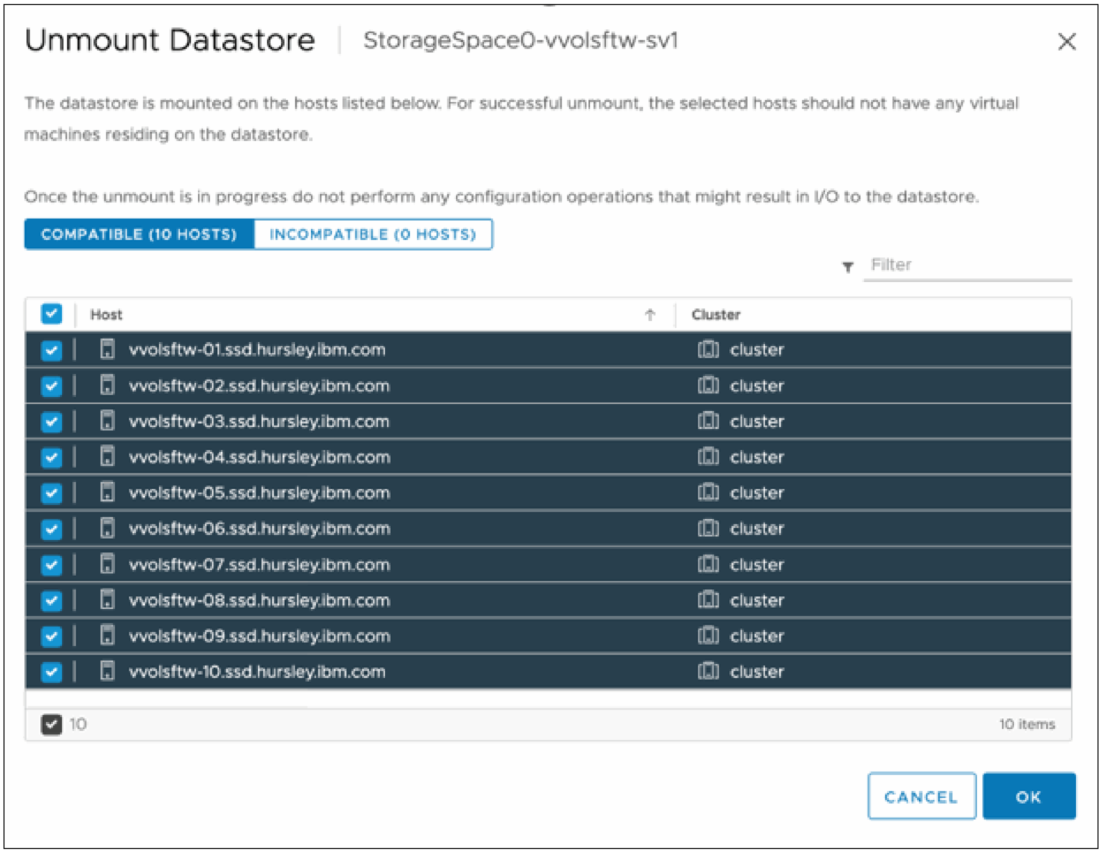


Figure 5-38 Selecting Unmount Datastore

2. Select **Unmount Datastore** and select all connected hosts to unmount the datastore from all hosts, as shown in Figure 5-39. Click **OK**.



Unmount Datastore | StorageSpace0-vvolsftw-sv1

The datastore is mounted on the hosts listed below. For successful unmount, the selected hosts should not have any virtual machines residing on the datastore.

Once the unmount is in progress do not perform any configuration operations that might result in I/O to the datastore.

☑ Host	Cluster
☑ vvolsftw-01.ssd.hursley.ibm.com	cluster
☑ vvolsftw-02.ssd.hursley.ibm.com	cluster
☑ vvolsftw-03.ssd.hursley.ibm.com	cluster
☑ vvolsftw-04.ssd.hursley.ibm.com	cluster
☑ vvolsftw-05.ssd.hursley.ibm.com	cluster
☑ vvolsftw-06.ssd.hursley.ibm.com	cluster
☑ vvolsftw-07.ssd.hursley.ibm.com	cluster
☑ vvolsftw-08.ssd.hursley.ibm.com	cluster
☑ vvolsftw-09.ssd.hursley.ibm.com	cluster
☑ vvolsftw-10.ssd.hursley.ibm.com	cluster

☑ 10 10 items

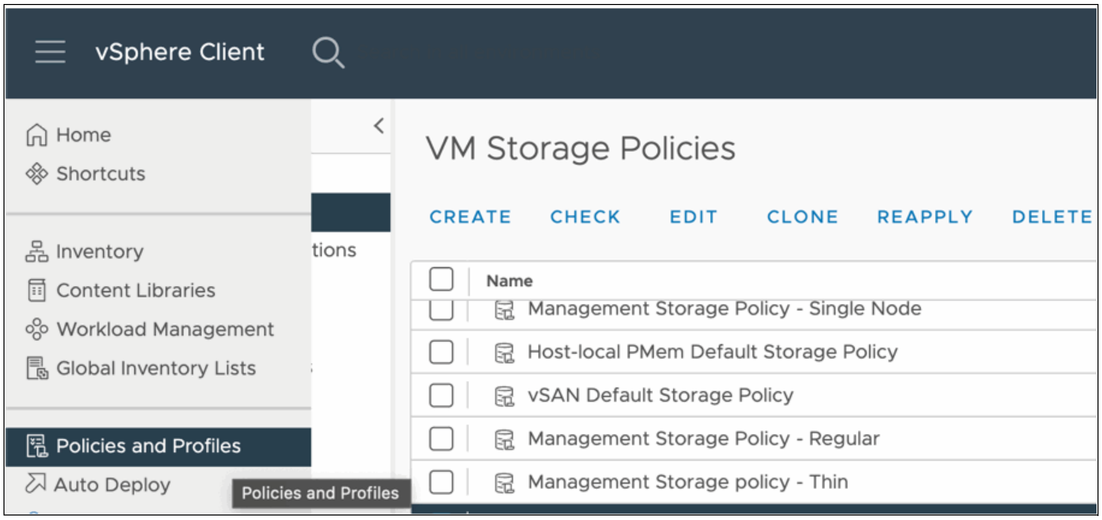
Figure 5-39 Unmount Datastore option

3. After the datastore is unmounted from all hosts, it is automatically removed from vCenter.
4. Repeat these steps for all the vVol datastores that are presented by IBM Spectrum Connect.

Removing Storage Policies

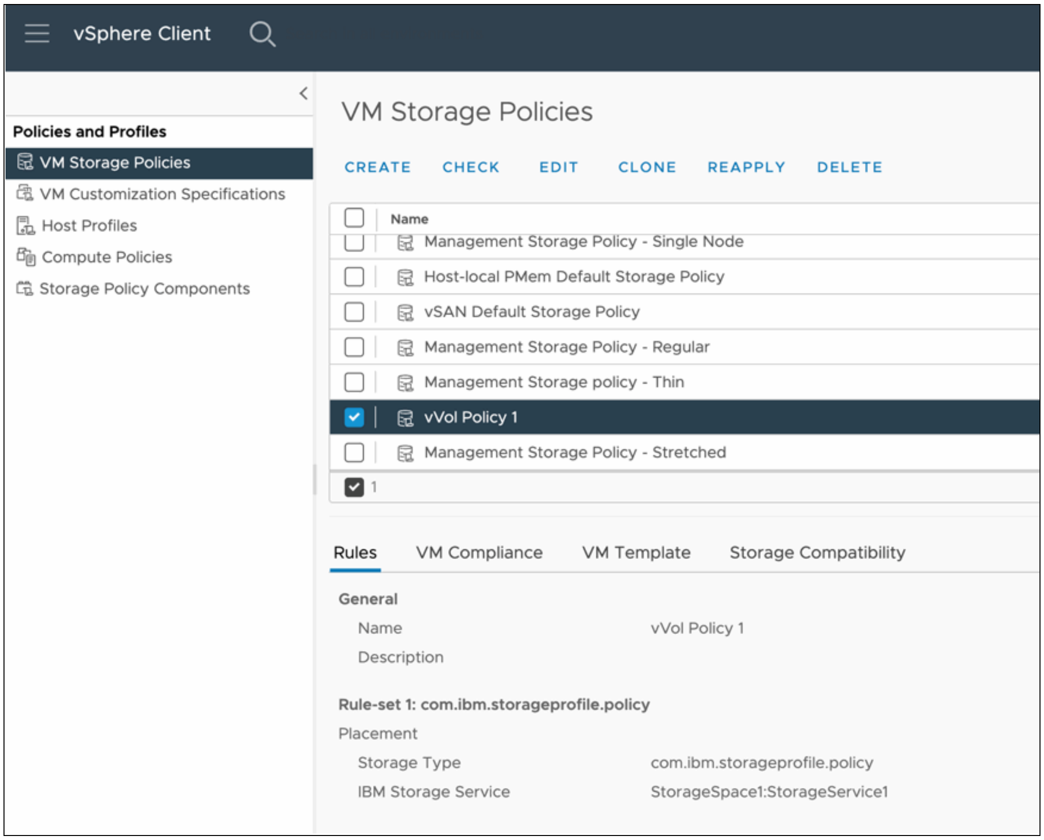
Check for any configured Storage Policies that correspond to IBM Spectrum Connect. Complete the following steps:

1. Go to the Policies and Profiles view within vCenter, as shown in Figure 5-40 on page 114.
2. Select **VM Storage Policies** and identify any policies that were created by using IBM Spectrum Connect.
3. Select the policy to remove, and click **DELETE**, as shown in Figure 5-41 on page 114.
4. Repeat these steps for any remaining policies that are associated with IBM Spectrum Connect.



☐	Name
☐	Management Storage Policy - Single Node
☐	Host-local PMem Default Storage Policy
☐	vSAN Default Storage Policy
☐	Management Storage Policy - Regular
☐	Management Storage policy - Thin

Figure 5-40 Policies and Profiles view



☐	Name
☐	Management Storage Policy - Single Node
☐	Host-local PMem Default Storage Policy
☐	vSAN Default Storage Policy
☐	Management Storage Policy - Regular
☐	Management Storage policy - Thin
☑	vVol Policy 1
☐	Management Storage Policy - Stretched

☑ 1

General

Name vVol Policy 1

Description

Rule-set 1: com.ibm.storageprofile.policy

Placement

Storage Type com.ibm.storageprofile.policy

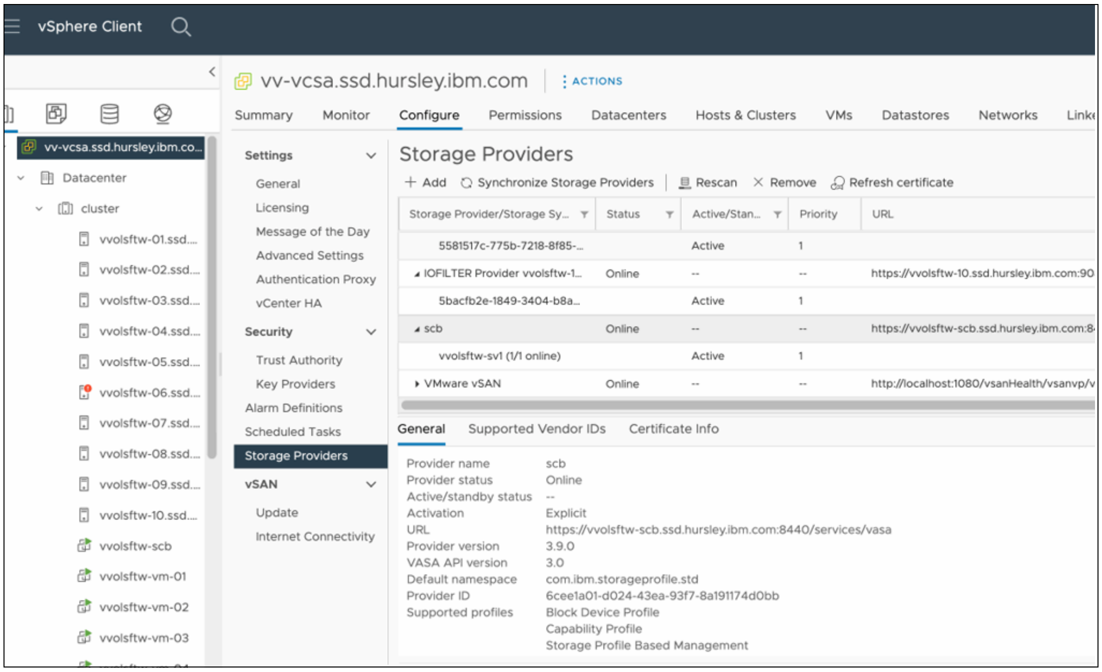
IBM Storage Service StorageSpace1:StorageService1

Figure 5-41 Selecting the policy to remove

Removing IBM Spectrum Connect Storage Provider

After all the vVol datastores are unmounted and removed, it is safe to remove the Storage Provider from within vCenter. Complete the following steps:

1. Find the vCenter entry in the inventory tree and click the **Configure** tab.
2. Select **Storage Providers**.
3. Identify the IBM Spectrum Connect Storage Provider in the list and select **REMOVE** (Figure 5-42).



Storage Providers

Storage Provider/Storage Sy...	Status	Active/Stan...	Priority	URL
5581517c-775b-7218-8f85-...		Active	1	
IOFILTER Provider vvolsftw-1...	Online	--	--	https://vvolsftw-10.ssd.hursley.ibm.com:90
5bacfb2e-1849-3404-b8a...		Active	1	
scb	Online	--	--	https://vvolsftw-scb.ssd.hursley.ibm.com:8
vvolsftw-sv1 (1/1 online)		Active	1	
VMware vSAN	Online	--	--	http://localhost:1080/vsanHealth/vsanvp/v

Provider name	scb
Provider status	Online
Active/standby status	--
Activation	Explicit
URL	https://vvolsftw-scb.ssd.hursley.ibm.com:8440/services/vasa
Provider version	3.9.0
VASA API version	3.0
Default namespace	com.ibm.storageprofile.std
Provider ID	6cee1a01-d024-43ea-93f7-8a191174d0bb
Supported profiles	Block Device Profile Capability Profile Storage Profile Based Management

Figure 5-42 Removing the IBM Spectrum Connect Storage Provider

5.5 Decommissioning IBM Spectrum Connect

IBM Spectrum Connect offers multiple integrations into different VMware products. Before continuing, review the integration interfaces that are configured, and be conscious of how they are being used in your environment.

5.5.1 Identifying and removing the vVol child pools for IBM Spectrum Connect

Identify the child pools that were allocated to any vVol Storage Spaces within the IBM Spectrum Connect GUI and delete them, as shown in Figure 5-43 on page 116.

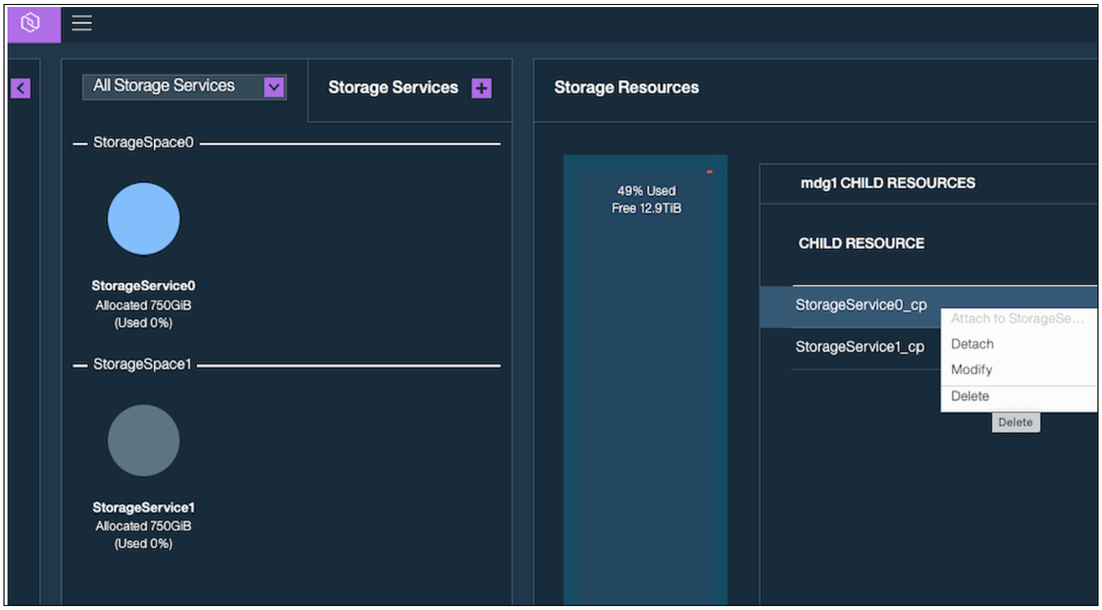


Figure 5-43 Deleting the child pools that were allocated to any vVol Storage Spaces

Alternatively, log on to the storage system CLI with a user account that has the VASA Provider role and run the following command to identify any existing vVol child pools that are used by IBM Spectrum Connect:

```
lsmdiskgrp -filtervalue owner_type=<vvol_child_pool>
```

Note the `mdiskgrp` name or ID. Verify that the vVol pool is no longer required and that the name and ID are correct because you cannot recover the pool after it is deleted. When you are sure, run the following command to remove the child pool:

```
rmmdiskgrp <name or id>
```

Warning: Removing the pool might fail if any vVols are in the pool. You might need to manually remove any vVols in the pool before removing the pool itself. To identify any vVols that are in the pool to be deleted, run the following command:

```
lsvdisk -filtervalue mdisk_grp_name=<child pool name>
```

For each vVol, identify the VDisk ID or name and run the following command to delete the vVol.

Warning: Verify that the vVol is no longer required and that the name and ID are correct because there is no way to recover the data after the volume is deleted.

```
rmvdisk -force <vVol name or id>
```

After any lingering vVols are deleted, retry the pool removal command until all IBM Spectrum Connect vVol pools are removed.

5.5.2 Removing the user account that is used by IBM Spectrum Connect

> **Warning:** If other integration interfaces are configured, for example, vCenter or vRealize Orchestration, do not remove the user account because its removal will cause future integration commands to fail.

Identify the user account that is used by IBM Spectrum Connect by either reviewing the Storage System Credentials window in the IBM Spectrum Connect GUI or by using the CLI.

In the GUI select **Menu** → **Storage credentials**, as shown in Figure 5-44.

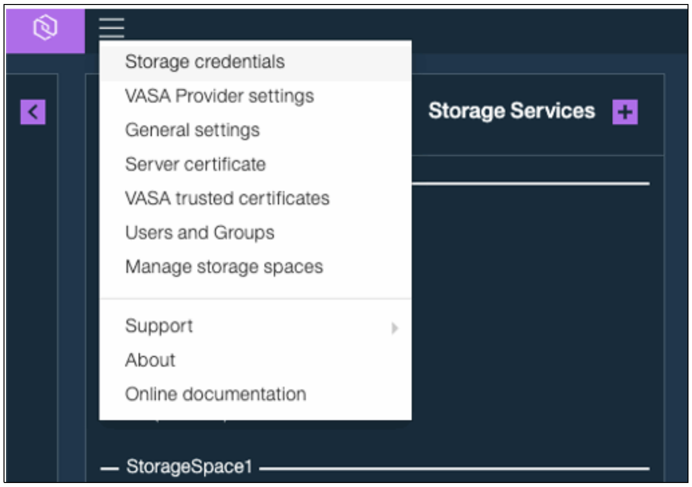
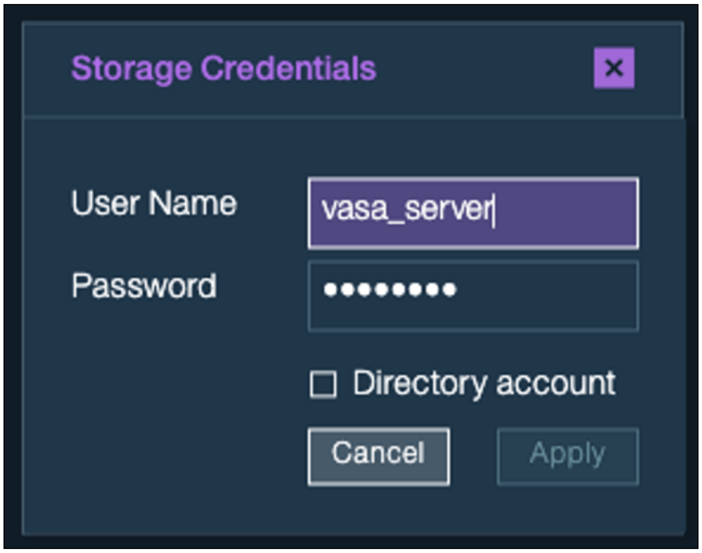


Figure 5-44 Storage credentials

You see the user account that is used by IBM Spectrum Connect, as shown in Figure 5-45.


Storage Credentials

User Name: vasa_server

Password: ●●●●●●●●●

☐ Directory account

Figure 5-45 User account that is used by IBM Spectrum Connect

You can also use the command in Example 5-5 on page 118 on the storage system CLI.

Example 5-5 Identifying the user account that is used by IBM Spectrum Connect by using the command-line interface

```
IBM_2145:vvolsftw-sv1:superuser>lsuser
id name        password ssh_key remote usergrp_id usergrp_name  owner_id owner_name locked password_change_required
0  superuser   yes      yes     no     0          SecurityAdmin                     no     no
1  vasa_server yes      no      no     6          VASAUsers                         no     no
```

Remove the user account that is used by IBM Spectrum Connect, and then run the following command:

```
rmuser <user_id or name>
```

To identify the User Group that is associated with the VASA Provider role, run the command in Example 5-6 on the storage system CLI.

Example 5-6 The lsusergrp command

```
IBM_2145:vvolsftw-sv1:superuser>lsusergrp
id name            role            remote multi_factor password_sshkey_required gui_disabled cli_disabled rest_disabled
0  SecurityAdmin   SecurityAdmin   no     no           no                       no           no           no
1  Administrator   Administrator   no     no           no                       no           no           no
2  CopyOperator    CopyOperator    no     no           no                       no           no           no
3  Service         Service         no     no           no                       no           no           no
4  Monitor         Monitor         no     no           no                       no           no           no
5  RestrictedAdmin RestrictedAdmin no     no           no                       no           no           no
6  VASAUsers       VasaProvider    no     no           no                       no           no           no
```

If no other user accounts are in the user group, remove the VASA Provider user group by running the following command:

```
rmusergrp <usergrp_id or name>
```

To identify the location of the metadata VDisk, run the command in Example 5-7 on the storage system CLI.

Example 5-7 The lsmetadatavdisk command

```
IBM_2145:vvolsftw-sv1:superuser>lsmetadatavdisk
vdisk_id 13
vdisk_name vdisk0
status online
```

Remove the metadata VDisk by running the following command on the storage system CLI.

Warning: The metadata VDisk contains all metadata that is associated with the vVol environment. This operation cannot be undone.

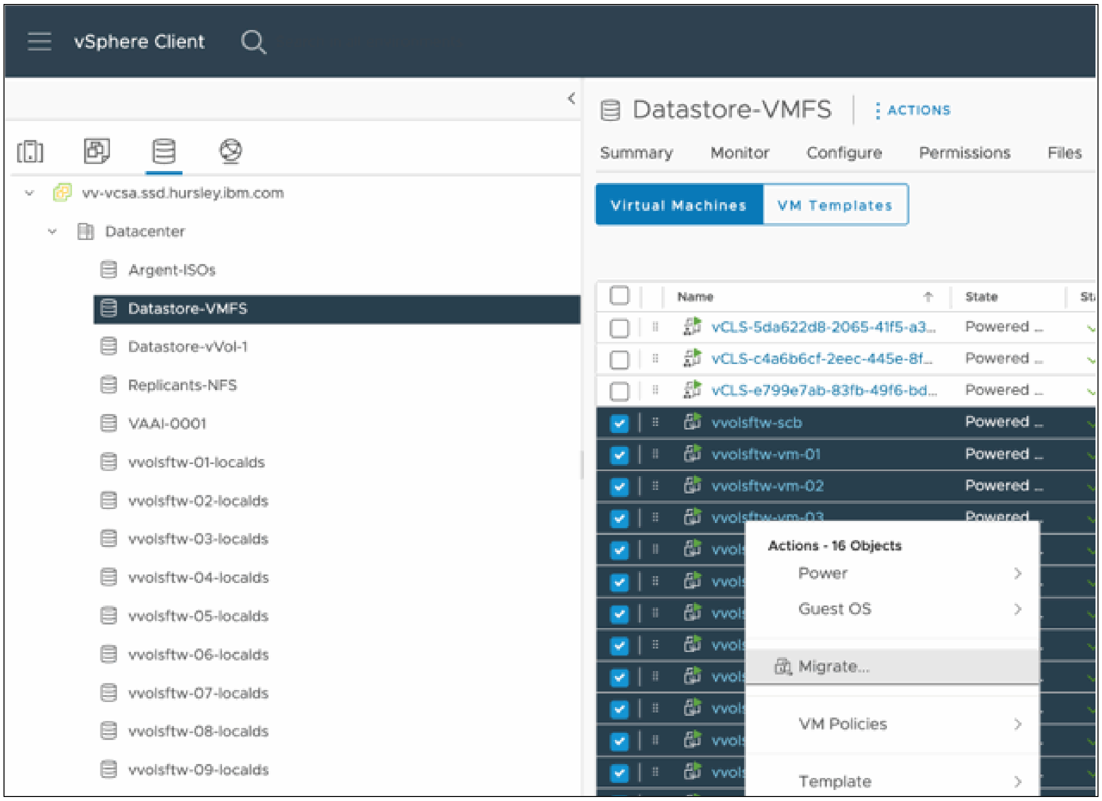
```
rmmetadatavdisk
```

5.5.3 Migrating virtual machines to the vVol datastore

When the IBM Spectrum Connect vVol configuration is removed, complete the steps in 5.3, “Enabling vVols by using an Embedded VASA Provider” on page 99 to enable and configure vVol functions through the Embedded VASA Provider.

After the new storage provider is registered, and a new vVol datastore is online, complete the migration by completing the following steps:

1. Identify the VMs to be migrated. Select them, right-click, and select **Migrate**, as shown in Figure 5-46.



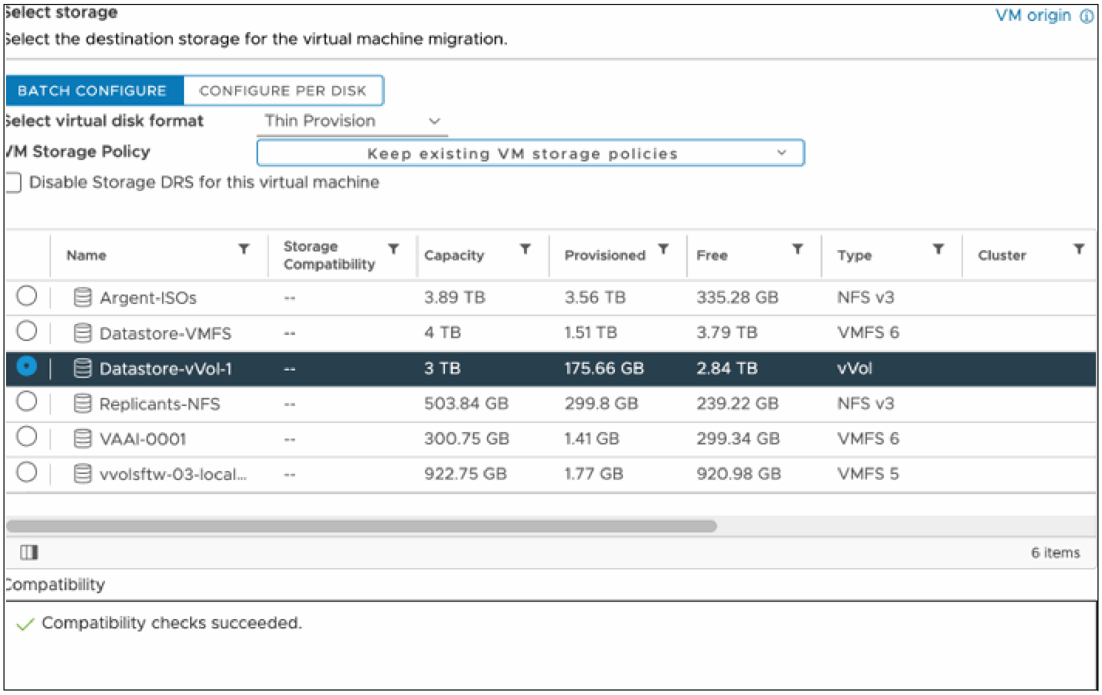
	Name	State
□	vCLS-5da622d8-2065-41f5-a3...	Powered ...
□	vCLS-c4a6b6cf-2eec-445e-8f...	Powered ...
□	vCLS-e799e7ab-83fb-49f6-bd...	Powered ...
☑	vvolsftw-scb	Powered ...
☑	vvolsftw-vm-01	Powered ...
☑	vvolsftw-vm-02	Powered ...
☑	vvolsftw-vm-03	Powered ...

Figure 5-46 Selecting Migrate

2. In the Select Storage window, identify the newly created vVol datastore and click **NEXT**, as shown in Figure 5-47 on page 120.

3. Complete the Storage vMotion workflow and review the tasks to ensure that the VMs successfully migrated (Figure 5-48 on page 120).

   During the migration operation, vVols are automatically created on the storage system within the child pool that was configured as a vVol storage container.



Select storage

Select the destination storage for the virtual machine migration.

VM origin ⓘ

BATCH CONFIGURE | CONFIGURE PER DISK

Select virtual disk format: Thin Provision

VM Storage Policy: Keep existing VM storage policies

□ Disable Storage DRS for this virtual machine

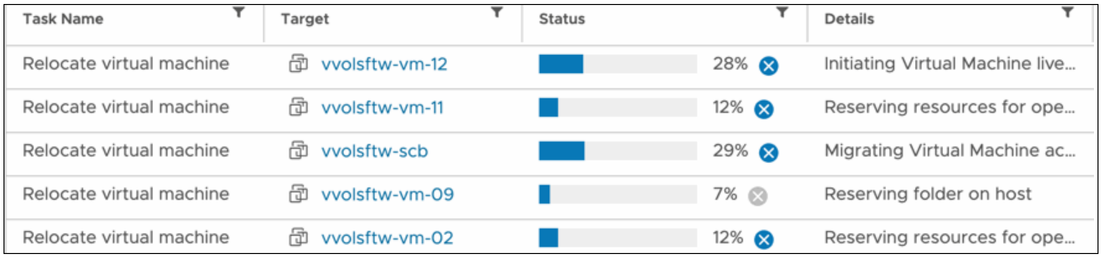
	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Cluster
○	Argent-ISOs	--	3.89 TB	3.56 TB	335.28 GB	NFS v3	
○	Datastore-VMFS	--	4 TB	1.51 TB	3.79 TB	VMFS 6	
●	Datastore-vVol-1	--	3 TB	175.66 GB	2.84 TB	vVol	
○	Replicants-NFS	--	503.84 GB	299.8 GB	239.22 GB	NFS v3	
○	VAAI-0001	--	300.75 GB	1.41 GB	299.34 GB	VMFS 6	
○	vvolsftw-03-local...	--	922.75 GB	1.77 GB	920.98 GB	VMFS 5	

6 items

Compatibility

✓ Compatibility checks succeeded.

Figure 5-47 Identifying the newly created vVol datastore



Task Name	Target	Status	Details
Relocate virtual machine	vvolsftw-vm-12	28% ⊗	Initiating Virtual Machine live...
Relocate virtual machine	vvolsftw-vm-11	12% ⊗	Reserving resources for ope...
Relocate virtual machine	vvolsftw-scb	29% ⊗	Migrating Virtual Machine ac...
Relocate virtual machine	vvolsftw-vm-09	7% ⊗	Reserving folder on host
Relocate virtual machine	vvolsftw-vm-02	12% ⊗	Reserving resources for ope...

Figure 5-48 Reviewing the tasks to ensure that the VMs successfully migrated

4. To review the vVol objects within IBM Storage Virtualize, select **Pools** → **Volumes by Pool** within the GUI, as shown in Figure 5-49 on page 121.

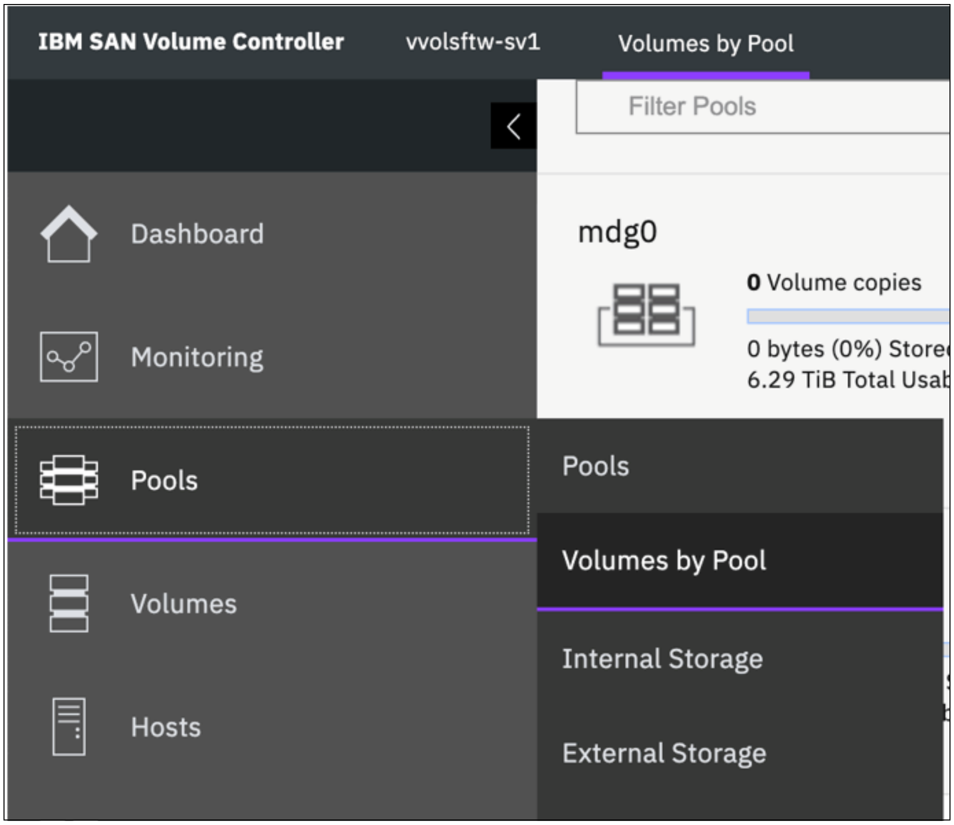
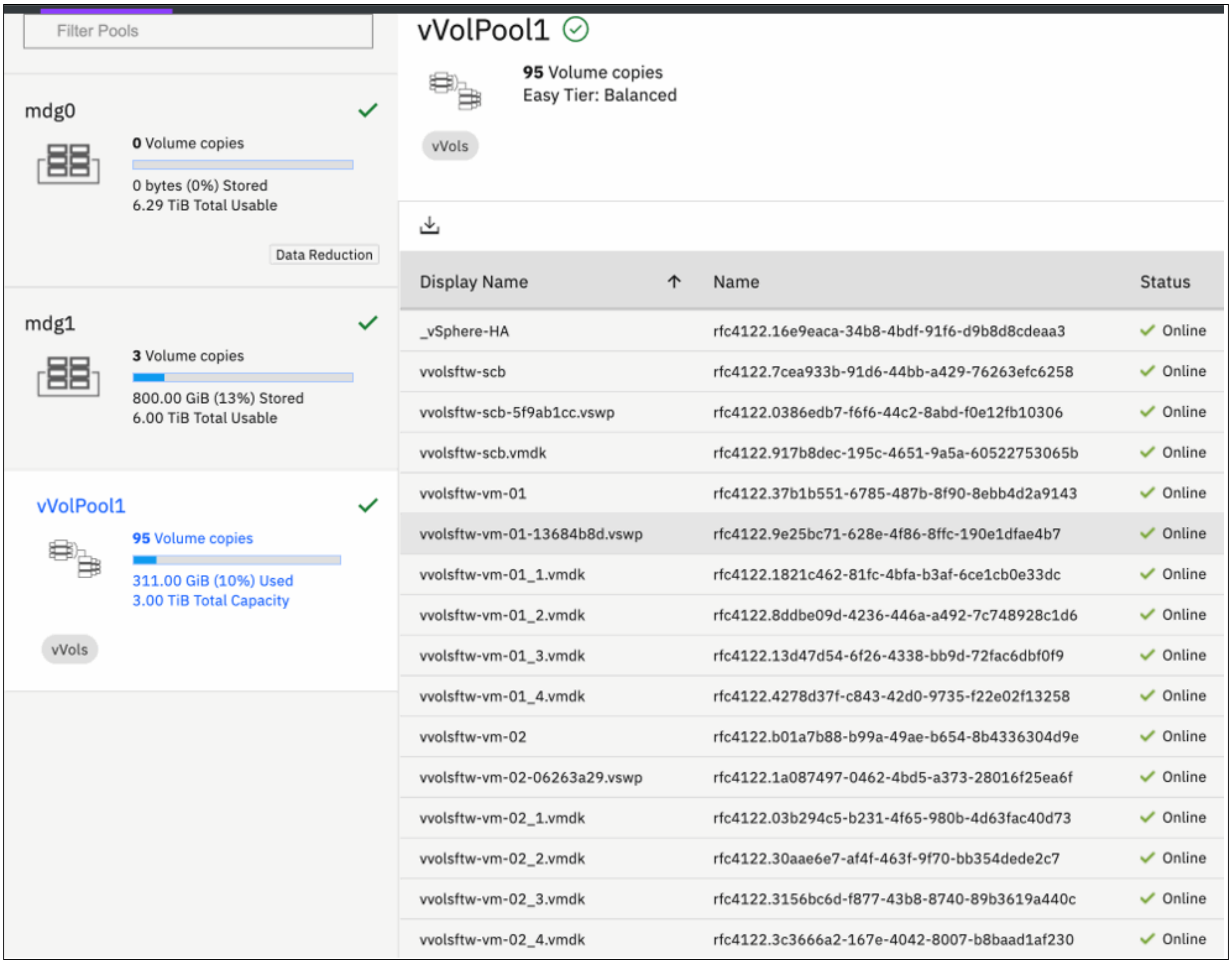


Figure 5-49   Volumes by Pool view

5. Select the vVol-enabled child pool in the list by identifying the vVol logo underneath the pool information on the left panel. When you select the vVol pool, the individual vVol objects appear, as shown in Figure 5-50 on page 122.



mdg0

0 Volume copies

0 bytes (0%) Stored
6.29 TiB Total Usable

mdg1

3 Volume copies

800.00 GiB (13%) Stored
6.00 TiB Total Usable

vVolPool1

95 Volume copies

311.00 GiB (10%) Used
3.00 TiB Total Capacity

vVolPool1

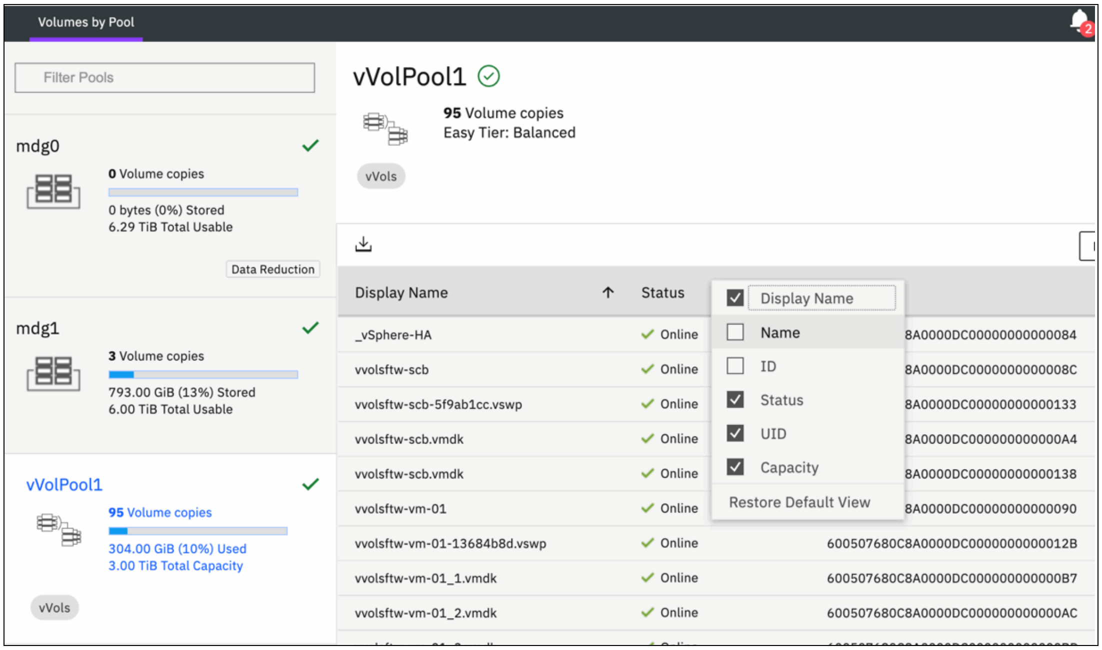
95 Volume copies
Easy Tier: Balanced

Display Name ↑	Name	Status
_vSphere-HA	rfc4122.16e9eaca-34b8-4bdf-91f6-d9b8d8cdeaa3	✓ Online
vvolsftw-scb	rfc4122.7cea933b-91d6-44bb-a429-76263efc6258	✓ Online
vvolsftw-scb-5f9ab1cc.vswp	rfc4122.0386edb7-f6f6-44c2-8abd-f0e12fb10306	✓ Online
vvolsftw-scb.vmdk	rfc4122.917b8dec-195c-4651-9a5a-60522753065b	✓ Online
vvolsftw-vm-01	rfc4122.37b1b551-6785-487b-8f90-8ebb4d2a9143	✓ Online
vvolsftw-vm-01-13684b8d.vswp	rfc4122.9e25bc71-628e-4f86-8ffc-190e1dfae4b7	✓ Online
vvolsftw-vm-01_1.vmdk	rfc4122.1821c462-81fc-4bfa-b3af-6ce1cb0e33dc	✓ Online
vvolsftw-vm-01_2.vmdk	rfc4122.8ddbe09d-4236-446a-a492-7c748928c1d6	✓ Online
vvolsftw-vm-01_3.vmdk	rfc4122.13d47d54-6f26-4338-bb9d-72fac6dbf0f9	✓ Online
vvolsftw-vm-01_4.vmdk	rfc4122.4278d37f-c843-42d0-9735-f22e02f13258	✓ Online
vvolsftw-vm-02	rfc4122.b01a7b88-b99a-49ae-b654-8b4336304d9e	✓ Online
vvolsftw-vm-02-06263a29.vswp	rfc4122.1a087497-0462-4bd5-a373-28016f25ea6f	✓ Online
vvolsftw-vm-02_1.vmdk	rfc4122.03b294c5-b231-4f65-980b-4d63fac40d73	✓ Online
vvolsftw-vm-02_2.vmdk	rfc4122.30aae6e7-af4f-463f-9f70-bb354dede2c7	✓ Online
vvolsftw-vm-02_3.vmdk	rfc4122.3156bc6d-f877-43b8-8740-89b3619a440c	✓ Online
vvolsftw-vm-02_4.vmdk	rfc4122.3c3666a2-167e-4042-8007-b8baad1af230	✓ Online

Figure 5-50 Selecting the vVol-enabled child pool

6. The Display Name column was added to provide more information about the vVol that can help to identify the specific VM to which it belongs (Figure 5-51 on page 123).

> **Note:** By default, the Name column is not displayed in the GUI table view, but it is an optional field that can be added by right-clicking the column headers and selecting the **Name** checkbox.



Volumes by Pool

mdg0

0 Volume copies

0 bytes (0%) Stored

6.29 TiB Total Usable

Data Reduction

mdg1

3 Volume copies

793.00 GiB (13%) Stored

6.00 TiB Total Usable

vVolPool1

95 Volume copies

304.00 GiB (10%) Used

3.00 TiB Total Capacity

vVols

vVolPool1

95 Volume copies

Easy Tier: Balanced

vVols

Display Name	Status	
_vSphere-HA	✓ Online	8A0000DC00000000000084
vvolsftw-scb	✓ Online	8A0000DC0000000000008C
vvolsftw-scb-5f9ab1cc.vswp	✓ Online	8A0000DC00000000000133
vvolsftw-scb.vmdk	✓ Online	8A0000DC000000000000A4
vvolsftw-scb.vmdk	✓ Online	8A0000DC00000000000138
vvolsftw-vm-01	✓ Online	8A0000DC00000000000090
vvolsftw-vm-01-13684b8d.vswp	✓ Online	600507680C8A0000DC0000000000012B
vvolsftw-vm-01_1.vmdk	✓ Online	600507680C8A0000DC000000000000B7
vvolsftw-vm-01_2.vmdk	✓ Online	600507680C8A0000DC000000000000AC

Figure 5-51   Displaying the Name column

6

Overview of the IBM Storage plug-in for vSphere

The IBM Storage Virtualize plug-in for vSphere is a Photon OS virtual machine. Photon OS is an open-source Linux operating system from VMware. By using the IBM Storage Virtualize plug-in for vSphere, you can provision and manage IBM Storage Virtualize objects directly from the VMware vSphere client. The IBM Storage plug-in workflows are integrated into the vSphere Client GUI so that VMware administrators can manage vSphere and Storage Virtualize objects within one window.

This chapter has the following chapters:

- 6.1, “Supported platforms for the IBM Storage plug-in for vSphere” on page 126
- 6.2, “Architecture of the IBM Storage plug-in for vSphere” on page 126
- 6.3, “Downloading and deploying the OVA” on page 127
- 6.4, “Upgrading from a previous version” on page 137
- 6.5, “Using the dashboard” on page 138
- 6.6, “Datastore actions and panels” on page 146
- 6.7, “Host panels” on page 159
- 6.8, “Cluster panels” on page 162
- 6.9, “Enforcing practical usage behavior” on page 165
- 6.10, “Troubleshooting” on page 166

6.1 Supported platforms for the IBM Storage plug-in for vSphere

The plug-in supports all block storage devices in the IBM Storage Virtualize family, which includes IBM FlashSystem, IBM Storwize, and IBM SAN Volume Controller.

To use these products with the plug-in, they must be on software level 8.4.2.0 or higher.

> **Note:** Base functionality is supported from 8.4.2.0 or higher. However, specific features are only available on supported platforms or software levels. Throughout the chapter, it is specified whether the requirements change for different features.

To register the plug-in to a VMware vSphere client, the vCenter environment must be on version 7.0 or higher.

6.2 Architecture of the IBM Storage plug-in for vSphere

The plug-in runs on a Photon OS virtual machine and is based on the VMware Remote Plug-in architecture.

6.2.1 Required resources

Consider the appliance and VMware vSphere environment requirements.

Appliance requirements

Running the plug-in requires the following resources on the vSphere appliance where the plug-in virtual machine is deployed:

- 2 vCPUs and 4 GB of memory
- 20 GB of datastore space (Either vSphere Virtual File Machine System (VMFS) or vVol)
- Networking (Ethernet, TCPIP)
  - One IP address (IPv4), Static or DHCP
  - Gateway
  - DNS
  - Netmask

VMware vSphere environment requirements

An installation of VMware vSphere includes the following environment requirements:

- vCenter 7.0 or higher
- IP connectivity between the vCenter, plug-in appliance, and IBM Storage System
- Fully qualified domain name (FQDN) or IP address of the vCenter(s)
- vCenter user account with administrative privileges
- Ports required:
  - 443 between plug-in and vCenter
  - 7443 between storage and plug-in

Demonstration videos: The following demonstration videos are available for VMware integration with IBM FlashSystem:

- Connecting IBM Storage to VMware vSphere
- Managing datastores provisioned in IBM FlashSystem storage from the vSphere client
- Creating a datastore on IBM FlashSystem storage, directly from the vSphere client.

You can also view Demo Videos to see a full list of the IBM Storage videos created by the IBM Redbooks authors.

6.3 Downloading and deploying the OVA

An Open IBM Informix Virtual Appliance (OVA) is a collection of necessary files stored in a single bundled .tar file. Examples of file types that are included in the OVA are Open Virtualization File (OVF), .vmdk, .nvram and .mf files.

Downloading the OVA

The OVA and fix package can be downloaded from Fix Central. To find either go to Fix Central and search for `IBM Storage Virtualize Plugin for vSphere` and navigate to the appropriate page for the appropriate product, from here the OVA can be downloaded.

You can also download an upgrade bundle from Fix Central, to learn more about upgrading from previous releases see the section 6.4, "Upgrading from a previous version" on page 137.

Deployment instructions

Perform the following steps to deploy the OVA into vSphere:

1. Right click either a Datacenter, ESX host or vSphere cluster to open the actions menu and click **Deploy OVF Template**. See Figure 6-1 on page 128.
2. When the OVF deployment wizard opens, click **UPLOAD FILES**, and in the file browser, select the recently downloaded .ova file. See Figure 6-2 on page 128.

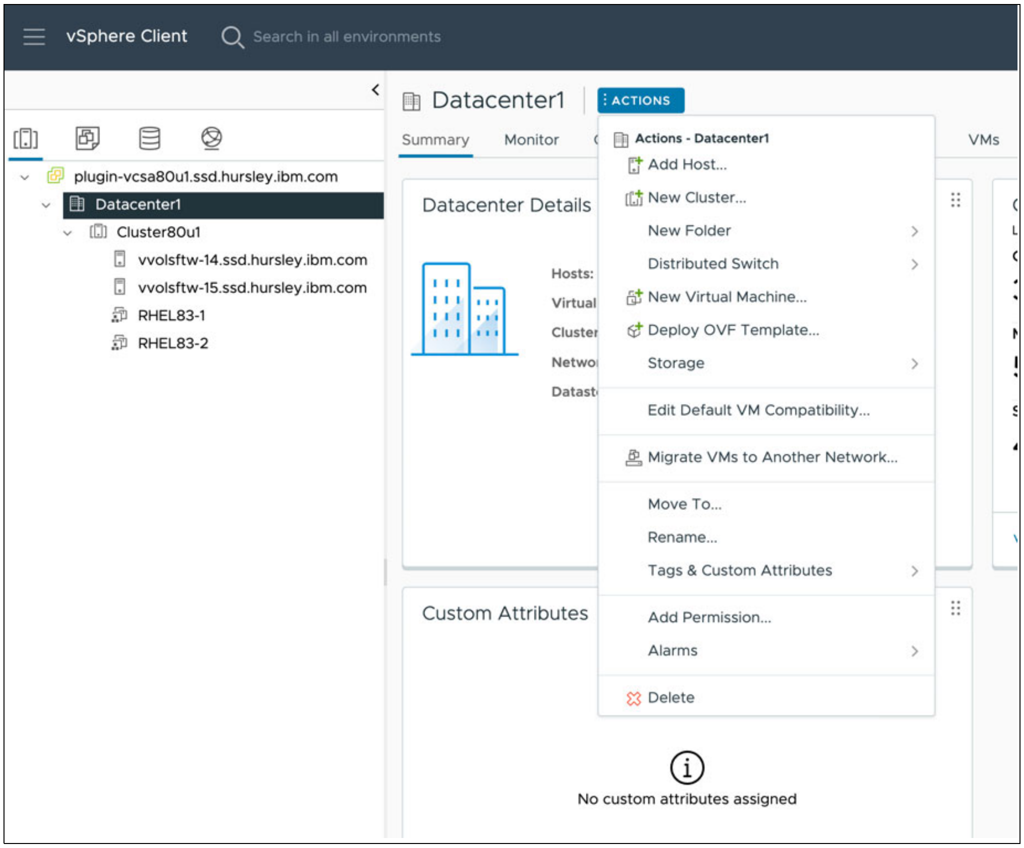
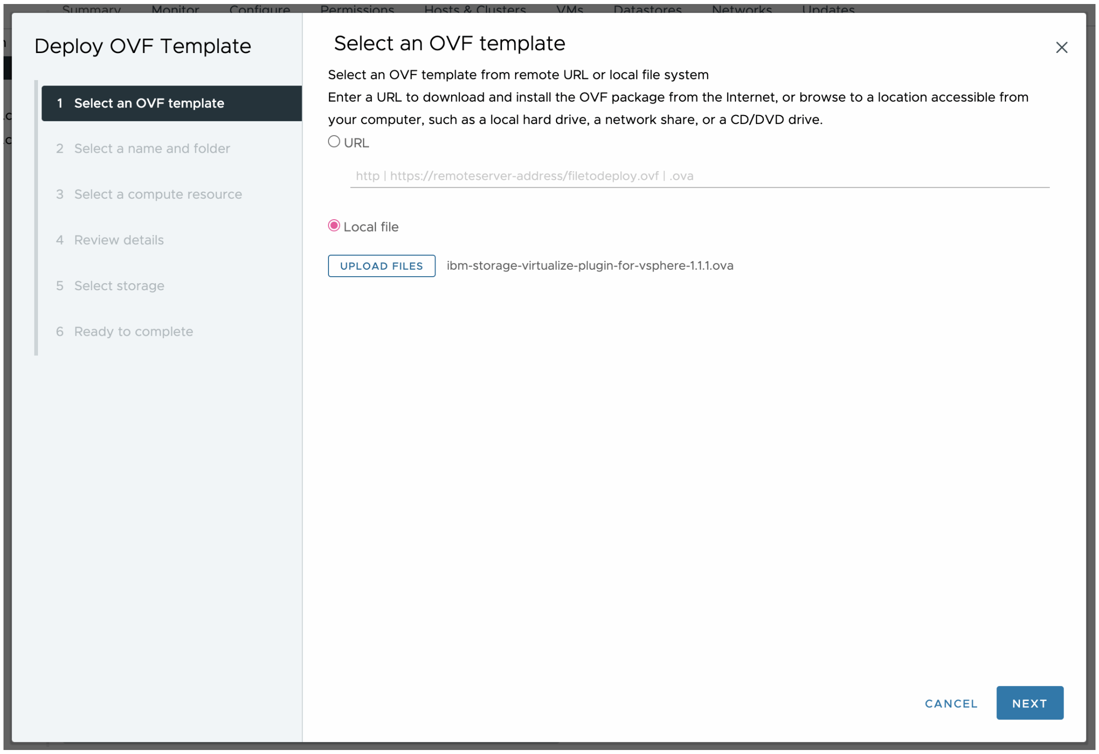


Figure 6-1 Datacenter Action menu



Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

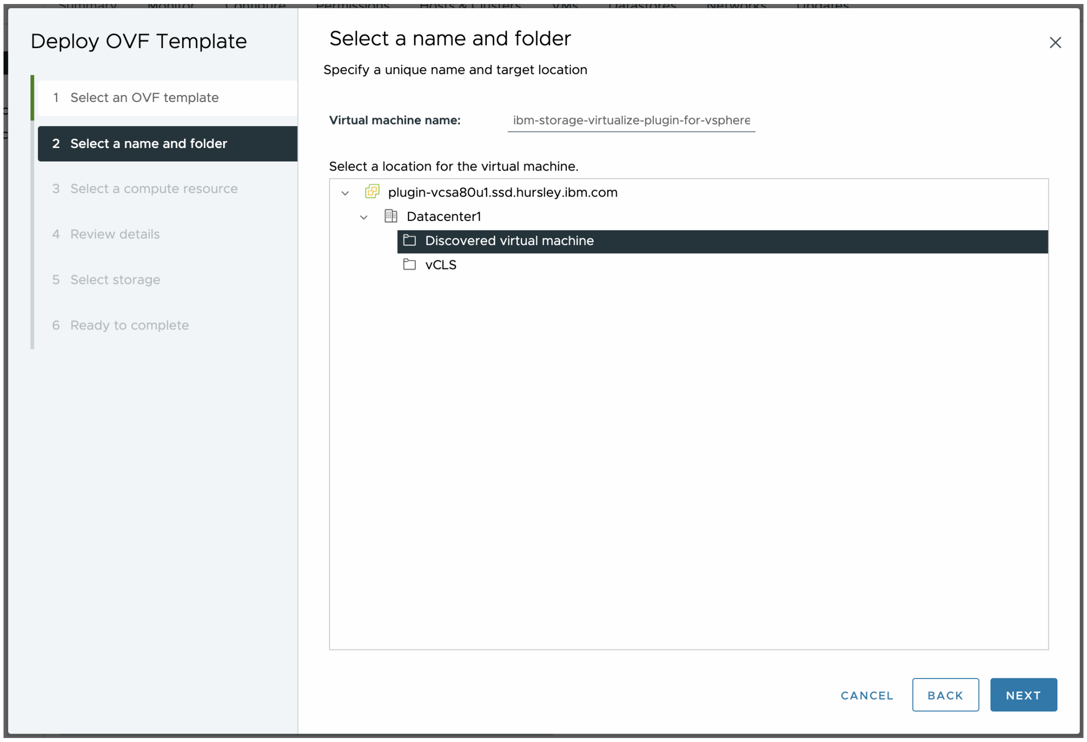
http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

UPLOAD FILES ibm-storage-virtualize-plugin-for-vsphere-1.1.1.ova

Figure 6-2 Deploy OVF Template: Select an OVF Template

3. Enter a name for the virtual machine (VM) and select a location within the vSphere inventory. See Figure 6-3.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder

Specify a unique name and target location

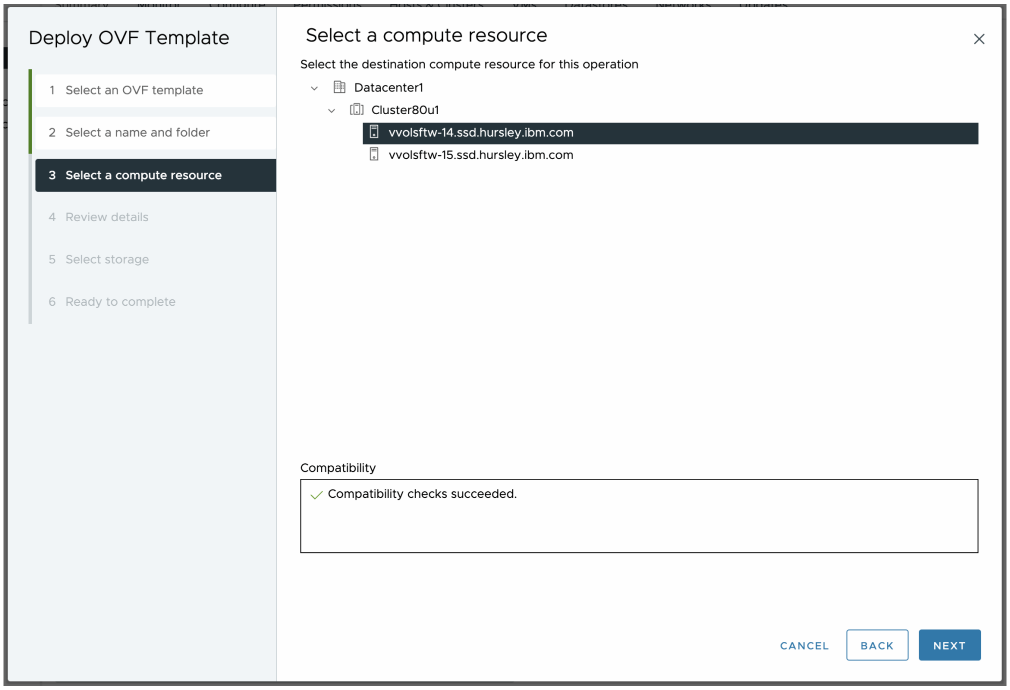
Virtual machine name: ibm-storage-virtualize-plugin-for-vsphere

Select a location for the virtual machine.

- plugin-vcsa80u1.ssd.hursley.ibm.com
  - Datacenter1
    - Discovered virtual machine
    - vCLS

Figure 6-3 Deploy OVF Template: Select a name and folder

4. Select which compute resource owns the VM. Evaluations are run on the selected host to determine compatibility. See Figure 6-4.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

- Datacenter1
  - Cluster80u1
    - vvolsftw-14.ssd.hursley.ibm.com
    - vvolsftw-15.ssd.hursley.ibm.com

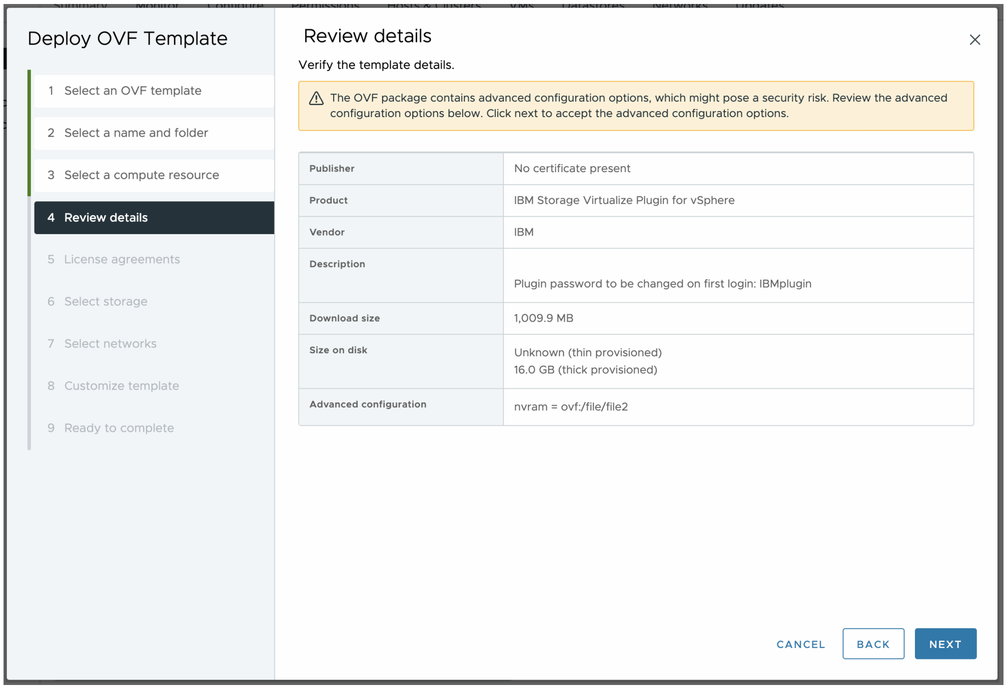
Compatibility

✓ Compatibility checks succeeded.

Figure 6-4 Deploy OVF Template: Select a compute resource

5. Review the information. See Figure 6-5.

> Note: The default VM password is available in the Description section. You are prompted to change the password on the first login.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Review details

Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Product	IBM Storage Virtualize Plugin for vSphere
Vendor	IBM
Description	Plugin password to be changed on first login: IBMplugin
Download size	1,009.9 MB
Size on disk	Unknown (thin provisioned) 16.0 GB (thick provisioned)
Advanced configuration	nvram = ovf:/file/file2

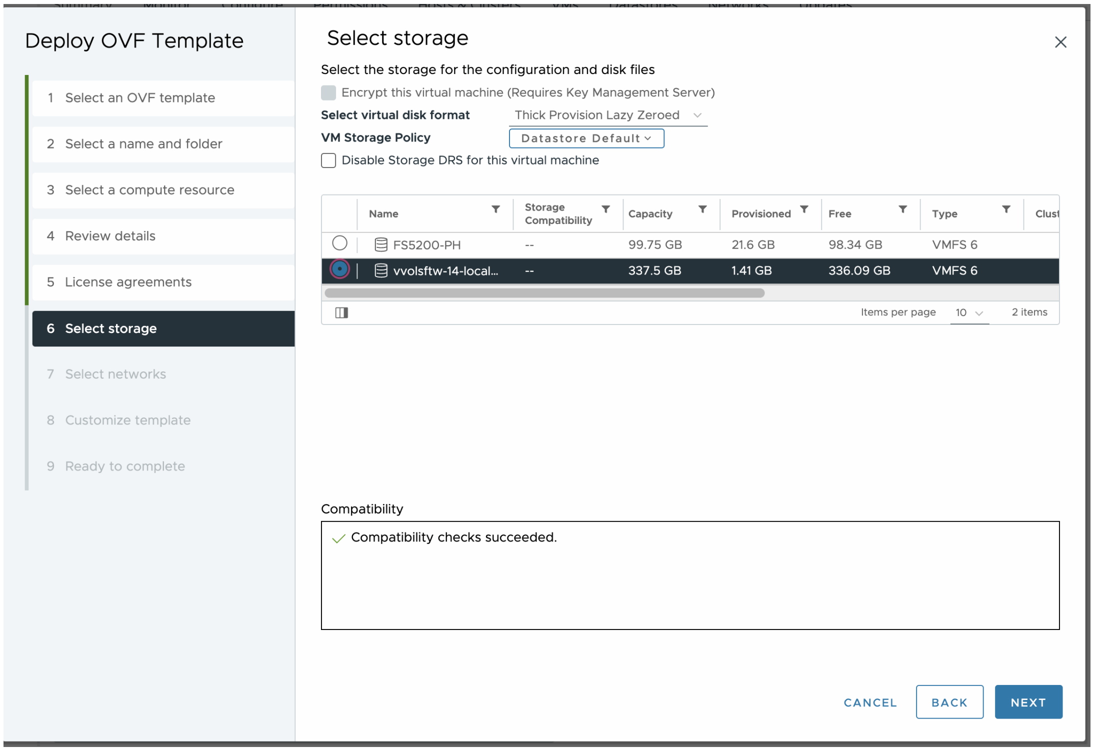
Figure 6-5 Deploy OVF Template: Review details

After reviewing details, the licenses must be accepted before continuing with the deployment of the OVA. The license to be accepted consists of 2 separate agreements:

- – The VMware end user license agreement
- – IBM License information, containing the license in multiple languages

6. After reading both licenses, confirm if you agree with the license and proceed.

7. Select the storage for the configuration and files that are associated with the VM to be deployed. Select whether the VM should be encrypted (which requires a *Key Management Server*), the format of the virtual disk, and the datastore where the VM is stored. If the selection is compatible, click **Next**. See Figure 6-6 on page 131.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format Thick Provision Lazy Zeroed

VM Storage Policy Datastore Default

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Clust
○	FS5200-PH	--	99.75 GB	21.6 GB	98.34 GB	VMFS 6	
●	vvolsftw-14-local...	--	337.5 GB	1.41 GB	336.09 GB	VMFS 6	

Items per page 10 2 items

Compatibility

✓ Compatibility checks succeeded.

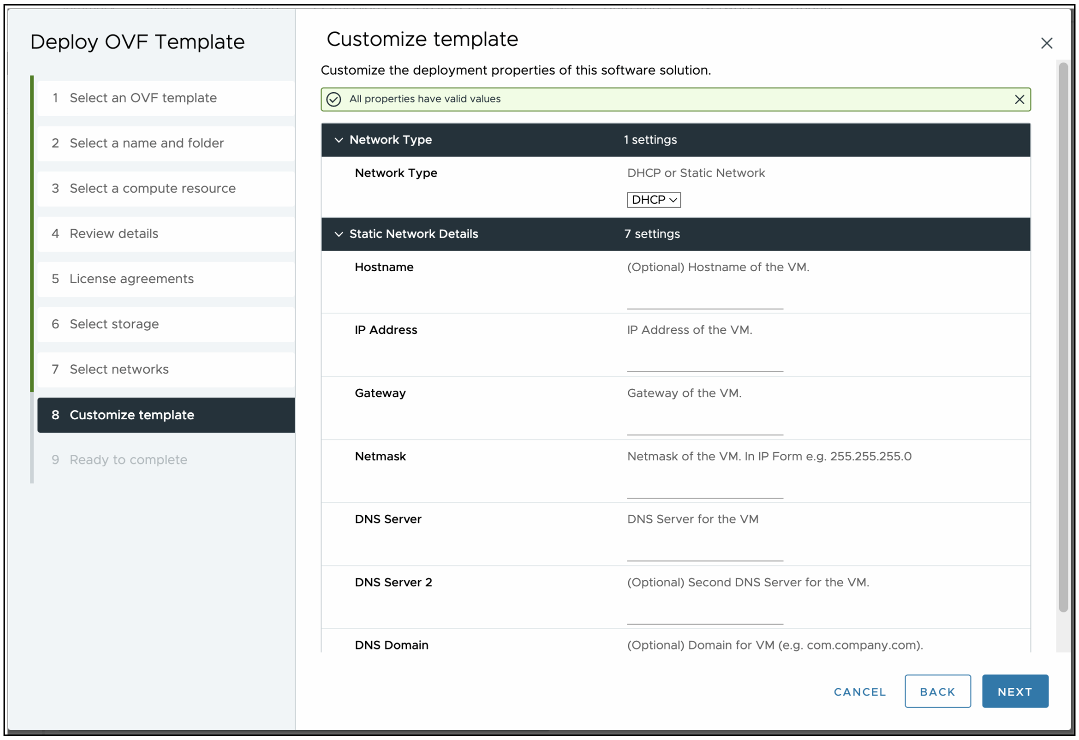
Figure 6-6 Deploy OVF Template: Select Storage

8. Select the destination network for the VM. Other fields on this page is pre-selected and cannot be changed.
9. Configure the network settings of the VM, using either static or DHCP networking.
   a. DHCP option. To configure DHCP for the plug-in VM use static networking, select **DHCP** from the dropdown in the Network Type section of the page. The only requirement is ensuring that the network supports DHCP. The static network details section does not need to be completed. See Figure 6-7 on page 132.
   b. If you choose to configure the VM with a static network, select **Static** from the dropdown in the Network Type section of the page.

      Fill out the following details in the static network details section:

      - Hostname
      - IP Address
      - Gateway
      - Netmask
      - DNS Server

      The remaining fields are optional. See Figure 6-8 on page 132.



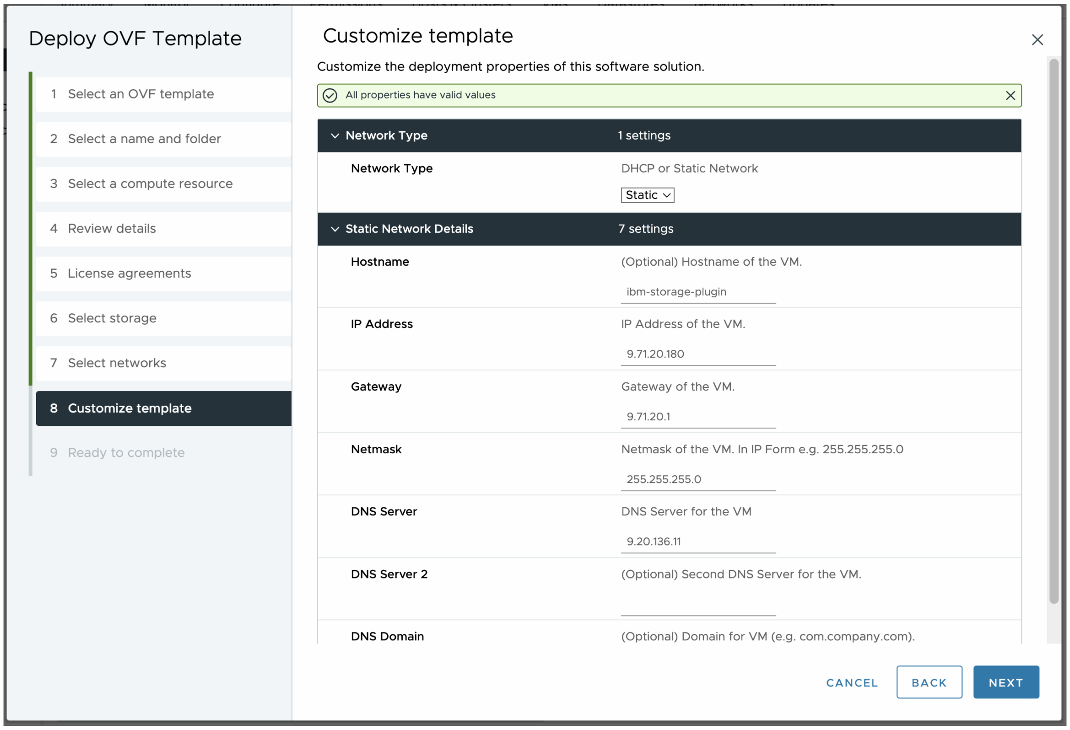
Customize template

Customize the deployment properties of this software solution.

All properties have valid values

Network Type	1 settings
Network Type	DHCP or Static Network DHCP
Static Network Details	**7 settings**
Hostname	(Optional) Hostname of the VM.
IP Address	IP Address of the VM.
Gateway	Gateway of the VM.
Netmask	Netmask of the VM. In IP Form e.g. 255.255.255.0
DNS Server	DNS Server for the VM
DNS Server 2	(Optional) Second DNS Server for the VM.
DNS Domain	(Optional) Domain for VM (e.g. com.company.com).

Figure 6-7 Deploy OVF Template: Example DHCP customization



Customize template

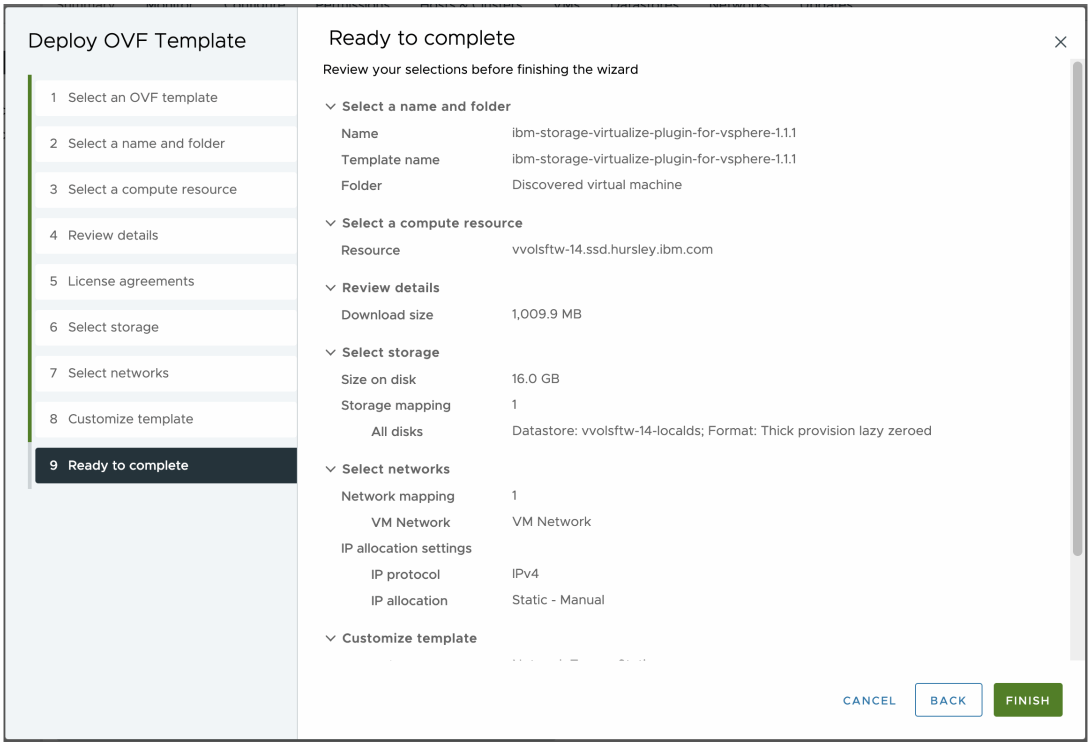
Customize the deployment properties of this software solution.

All properties have valid values

Network Type	1 settings
Network Type	DHCP or Static Network Static
Static Network Details	**7 settings**
Hostname	(Optional) Hostname of the VM. ibm-storage-plugin
IP Address	IP Address of the VM. 9.71.20.180
Gateway	Gateway of the VM. 9.71.20.1
Netmask	Netmask of the VM. In IP Form e.g. 255.255.255.0 255.255.255.0
DNS Server	DNS Server for the VM 9.20.136.11
DNS Server 2	(Optional) Second DNS Server for the VM.
DNS Domain	(Optional) Domain for VM (e.g. com.company.com).

Figure 6-8 Deploy OVF Template: Example static customization

10. Review the summary of all the deployment details. Click **Finish** to deploy the OVA as a VM. See Figure 6-9.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Ready to complete

Review your selections before finishing the wizard

Select a name and folder

Name	ibm-storage-virtualize-plugin-for-vsphere-1.1.1
Template name	ibm-storage-virtualize-plugin-for-vsphere-1.1.1
Folder	Discovered virtual machine

Select a compute resource

Resource	vvolsftw-14.ssd.hursley.ibm.com

Review details

Download size	1,009.9 MB

Select storage

Size on disk	16.0 GB
Storage mapping	1
All disks	Datastore: vvolsftw-14-localds; Format: Thick provision lazy zeroed

Select networks

Network mapping	1
VM Network	VM Network
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual

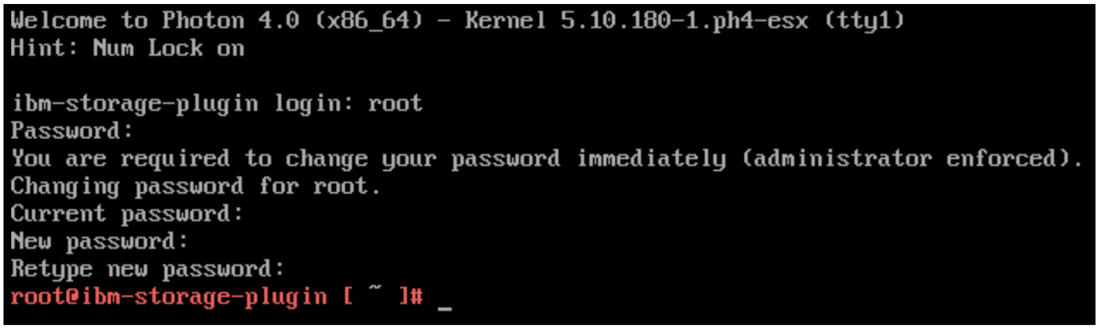
Customize template

Figure 6-9 Deploy OVF Template: Ready to complete

6.3.1 First time boot

After the VM is deployed into your vSphere environment, start the VM. To start the VM, navigate to the VM in your vSphere client and start it using either the play button or the Actions menu.

After the VM has successfully booted, you can connect to it by using ssh and by using the root user with the password `IBMplugin`. Alternatively, you can use the web console from the vSphere GUI to log in to the VM. The first time that you log in you are asked to change your password. This is a requirement. See Figure 6-10.



```
Welcome to Photon 4.0 (x86_64) - Kernel 5.10.180-1.ph4-esx (tty1)
Hint: Num Lock on

ibm-storage-plugin login: root
Password:
You are required to change your password immediately (administrator enforced).
Changing password for root.
Current password:
New password:
Retype new password:
root@ibm-storage-plugin [ ~ ]# _
```

Figure 6-10 Change password

6.3.2 Registering and unregistering the plug-in

Before using the IBM Storage plug-in for vSphere, register the plug-in to the vCenter instance. The following section reviews how to register and unregister the plug-in.

When registering or unregistering the plug-in, you must first be connected to your plug-in appliance. To connect, either use the web console or ssh and login as root using the updated password.

When you are logged in, the **`ibm-plugin`** command can be used for registration or un-registration.

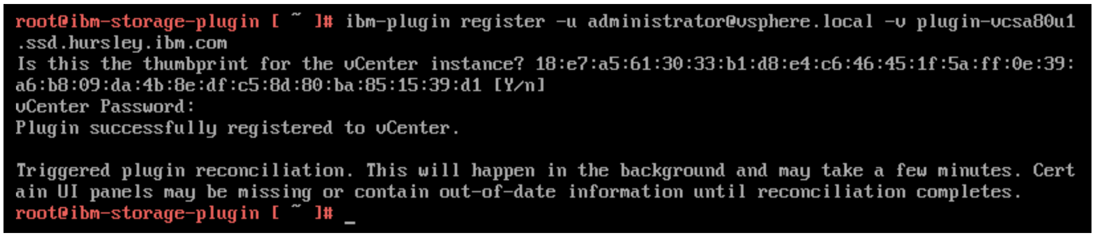
Registering the plug-in

To register the plug-in to a vCenter, run the following command:

```
ibm-plugin register -u <vCenter username> -v <IP or FQDN of the vCenter instance>
```

Note: The specified FQDN of the vCenter must be either the fully qualified domain name (FQDN) or the IP address of the vCenter instance. Registering the plug-in to a vCenter with a short hostname can cause errors when you use the plug-in.

After issuing the **`registration`** command, the thumbprint of the vCenter is shown. Confirm this is correct by selecting the Return or Enter key. Enter the password of the specified user to the vCenter instance. See Figure 6-11.



```
root@ibm-storage-plugin [ ~ ]# ibm-plugin register -u administrator@vsphere.local -v plugin-vcsa80u1
.ssd.hursley.ibm.com
Is this the thumbprint for the vCenter instance? 18:e7:a5:61:30:33:b1:d8:e4:c6:46:45:1f:5a:ff:0e:39:
a6:b8:09:da:4b:8e:df:c5:8d:80:ba:85:15:39:d1 [Y/n]
vCenter Password:
Plugin successfully registered to vCenter.

Triggered plugin reconciliation. This will happen in the background and may take a few minutes. Cert
ain UI panels may be missing or contain out-of-date information until reconciliation completes.
root@ibm-storage-plugin [ ~ ]# _
```

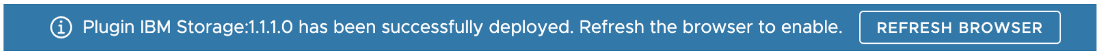
Figure 6-11 Registration command

If this command is successful, you see the following message:

```
Plugin successfully registered to vCenter.
```

For any issues when registering the plug-in, see 6.10, “Troubleshooting” on page 166. To register the plug-in to multiple linked vCenters, refer to “Registering with linked vCenters” on page 135.

After successful registration, a banner alert is shown in the vSphere Client and prompts for a page refresh. If you are logged in, click **Refresh Browser** in the prompt to refresh the browser and activate the plug-in. See Figure 6-12.



Plugin IBM Storage:1.1.1.0 has been successfully deployed. Refresh the browser to enable.

Figure 6-12 Refresh browser banner

Note: The browser must be refreshed to activate the plug-in. If the browser is not refreshed, the plug-in does not appear.

Populating information from IBM Storage Systems

Several tasks appear in the Recent Tasks panel at the bottom of the vSphere Client GUI. A task titled **Populating information from IBM Storage Systems** is a plug-in specific task that discovers existing host and datastore information within the vSphere environment and correlates to storage systems registered in the plug-in dashboard.

The population task is triggered when the plug-in is restarted or registered to a vCenter instance, a storage system is added to the plug-in dashboard, or is manually initiated by the user on the plug-in dashboard.

The time required for the task to finish depends on the size of the vSphere and storage systems configurations. During this time there might be inconsistencies or inaccuracies with the information displayed within the IBM Storage pages and the dashboard.

The plug-in is now ready to use. The rest of this chapter describes how to navigate and use the plug-in.

Registering with linked vCenters

The plug-in can be registered to multiple vCenters that are set up in a linked mode configuration. This allows for multiple vCenter instances to share the same plug-in appliance. Registration must be triggered individually for each vCenter in the linked configuration registration. However, the storage systems need to be registered only once to be shared between the linked vCenters.

> **Note**: Although the plug-in supports multiple vCenters, it does not support multiple vCenters, which are not in a linked-mode configuration. If multiple vCenters are to be used that are not in linked mode, they must have their own instance of the plug-in appliance.

6.3.3 Unregistering the plug-in

Unregister the plug-in is to remove the IBM Storage pages and remove the ability to manage your storage systems from the vSphere Client. Unregistering also removes the vCenter appliance from the plug-in.

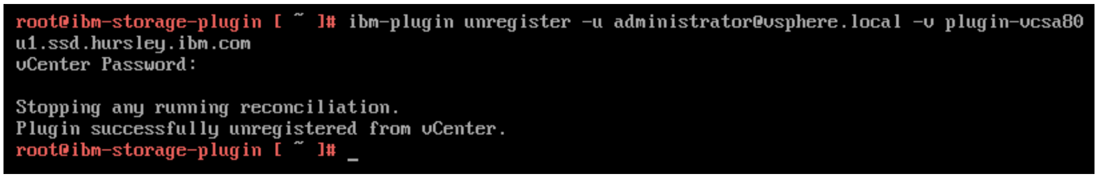
To unregister the plug-in from a vCenter run the following command:

```
ibm-plugin unregister -u <vCenter username used for registration> -v <IP or FQDN
of the vCenter instance>
```

The following output will be displayed after a successful unregistration (Figure 6-13.):

```
Plugin successfully unregistered from vCenter.
```

To finalize unregistration in the vSphere Client, click **Refresh Browser**.



```
root@ibm-storage-plugin [ ~ ]# ibm-plugin unregister -u administrator@vsphere.local -v plugin-vcsa80
u1.ssd.hursley.ibm.com
vCenter Password:

Stopping any running reconciliation.
Plugin successfully unregistered from vCenter.
root@ibm-storage-plugin [ ~ ]# _
```

Figure 6-13 Unregister plug-in command

Forcing unregistration

Unregistration of the plug-in requires communication between the plug-in appliance and the vCenter. If communication has been lost between the two objects, it might be necessary to force unregistration of the plug-in. This removes the registration from the appliance only.

The following message is displayed if the appliance cannot communicate to the vSphere instance:

```
Cannot connect to registered vCenter instance at
plugin-vcsa-wrong.ssd.hursley.ibm.com.
```

Press the Y key to confirm and start the removal of the local registration of the plug-in appliance. The plug-in is not removed from the vSphere client. In this scenario it would be required to do a manual removal of the plug-in from the vCenter. Instructions for completing this can be found in Manual unregistration on vCenter version 8.0 or higher and Manual unregistration on vCenter version lower than 8.0.

Manual unregistration on vCenter version 8.0 or higher

To manually unregister the plug-in on vCenter version 8.0 or higher, follow the below steps:

1. Within the vSphere client from the Shortcuts menu, select **Administration** → **Solutions** → **Client Plugins**.
2. Select the **IBM Storage** plug-in.
3. Select the specific plug-in instance to be removed and click **Remove**.
4. When prompted, confirm the removal of the plug-in by clicking **Yes**.
5. When prompted, refresh the browser to complete the plug-in removal.

Manual unregistration on vCenter version lower than 8.0

To manually unregister the plug-in on a vCenter on a version lower than 8.0, follow the below steps:

1. Navigate to the Extension Manager of the vCenter:
   `https://vcenter.fqdn/mob/?moid=ExtensionManager`

 where `vcenter.fqdn` is the FQDN of the vCenter.

2. Select **Methods** → **Name** and click **UnregisterExtension**.
3. In the value field, enter `com.ibm.storageplugin`.
4. Click **Invoke method**.

If the unregistration is successful the message: `Method Invocation Result: void` is displayed, and if unsuccessful an error message is displayed.

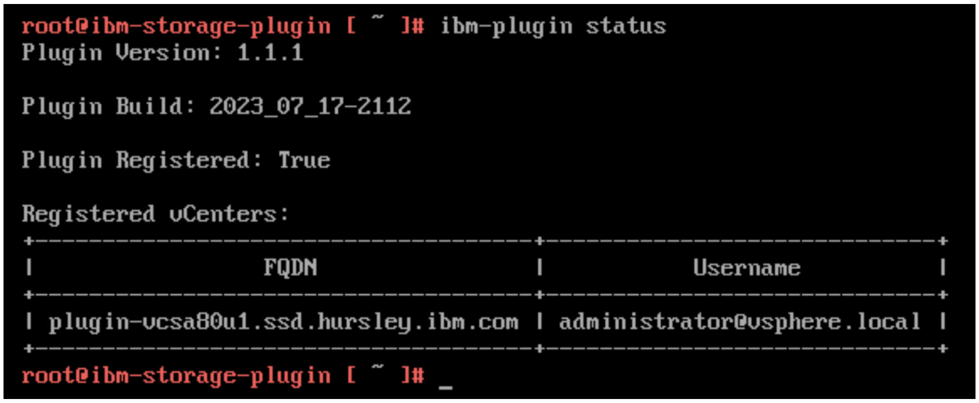
6.3.4 Checking the status of the plug-in

The **`ibm-plugin`** command can also be used to check the status of the plug-in appliance. Checking the status of the plug-in shows the plug-in version information, any registered vCenter instances, and the associated user account.

To display the status of the plug-in, when connected to the VM run the command **ibm-plugin status**.

The output is displayed in the console.

Any plug-in registrations appear in a table under the "Registered vCenters" section of the output.



```
root@ibm-storage-plugin [ ~ ]# ibm-plugin status
Plugin Version: 1.1.1

Plugin Build: 2023_07_17-2112

Plugin Registered: True

Registered vCenters:
+-------------------------------------+------------------------------+
|                FQDN                 |           Username           |
+-------------------------------------+------------------------------+
| plugin-vcsa80u1.ssd.hursley.ibm.com | administrator@vsphere.local  |
+-------------------------------------+------------------------------+
root@ibm-storage-plugin [ ~ ]# _
```

Figure 6-14 Status of registrations

6.4 Upgrading from a previous version

This section describes upgrading the IBM Storage plug-in for vSphere from a previous version.

6.4.1 What you need to know before upgrading

When upgrading the plug-in from version 1.0.0 to any other later version, it is required that the plug-in is unregistered from all registered vCenter instances. Furthermore, this upgrade path requires the internal plug-in database to be reset, meaning that all registered storage systems are no longer managed within the plug-in and will need re-adding into the plug-in dashboard after the upgrade has completed. To learn about adding storage systems to the plug-in go to 6.5.2, “Adding storage systems” on page 139.

> **Note:** No existing data will be lost from datastores. Volumes, and volume mappings will also be undisturbed.

For unregistration instructions see 6.3.3, “Unregistering the plug-in” on page 135.

There is an alternative to following the upgrade process You can unregister the plug-in from any registered vCenters, power off and delete the VM, and then re-deploy the OVA by using the v1.1.0 OVA.

6.4.2 Upgrade process

To upgrade the plug-in appliance, copy the upgrade package to the VM. The upgrade package is found on Fix Central. If you want to download the upgrade package navigate to `https://www.ibm.com/support/fixcentral` and search for `IBM Storage plugin for vSphere - Upgrade pack`. There should be one or more results. Select the option that is associated with your product and follow the steps to download the package.

1. After the package is downloaded, it can be copied onto the VM. Use the **`scp`** command to copy the package into the directory of your choice by using the root user and password that you defined when you deployed the appliance.

2. To install the package, use the **ibm-install** command followed by the full path to the upgrade file:

   ```
   ibm-install /tmp/ibm-storage-virtualize-plugin-upgrade-2023_06_12-1314.tar.gz
   ```

   The command starts the installation process, which removes the package after the installation is completed. See Example 6-1.

Example 6-1 Install process

```
Plugin started
Updating registration for plugin-vcsa80u1.ssd.hursley.ibm.com... Done
~
Removing the install package
ibm-storage-virtualize-plugin-upgrade-2023_06_12-1314.tar.gz
Successfully installed the plugin package.
```

After the upgrade is done, register the plug-in by following the instructions provided in “Registering the plug-in” on page 134.

6.4.3 Updating Photon OS packages

The plug-in package comes with a fixed version of Photon OS packages. By updating the Photon OS packages, it allows you to apply any security patches that addresses vulnerabilities.

Updating the Photon OS packages requires that your VM has internet access, if the VM does not have internet access, then it is best to follow the steps in 6.3, “Downloading and deploying the OVA” on page 127 with the latest version of the appliance.

To upgrade your Photon OS packages, connect to the VM and use the following procedure:

1. Run the following command **cd /opt/ibm-plugin**.
2. Shutdown the plug-in by running **docker-compose down**.
3. Update the Photon OS packages by running **tdnf update**.
4. After the updates are done, reboot the VM. The plug-in should auto-start.

If the plug-in does not auto-start, run the following commands to manually start the plug-in:

- **cd /opt/ibm-plugin**
- **docker-compose up -d**

6.5 Using the dashboard

This section includes a description of the IBM Storage plug-in for vSphere dashboard.

6.5.1 Navigating to the dashboard

To navigate to the IBM Storage Dashboard, where you manage your storage systems, from the vSphere menu select **IBM Storage** under Plugins. See Figure 6-15 on page 139.

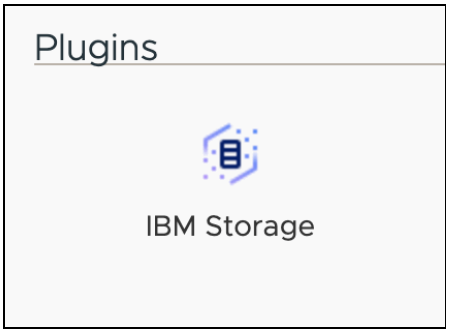
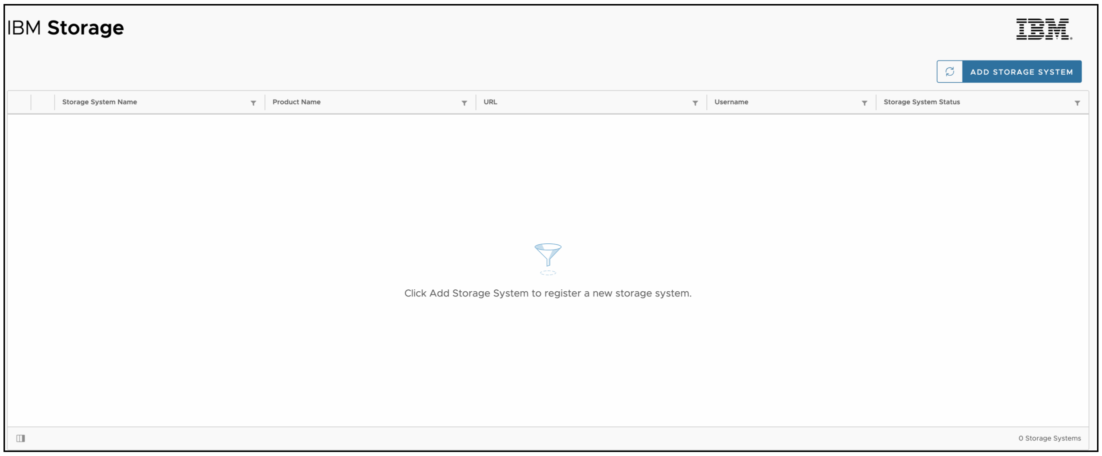


Figure 6-15 Main dashboard entry point from shortcuts page

The dashboard opens and includes information about any registered storage system and lists them in the main datagrid. See Figure 6-16.



Click Add Storage System to register a new storage system.

Figure 6-16 Empty dashboard

6.5.2 Adding storage systems

Add a storage system to the plug-in. When you click **Add Storage System** that is located on the right side above the datagrid, the Connect to Storage wizard opens. See Figure 6-17 and Figure 6-18 on page 140.

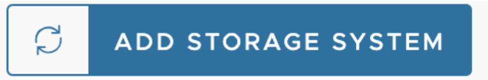
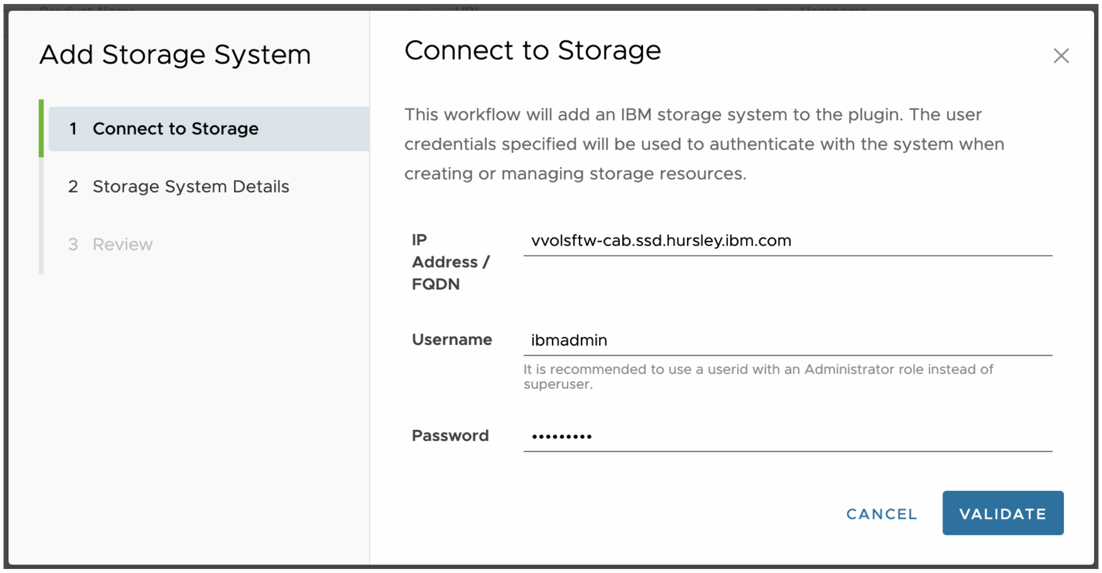


Figure 6-17 Sync icon button next to add storage system primary action

1. In the wizard, enter the IP or FQDN of the storage system you want to add, and the username and password of the user account you wish to use with the plug-in. Click **Validate**. See Figure 6-18 on page 140.



Add Storage System

1 Connect to Storage

2 Storage System Details

3 Review

Connect to Storage

This workflow will add an IBM storage system to the plugin. The user credentials specified will be used to authenticate with the system when creating or managing storage resources.

IP Address / FQDN: vvolsftw-cab.ssd.hursley.ibm.com

Username: ibmadmin

It is recommended to use a userid with an Administrator role instead of superuser.

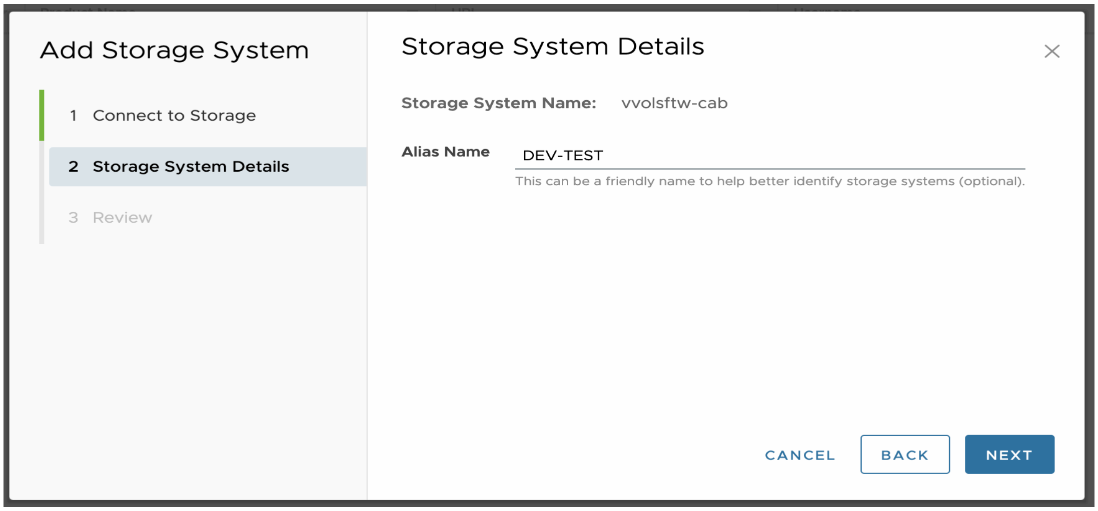
Password: •••••••••

Figure 6-18 Add storage system: Validating details to storage system

Note: Clicking **VALIDATE** establishes the network connectivity between the plug-in appliance and the storage system. If any network conditions exist that prevent connectivity between the appliance VM and the storage system IP on port 7443, such as restrictive VLANs or traffic filtering, then the connection might fail validation.

There is an optional alias input, which can be defined as a friendlier name to refer to each registered storage system. This can be useful when you have multiple storage systems registered to the plug-in and want an informal, unique identifier for the storage system used throughout the plug-in's interfaces.

2. Enter an alias name. See Figure 6-19.



Add Storage System

1 Connect to Storage

2 Storage System Details

3 Review

Storage System Details

Storage System Name: vvolsftw-cab

Alias Name: DEV-TEST

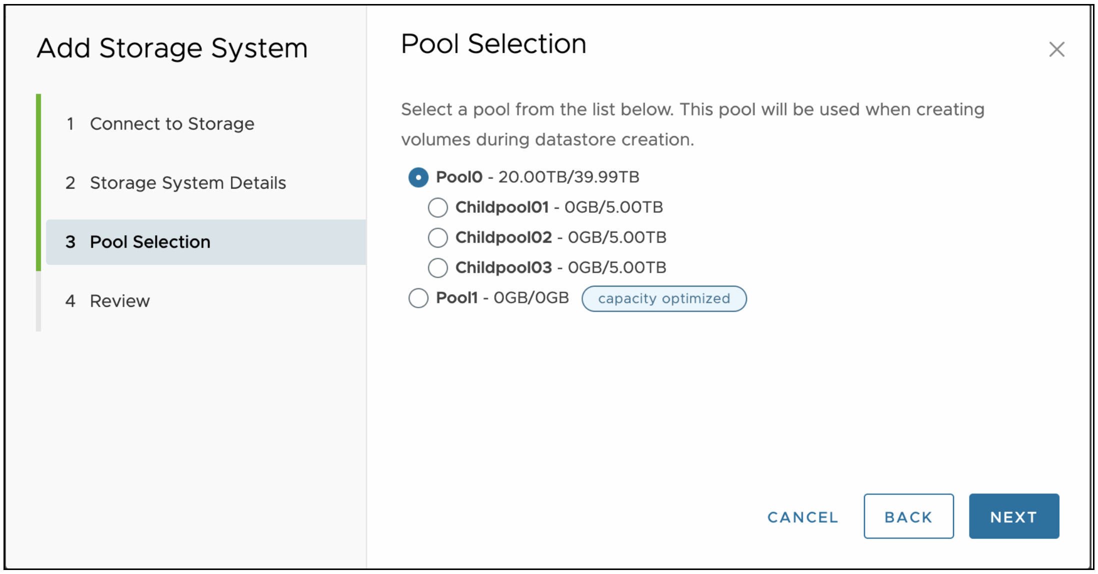
This can be a friendly name to help better identify storage systems (optional).

Figure 6-19 Add storage system: Assigning an alias name

3. If there are multiple pools on your storage system, you are asked to select a pool to register to the plug-in, select the pool you want to use.

If there is a provisioning policy attached to the pool, it is displayed in a label to the right of the capacity. For more information about provisioning policies, see 6.9.3, “Provisioning policies” on page 165.

Note: The pool that is selected is used when creating volumes. If there is only 1 pool available, this page is not shown.



Add Storage System

1 Connect to Storage
2 Storage System Details
3 Pool Selection
4 Review

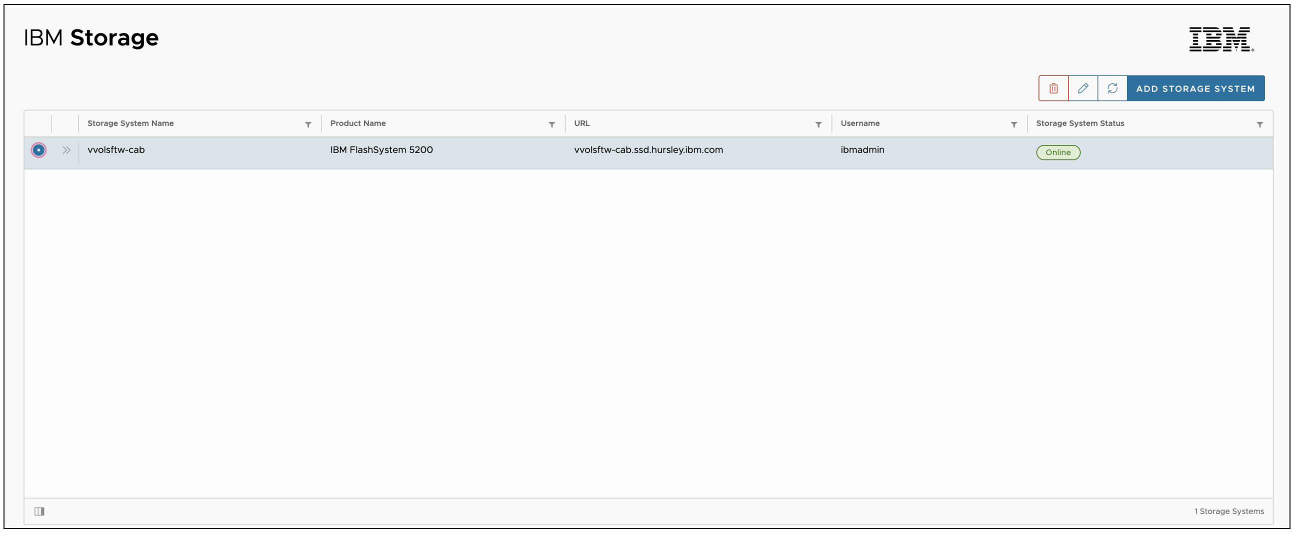
Pool Selection

Select a pool from the list below. This pool will be used when creating volumes during datastore creation.

- ● **Pool0** - 20.00TB/39.99TB
  - ○ **Childpool01** - 0GB/5.00TB
  - ○ **Childpool02** - 0GB/5.00TB
  - ○ **Childpool03** - 0GB/5.00TB
- ○ **Pool1** - 0GB/0GB capacity optimized

Figure 6-20 Add storage system: Selecting the pool to be used throughout the plug-in

4. Confirm if the storage system details are correct and click the **Add** button. See Figure 6-21.



IBM **Storage**

		Storage System Name	Product Name	URL	Username	Storage System Status
●	»	vvolsftw-cab	IBM FlashSystem 5200	vvolsftw-cab.ssd.hursley.ibm.com	ibmadmin	Online

1 Storage Systems

Figure 6-21 Add storage system: Populated dashboard

The wizard closes, and the dashboard refreshes and lists the recently added storage system in the datagrid.

Tip: There is no restriction on the number of systems that can be added to the plug-in.

After a storage system has been added to the plug-in, a task will appear within the vSphere client to show that the plug-in is discovering vSphere managed objects that are associated with that storage system. See “Populating information from IBM Storage Systems” on page 135. Some panels might show incorrect information or work incorrectly until this is completed.

6.5.3 Refreshing the inventory of registered storage systems

The database behind the plug-in stores various information and relationships between different vSphere and Storage Virtualize objects. When various panels open, a direct database read is performed to get the displayed information. This means that some information might be out of date since the last database update.

To refresh the storage system objects in the database, click the sync icon on the dashboard, a recent task appears as the plug-in discovers potential matches between vSphere and registered storage system environments. See Figure 6-22.

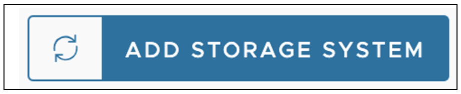


Figure 6-22 Sync icon button next to add storage system primary action

This action creates an inventory of all storage systems registered in the plug-in dashboard and compares any discovered objects against any existing ESXi hosts and VMFS datastores that are configured in vSphere. When the discovery task is finished, you can use the plug-in workflows to manage pre-existing datastores.

6.5.4 Editing storage systems

After a storage system is registered to the plug-in, you can edit the details associated with a selected system. During this workflow, you can update the user credentials and edit the alias given to the storage system. Cases where this is most useful includes the following situations:

- The status of your storage system is presenting a warning for "Invalid Credentials". This means that the token has expired, and the stored details are not reauthenticating. This might be because the password or username has changed on the system. Until this warning is resolved, you cannot see any information about the system, and you cannot perform any actions by using the plug-in. Follow this workflow to re-authenticate your system.
- You want to update the alias name given to the storage system.

Note: Editing your storage system by using the plug-in updates only the alias name as displayed in the plug-in. No changes are made on the underlying storage system.

Perform the following steps to edit your storage system:

1. Select anywhere in the row of the system that you want to edit.
2. Click the pencil icon button, just above the datagrid. See Figure 6-23.

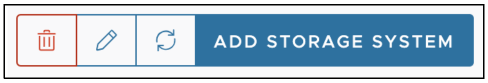
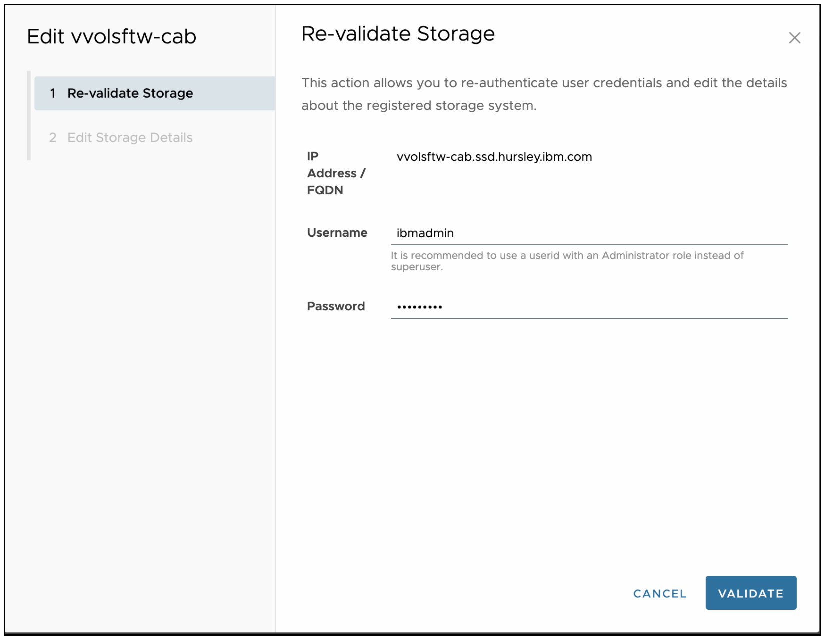


Figure 6-23 Edit storage system: Delete storage system icon button next to edit storage system icon button

3. Re-validate your storage system by entering the password associated with the pre-filled user account. Alternatively, you can change the user account that is used by the plug-in but ensure that the new user has visibility of the previously selected pool. See Figure 6-24.

Tip: To find the registered pool, go to expand the storage system and select the **Pool Details** tab.

Note: You cannot edit the IP/FQDN of the system because the system interprets the change as registering a new storage system. To update the connection address for an existing storage system registration, remove the selected storage system from the dashboard, and then re-add using the new IP/FQDN.



Re-validate Storage

This action allows you to re-authenticate user credentials and edit the details about the registered storage system.

IP Address / FQDN: vvolsftw-cab.ssd.hursley.ibm.com

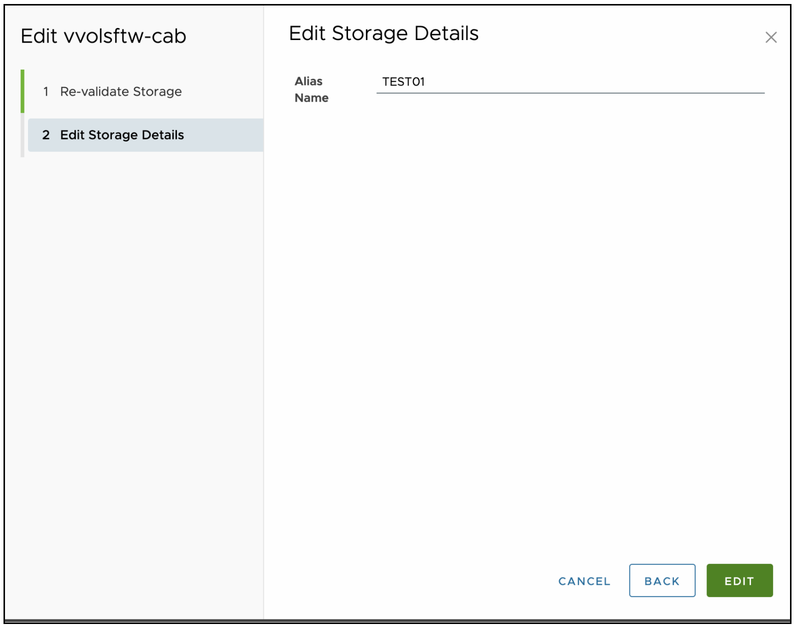
Username: ibmadmin

It is recommended to use a userid with an Administrator role instead of superuser.

Password: •••••••••

Figure 6-24 Edit storage system: Revalidate registered user's details

4. After re-authenticating, you can edit your alias name. This is pre-filled with the current alias but is not compulsory.


Edit vvolsftw-cab

1 Re-validate Storage

2 Edit Storage Details

Edit Storage Details

Alias Name: TEST01

Figure 6-25 Edit storage system: Edit the alias name of the storage system

5. Click the **Edit** button to finalize the details and update the plug-in's database. See Figure 6-25.

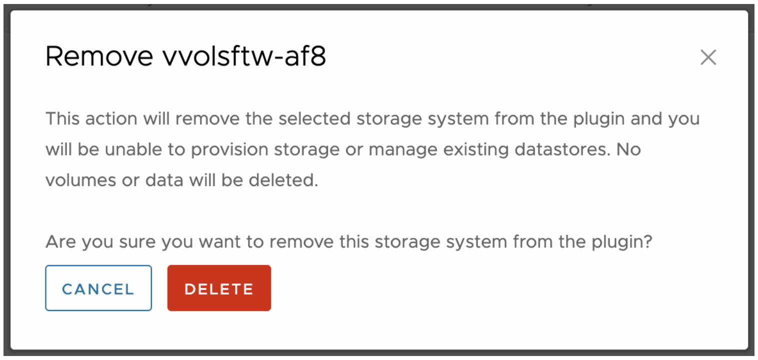
   The dashboard refreshes, and the new details are shown. The errors for invalid credentials are resolved.

6.5.5 Deleting storage systems

Deleting storage systems from the plug-in removes the storage system from the dashboard and make any associated vSphere objects, such as hosts, clusters, and datastores, show as not being managed by the plug-in. By removing a storage system from the plug-in no data is lost. Only the relationship between that storage system and the vSphere objects is removed. If the storage system is added back to the plug-in, a discovery task is run to identify any related objects on the storage system and their association to objects within the vSphere inventory. The association between the storage system and vSphere managed objects is restored.

To delete a storage system from the plug-in:

1. Select the storage system that you want to remove, edit, and delete icon buttons are shown.
2. Select the red trash bin icon.
3. A warning message is displayed. To continue, click **Delete**. See Figure 6-26 on page 145.



Remove vvolsftw-af8

This action will remove the selected storage system from the plugin and you will be unable to provision storage or manage existing datastores. No volumes or data will be deleted.

Are you sure you want to remove this storage system from the plugin?

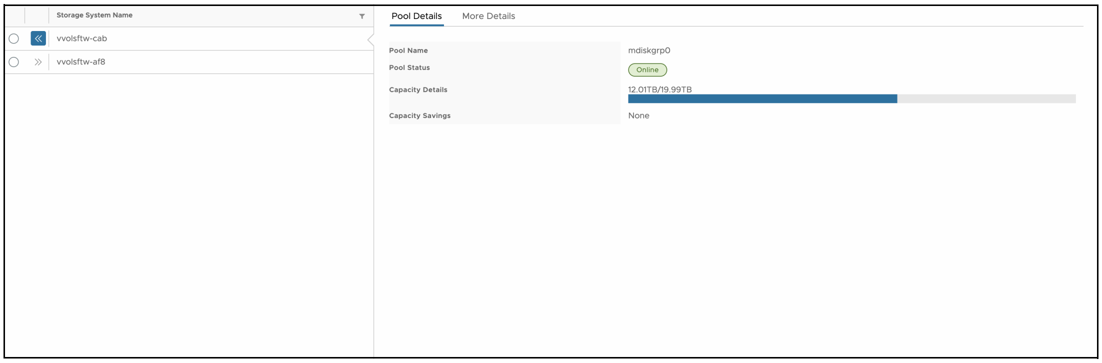
Figure 6-26 Delete storage system: Delete confirmation message

The dashboard refreshes, and the storage system removes any relationship between the system and any objects within the vSphere inventory.

6.5.6 Viewing more information about storage systems

On the dashboard, click the expand arrow to the right of the radio button for each registered storage system. This opens a further details page, which displays information about the registered pool and the underlying storage system.

This information can be useful when identifying specific characteristics of a system or in cases such as assessing if there is enough free capacity to create or expand a datastore. See Figure 6-27.

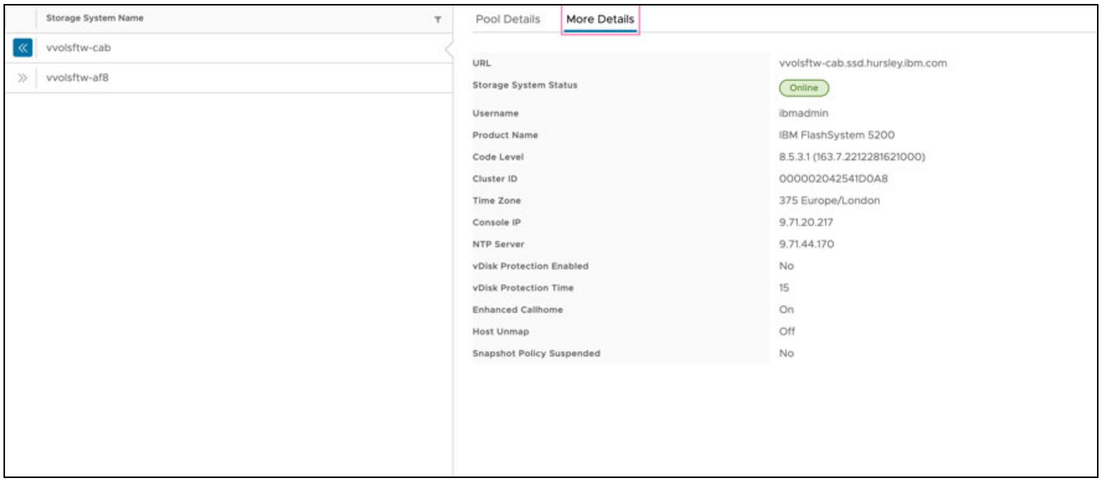


		Storage System Name
○	«	vvolsftw-cab
○	»	vvolsftw-af8

Pool Name	mdiskgrp0
Pool Status	Online
Capacity Details	12.01TB/19.99TB
Capacity Savings	None

Figure 6-27 Dashboard: A storage system's pool details

Click **More Details** to see more details of the storage system. See Figure 6-28 on page 146.



URL	vvolsftw-cab.ssd.hursley.ibm.com
Storage System Status	Online
Username	ibmadmin
Product Name	IBM FlashSystem 5200
Code Level	8.5.3.1 (163.7.2212281621000)
Cluster ID	000002042541D0A8
Time Zone	375 Europe/London
Console IP	9.71.20.217
NTP Server	9.71.44.170
vDisk Protection Enabled	No
vDisk Protection Time	15
Enhanced Callhome	On
Host Unmap	Off
Snapshot Policy Suspended	No

Figure 6-28 Dashboard: More details about a selected storage system

6.6 Datastore actions and panels

This section includes descriptions of datastore actions and panels.

6.6.1 Creating datastore(s)

In the current version of the plug-in, you can create single or multiple datastores within one workflow. To create a datastore:

1. Right click a cluster in the inventory or navigate to the cluster and expand the actions menu. Navigate to **Create VMFS Datastore** and select **IBM Storage**. See Figure 6-29 on page 147.
2. Enter the details of the one or more datastore that you want to create.

   The options are:

   – Name. What the datastore is called
   – Version. Which will always be VMFS 6
   – Size. Size of the datastore in TB or GB
   – Number of Datastores. Number of datastores to create

   See Figure 6-30 on page 147.

Tip: To change the unit from TB to GB, select TB to open a menu.

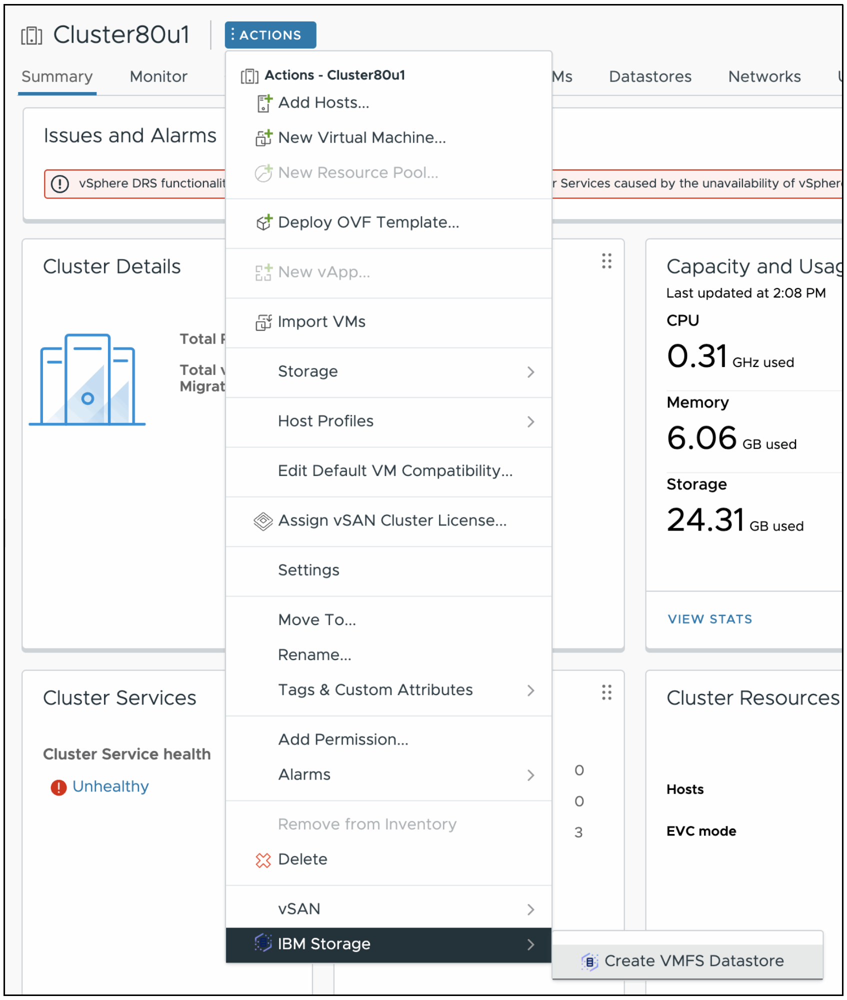
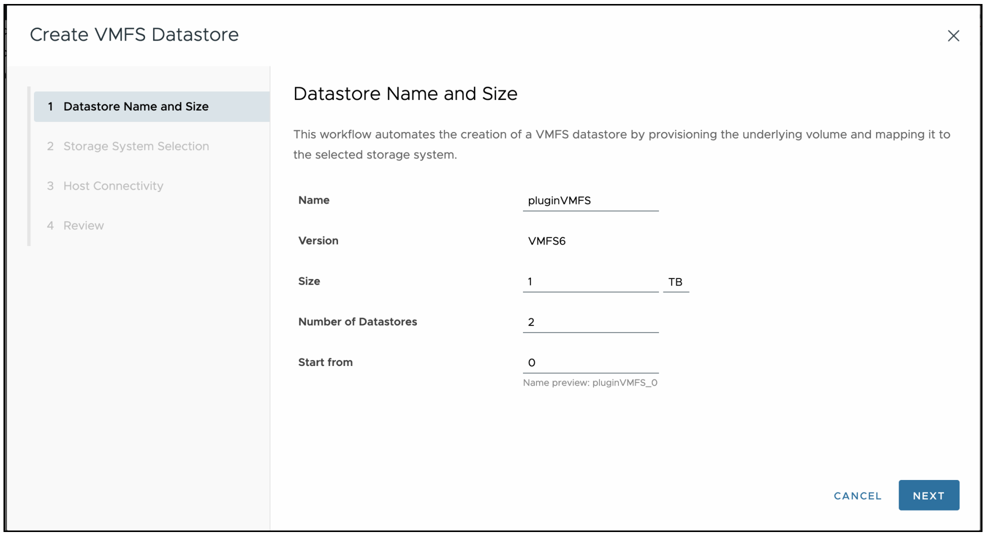


Figure 6-29 Navigating to the Create VMFS Datastore workflow



Create VMFS Datastore

1 Datastore Name and Size
2 Storage System Selection
3 Host Connectivity
4 Review

Datastore Name and Size

This workflow automates the creation of a VMFS datastore by provisioning the underlying volume and mapping it to the selected storage system.

Name	pluginVMFS
Version	VMFS6
Size	1 TB
Number of Datastores	2
Start from	0

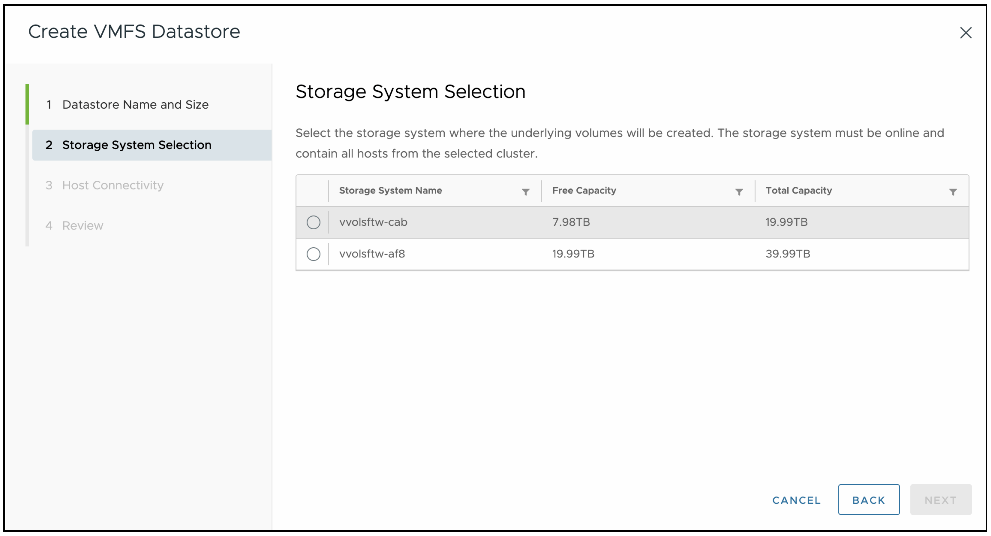
Name preview: pluginVMFS_0

Figure 6-30 Create datastore: Declaring the name, size and number of datastores to be created

To create multiple datastores, you can use the field **Start from**. This field specifies the suffix that is added to the defined datastore name. For example, if 3 datastores named **dstore** are created and if **Start from** is set to **1** the names of the datastores created are **dstore_1, dstore_2, and dstore_3**.

This naming convention is useful for adding multiple datastores of the same name with a different suffix so that datastores can be grouped by name.

3. Select a storage system on which to create the volume. To aid in the selection of the storage system, the capacity information is displayed. See Figure 6-31.



Storage System Selection

Select the storage system where the underlying volumes will be created. The storage system must be online and contain all hosts from the selected cluster.

	Storage System Name	Free Capacity	Total Capacity
○	vvolsftw-cab	7.98TB	19.99TB
○	vvolsftw-af8	19.99TB	39.99TB

Figure 6-31 Create datastore: Selecting the storage system to support the underlying volumes

When you select a storage system, the plug-in verifies the following factors:

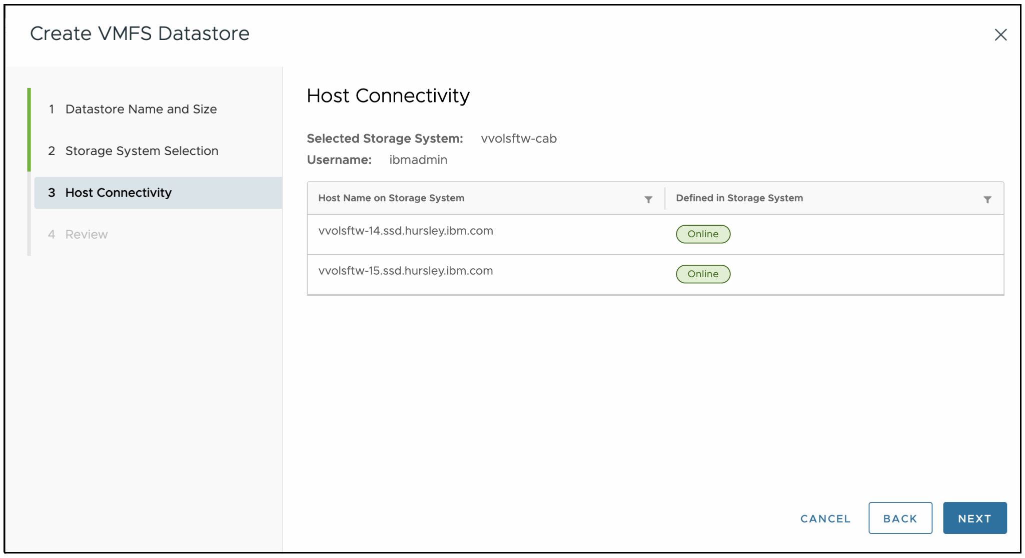
– The host objects exist on the selected storage system. If not, an error is displayed.

– The hosts belong to the same ownership group as the registered user for that storage system. If not, then an error is displayed.

– All hosts in the selected vSphere cluster are members of the same host cluster on the specified storage system. If the hosts are not in the same host cluster, an error is displayed.

– All the hosts are not in a host cluster. If the hosts do not belong to a host cluster, then a warning is raised but you can continue.

See Figure 6-32 on page 149.


Create VMFS Datastore

1 Datastore Name and Size
2 Storage System Selection
3 Host Connectivity
4 Review

Host Connectivity

Selected Storage System: vvolsftw-cab
Username: ibmadmin

Host Name on Storage System	Defined in Storage System
vvolsftw-14.ssd.hursley.ibm.com	Online
vvolsftw-15.ssd.hursley.ibm.com	Online

Figure 6-32 Create datastore: Assessing the host connectivity between vSphere and Storage Virtualize

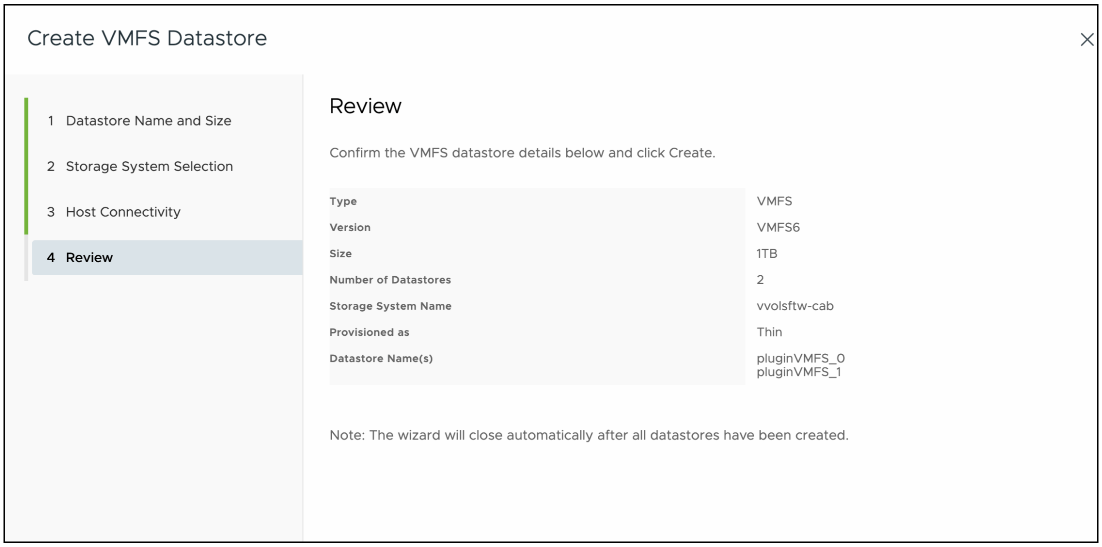
Note: The number of hosts in the vSphere cluster and the storage system host cluster must match before you can continue creating the datastores.

The review page shows the selections made and lists a summary of the defined parameters.

4. Review the summary information and click **Create**.

   A progress bar shows that status as the plug-in creates and maps volumes on the storage system and creates the datastore(s).

   The time it takes for the process to finish depends on the vSphere environment or the storage system configuration. See Figure 6-33.


Create VMFS Datastore

1 Datastore Name and Size
2 Storage System Selection
3 Host Connectivity
4 Review

Review

Confirm the VMFS datastore details below and click Create.

Type	VMFS
Version	VMFS6
Size	1TB
Number of Datastores	2
Storage System Name	vvolsftw-cab
Provisioned as	Thin
Datastore Name(s)	pluginVMFS_0 pluginVMFS_1

Note: The wizard will close automatically after all datastores have been created.

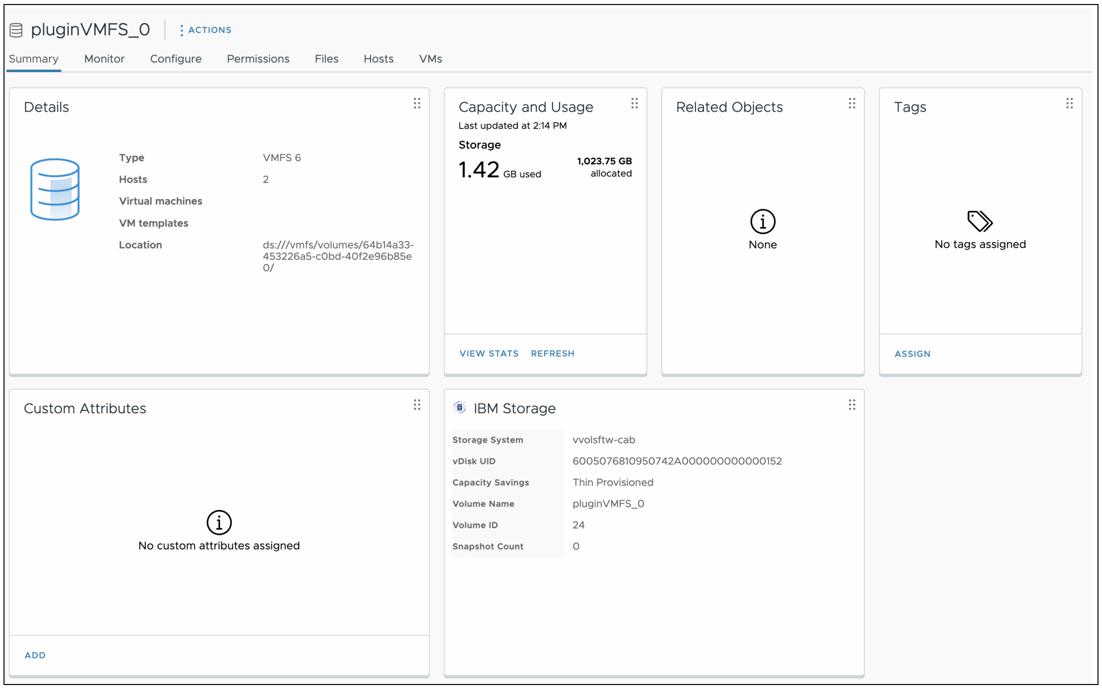
Figure 6-33 Create datastore: Review the details for the datastore workflow

6.6.2 Summary panel

You can use the plug-in to view vSphere Client objects that can be managed and modified by the plug-in. The windows that open provide further insight into the object's representation on registered storage systems.

The datastore summary card can be found on the summary tab of the datastore. Navigate to the IBM Storage panel by scrolling down the page. See Figure 6-34.

> **Tip:** The panel can be moved to another location by dragging and dropping the card. This action changes the layout, and saves the layout for the next time you navigate to this view.



Details

Type	VMFS 6
Hosts	2
Virtual machines	
VM templates	
Location	ds:///vmfs/volumes/64b14a33-453226a5-c0bd-40f2e96b85e0/

Capacity and Usage
Last updated at 2:14 PM
Storage
1.42 GB used
1,023.75 GB allocated

Related Objects
None

Tags
No tags assigned

Custom Attributes
No custom attributes assigned

IBM Storage

Storage System	vvolsftw-cab
vDisk UID	6005076810950742A000000000000152
Capacity Savings	Thin Provisioned
Volume Name	pluginVMFS_0
Volume ID	24
Snapshot Count	0

Figure 6-34 Managed datastore summary panel

The table in this view shows information that can be used to access characteristics of the datastore's representation on the storage system without accessing the IBM Storage Virtualize GUI. Following vSphere best practices, each datastore is created with a single underlying volume, the UID, name, and ID can all be used to determine the specific volume on the storage system.

By default, during the create datastore workflow, each volume is created as a thin provisioned volume, unless the registered pool has a provisioning policy specifying thick-provisioned. In which case, the volume will have no capacity savings. To read more about capacity savings go to 6.9.3, “Provisioning policies” on page 165.

If the volume is part of a volume on the storage system, the volume group name is also listed. This is useful when dealing with snapshots. The snapshot count field can also be used to identify datastores with the snapshots associated to them. To see how this information can be useful when creating a new datastore from a snapshot, see 6.6.5, “Creating a new datastore from a snapshot” on page 153.

6.6.3 Expanding a datastore

Expanding a datastore automates the expansion of the underlying volume on the storage system, the rescanning of any connected ESXi server's HBA's, and the datastore capacity increase within vSphere in one action.

To expand a datastore:

1. Right-click the datastore that you want to expand or navigate to the datastore and select the actions menu. Select **IBM Storage** → **Expand VMFS Datastore**. See Figure 6-35.

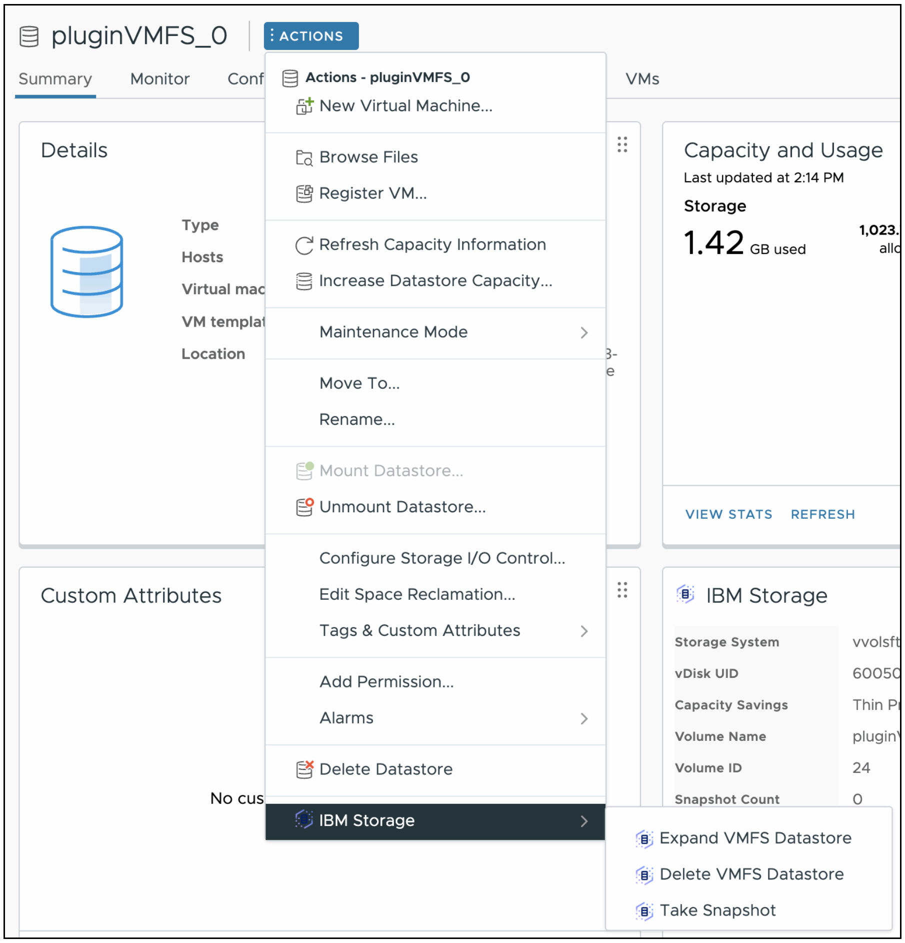
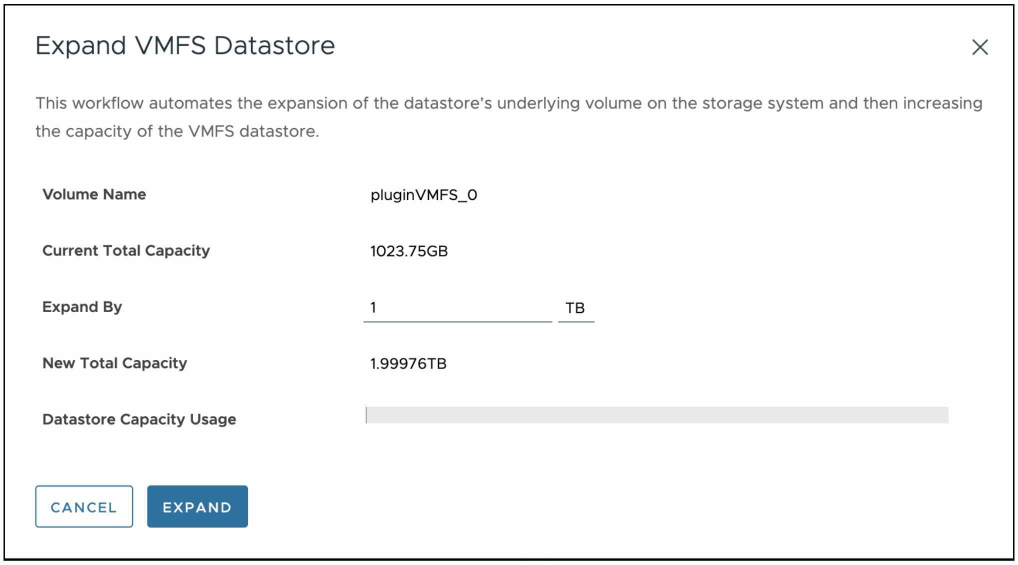


Figure 6-35 Datastore actions entry point

A window opens within the vSphere UI (Figure 6-36 on page 152) that shows the following information:

- Name of the selected datastore
- Current total capacity of the datastore
- New total capacity after expanding



Expand VMFS Datastore

This workflow automates the expansion of the datastore's underlying volume on the storage system and then increasing the capacity of the VMFS datastore.

Volume Name	pluginVMFS_0
Current Total Capacity	1023.75GB
Expand By	1 TB
New Total Capacity	1.99976TB
Datastore Capacity Usage	

Figure 6-36 Expand datastore modal

enter the amount to expand the datastore. There is also an entry field to enter the amount to expand the datastore by.

2. Declare the number value to expand the datastore by in the **Expand By** field, then select either **GB** or **TB** by selecting **TB** to open drop-down menu.

   The Datastore Capacity Usage bar changes as you enter new values to show how much of the datastore will be used after the datastore is expanded.

3. Click **Expand**. The plug-in expands the datastore by doing the following actions:
   - Expand the capacity of the volume on the storage system.
   - Rescan the storage of the hosts mounted to the datastore.
   - Expand the datastore to fill the capacity of the volume presented.

During expansion, a plug-in specific recent task shows that the attempt to expand the volume has happened. Errors are listed in the details column.

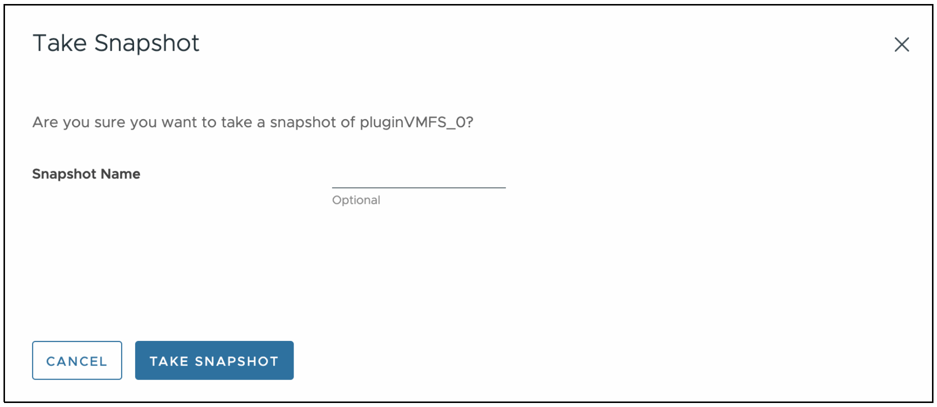
6.6.4 Datastore snapshots

As of this writing, the most recent version of the plug-in supports taking manual snapshots directly from a selected datastore using Volume Group Snapshots.

> **Note:** Volume Group Snapshots are only available on storage systems on a minimum code level of 8.5.1.0. Platforms FlashSystem 5015, FlashSystem 5035, FlashSystem 5035 and FlashSystem 5045 do not support this feature.

You can take a volume group snapshot by using the plug-in:

1. Navigate to a datastore and click **Actions** (or right-click the datastore) and select **IBM Storage** → **Take Snapshot** action.


Take Snapshot

Are you sure you want to take a snapshot of pluginVMFS_0?

Snapshot Name

Optional

Figure 6-37 Take snapshot modal

2. You can name the snapshot to support a naming convention or to help you identify the snapshot more easily. By default, the name follows the standard snapshot naming convention.
3. Click the **Take Snapshot** button.

   After clicking **Take Snapshot**, a volume group is created, the datastore's underlying volume is put into this newly created volume group and a snapshot is taken from the volume group level. If the volume is already a member of a volume group, the snapshot is taken of the existing volume group and a new one is not created.
4. Monitor the recent tasks to ensure completion of the Take Snapshot task. Any errors are displayed in the details column.

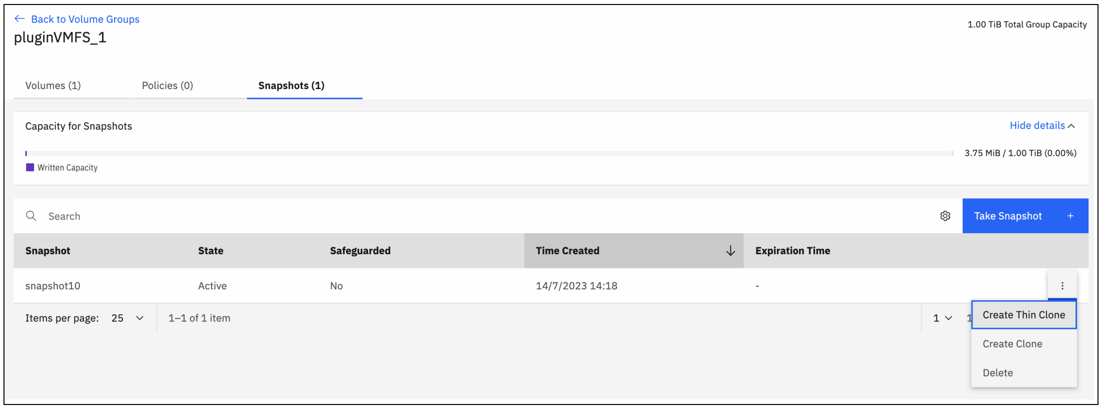
6.6.5 Creating a new datastore from a snapshot

In Version 1.1 of the plug-in, creating a new datastore from an existing snapshot is not automated. However, you can use the IBM Plugin Datastore Summary and Cluster Configure panels to find important information to identify the storage system and volume group name of which the underlying volume is a member.

Perform the following steps to create a new datastore from an existing snapshot:

> **Note:** These actions are done from the Storage Virtualize GUI, not from the plug-in.

1. Identify the storage system and volume group of the volume of the datastore. Click the **3 dots** on the far right side of the row of the snapshot that you are cloning.



← Back to Volume Groups

pluginVMFS_1

1.00 TiB Total Group Capacity

Volumes (1) Policies (0) **Snapshots (1)**

Capacity for Snapshots

Hide details ^

3.75 MiB / 1.00 TiB (0.00%)

■ Written Capacity

Search

Take Snapshot +

Snapshot	State	Safeguarded	Time Created ↓	Expiration Time
snapshot10	Active	No	14/7/2023 14:18	-

Items per page: 25 ⌄ 1–1 of 1 item

Create Thin Clone

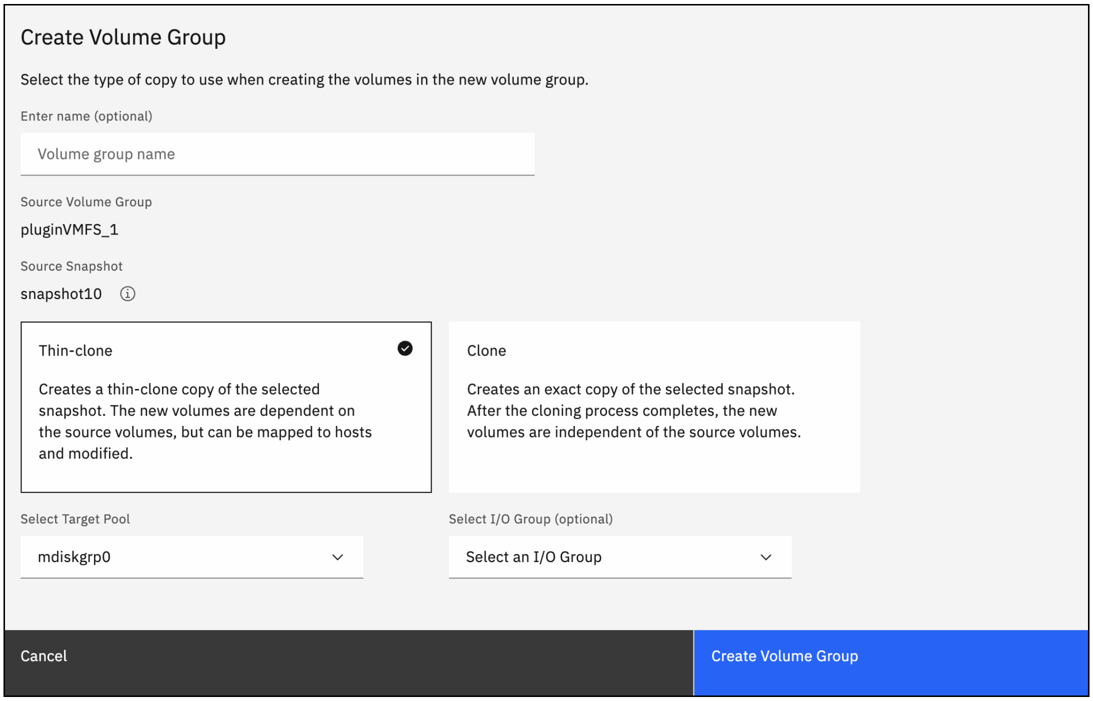
Create Clone

Delete

Figure 6-38 Storage virtualize, clone/thin clone action point

Tip: You can edit the columns that are shown in the storage system's GUI by clicking the cog icon to the left of the **Take Snapshot** button. This additional information might help you make a more informed decision about which snapshot you want to restore if there are multiple snapshots in a volume group.

2. In the Create Volume Group panel, take a Clone or Thin Clone of the volume. See Figure 6-39.



Create Volume Group

Select the type of copy to use when creating the volumes in the new volume group.

Enter name (optional)

Volume group name

Source Volume Group

pluginVMFS_1

Source Snapshot

snapshot10 ⓘ

Thin-clone ●

Creates a thin-clone copy of the selected snapshot. The new volumes are dependent on the source volumes, but can be mapped to hosts and modified.

Clone

Creates an exact copy of the selected snapshot. After the cloning process completes, the new volumes are independent of the source volumes.

Select Target Pool

mdiskgrp0 ⌄

Select I/O Group (optional)

Select an I/O Group ⌄

Cancel

Create Volume Group

Figure 6-39 Creating a new volume group from a thin clone/clone

A clone creates a volume that is independent from its source after all the required data is copied. A thin clone keeps the differences between the source volume and the clone and is always dependent on the source volume. See Figure 6-40 on page 155.

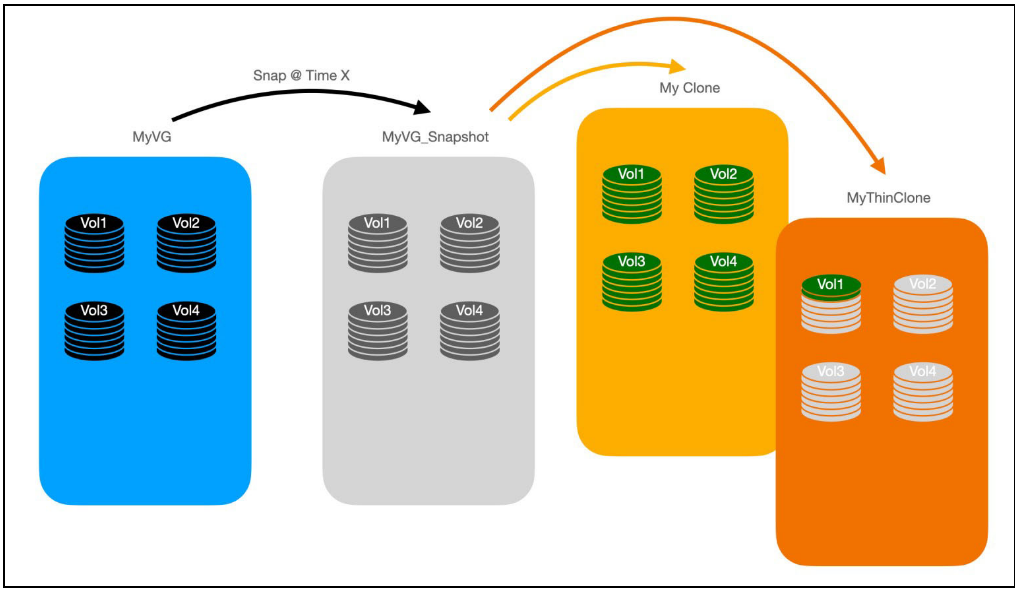


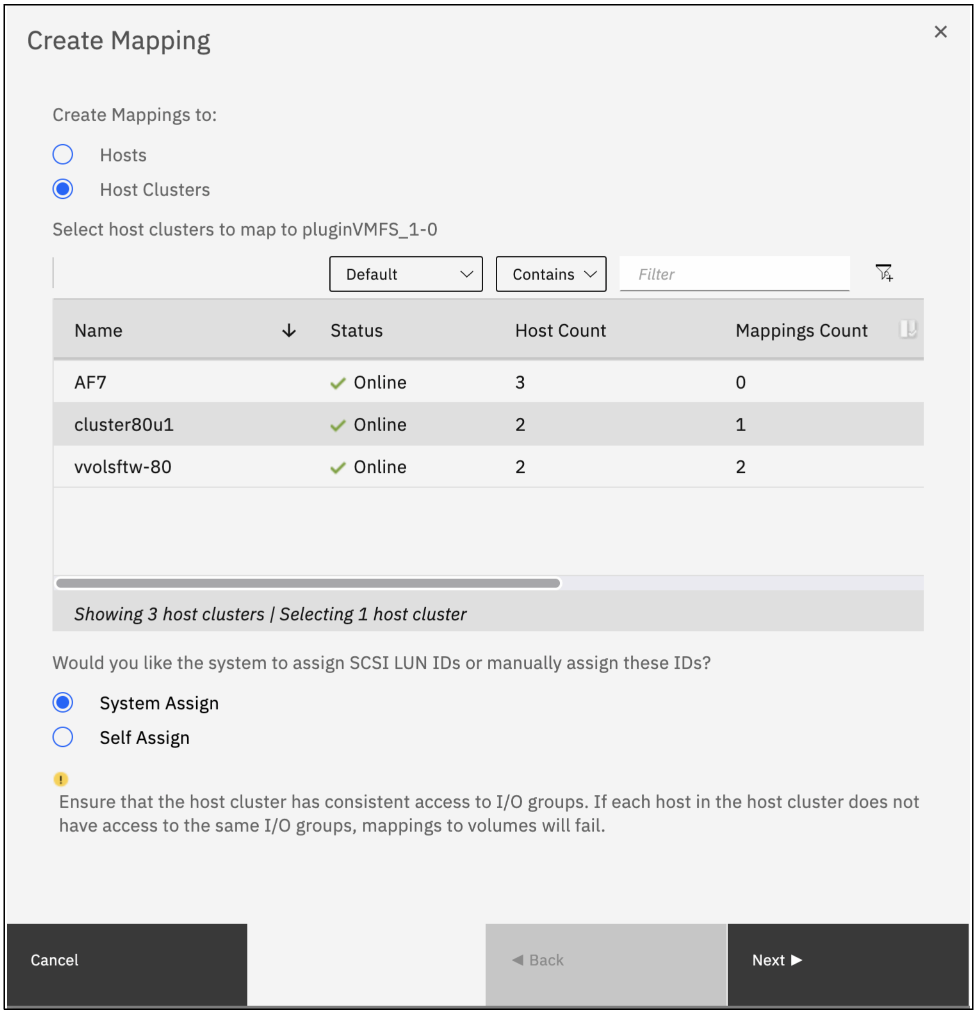
Figure 6-40 Visualization of the difference between a clone and a thin clone

A new volume group would have been made with a copy of the volume inside. By default, the name of the volume group is the source volume group name followed by '-N'. Where N is the number of clones taken from the source.

3. Map the new volume to the hosts or host cluster by navigating to the new volume group, and right-clicking the volume and select **Map to Host or Host Cluster**. See Figure 6-41 on page 156

> **Tip:** To identify the hosts or host clusters that are correctly configured between the vSphere and Storage Virtualize environments, use the vSphere cluster to create the new datastore and select **Configure tab** → **IBM Storage** → **Host Connections** and expand the storage system's details.

4. From the vSphere Client, rescan the storage for the vSphere Cluster. See Figure 6-42 on page 156.



Create Mapping

Create Mappings to:

○ Hosts

● Host Clusters

Select host clusters to map to pluginVMFS_1-0

Name	Status	Host Count	Mappings Count
AF7	✓ Online	3	0
cluster80u1	✓ Online	2	1
vvolsftw-80	✓ Online	2	2

Showing 3 host clusters | Selecting 1 host cluster

Would you like the system to assign SCSI LUN IDs or manually assign these IDs?

● System Assign

○ Self Assign

Ensure that the host cluster has consistent access to I/O groups. If each host in the host cluster does not have access to the same I/O groups, mappings to volumes will fail.

Figure 6-41 Create Mapping

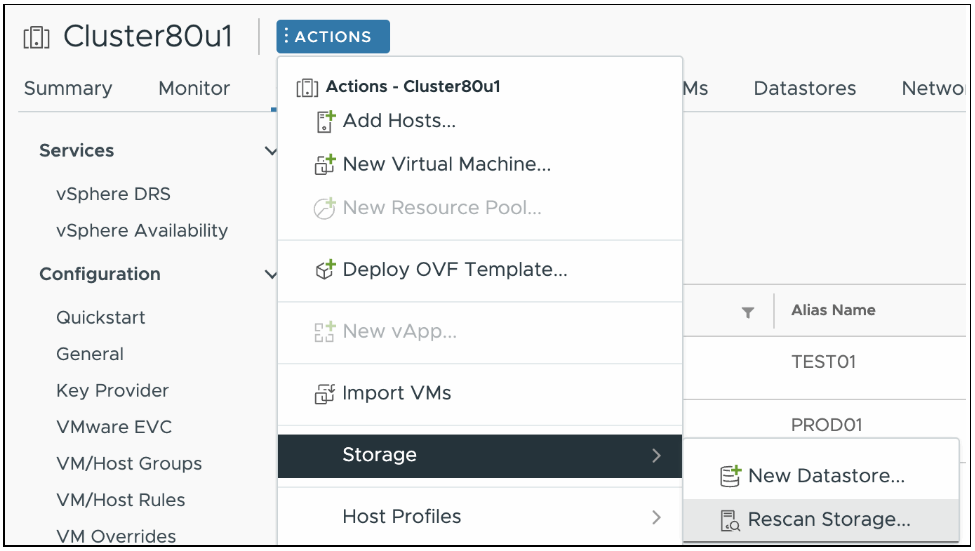
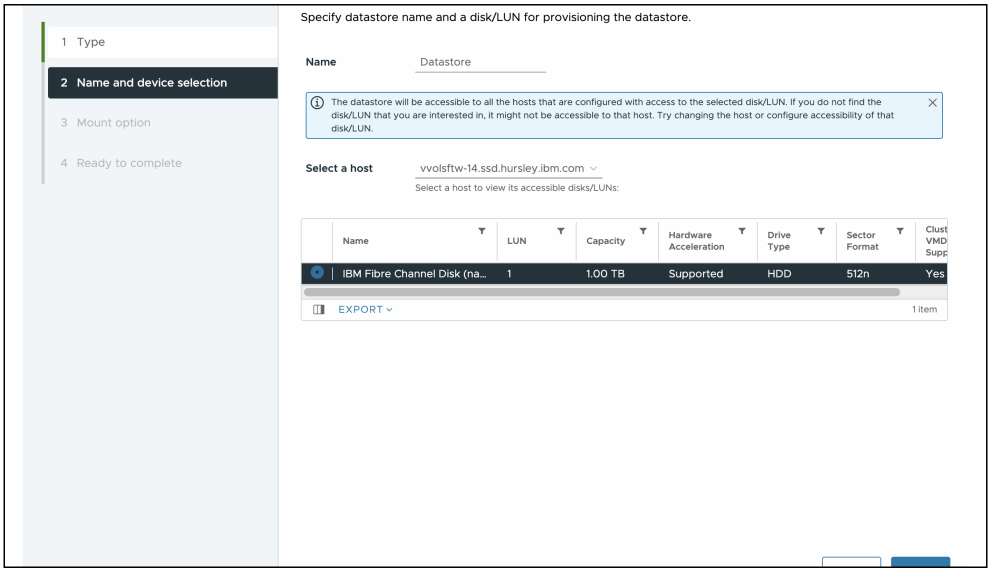


Figure 6-42 Rescan storage in vSphere

5. Using vSphere's workflow, follow the steps to create a new datastore. Select the disk/LUN of the cloned volume. If you cannot see the cloned volume, rescan the storage. See Figure 6-43.



Specify datastore name and a disk/LUN for provisioning the datastore.

Name: Datastore

The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN.

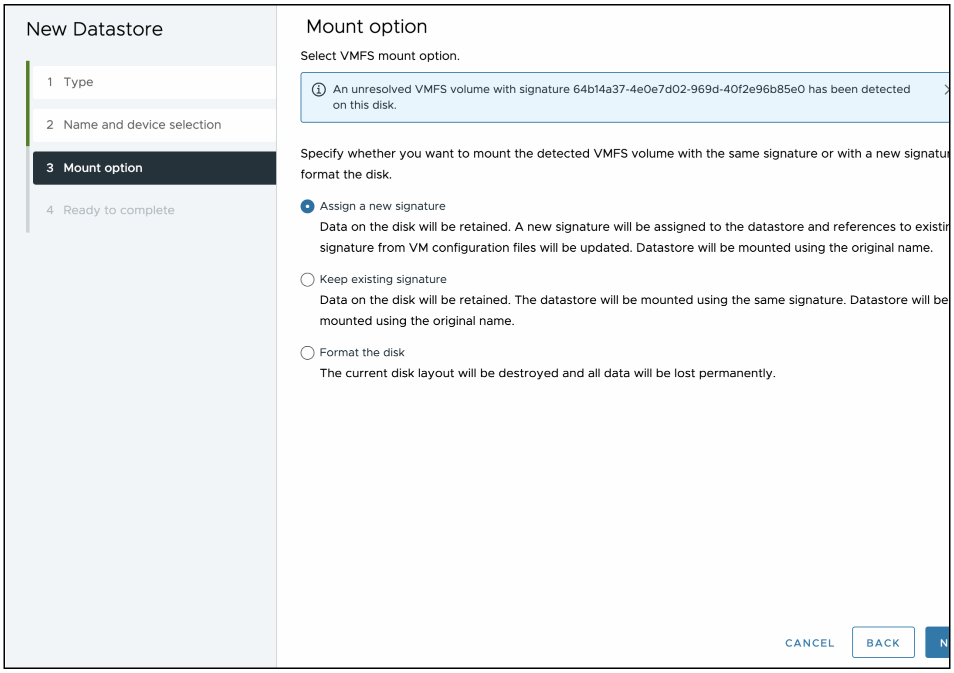
Select a host: vvolsftw-14.ssd.hursley.ibm.com

Select a host to view its accessible disks/LUNs:

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Clust VMD Supp
●	IBM Fibre Channel Disk (na...	1	1.00 TB	Supported	HDD	512n	Yes

Figure 6-43 New datastore: Find a newly created volume to provision the datastore to

6. Assign a new signature to the datastore. See Figure 6-44.



Mount option

Select VMFS mount option.

An unresolved VMFS volume with signature 64b14a37-4e0e7d02-969d-40f2e96b85e0 has been detected on this disk.

Specify whether you want to mount the detected VMFS volume with the same signature or with a new signatur format the disk.

● Assign a new signature
Data on the disk will be retained. A new signature will be assigned to the datastore and references to existir signature from VM configuration files will be updated. Datastore will be mounted using the original name.

○ Keep existing signature
Data on the disk will be retained. The datastore will be mounted using the same signature. Datastore will be mounted using the original name.

○ Format the disk
The current disk layout will be destroyed and all data will be lost permanently.

Figure 6-44 New datastore: Assign a new signature to the datastore

7. Review the information and click **Finish** on the wizard to create the new datastore.

   The datastore is set up correctly using a restored snapshot of another datastore. Use the dashboard to sync the plug-in database with the manually created datastore so that you can use the plug-in to manage this datastore.

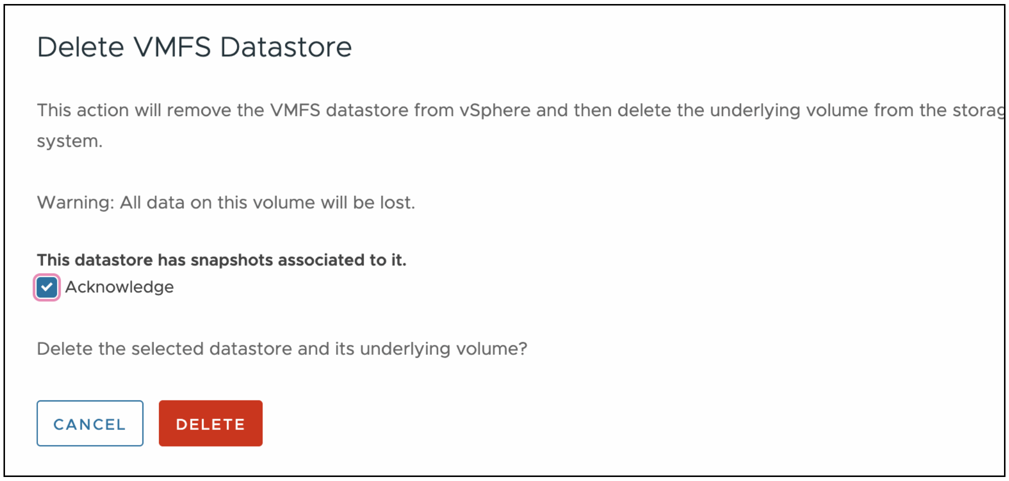
6.6.6 Deleting a datastore

Deleting a datastore removes a datastore from the vSphere client, deletes the volume on the storage system, and unmaps the volume from the host. A datastore can be deleted only if no VMs are associated with the datastore.

Perform the following steps to delete a datastore:

1. Right-click the datastore you want to delete, or navigate to the datastore and select the **Actions** menu. At the bottom of the menu, there is an **IBM Storage** option, select **Delete VMFS Datastore**.
2. The Delete VMFS Datastore window opens and asks you to confirm that you want to o delete the datastore.

   If there are any VMs on the datastore, the **Delete** button is disabled, and a warning is posted. To continue deleting the datastore either migrate any VMs to a different datastore by using Storage vMotion or delete the VMs from the vSphere client inventory. See Figure 6-45.



Delete VMFS Datastore

This action will remove the VMFS datastore from vSphere and then delete the underlying volume from the storag system.

Warning: All data on this volume will be lost.

This datastore has snapshots associated to it.

☑ Acknowledge

Delete the selected datastore and its underlying volume?

Figure 6-45 Deleting a managed datastore with snapshots

   If any snapshots are associated with the datastore, you are asked to acknowledge it before proceeding with the deletion. If you click **Delete,** the volume state changes to *deleting* on the storage system, which means the volume is not visible in the Storage Virtualize GUI. However, the volume is visible from the CLI. When you view the volume on the CLI, the name is changed by attaching a prefix of `del_` and the time of deletion as a suffix.

Note: When a volume is in the *deleting* state, it is not removed from the storage system until all associated snapshots are also deleted.

   Deleting the datastore through the plug-in does the following actions:

   – Unmount the VMFS volume on each host associated with the datastore
   – Remove the volume on the storage system
   – Rescan the storage on each host associated with the datastore

   The rescan removes the datastore from the vSphere client. During this process, a new task is listed in the vSphere client that shows whether the volume on the storage system was deleted successfully. If the volume on the storage system has volume protection enabled, then the datastore is left in an inaccessible state, with the recent task displaying the error returned from the storage system.

Note: To remove this inaccessible datastore, the storage admin will need to remove the volume from the storage system after the volume protection period expires. Then, each host should run a rescan to remove the datastore from the vSphere client.

6.7 Host panels

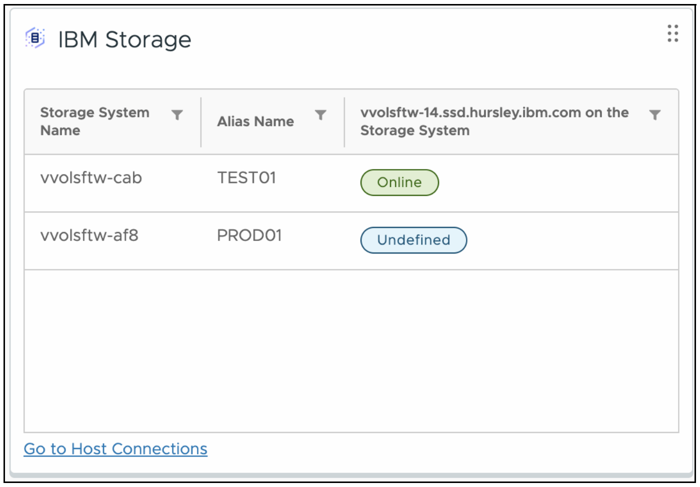
This section includes a description of the host panels.

6.7.1 Summary panel

You can use the plug-in to view the vSphere Client objects that can be managed or manipulated by the plug-in. You can also view the object's representation on registered storage systems.

The host summary window can be found on the summary tab of the ESX host object. Scroll down to view the IBM Storage panel. See Figure 6-46.

Tip: The panel can be moved to another location by dragging and dropping it. This action changes the layout and is saved for the next time the user navigates to this view.



Storage System Name	Alias Name	vvolsftw-14.ssd.hursley.ibm.com on the Storage System
vvolsftw-cab	TEST01	Online
vvolsftw-af8	PROD01	Undefined

Figure 6-46 Host summary card

The table in this view shows how the selected ESX host is represented on each of the registered storage systems. If the plug-in finds a match for the ESX host, the latest status of the host on the storage system is listed. However, if the plug-in does not find a match, the status is Undefined. If the plug-in finds a match for the ESX host, the latest status of the host on the storage system is listed. However, if the plug-in does not find a match, the status is Undefined.

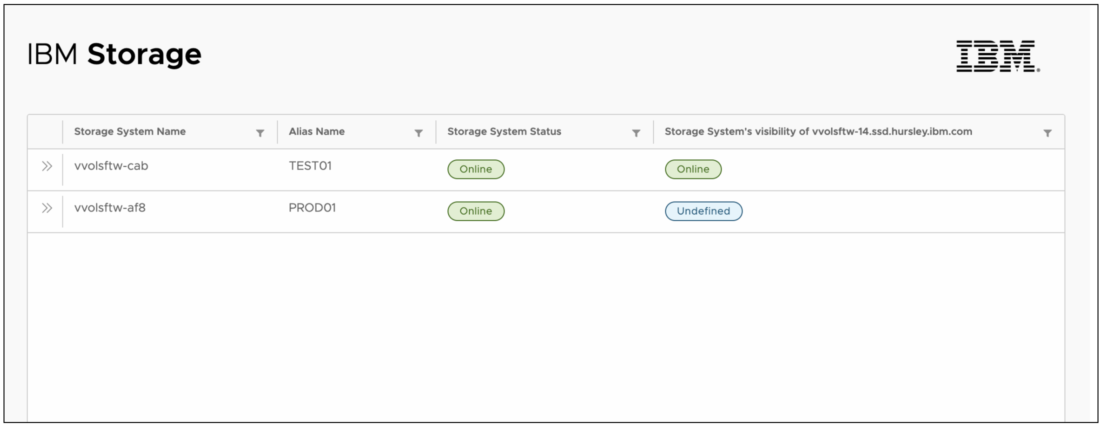
If a host is in an Undefined state, you cannot create datastores by using the vSphere Cluster that the ESX host is a member of, and errors are listed in other UI panels. It is possible to resolve this error using the plug-in. See 6.7.3, “Creating a new host” on page 161 to find out how to create a host.

> **Note:** This might mean that information is outdated in this summary view. To refresh the database and get a live view of the hosts representation and for further details, click the **Go to Host Connections** link, which will take you to the Host Configure Panel.

6.7.2 Configure panel

The Host Configure panel provides further insights into defined hosts, and it is also the entry point to create an undefined host. For more information, see 6.7.3, “Creating a new host” on page 161.

> **Note:** The time it takes for the view to update depends on both your vSphere and registered storage system's configuration.



IBM **Storage**

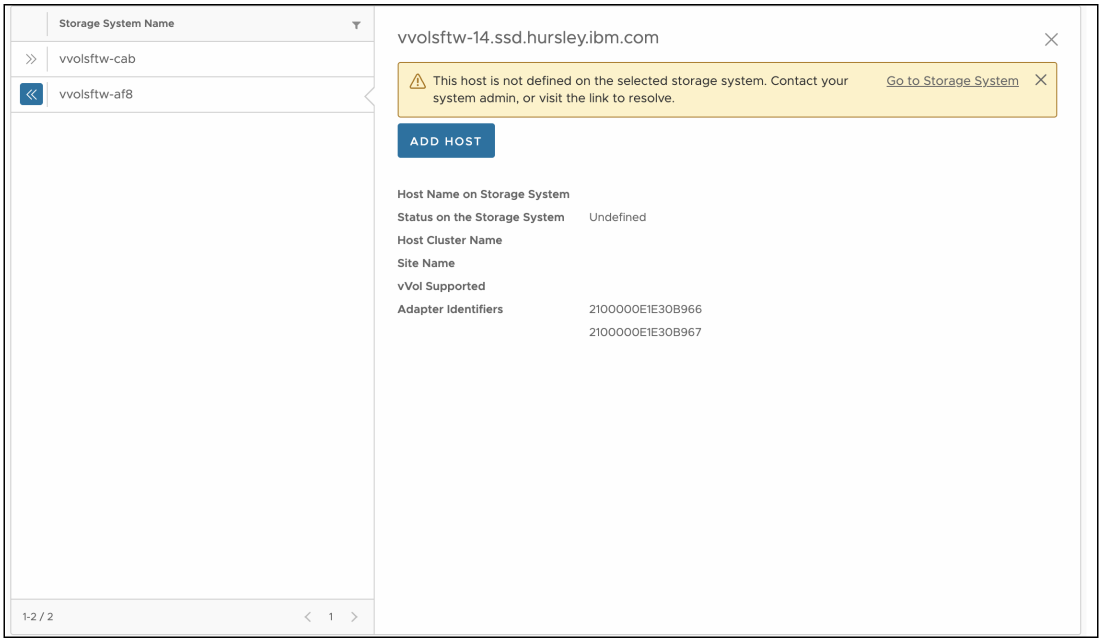
	Storage System Name	Alias Name	Storage System Status	Storage System's visibility of vvolsftw-14.ssd.hursley.ibm.com
»	vvolsftw-cab	TEST01	Online	Online
»	vvolsftw-af8	PROD01	Online	Undefined

Figure 6-47 Host configure panel

The datagrid by default shows details about each of the registered storage systems and the visibility of the ESX host on the associated system. Similarly, to the host summary view, if no match is found on the storage system the visibility Undefined. Otherwise, the live status of the host is presented with a status label. Each of the columns in the datagrid can be filtered and sorted alphabetically by clicking the column header.

> **Tip:** To change the columns that are shown in the grid, click the column toggle icon in the lower left of the datagrid.

To view more details about a defined storage system or to access the create host workflow on an undefined host, toggle the detail caret icon on the left side of each storage system name. See Figure 6-48 on page 161.



vvolsftw-14.ssd.hursley.ibm.com

This host is not defined on the selected storage system. Contact your system admin, or visit the link to resolve.

Host Name on Storage System
Status on the Storage System Undefined
Host Cluster Name
Site Name
vVol Supported
Adapter Identifiers 2100000E1E30B966
2100000E1E30B967

Figure 6-48 Expanded host details of an undefined host

In this view, details are presented about the host. The details are taken directly from the storage system. The adapter identifiers are taken from the ESX Hosts Storage Adapters view and are always visible whether the host is defined. If the host is not defined, a warning message is displayed that provides a link to the system's IP/FQDN. Clicking the link opens a new tab and allows the user to create the host by using the storage system's GUI. Alternatively, you can click the **Add Host** button to start the create host workflow. See 6.7.3, “Creating a new host” on page 161 for how to proceed with this workflow.

6.7.3 Creating a new host

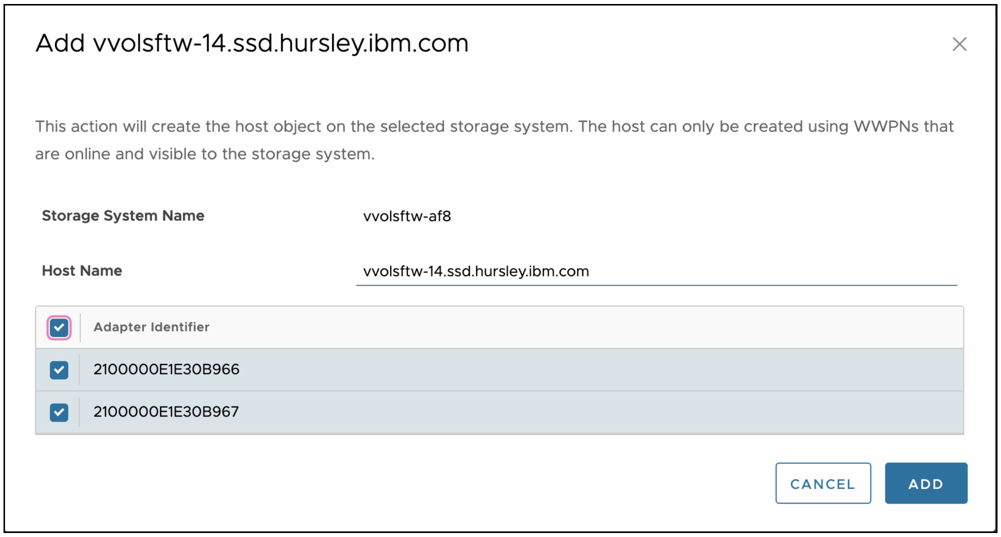
It is possible to directly create a new host object on a registered storage system. The new host object must have a corresponding ESX host with storage adapters configured. When the ESX host is represented on the storage system, the workflow to create a new host is no longer available.

> **Note:** To enable support for vSphere Virtual Volumes, hosts are created with a vVol host type by default.
>
> You cannot manage host clusters in this workflow. If you are using host clusters on the storage system, select the link to the GUI and add the host into a host cluster. If you do not ensure that vSphere clusters and host clusters are configured in the same way, then you cannot create datastores, and some UI panels present warnings.
>
> Ensure that fibre channel zoning has been completed, so host FC initiators can communicate with the FC target ports on the storage system. This is a prerequisite for creating a new host

To create a new host object:

1. By default, the vSphere ESX host name is used to pre-fill the hostname field. However, this can be changed if necessary.

2. Adapters that are visible to the selected storage system are selectable in the GUI. Select at least 1 adapter to use when you create the host.
3. Click **Add** to issue the command to create the host object. See Figure 6-49.



Add vvolsftw-14.ssd.hursley.ibm.com

This action will create the host object on the selected storage system. The host can only be created using WWPNs that are online and visible to the storage system.

Storage System Name	vvolsftw-af8
Host Name	vvolsftw-14.ssd.hursley.ibm.com

☑	Adapter Identifier
☑	2100000E1E30B966
☑	2100000E1E30B967

Figure 6-49   Create host modal with selected adapter identifiers

The Host Configure panel is refreshed as the newly created host object is added to the plug-in's database.

4. Monitor the recent tasks to ensure completion of the Create Host task. Any errors are displayed in the details column.

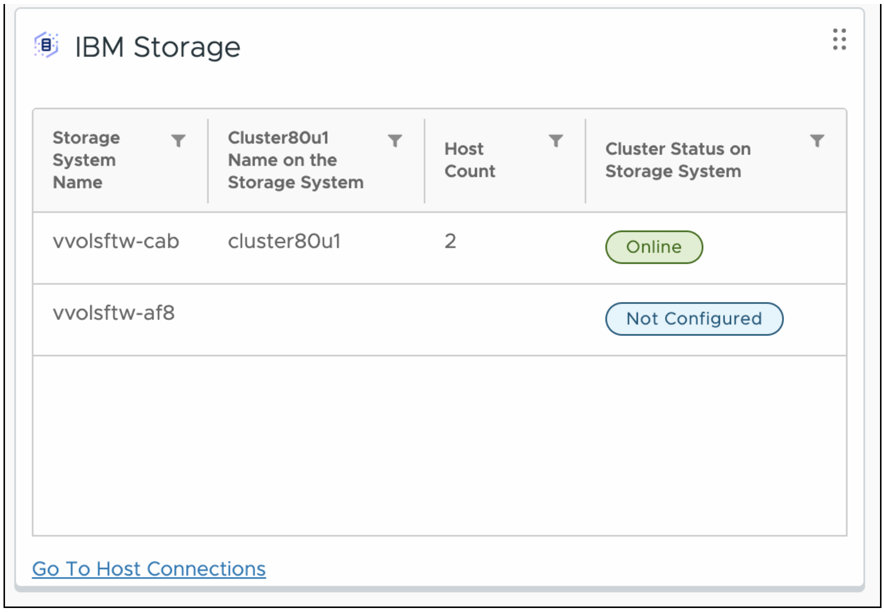
6.8 Cluster panels

This section includes a discussion of the host panels.

6.8.1 Summary panel

The cluster summary card is located within the summary tab of a vSphere cluster.

> **Tip:** The IBM Storage panel can be moved to another location within the page by dragging and dropping the card. The change is saved, so the storage panel is in the saved location when the summary page is opened.



IBM Storage

Storage System Name	Cluster80u1 Name on the Storage System	Host Count	Cluster Status on Storage System
vvolsftw-cab	cluster80u1	2	Online
vvolsftw-af8			Not Configured

Go To Host Connections

Figure 6-50 Cluster summary card

The table displayed within the IBM Storage panel shows whether the cluster is configured on each of the IBM storage systems registered to the plug-in as of the last database write. If the cluster is found within the database and on the storage system, the live status of the cluster is shown. However, if the cluster is not present in both environments it is labeled as **Not Configured**.

Note: This might mean that information in the cluster summary panel is out of date. For more information about updating the cluster information and about how to view the current state of a cluster, see 6.7.2, “Configure panel” on page 160.

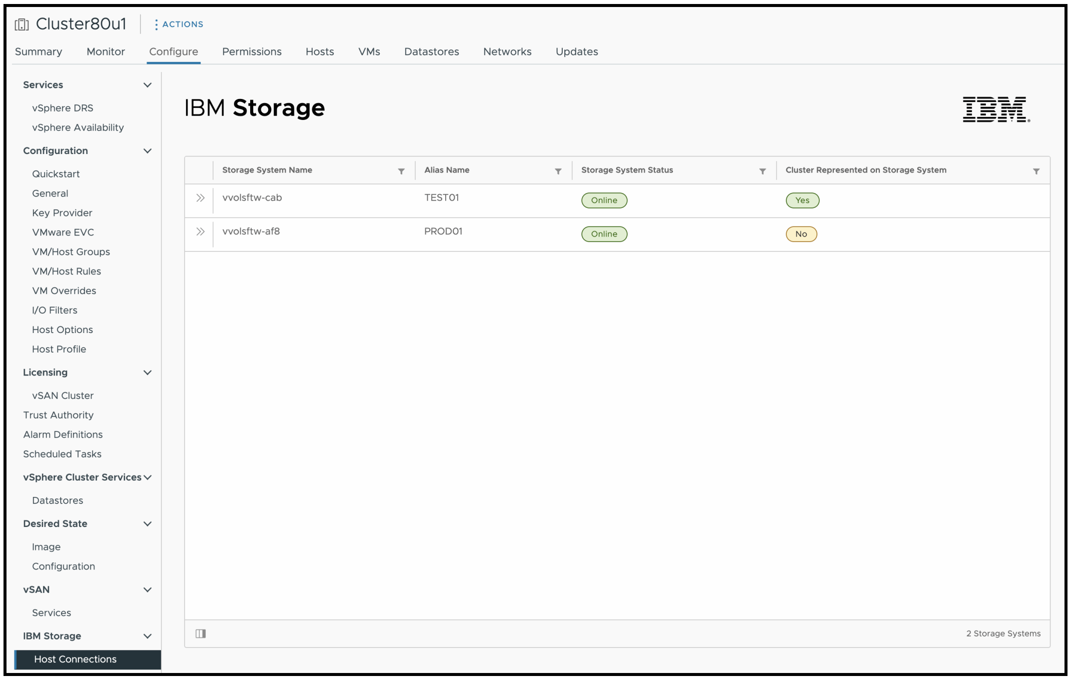
If a vSphere Cluster is not represented in a storage system, you cannot use that system to create a datastore.

The **Go To Host Connections** link will automatically redirect to the plug-in's IBM Storage page under the cluster's configure page. For more information, see 6.7.2, “Configure panel” on page 160.

6.8.2 Configuration panel

The IBM Storage Cluster Configure panel provides an up-to-date view of vSphere clusters and the ESX hosts that are part of the cluster. This view reads the database for the cluster. If a match is not found, there is an attempt to discover the corresponding hostcluster on each registered storage system. If a manual match is found, the database is updated.

Tip: It can take some time for the panel to load, depending on the number of hosts in the cluster, and the storage system configuration.

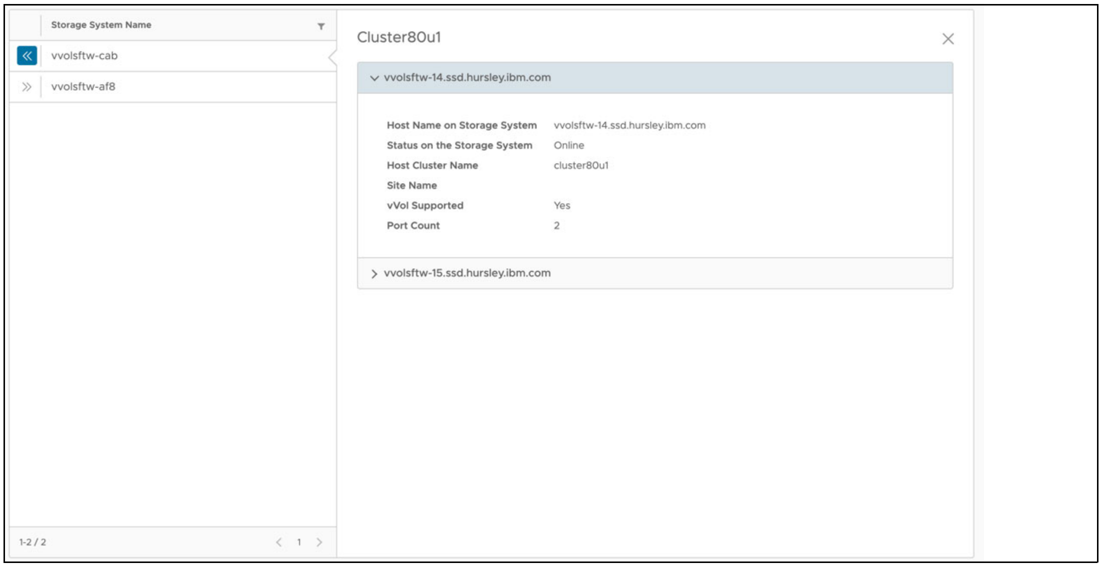


Storage System Name	Alias Name	Storage System Status	Cluster Represented on Storage System
vvolsftw-cab	TEST01	Online	Yes
vvolsftw-af8	PROD01	Online	No

2 Storage Systems

Figure 6-51 Cluster configure panel and entry point

By default, the table in this panel shows the storage system name, the storage system status, and whether the cluster is represented on the storage system. This can be expanded to show more details about each ESX host that belong to the vSphere Cluster and the status of the cluster on the storage system. See Figure 6-52.


Storage System Name
vvolsftw-cab
vvolsftw-af8
1-2 / 2
1
Cluster80u1
vvolsftw-14.ssd.hursley.ibm.com
vvolsftw-15.ssd.hursley.ibm.com

Host Name on Storage System vvolsftw-14.ssd.hursley.ibm.com
Status on the Storage System Online
Host Cluster Name cluster80u1
Site Name
vVol Supported Yes
Port Count 2

Figure 6-52 Expanded vSphere Cluster example

If there are differences between the vSphere Cluster or ESX hosts and the registered storage system environment, then a mismatch error is displayed when the row is expanded. You can directly access the storage system's GUI by using the link.

Note: If the storage system hosts are not in a host cluster, then the cluster is not represented, but the label is green, which indicates success because the host clusters are not enforced throughout the plug-in.

6.9 Enforcing practical usage behavior

As of this writing, the most recent version of the plug-in supports multiple Storage Virtualize features that can assist with the management of resource allocation and reduce the chance that a user can do harm on a storage system.

6.9.1 Child pools

A child pool is a subset of usable capacity that is taken from a defined parent pool. This option might be useful to include if only a portion of capacity is desired to be used by the vSphere environment.

Child pools can be assigned to an ownership group to further restrict access. See 6.9.2, “Ownership groups” on page 165 for more information.

Child pools are represented in the plug-in as indented from their parent to highlight that they are children. However, the view can be different in combination with ownership groups because only the children are visible to the authenticated user.

6.9.2 Ownership groups

An ownership group is used to restrict the access of certain resources to users within only that group. A user in an ownership group cannot manage any resources outside of the ownership group. Therefore, it is important that the ownership group is configured properly between vSphere and Storage Virtualize.

When authenticating with a user that is part of an ownership group to register a storage system, only the visible child pools are displayed and selectable.

When you create a datastore, if the user associated to the selected storage system is not in the same ownership group as the defined hosts, an ownership error is displayed. To resolve the error, open the management GUI using the link and ensure that the hosts are part of the same ownership group.

6.9.3 Provisioning policies

Provisioning policies are used to define behavior for allocating capacity on a pool level. Informational labels are provided throughout the plug-in that indicate the type of capacity savings that are used for different objects.

All volumes created in a pool with a provisioning policy are automatically created with the same provisioning policy assigned. This option can be useful if you want to define a consistent behavior between all objects that are created in a registered pool.

Volumes created through the plug-in are thin-provisioned by default. However, if the pool has a predefined provisioning policy, the plug-in uses the definitions in the policy for the pool.

6.9.4 Volume protection

Volume protection prevents a user from deleting a volume that has had recent I/O activity. Volume group protection can be enabled on a system or pool level. If volume protection is enabled, even forcing the deletion of a volume fails if the period has not expired.

When you delete a datastore, the system displays an informational alert if volume protection is enabled on the underlying system. If the defined period has not elapsed since the last I/O activity, the underlying volume has had recent I/O activity within the volume protection time, the delete datastore action fails. To resolve this wait for the period to pass and try again.

6.10 Troubleshooting

This section includes a discussion of troubleshooting the plug-in configuration.

6.10.1 Collecting a snap

If you encounter an issue while using the plug-in, you can run the command **ibm-plugin snap** to capture the current state of the plug-in.

The command collects the current database, logs, plug-in config file and other files that can be useful for debugging the issue and places them in a single .tgz file, in the /tmp directory. When the snap is generated, you see a message, for example:

```
Snap file created at /tmp/snap.ibm-plugin.230718.173615.tgz
```

The snap can then be copied to a local machine by using **scp**. If your VM reboots before the snap is copied to a storage system, then the snap is lost and a new one must be taken.

6.10.2 Copying a snap to an IBM storage system

Another way to access the snap file is by copying it to an IBM storage system directly from the plug-in VM. After the snap file is copied to the storage system, it can be downloaded from the storage system using the web browser. It is recommended that you copy the snap to the /dumps directory of the storage system.

After the snap is on the storage system, it can be downloaded by doing the following:

1. Access the management interface of the IBM storage system by using the web browser and select **Settings** → **Support** → **Support Package**.
2. Select **Download Support Package** → **Download Existing Package**.
3. Filter the list of support files by the plug-in snap, for example, snap.ibm-plugin and click **Download** on the appropriate snap file.

6.10.3 Viewing the logs

Do the following steps to view the logs locally on your plug-in VM:

1. Run the command **cd /opt/persistent**
2. To list the log, run the command **ls | grep log**
3. Use **cat**, **vi** or **vim** to view the contents of the log files.

Note: The Linux command `less` is not installed by default. You can install it by using the command `tdnf install less` if you have internet connection on your plug-in VM.

6.10.4 vSphere task names being misreported

The IBM Storage Virtualize plug-in for vSphere includes some dedicated tasks that run on the vSphere client. The tasks detail progress and provide visibility of actions that happen against the registered storage systems.

In some circumstances, these tasks might be listed incorrectly in the vSphere client, displaying the task identifier, instead of the correct task name or task description. In some scenarios. these issues can be corrected by simply refreshing the browser or logging out of the vSphere client, and re-authenticating in a new window, if these do not resolve the issue see 6.10.5, “Restarting the vSphere Client Service in vCenter” on page 167.

6.10.5 Restarting the vSphere Client Service in vCenter

If vSphere tasks are not displayed correctly after starting a new browser session, you might have to restart the vSphere Client service for them to display correctly. You can restart the service by using the vCenter Server Appliance Management Interface (VAMI).

To restart the vSphere Client Service in the VAMI:

1. In a web browser, go to the VAMI on port **5480**:
   `https://<vCenter-FQDN-or-IP-address>:5480`
2. Log in as root. The root password is the password set when the vCenter server was deployed.
3. Select **Services**.
4. Select the service **VMware vSphere Client** and click **Restart**.

Note: The vSphere client is inaccessible for a few minutes while the VMware vSphere Client service restarts.

If a restart of the vSphere Client does not resolve the issue, a restart of the vCenter Server might be required.

6.10.6 Pinging the appliance

By default, the plug-in VM does not respond to ping (ICMP) requests because it is protected by a security policy that includes a firewall. The firewall drops all ping requests by default. However, it is possible to enable ping requests.

To enable ping requests :

1. Connect to the plug-in VM as root, through ssh or through the VM console within the vSphere client.
2. Run `iptables -A OUTPUT -p icmp -j ACCEPT`
3. Run `iptables -A INPUT -p icmp -j ACCEPT`

6.10.7 Changing the network configuration

If you want to change a static IP network configuration, you might have to do it manually. When you change the plug-in VM network settings, the plug-in might need to be re-registered to any registered vCenters. For more information about registering and unregistering the plug-in, see 6.3.2, “Registering and unregistering the plug-in” on page 134.

Use the following steps to update your static network configuration:

1. Go to the vSphere appliance on which the plug-in VM was deployed.
2. Log in and navigate to the plug-in VM within the inventory.
3. Open the web console from the VM summary page by clicking **Launch Web Console**.
4. Log in to the VM as root by using your credentials, which were set when the VM was deployed.
5. Edit the network config file found in `/etc/systemd/network/`. Typically, this file is called `10-gosc-eth0.network`. The file can be edited by using **`vi`** or **`vim`**.
6. In the editor, enter `i` to edit the contents of the file.
7. Change the appropriate values to the new values.
8. Exit and save the file by pressing the escape key and then typing **`:wq`**.
9. Apply the network changes by running **`systemctl restart systemd-networkd`**.

After completing this process, ensure that the VM can be reached with the new network settings.

7

IBM Storage Insights

This chapter describes IBM Storage Insights integration with VMware.

IBM Storage Insights is an IBM Cloud® software as a service (SaaS) offering that can help you monitor and optimize the storage resources in the system and across your data center.

IBM Storage Insights provides cognitive support capabilities, monitoring, and reporting for storage systems, switches and fabrics, and VMware vSphere hosts in a single dashboard.

IBM Storage Insights provides the following features:

- Enterprise monitoring dashboard
- Device event alerting
- Performance checking
- Capacity checking
- Service ticket processing
- Streamlined uploading of diagnostic data

This chapter includes the following sections:

- 7.1, “IBM Storage Insights editions” on page 170
- 7.2, “IBM Storage Insights architecture” on page 173
- 7.3, “IBM Storage Insights Monitoring” on page 174
- 7.4, “IBM Storage Insights VMware integration” on page 174

7.1 IBM Storage Insights editions

Two versions of IBM Storage Insights are available: IBM Storage Insights and IBM Storage Insights Pro (Table 7-1):

- IBM Storage Insights is available at no additional charge to owners of IBM block storage systems. IBM Storage Insights provides an environment overview, an integration into support processes, and shows you IBM analysis results.
- The IBM Storage Insights Pro capacity-based subscription version includes all IBM Storage Insights no-charge functions, plus more information, a longer history, and more capabilities through a monthly subscription.

Table 7-1 Different features of both versions

Resource management	Functions	IBM Storage Insights	IBM Storage Insights Pro (subscription)
Monitoring	Inventory management	IBM block storage, switches, fabrics, and VMware ESXi hosts	IBM and non-IBM block storage, file storage, object storage, switches, fabrics, and VMware ESXi hosts
	Logical configuration	Basic	Advanced
	Health	Call Home events	Call Home events
	Performance	► 3 storage system metrics: I/O rate, data rate, and response times aggregated for storage systems ► 4 switch metrics: port saturation, port congestion, port hardware errors, and port logical errors ► 3 host metrics: host I/O rate, host data rate, and host response time ► 3 virtual machine (VM) metrics: VM I/O rate, VM data rate, and VM response time	► 100+ metrics for storage systems and their components ► 40+ metrics for switches and related components ► 10+ metrics for hosts and related components ► 10+ metrics for VMs and related components

Resource management	Functions	IBM Storage Insights	IBM Storage Insights Pro (subscription)
Monitoring (cont.)	Capacity	► 4 metrics: used capacity, available capacity, total capacity, and compression savingsaggregated for storage systems ► 2 host metrics: storage area network (SAN) capacity and used SAN capacity ► 2 VM metrics: SAN capacity and used SAN capacity	► 25+ metrics for storage systems and their components ► 10+ metrics for hosts and related components ► 10+ metrics for VMs and related components
	Drill-down performance workflows to enable deep troubleshooting	No	Yes
	Explore virtualization relationships.	No	Yes
	Explore replication relationships.	No	Yes
	Retention of configuration and capacity data	Can view the previous 24 hours	2 years
	Retention of performance data	Can view the previous 24 hours	1 year
	Exporting performance data to a file	No	Yes
Service	Filter events to quickly isolate trouble spots.	Yes	Yes
	Hassle-free log collection	Yes	Yes
	Simplified ticketing	Yes	Yes
	Show active Problem Management Reports (PMRs) and ticket history.	Yes	Yes

Resource management	**Functions**	**IBM Storage Insights**	**IBM Storage Insights Pro (subscription)**
Reporting	Inventory, capacity, performance, and storage consumption reports	► Capacity reports for block storage systems and pools ► Inventory reports for block storage systems, switches, chassis, and switch ports	All reports
Alerting and Analytics	Predictive alerts	Yes	Yes
	Customizable, multi-conditional alerting, including alert policies	Yes	Yes
	Performance planning	No	Yes
	Capacity planning	No	Yes
	Business impact analysis (applications, departments, and groups)	No	Yes
	Optimize data placement with tiering.	No	Yes
	Optimize capacity with reclamation.	No	Yes
Security	ISO/IEC 27001 Information Security Management standards certified	Yes	Yes
Entitlements		No additional charge	Capacity-based subscription

Restriction: You must have a current warranty or maintenance agreement for the IBM block storage system to open tickets and send log packages.

IBM Storage Insights for IBM Spectrum Control

IBM Storage Insights for IBM Spectrum Control is an IBM Cloud service that can help you predict and prevent storage problems before they impact your business. It is complementary to IBM Spectrum Control.

As an on-premises application, IBM Spectrum Control does not send the metadata about monitored devices off-site, which is ideal for sites that do not want to open ports to the cloud. However, if your organization allows for communication between your local network and the cloud, you can use IBM Storage Insights for IBM Spectrum Control to support your IBM block storage.

IBM Storage Insights for IBM Spectrum Control is like IBM Storage Insights Pro in capability. IBM Storage Insights is available for no additional cost if you have an active license with a current subscription and support agreement for IBM Virtual Storage Center, IBM Spectrum Storage Suite, or any edition of IBM Spectrum Control.

7.2 IBM Storage Insights architecture

IBM Storage Insights provides a lightweight data collector that is deployed on a Linux, Windows, or IBM AIX server, or a guest in a VM, such as a VMware guest).

The data collector streams performance, capacity, asset, and configuration metadata to your IBM Cloud instance.

The metadata flows in one direction, that is, from your data center to IBM Cloud over HTTPS. In the IBM Cloud, your metadata is protected by physical, organizational, access, and security controls. IBM Storage Insights is ISO/IEC 27001 Information Security Management certified.

Figure 7-1 shows the architecture of the IBM Storage Insights application, the supported products, and the three main teams who can benefit from using the tool.

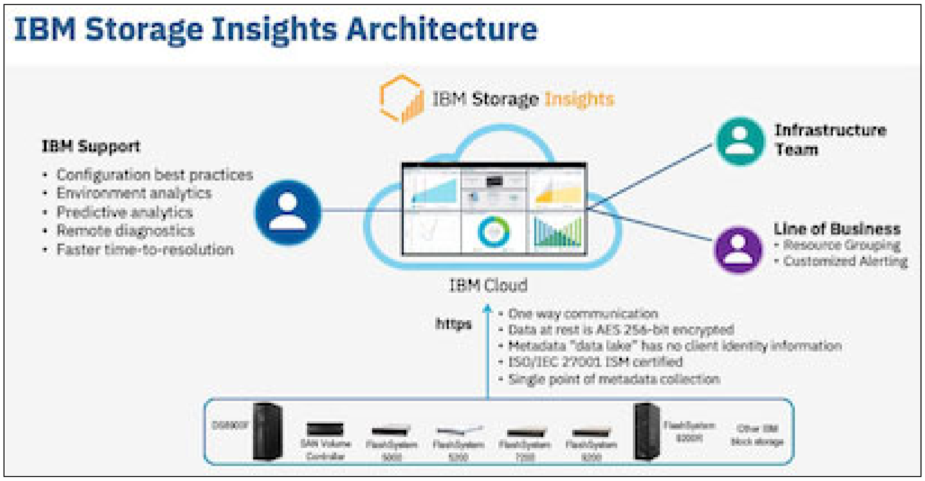


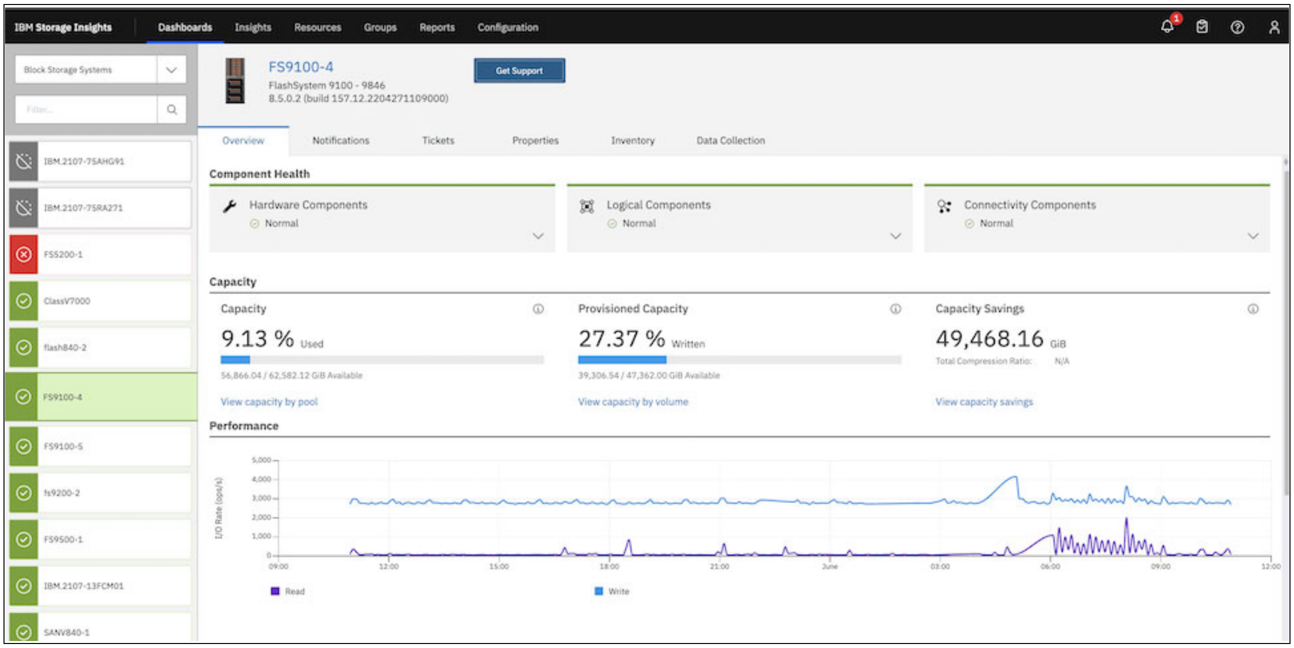
Figure 7-1 IBM Storage Insights architecture

For more information about IBM Storage Insights and to sign up and register for the no-charge service, see the following resources:

- Fact sheet
- Demonstration
- Security guide

7.3 IBM Storage Insights Monitoring

With IBM Storage Insights, you get the information that you need to monitor the health of your block storage environment and fabrics on the Operations dashboard, as shown in Figure 7-2.


FS9100-4
FlashSystem 9100 - 9846
8.5.0.2 (build 157.12.2204271109000)

Capacity: 9.13 % Used
56,866.04 / 62,582.12 GiB Available

Provisioned Capacity: 27.37 % Written
39,306.54 / 47,362.00 GiB Available

Capacity Savings: 49,468.16 GiB
Total Compression Ratio: N/A

Hardware Components: Normal
Logical Components: Normal
Connectivity Components: Normal

Figure 7-2 IBM Storage Insights System overview for block storage

The block storage dashboard is a default one that is shown when you go to the Operations dashboard. To view the storage systems that are being monitored, select **Dashboards** → **Operations**. Then, click the storage system in which you are interested in the left panel of the dashboard. For example, you can see the health, capacity, and performance information for a block storage system in the Operations dashboard. The storage system is colored red because there are problems with nodes and logical components.

IBM Storage Insights supports Brocade and Cisco switches and fabrics so that you can detect and investigate performance issues throughout your storage environment. You can follow the trail of storage requests through the components in the SAN fabric to the target storage systems.

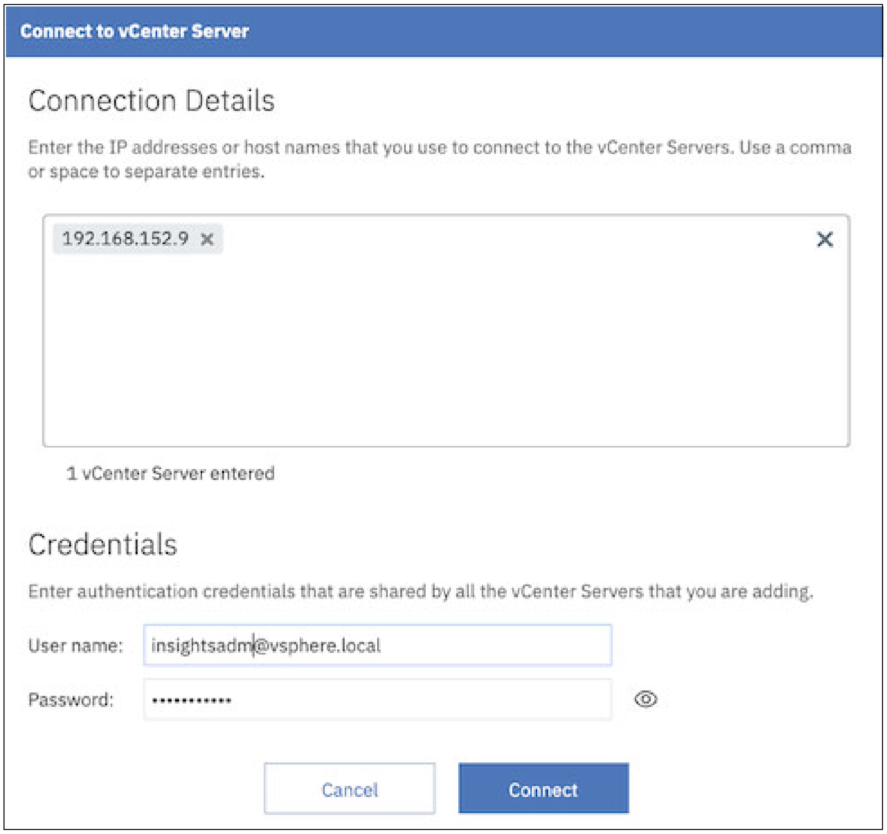
For more information, see Key features of IBM Storage Insights.

7.4 IBM Storage Insights VMware integration

You can add VMware ESXi hosts and their VMs for monitoring with IBM Storage Insights by specifying connection information for a vCenter Server. When you add VMware ESXi hosts, then you can collect data, generate reports, and manage storage that is related to hosts and VMs.

Identify the IP addresses and user credentials of the vCenter Servers that manage the VMware ESXi hosts and VMs that you want to monitor. IBM Storage Insights uses this information to connect to the vCenter Servers and discover their managed VMware ESXi hosts and VMs. You can add multiple vCenter Servers concurrently if they share the same user credentials by completing the following steps:

1. In the menu bar, select **Resources** → **Hosts**.
2. Click **Add vCenter Server**.
3. Enter the IP addresses or hostnames that you use to connect to the vCenter Server, and then enter the username and password that are shared by all the vCenter Servers that you are adding as shown in Figure 7-3.



Connect to vCenter Server

Connection Details

Enter the IP addresses or host names that you use to connect to the vCenter Servers. Use a comma or space to separate entries.

192.168.152.9

1 vCenter Server entered

Credentials

Enter authentication credentials that are shared by all the vCenter Servers that you are adding.

User name: insightsadm@vsphere.local

Password: •••••••••••

Figure 7-3 Adding vCenter Server

> **Note:** When you add vCenter Servers for monitoring, you must specify the connection credentials of users that are used to collect metadata. The users must meet the following requirements:
>
> - Role. Read Only (minimum). For example, the Administrator role or the Virtual Machine Power User role
> - Privilege. Browse datastore

After the vCenter server initial discovery starts, all ESXi hosts and VMs that are managed by vCenter are discovered by IBM Storage Insights. You can see details of each ESXi host on the IBM Storage Insights Pro edition, as shown in Figure 7-4 on page 176.

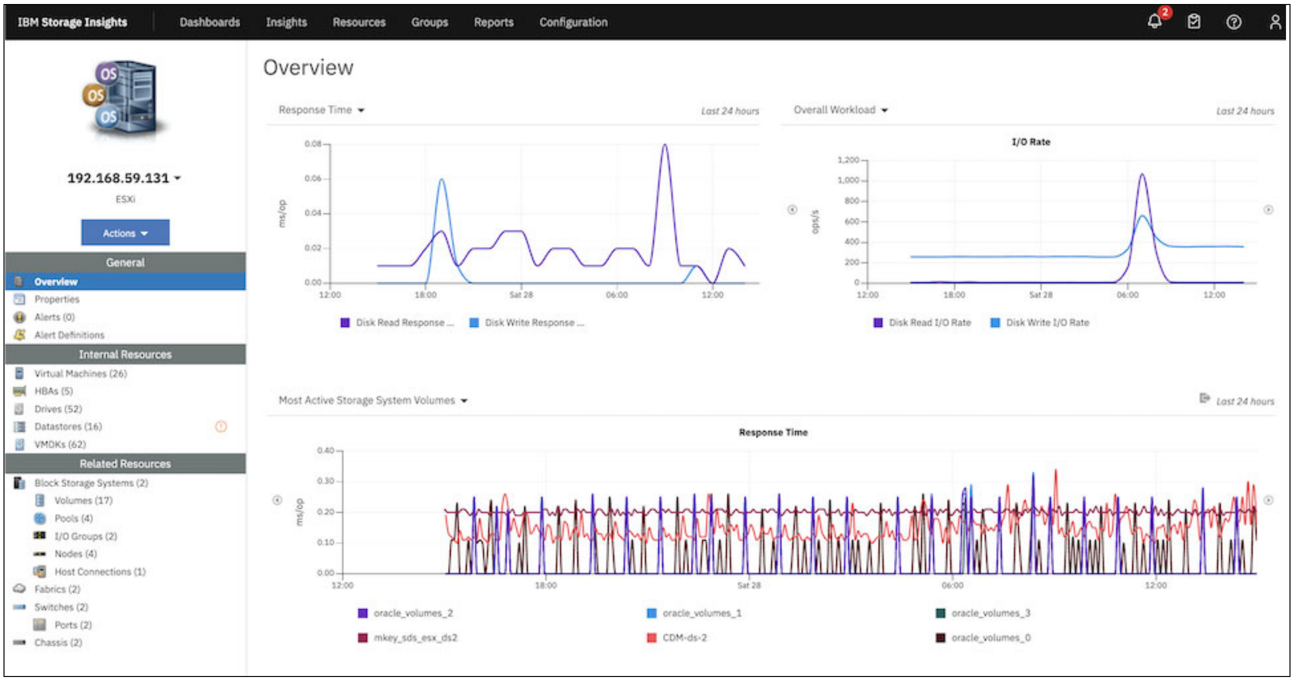


Figure 7-4 ESXi host details with daily response time, IO rate, and most active volumes on IBM Storage Insights

End-to-end SAN connectivity is visible when IBM Storage systems, SAN switches, and VMware ESXi servers are added to IBM Storage Insights.

Most of the time, it is a complex process to find which VM creates heavy I/O on a datastore volume. IBM Storage Insights Pro can monitor virtual machine disk (VMDK) level I/O performance, and you can find the more heavily used VM, as shown in Figure 7-5.

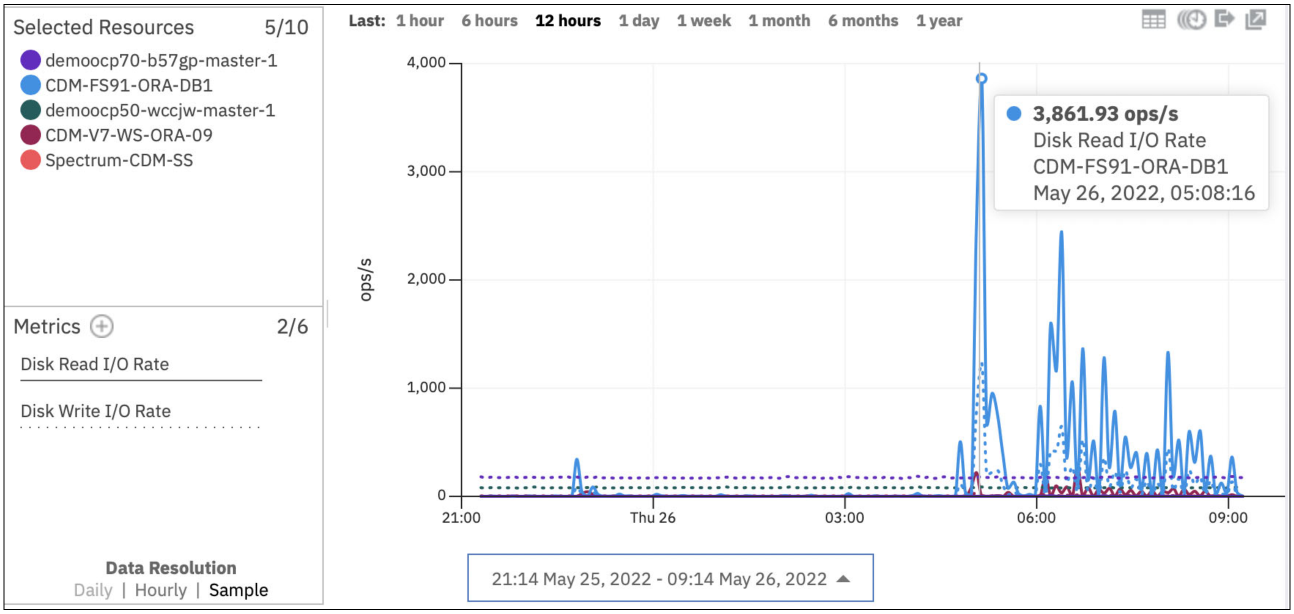
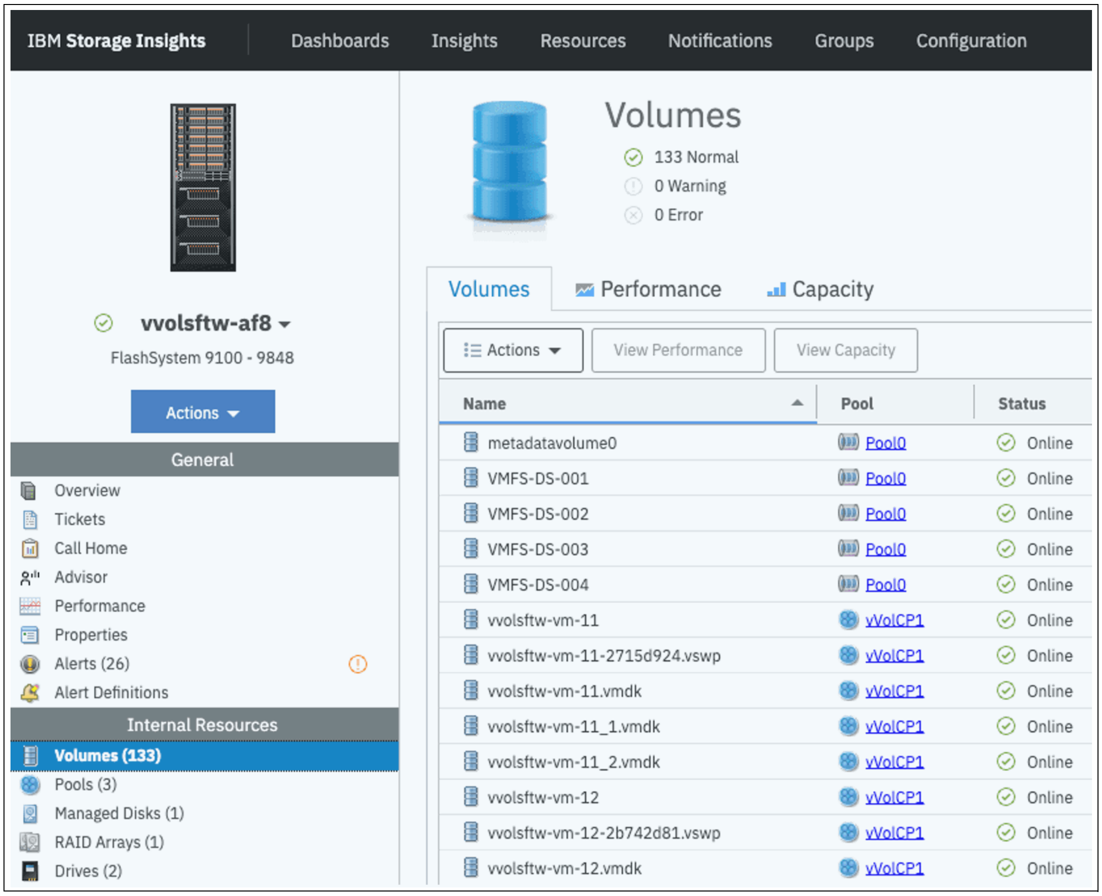


Figure 7-5 VMDK level performance monitoring on IBM Storage Insights Pro

With the introduction of the Embedded VASA Provider in version 8.6.0.0, an additional field was added to the output of **lsvdisk** to include the `display_name` for individual virtual volumes on the system. This field is populated by the VASA provider whenever a vVol is created, and contains information provided by vSphere to better identify the volume within the storage system.

To help identify the individual vVols when reviewing performance information, this information can be accessed by Storage Insights. For any virtual volume on the storage system, the value as reported in the `display_name` field replaces the traditional value of volume name. See Figure 7-6.



133 Normal
0 Warning
0 Error

Name	Pool	Status
metadatavolume0	Pool0	Online
VMFS-DS-001	Pool0	Online
VMFS-DS-002	Pool0	Online
VMFS-DS-003	Pool0	Online
VMFS-DS-004	Pool0	Online
vvolsftw-vm-11	vVolCP1	Online
vvolsftw-vm-11-2715d924.vswp	vVolCP1	Online
vvolsftw-vm-11.vmdk	vVolCP1	Online
vvolsftw-vm-11_1.vmdk	vVolCP1	Online
vvolsftw-vm-11_2.vmdk	vVolCP1	Online
vvolsftw-vm-12	vVolCP1	Online
vvolsftw-vm-12-2b742d81.vswp	vVolCP1	Online
vvolsftw-vm-12.vmdk	vVolCP1	Online

Figure 7-6 List of volumes on the storage system

Figure 7-6 displays the view of volumes on the storage system. Traditional VMFS datastores, such as VMFS-DS-001, 002, and 003, are listed with the individual vVols associated with a VM named, `vvolsftw-vm-11, such as vvolsftw-vm-11, vvolsftw-vm-11.vmdk, vvolsftw-vm-11_1.vmdk, and volsftw-vm-11_2.vmdk`.

Note: Because vVols are dynamically attached and detached from ESXi hosts during VM power state changes or vMotion, the host column always reflects the currently connected ESXi host for that specific vVol.

8

Integrating with VMware by using IBM Spectrum Connect

This chapter describes the configuration steps to integrate VMware and IBM Spectrum Connect, best-practice considerations, and troubleshooting tips.

This chapter includes the following sections:

- 8.1, “Overview of IBM Spectrum Connect” on page 180
- 8.2, “Understanding Storage Spaces and Storage Services” on page 188
- 8.3, “VMware vSphere Virtual Volumes” on page 195
- 8.4, “Best-practice considerations and troubleshooting” on page 210
- 8.5, “IBM Storage Enhancements for VMware vSphere Web Client plug-in” on page 218
- 8.6, “Performing more storage volume management tasks” on page 227
- 8.7, “IBM Storage Plug-in for VMware vRealize Orchestrator” on page 228
- 8.8, “IBM Storage Management Pack for VMware vRealize Operations Manager” on page 234

8.1 Overview of IBM Spectrum Connect

IBM Spectrum Connect is a dedicated Linux-based application that provides centralized management of IBM storage platforms for multiple virtualization, cloud, and container interfaces. By implementing advanced storage-provisioning techniques, IBM Spectrum Connect provides a way for storage and hybrid-cloud administrators to supply and integrate IBM storage with a range of VMware solutions, Kubernetes container clusters, and Microsoft PowerShell automation methods.

IBM Spectrum Connect provides a web-based GUI that can help make administration easier and more straightforward. The GUI can save time when you set up, connect and integrate the required storage resources into your cloud environment.

Through its user credential, storage system, storage space, and service management options, IBM Spectrum Connect facilitates the integration of IBM storage system resources with the supported virtualization, cloud, and container platforms.

The following storage services, which can be considered as storage profiles, are defined in IBM Spectrum Connect and delegated for use in VMware for profile-based volume provisioning:

- VMware vSphere Web Client (vWC)
- VMware vSphere Storage APIs - Storage Awareness (VASA)
- VMware vRealize Operations (vROps) Manager
- VMware vRealize Automation, and VMware vRealize Orchestrator (vRO)
- Microsoft PowerShell

Note: The VASA for VMware vSphere Virtual Volumes (vVols) function is also available through the embedded VASA Provider in IBM Storage Virtualize 8.5.1.0 or later. For more information about using VASA or vVols with the embedded VASA Provider, see Chapter 5, “Embedded VASA Provider for Virtual Volumes (vVol)” on page 83.

8.1.1 Supported cloud interfaces

This book focuses on the following cloud interfaces that are compatible with VMware integrations that use IBM Spectrum Connect:

- IBM Storage Provider for VMware VASA
- IBM Storage Enhancements for VMware vSphere Web Client
- IBM Storage Plug-in for VMware vRO
- IBM Storage Management Pack for VMware vROps Manager

In addition, the IBM Spectrum Connect lifecycle and compatibility matrix in IBM Documentation describes the IBM Spectrum Connect lifecycle with compatible storage-system microcodes and supported cloud interfaces.

8.1.2 Installation considerations

You can install the IBM Spectrum Connect software on a compatible version of Red Hat Enterprise Linux (RHEL) or CentOS. For more information about supported operating systems, see IBM Spectrum Connect 3.11.0 Release Notes.

As shown in Figure 8-1, the IBM Spectrum Connect application communicates with IBM storage systems by using command-line interface (CLI) commands over secure shell (ssh). VMware also issues application programming interface (API) calls directly to IBM Spectrum Connect over TCP/IP. Therefore, IP connectivity must exist between the IBM Spectrum Connect server and the Management IP address, sometimes referred to as the cluster IP address, of the storage system. For security, some network infrastructures might be segmented into virtual local area networks (VLANs) or are isolated. The isolation prevents the management of the storage system from being accessible from virtual machines (VMs) within a vSphere environment. Check with your network administrator to ensure that IP connectivity exists between the different components.

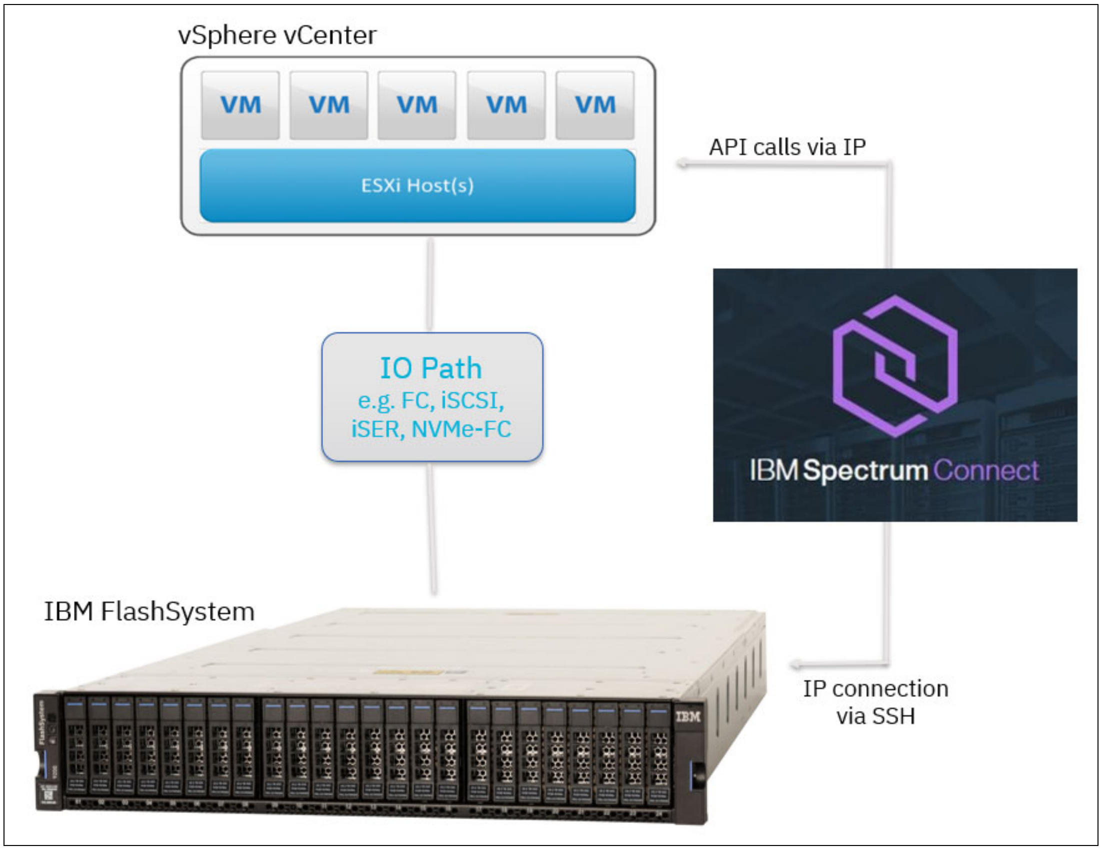


Figure 8-1 IBM FlashSystem and vSphere vCenter integration architecture

Communication between VMware vRO, vSphere, or vCenter and the IBM storage system by using IBM Spectrum Connect is out-of-band and is therefore separate from I/O traffic between a host and the storage system.

If network connectivity issues occur, which prevent IBM Spectrum Connect from communicating with either the cloud interface or the storage system, the I/O workload that is running on the hosts is unaffected.

> **Note:** When you use vVols, IBM Spectrum Connect can operate in a high availability (HA) model, where two IBM Spectrum Connect servers can be configured to run in Active/Standby. For more information about this feature, see IBM Spectrum Connect Version 3.11.0.

VM resource requirements might depend on the roles that are performed by the IBM Spectrum Connect Server. The IBM Spectrum Connect server periodically queries the storage system for an inventory of objects such as VDisks, hosts, and FlashCopy mappings By default, it is configured to run in 10-minute intervals. This query populates a local cache of the configuration, which can be used by the following services:

- vROps for performance data
- The IBM Storage Enhancements plug-in, which maintains constant awareness of host objects that are defined on the storage system

Depending on the size and complexity of the IBM Storage Virtualize configuration, the population task might take some time.

> **Tip:** In large environments, consider increasing the population interval to allow sufficient time for the task to complete. For more information about IBM Spectrum Connect, see
>
> IBM Spectrum Connect Version 3.11.0

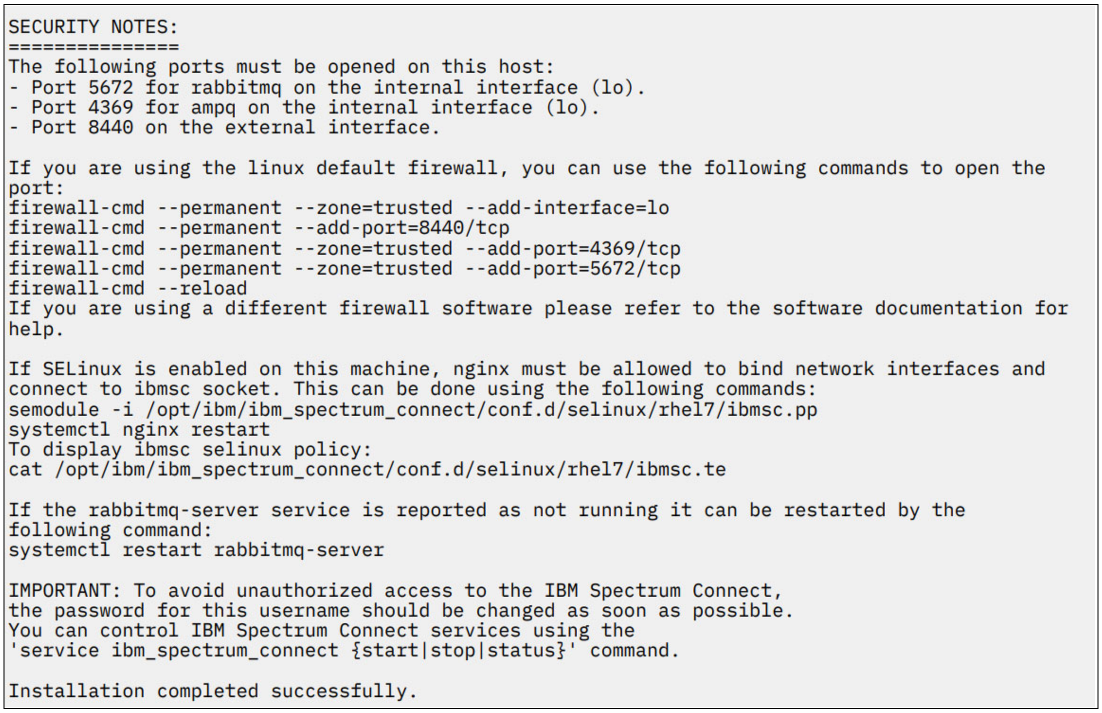
8.1.3 Downloading and installing IBM Spectrum Connect

IBM Spectrum Connect is available to download from IBM Fix Central.

> **Note:** Before you install the IBM Spectrum Connect application, it is a best practice to configure a Network Time Protocol (NTP) client on the Linux operating system. A common time frame for all components can make it easier to review log during debug operations.

For more information about installation instructions and minimum requirements, see IBM Spectrum Connect Version 3.11.0.

The installation summary screen (Figure 8-2) provides details about additional steps to configure firewall rules and SELinux, if required.



```
SECURITY NOTES:
===============
The following ports must be opened on this host:
- Port 5672 for rabbitmq on the internal interface (lo).
- Port 4369 for ampq on the internal interface (lo).
- Port 8440 on the external interface.

If you are using the linux default firewall, you can use the following commands to open the
port:
firewall-cmd --permanent --zone=trusted --add-interface=lo
firewall-cmd --permanent --add-port=8440/tcp
firewall-cmd --permanent --zone=trusted --add-port=4369/tcp
firewall-cmd --permanent --zone=trusted --add-port=5672/tcp
firewall-cmd --reload
If you are using a different firewall software please refer to the software documentation for
help.

If SELinux is enabled on this machine, nginx must be allowed to bind network interfaces and
connect to ibmsc socket. This can be done using the following commands:
semodule -i /opt/ibm/ibm_spectrum_connect/conf.d/selinux/rhel7/ibmsc.pp
systemctl nginx restart
To display ibmsc selinux policy:
cat /opt/ibm/ibm_spectrum_connect/conf.d/selinux/rhel7/ibmsc.te

If the rabbitmq-server service is reported as not running it can be restarted by the
following command:
systemctl restart rabbitmq-server

IMPORTANT: To avoid unauthorized access to the IBM Spectrum Connect,
the password for this username should be changed as soon as possible.
You can control IBM Spectrum Connect services using the
'service ibm_spectrum_connect {start|stop|status}' command.

Installation completed successfully.
```

Figure 8-2 Installation summary screen

8.1.4 Initial configuration

When the IBM Spectrum Connect application is installed, you can access the management web interface (Figure 8-3), by connecting to `http://<IP or FQDN>:8440. The` default credentials are:

- Name: `admin`
- Password: `admin1!`

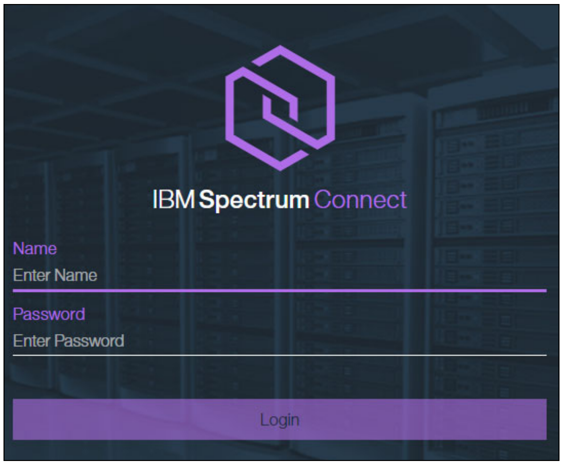


Figure 8-3 Management web interface

After a successful login, complete the initial setup wizard, which includes the following mandatory configuration steps:

- Set up an HA group and IBM Spectrum Connect server identity
- Provide details for the SSL certificate
- Define storage system credentials
- Change the default IBM Spectrum Connect credentials

Notes:

- When you specify the storage-system credentials, it is a best practice to create a dedicated user account on the storage-system, which is easily identifiable as being from an IBM Spectrum Connect server. This account is the user account that is used when IBM Spectrum Connect issues CLI commands to the storage system. Having an easily recognizable username can help make some tasks easier, such as reviewing audit logs within IBM Storage Virtualize, and can make it clear if the CLI commands were issued by IBM Spectrum Connect.
- The storage-system credentials are global and apply to all storage systems being registered in IBM Spectrum Connect. When possible, consider using Lightweight Directory Access Protocol (LDAP) authentication on the storage system to simplify user account management.

Ensure that the associated user account is created on every storage system that is to be registered and that the account was granted a suitable role.

For example, when using VMware vSphere Virtual Volumes, the storage-system user account must be assigned the “VASA Provider” role on each storage system. Create a User Group with the “VASA Provider” role in IBM Storage Virtualize, as described in the following steps:

1. Open the IBM Storage Virtualize management interface and click **Access option** in the navigation menu. Click **Create User Group** at the bottom of the window (Figure 8-4).
2. Enter a name for the User Group to be created, and select **VASA Provider**. Click **Create** (Figure 8-5 on page 185).

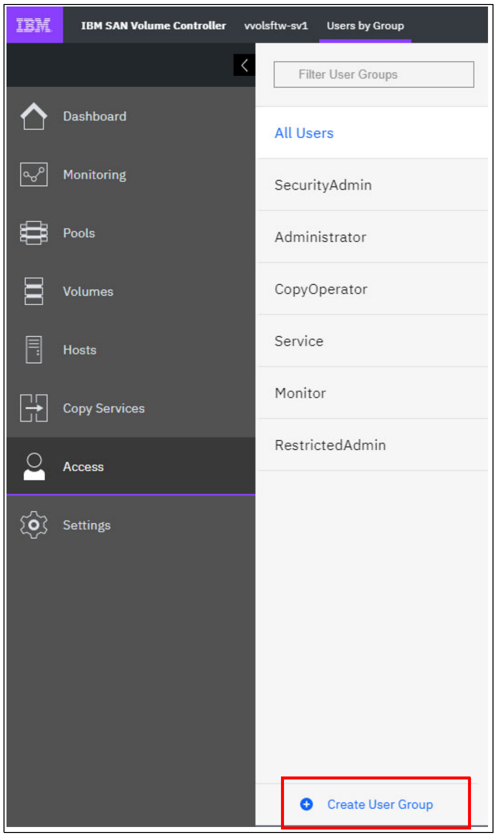
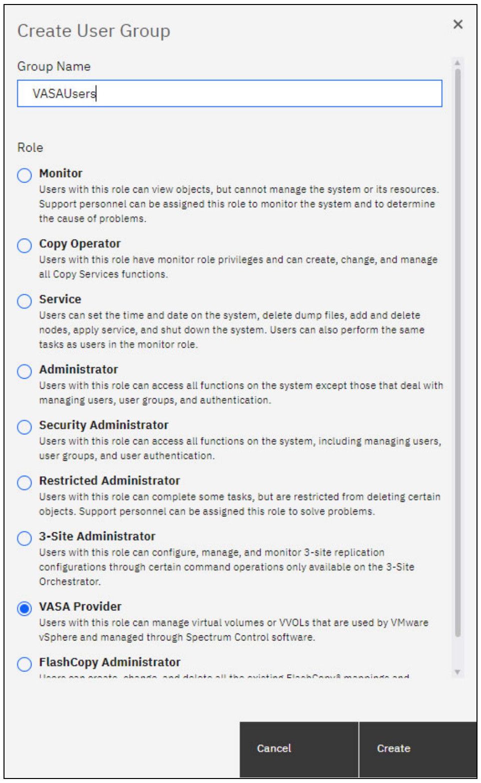


Figure 8-4 Create User Group: 1



Create User Group

Group Name

VASAUsers

Role

○ **Monitor**
Users with this role can view objects, but cannot manage the system or its resources. Support personnel can be assigned this role to monitor the system and to determine the cause of problems.

○ **Copy Operator**
Users with this role have monitor role privileges and can create, change, and manage all Copy Services functions.

○ **Service**
Users can set the time and date on the system, delete dump files, add and delete nodes, apply service, and shut down the system. Users can also perform the same tasks as users in the monitor role.

○ **Administrator**
Users with this role can access all functions on the system except those that deal with managing users, user groups, and authentication.

○ **Security Administrator**
Users with this role can access all functions on the system, including managing users, user groups, and user authentication.

○ **Restricted Administrator**
Users with this role can complete some tasks, but are restricted from deleting certain objects. Support personnel can be assigned this role to solve problems.

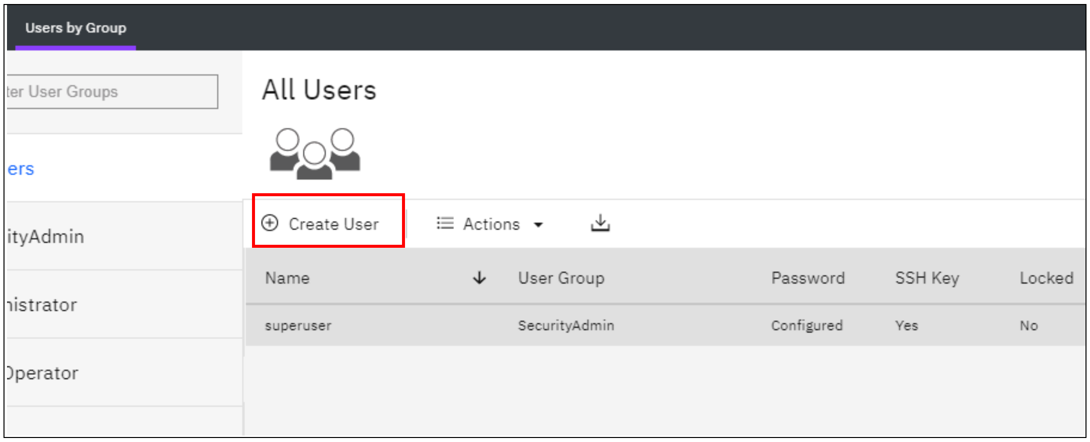
○ **3-Site Administrator**
Users with this role can configure, manage, and monitor 3-site replication configurations through certain command operations only available on the 3-Site Orchestrator.

● **VASA Provider**
Users with this role can manage virtual volumes or VVOLs that are used by VMware vSphere and managed through Spectrum Control software.

○ **FlashCopy Administrator**
Users can create, change, and delete all the existing FlashCopy® mappings and

Figure 8-5 VASA Provider option

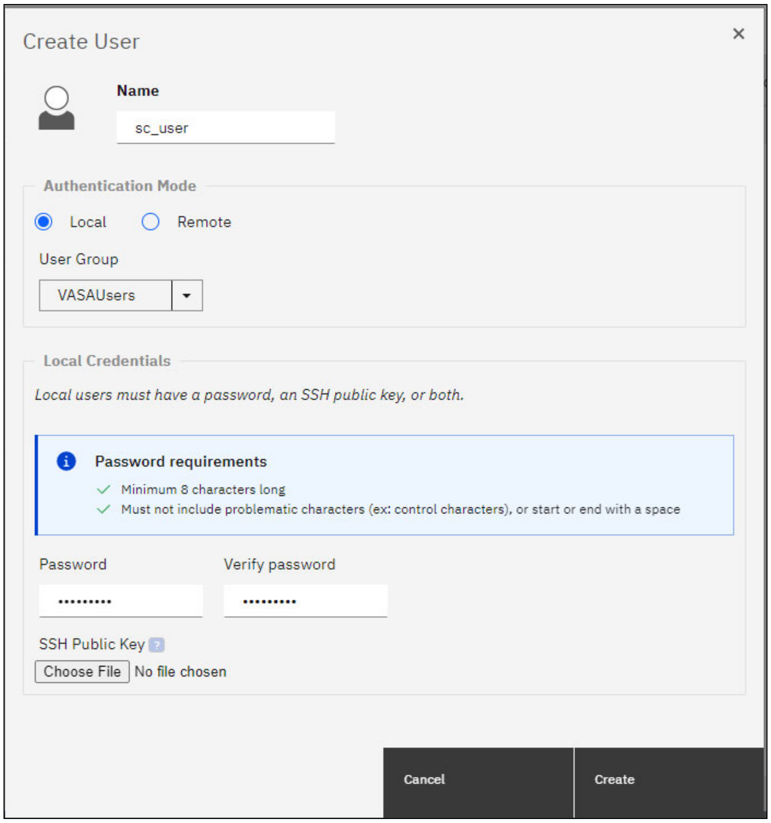
3. Click **Create User** (Figure 8-6).



Name	User Group	Password	SSH Key	Locked
superuser	SecurityAdmin	Configured	Yes	No

Figure 8-6 Create User: 1

4. Enter a suitable username and select the **VASAUsers** group created previously. Enter and confirm the password for this user account then click **Create**, as shown in Figure 8-7 on page 186.



Create User

Name

sc_user

Authentication Mode

● Local ○ Remote

User Group

VASAUsers

Local Credentials

Local users must have a password, an SSH public key, or both.

Password requirements

- ✓ Minimum 8 characters long
- ✓ Must not include problematic characters (ex: control characters), or start or end with a space

Password: ••••••••• Verify password: •••••••••

SSH Public Key

Choose File No file chosen

Figure 8-7 Create User: 2

5. When the initial configuration wizard is complete, in the IBM Spectrum Connect management interface, you see a “Guided tour” that provides a brief overview of the interface. When the tour is completed, an empty inventory of IBM Spectrum Connect is displayed (Figure 8-8).

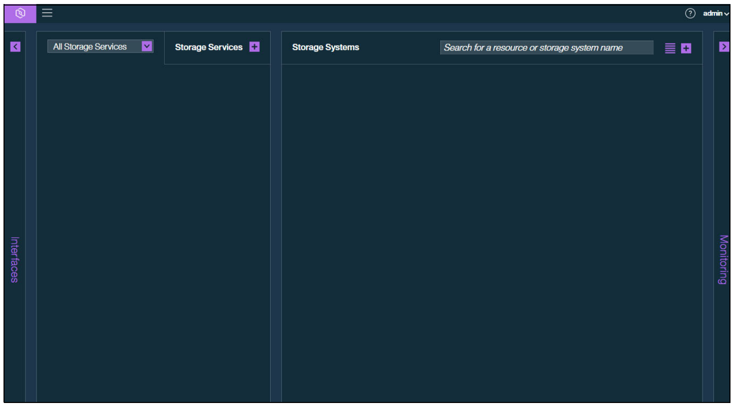


Figure 8-8 Empty inventory of IBM Spectrum Connect

6. Click the Interfaces pane, on the left side of the screen, to view and configure the Cloud Interfaces. You can configure items such as a vCenter server for the IBM Storage Enhancements or the connector for vRO.

   Alternatively, click the Monitoring pane, on the right side of the screen, to configure the vROps Manager integration.

8.1.5 Registering a Storage System into IBM Spectrum Connect

On the main page of the IBM Spectrum Connect management interface, click the plus (**+**) icon, and enter the fully qualified domain name (FQDN) or IP address for the storage system (Figure 8-9).

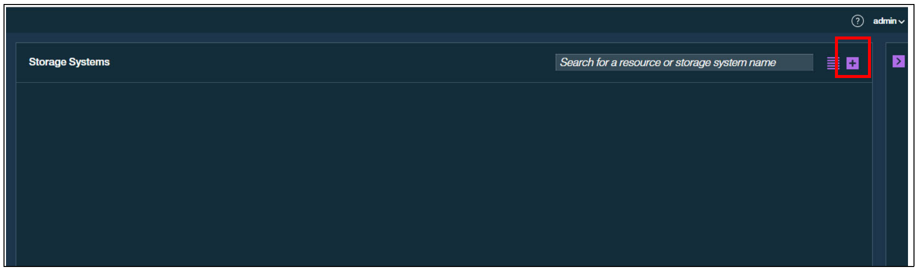
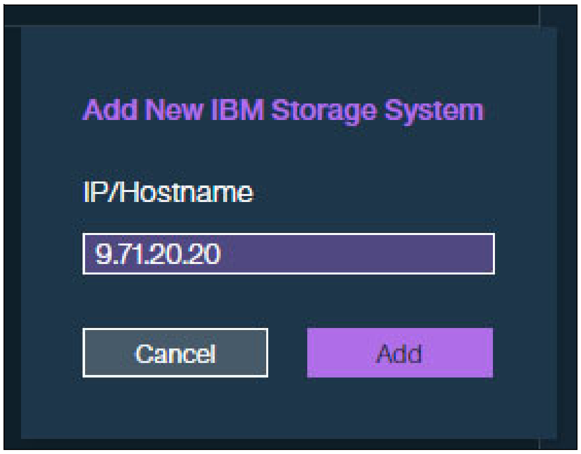


Figure 8-9 Clicking the plus icon

You are prompted to enter only the IP or hostname of the storage system because the Storage Credentials were defined in the initial configuration wizard (Figure 8-10).

Note: If you use VMware vSphere Virtual Volumes, ensure that the Storage Credentials are configured with the VASA Provider role.


Add New IBM Storage System

IP/Hostname: 9.71.20.20

Figure 8-10 Entering the IP or hostname

7. Click **Add**. The Storage System is now represented in the IBM Spectrum Connect UI (Figure 8-11).

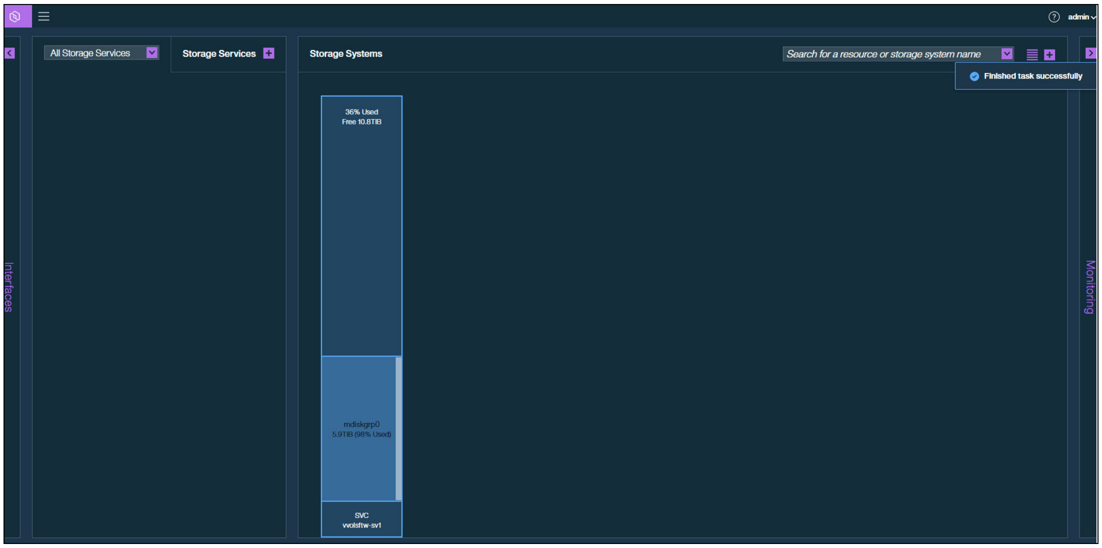


Figure 8-11 Storage System shown in the IBM Spectrum Connect UI

8.2 Understanding Storage Spaces and Storage Services

To allow a cloud interface the ability to create objects on the storage system, relationships must be created between the specific interface and a specific storage system. Also, you must define how volumes should be created without exposing every configuration option to the VMware interface. For example, should the volumes be Space Efficient, Deduplicated, or Encrypted? Perhaps a storage administrator wants every volume mirrored between two different external storage controllers, or that every volume must be thin-provisioned to ensure the maximum use of the available storage capacity.

IBM Spectrum Connect uses the concept of a Storage Service for simpler and more flexible storage management. A Storage Service can also be described as a Storage Provisioning Profile. If a storage administrator defines the capabilities on the service or profile, all volumes that are created in that service are created the same way and inherit the same attributes.

Multiple Storage Services can be presented to the VMware interface to present multiple provisioning options to the vSphere administrator (Figure 8-12).

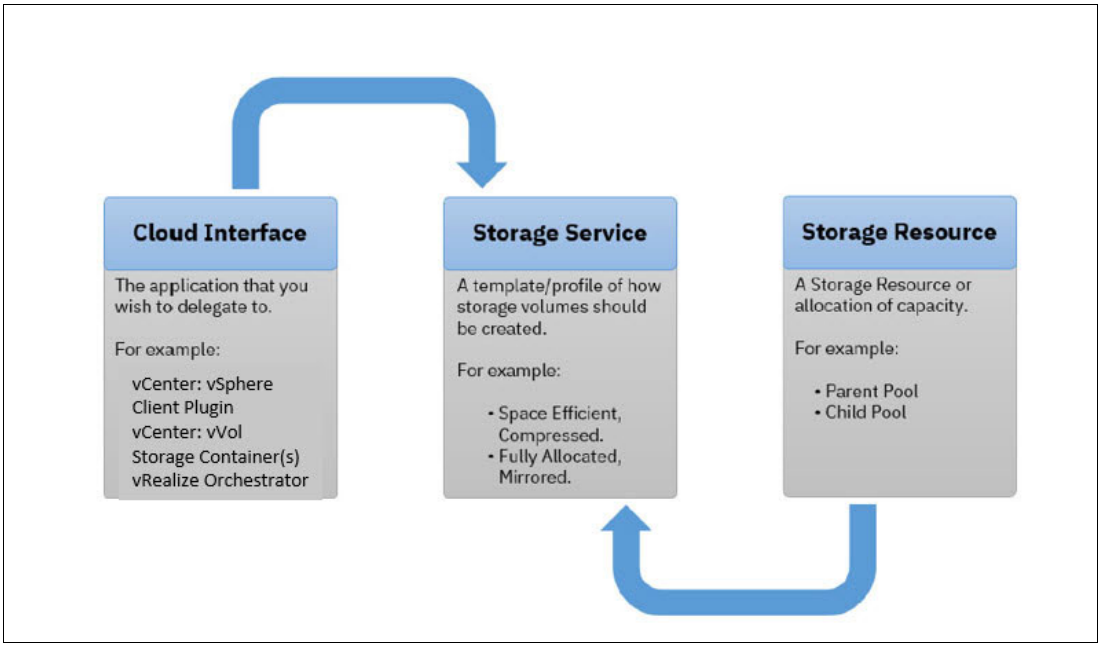

Cloud Interface
The application that you wish to delegate to.
For example:
vCenter: vSphere Client Plugin
vCenter: vVol Storage Container(s)
vRealize Orchestrator
Storage Service
A template/profile of how storage volumes should be created.
For example:
• Space Efficient, Compressed.
• Fully Allocated, Mirrored.
Storage Resource
A Storage Resource or allocation of capacity.
For example:
• Parent Pool
• Child Pool

Figure 8-12 Storage Spaces and Storage Services

However, a storage administrator might be reluctant to grant full access to a storage system because if too many volumes are created, the capacity is difficult to manage. In this scenario, the storage administrator can create child pools to present ring-fenced allocations of storage capacity to a Storage Service. A vSphere administrator can then create volumes on-demand within that storage allocation.

8.2.1 Creating Storage Services

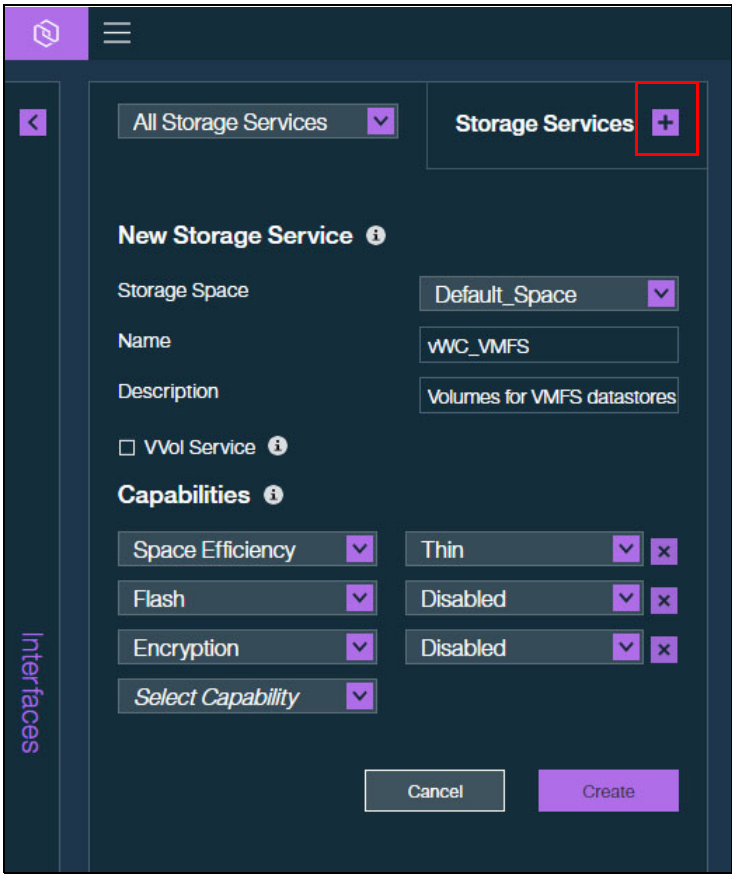
To create Storage Services, complete the following steps:

1. Identify a suitable Storage Space and click the plus icon (**+**) to create a new Storage Service (Figure 8-13 on page 190). Enter text into the Name and Description fields to later identify the intended use and select the capabilities that best suit the application requirements.

   Multiple Storage Services, with different capabilities can be associated to the vCenter interface, which allows the vSphere administrator to select which profile of storage should be used for a situation.

Tips:

- When a Storage Service is dedicated to use with VMware vSphere Virtual Volumes, ensure that the **vVol Service** checkbox is selected.
- Consider a mix of configuration options, such as Space Efficiency, Encryption, Tier, and Data Reduction.



New Storage Service

Storage Space: Default_Space

Name: vWC_VMFS

Description: Volumes for VMFS datastores

☐ VVol Service

Capabilities

Space Efficiency	Thin
Flash	Disabled
Encryption	Disabled
Select Capability	

Figure 8-13 Creating Storage Services

Note: When you create the Storage Service and select the capabilities, Storage Systems that are not compatible with the current selection are unavailable, such as:

- When **Synchronous Replication** is selected, but the Storage System that is registered in IBM Spectrum Connect is not yet configured for HyperSwap.
- When Flash storage is requested, but storage pools do not exist in the Flash devices.

2. After you define the required capabilities of the storage profile, click **Create**.

   The newly created Storage Service is listed. Notice that allocated storage capacity does not exist for this Storage Service. A storage resource needs to be associated to the Storage Service.

8.2.2 Allocating capacity to Storage Services

To allocate storage capacity to the Storage Services, complete the following steps:

1. Right-click the Storage Service and select **Manage Resources** (Figure 8-14).

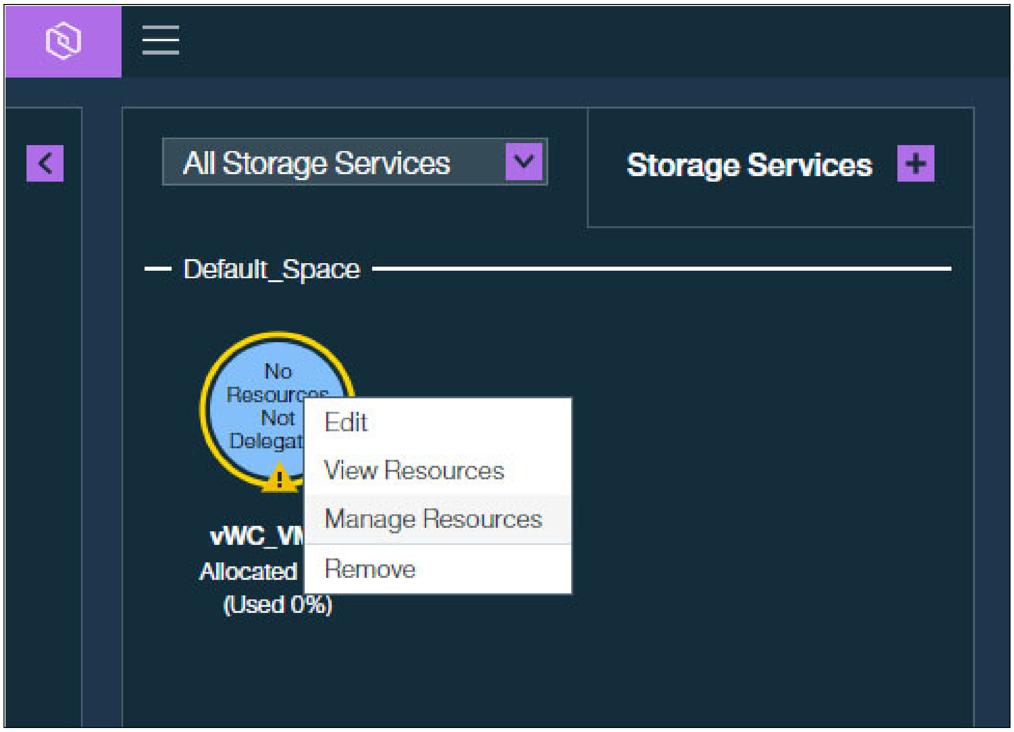


Figure 8-14 Selecting Manage Resources

The Manage Resources window opens (Figure 8-15 on page 192).

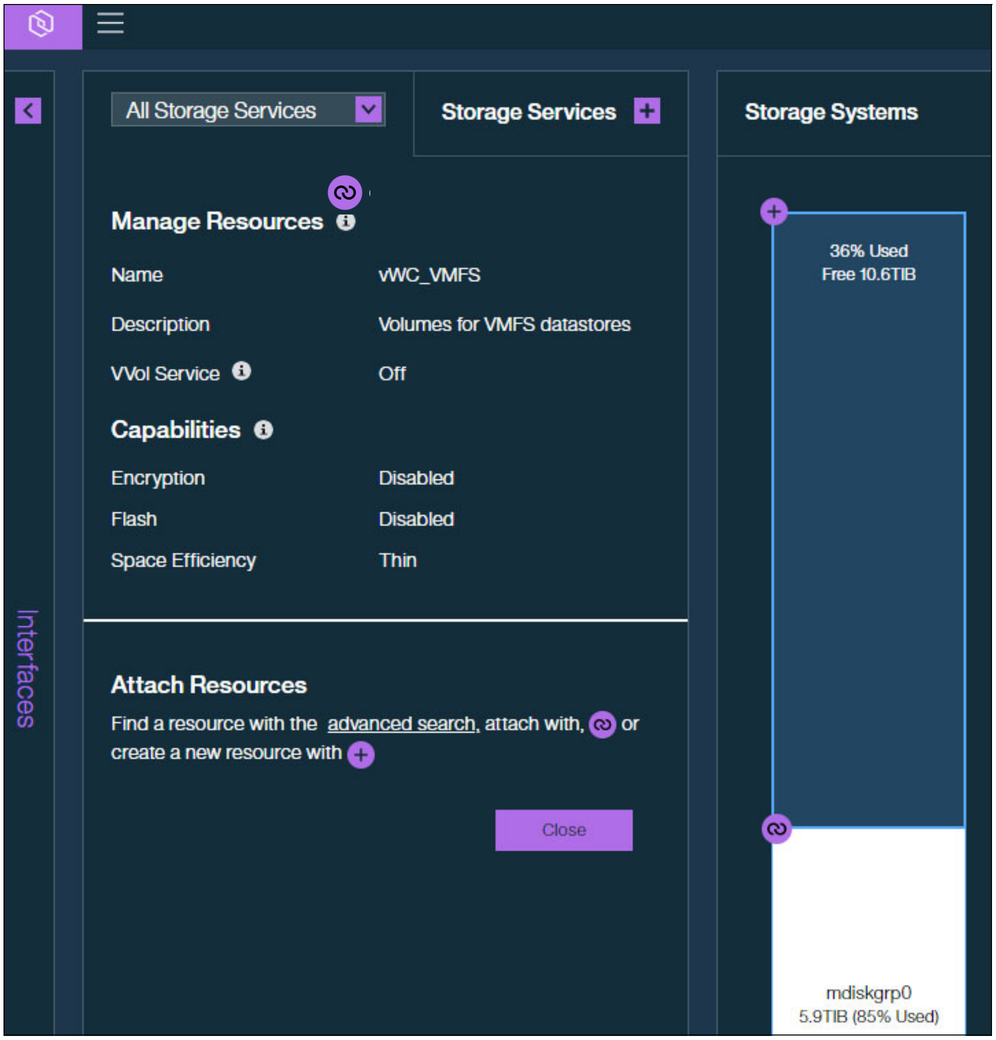
> **Note:** A Storage Resource can be either an existing parent pool within the IBM Storage Virtualize storage system, or a new or existing child pool. A child pool is a ring-fenced allocation of storage capacity that is taken from an existing parent pool.

2. To associate an existing parent pool to the selected Storage Service (Figure 8-16 on page 192), click the Delegate icon (⊘) associated with the specific parent pool.

   Alternatively, to create and associate a new child pool, click the **Plus** icon (**+**) at the top of the Storage System to create a Storage Resource.

   This step creates a child pool of a defined name and capacity within a specified parent pool.

   > **Note:** When using a HyperSwap configuration, you are asked to specify the parent pool at both sites (Figure 8-17). This specification creates a paired child pool with the same capacity that is defined at each site.



Manage Resources

Name	vWC_VMFS
Description	Volumes for VMFS datastores
VVol Service	Off

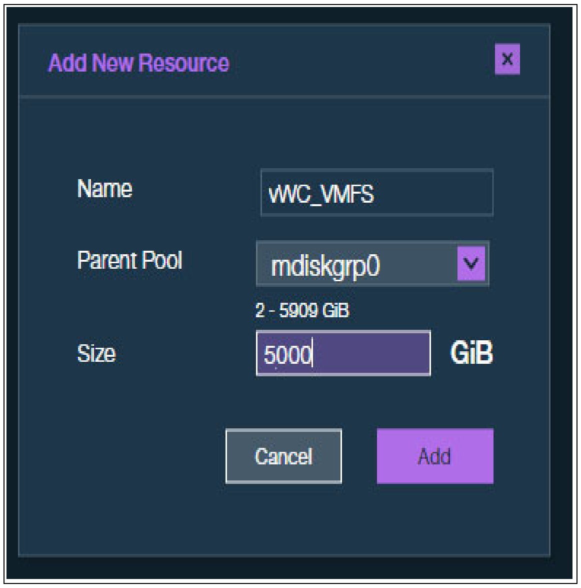
Capabilities

Encryption	Disabled
Flash	Disabled
Space Efficiency	Thin

Attach Resources

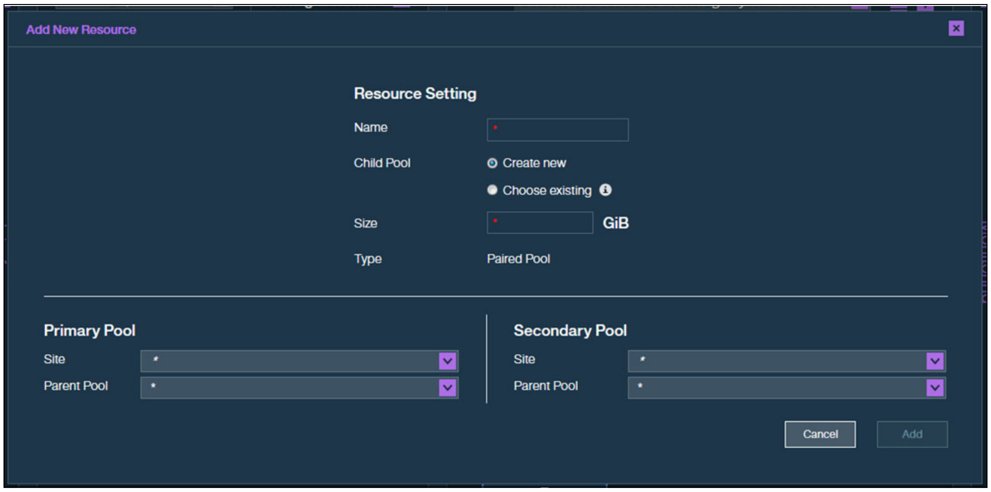
Find a resource with the advanced search, attach with, or create a new resource with

Figure 8-15 Manage Resources window



Name	vWC_VMFS
Parent Pool	mdiskgrp0
	2 - 5909 GiB
Size	5000 GiB

Figure 8-16 Add New Resource



Add New Resource

Resource Setting

Name *

Child Pool ○ Create new ● Choose existing

Size * GiB

Type Paired Pool

Primary Pool

Site *

Parent Pool *

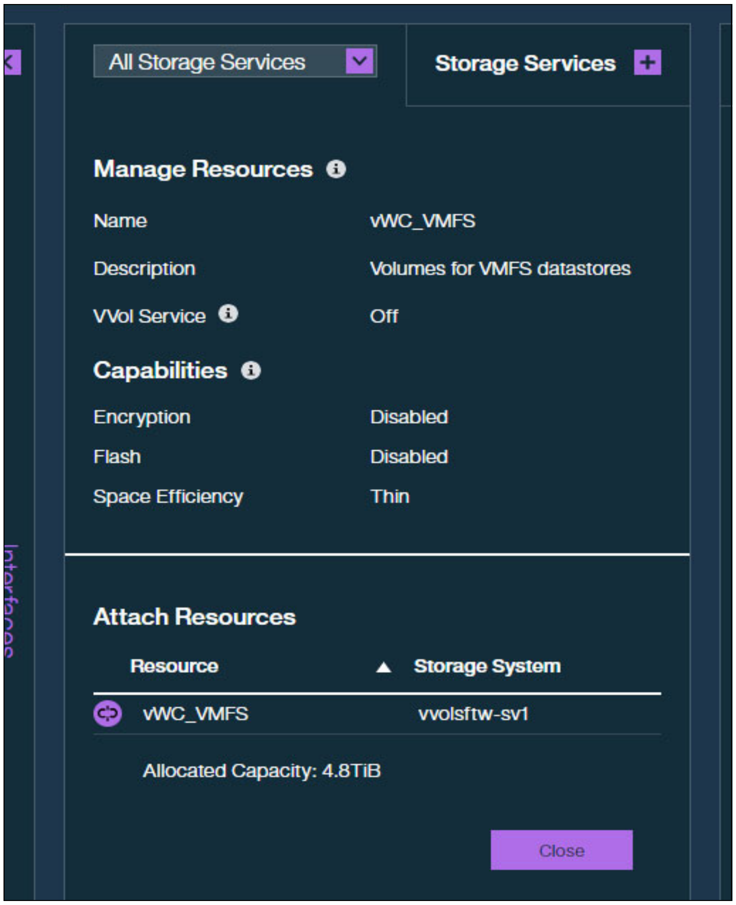
Secondary Pool

Site *

Parent Pool *

Figure 8-17 HyperSwap configuration

3. Verify that the Storage Resource allocation for the Storage Service is correct and click **Close** (Figure 8-18).



Manage Resources

Name	vWC_VMFS
Description	Volumes for VMFS datastores
VVol Service	Off

Capabilities

Encryption	Disabled
Flash	Disabled
Space Efficiency	Thin

Attach Resources

Resource	Storage System
vWC_VMFS	vvolsftw-sv1

Allocated Capacity: 4.8TiB

Figure 8-18 Verifying the Storage Resource allocation

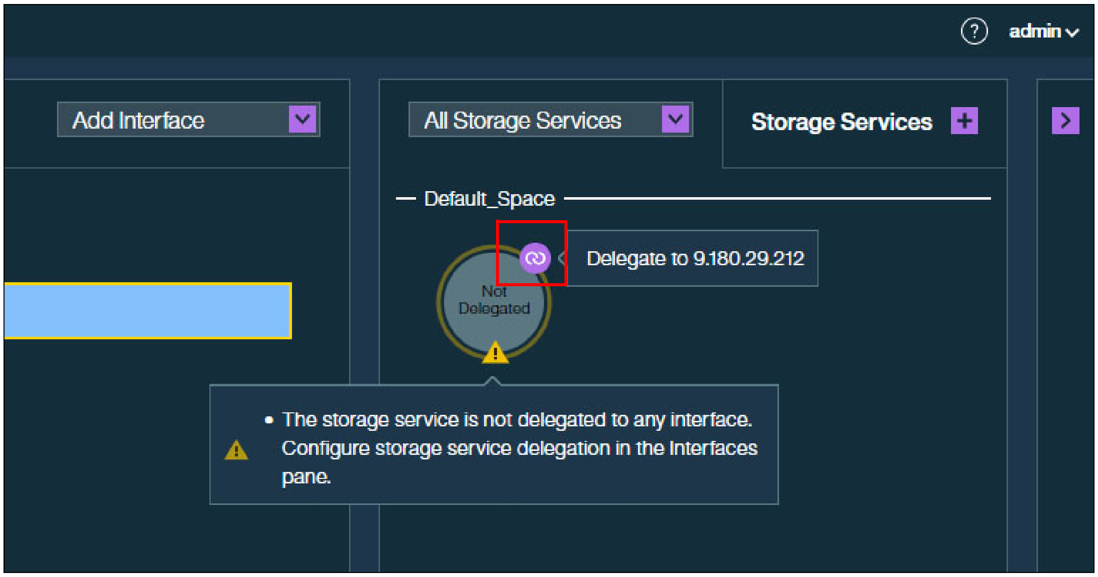
8.2.3 Delegating Storage Services to vCenter

The Storage Service is created and some storage capacity is allocated. You can now delegate the Storage Service to the vCenter interface.

> **Tip:** When you use vVol-enabled Storage Services, this step is optional. However, it is a best practice because it provides more visibility of the individual vVol-to-VM relationships.

To delegate Storage Services to vCenter:

1. In the Interfaces window, select the **vCenter interface** to which you want the Storage Service to have access (Figure 8-19). Click the Delegate icon ( ).



- The storage service is not delegated to any interface. Configure storage service delegation in the Interfaces pane.

Figure 8-19 Storage Service delegation

Note the changes that occur when the Storage Service is delegated:

– The color changes to yellow on the Storage Service (Figure 8-19).

– The Delegate icon changes from to (Figure 8-20).

– The Allocated Storage capacity, which is described just under the selected vCenter interface, is updated to reflect the new Storage Service delegation (Figure 8-20).

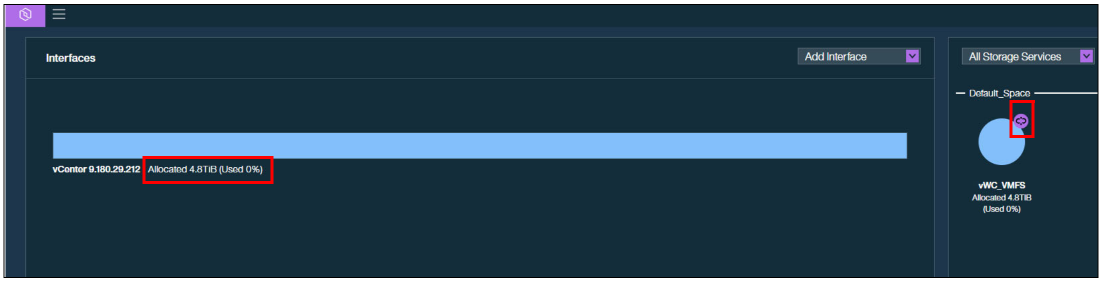


Figure 8-20 New Storage Service delegation

2. If you want to remove the delegation, click the Delegate icon ( ) icon to disassociate the Storage Service mapping (Figure 8-20).

Note: The creation and removal of delegation of Storage Service to the interface does not impact the existing volumes or host mappings on the storage system.

8.3 VMware vSphere Virtual Volumes

This section provides an overview of VMware vSphere Virtual Volumes and describes how to configure IBM Storage Virtualize to support vVols.

For IBM Storage Virtualize version 8.5.1.0 and later, the vVol function can be provided in either of two ways:

1. IBM Spectrum Connect. An isolated application that runs on a separate VM within the vSphere environment that converts API calls from vSphere into CLI commands that are issued to the IBM FlashSystem array.
2. Embedded VASA Provider. This application runs natively as a service on the IBM FlashSystem configuration node, communicates directly with vSphere, and is not dependent on any other external application or server.

The two models *cannot* be run in parallel, so you must choose which one to implement in your infrastructure.

To learn more about the Embedded VASA Provider feature and to see whether it is appropriate for your environment, see Chapter 5, “Embedded VASA Provider for Virtual Volumes (vVol)” on page 83.

8.3.1 VMware vSphere Virtual Volumes overview

IBM Spectrum Connect provides comprehensive storage-virtualization support that uses vVol technology.

The vVol architecture, introduced in VMware vSphere 6.0 with VASA 2.0, preserves the concept of a traditional datastore, maintaining familiarity and functions and also offers some benefits of legacy Raw Device Mappings.

Virtual Machine File System datastores

A large volume from an IBM Storage Virtualize storage system can be formatted as a Virtual Machine File System (VMFS) datastore and shared between a number of hosts in the vSphere cluster. On traditional VMFS datastores, each virtual machine disk (VMDK) that is associated to a VM is a file on a file system, which is a layer of abstraction apart from how the storage system processes the workload.

VM-level snapshots provide an excellent way of providing a point-in-time copy of a VM. However, the read/write overhead when using snapshots for anything beyond a 24–72 hour period can greatly impact the performance of the VM.

Also, in this scenario there are several VMs, distributed across many ESXi hosts. The VMs perform I/O operations to that volume, which can generate a high workload. When investigating these performance issues, the storage administrator might observe a high number of IOPS and high response times against that volume. In this example, the storage system has limited knowledge of the source of the I/O workload or the cause of the performance issues.

When multiple VMs on the ESXi host perform sequential I/O operations to their VMDK disks, the ESXi layer might not be able to fully optimize the data stream for IBM Storage Virtualize's advanced caching features.

When performing logical unit number (LUN)-level operations on the storage system, such as, volume-level snapshots that use a FlashCopy map, all VMs that are on the VMFS datastore that is backed by that volume are affected.

Raw Device Mappings

Raw Device Mappings (RDMs) provide a more traditional method of storage provisioning where a single volume from a storage system is dedicated to a VM's VMDK disk. This method provides a direct mapping of logical block addressing from a VMDK file to the volume as presented by the storage system.

However, RDMs do not offer the same level of functions when compared with VMFS datastores, specifically regarding VM cloning and snapshots. RDMs also require a storage administrator to present dedicated volumes for each VMDK file, which can increase the storage-provisioning management workload.

VMware vSphere Virtual Volumes

vVols can be viewed as taking the benefits from both VMFS and RDM storage concepts, with none of the associated limitations. The vVols model provides a 1:1 association of VMDK files to Volumes in the storage system. For every VMDK file that is created for a VM, a volume is created on the storage array similar to how RDMs are configured.

The main advantages of vVols include the following features:

- Automated storage provisioning. The vVols are created, deleted, and mapped or unmapped automatically. As a VMware administrator performs tasks in vCenter, such as creating VMs or adding more VMDKs to an existing VM, the associated API calls are sent to the IBM Spectrum Connect server. The API calls are then processed and converted into CLI commands to run against the storage system by using ssh. This action reduces the amount of time that is dedicated to managing VM storage when compared to RDM volumes because action is not required from the storage administrator.
- Improved VM snapshots, storage migration, and clones. Because each VMDK file exists natively as a volume within IBM Storage Virtualize, VM-level snapshots, storage migrations, and VM clone operations are offloaded to the storage system in the form of FlashCopy operations that are processed asynchronously.
- Storage Policy Based Management.: To aid storage provisioning, Storage Policies can be created in vCenter and allocated on a per-VMDK basis, which can then be associated to Storage Services within IBM Spectrum Connect.
- Granularity. More granular visibility of VM storage consumption and performance. Because each VMDK exists as a volume within IBM Storage Virtualize, the storage administrator can see the precise workload for an application rather than a combination of all I/O from multiple VMs to a volume.
- No shared storage. No per-LUN I/O contention or VMFS overhead. Sequential I/O from multiple VMs can be easily identified and processed in a more efficient manner on the storage system.

With vVol, the IBM storage systems recognize individual VMDKs, which allows data operations, such as snapshots, to be performed directly by the storage system at the VM level. The storage system uses the VASA provider IBM Spectrum Connect to present vVols to the ESXi host and inform the vCenter of the availability of vVol-aware storage by using Protocol Endpoints (PEs).

One PE, also known as Administrative LUN or PE, is presented at each node in the IBM Storage Virtualize cluster. A PE presents itself as a traditional storage device and is detected by an ESXi server like a normal volume mapping. However, PEs offer a more efficient method for vVols to be mapped and detected by ESXi hosts when compared to traditional volume mappings and do not require a rescan of host bus adapter (HBA).

IBM Storage Virtualize automatically provisions PEs to all ESXi hosts that meet the following configuration requirements:

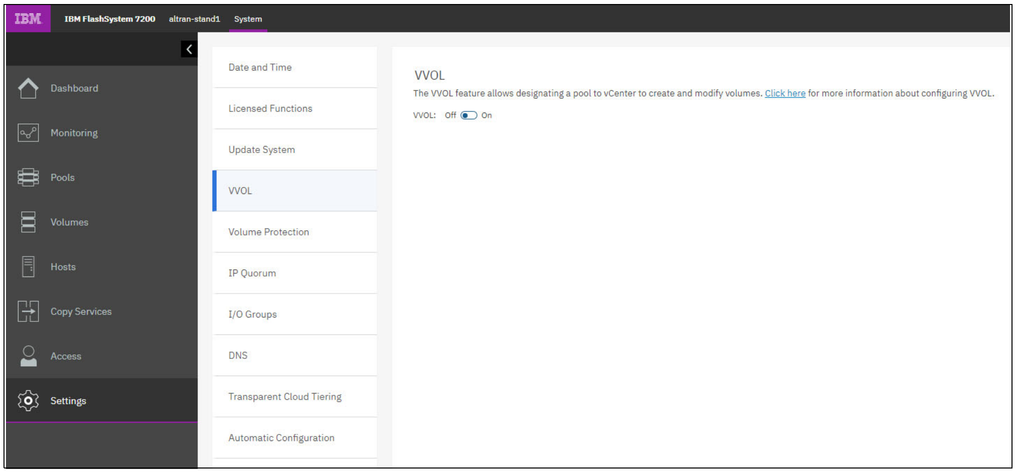
- The vVol host type, when the UI is used to perform configuration
- The **`adminlun`** option, when the CLI is used to perform configuration

Storage services are configured on the IBM Spectrum Connect server by the storage administrator. Storage services are then used to configure various storage containers with specific capabilities that can later be configured as vVol datastores in the vSphere Client.

8.3.2 Configuring IBM Storage Virtualize to support vVols

To enable vVols on the IBM Storage Virtualize storage system, complete the following steps:

1. Go to the Settings window of the management interface, and select **vVol** (Figure 8-21).



VVOL

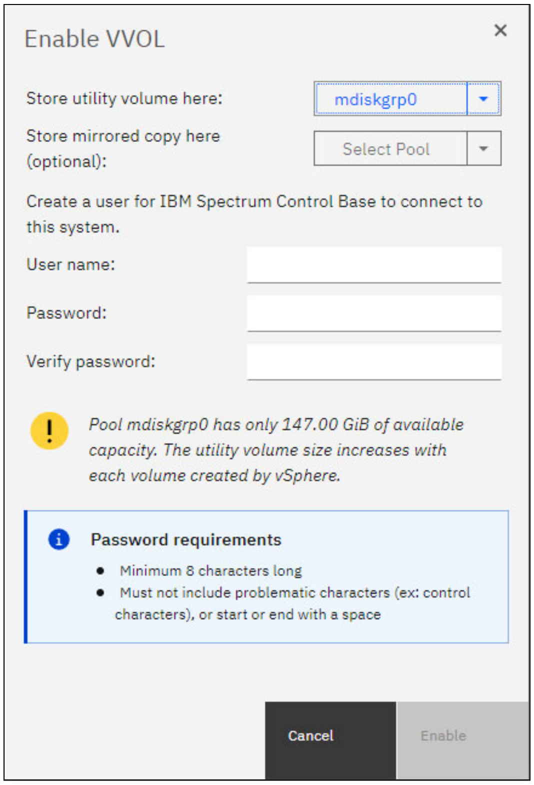
The VVOL feature allows designating a pool to vCenter to create and modify volumes. Click here for more information about configuring VVOL.

VVOL: Off ○ On

Figure 8-21 Settings window: VVOL

> **Note:** To keep time synchronized between all components of the vVol infrastructure, ensure that an NTP server is defined on the storage system, IBM Spectrum Connect server, vCenter, and ESXi hosts.

2. Set the VVOL switch to **ON** to display more options (Figure 8-22).



Enable VVOL

Store utility volume here: mdiskgrp0

Store mirrored copy here (optional): Select Pool

Create a user for IBM Spectrum Control Base to connect to this system.

User name:

Password:

Verify password:

Pool mdiskgrp0 has only 147.00 GiB of available capacity. The utility volume size increases with each volume created by vSphere.

Password requirements

- Minimum 8 characters long
- Must not include problematic characters (ex: control characters), or start or end with a space

Figure 8-22 Enable VVOL:1

3. Choose a storage pool to store the 2 TB Utility Volume. This space-efficient volume holds the IBM Spectrum Connect metadata database, which is essential for managing your vVol environment.

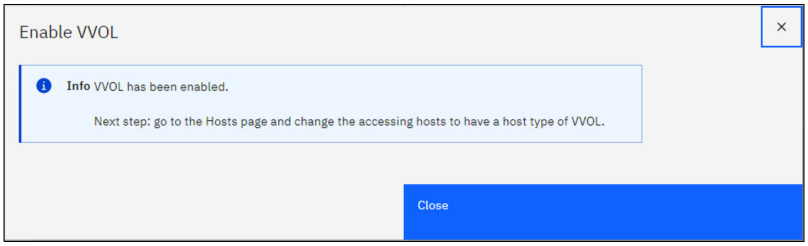
   Although the volume is created with a capacity of 2 TB, it is unlikely to require more than 2 GB of capacity.

   If possible, consider creating a mirrored copy of this Utility Volume by selecting a second pool to store the additional copy.

4. Define credentials for a newly dedicated user account, which enables the IBM Spectrum Control server to connect to the CLI of the storage system.

   This process initially creates a User Group within the IBM Storage Virtualize Storage system that is assigned with the VASA Provider role, and then creates the User Account by using the specified credentials within that user group.

5. Click **Enable** (Figure 8-22).



Enable VVOL

Info VVOL has been enabled.

Next step: go to the Hosts page and change the accessing hosts to have a host type of VVOL.

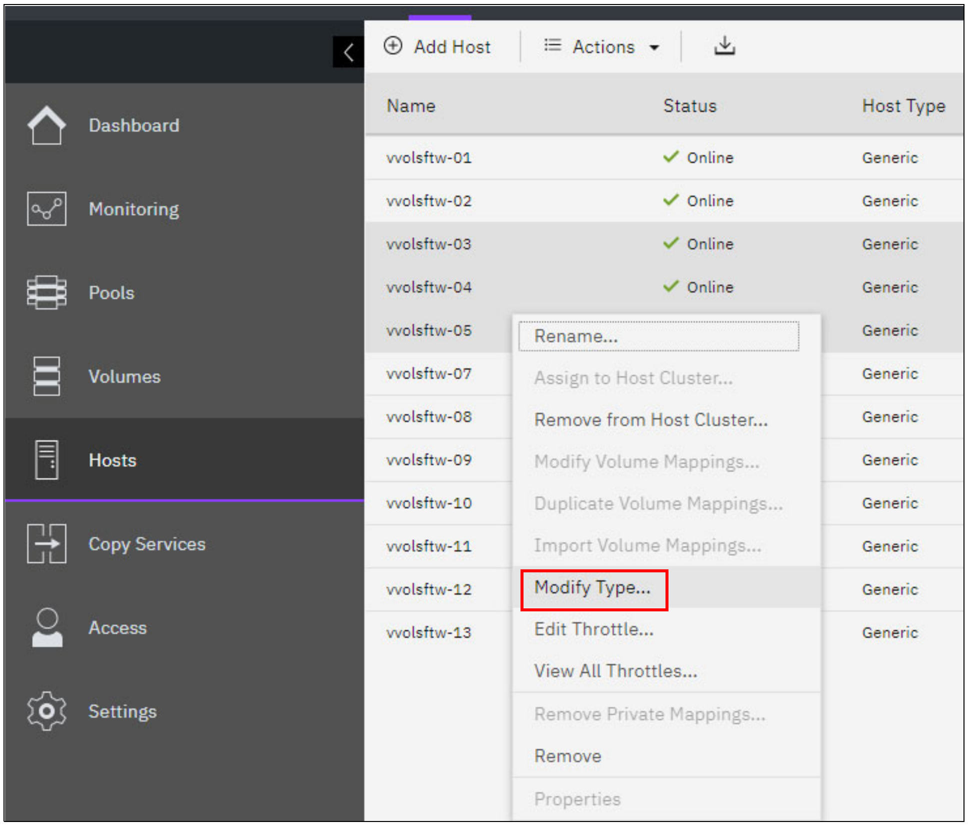
Figure 8-23 Enable VVOL: 2

6. Configure host objects to be vVol-enabled.

   You can modify host types on either an individual host or a host-cluster basis, as follows:

   – Individual hosts:

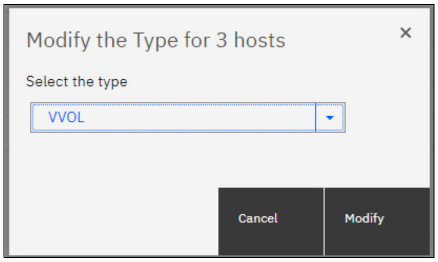
     i. Select **Hosts**. Right-click the hosts that you want to enable and select **Modify Type** (Figure 8-24).


Add Host
Actions
Dashboard
Monitoring
Pools
Volumes
Hosts
Copy Services
Access
Settings
Rename...
Assign to Host Cluster...
Remove from Host Cluster...
Modify Volume Mappings...
Duplicate Volume Mappings...
Import Volume Mappings...
Modify Type...
Edit Throttle...
View All Throttles...
Remove Private Mappings...
Remove
Properties

Name	Status	Host Type
vvolsftw-01	✓ Online	Generic
vvolsftw-02	✓ Online	Generic
vvolsftw-03	✓ Online	Generic
vvolsftw-04	✓ Online	Generic
vvolsftw-05		Generic
vvolsftw-07		Generic
vvolsftw-08		Generic
vvolsftw-09		Generic
vvolsftw-10		Generic
vvolsftw-11		Generic
vvolsftw-12		Generic
vvolsftw-13		Generic

Figure 8-24 Selecting Modify Type

     ii. Select **VVOL** and click **Modify** (Figure 8-25).



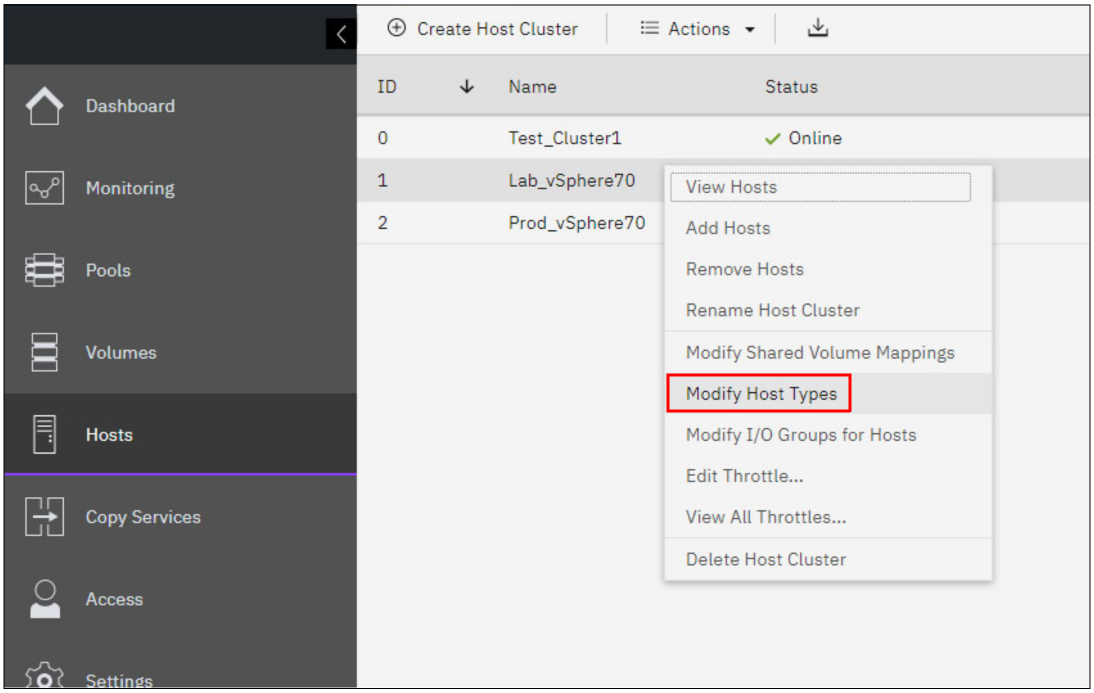
Modify the Type for 3 hosts

Select the type: VVOL

Figure 8-25 Clicking Modify

– Configure host clusters:

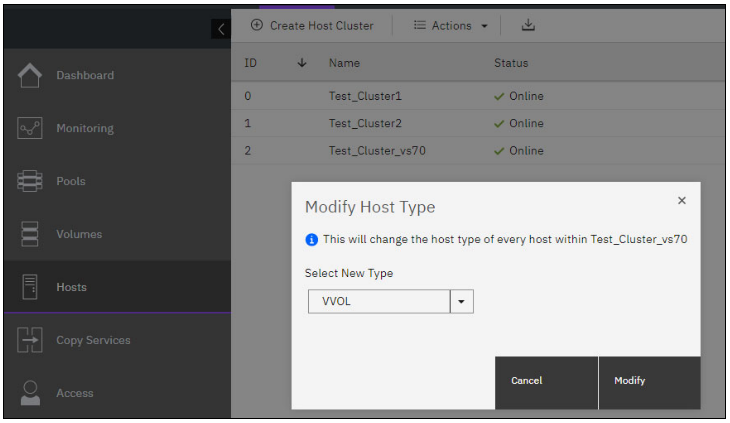
i. Select **Hosts** → **Host Clusters**. Right-click the host cluster that you want to enable and select **Modify Host Types**, as shown in Figure 8-26.



ID	Name	Status
0	Test_Cluster1	✓ Online
1	Lab_vSphere70	
2	Prod_vSphere70	

Figure 8-26 Selecting Modify Types

ii. Select **VVOL** and click **Modify** (Figure 8-27).



ID	Name	Status
0	Test_Cluster1	✓ Online
1	Test_Cluster2	✓ Online
2	Test_Cluster_vs70	✓ Online

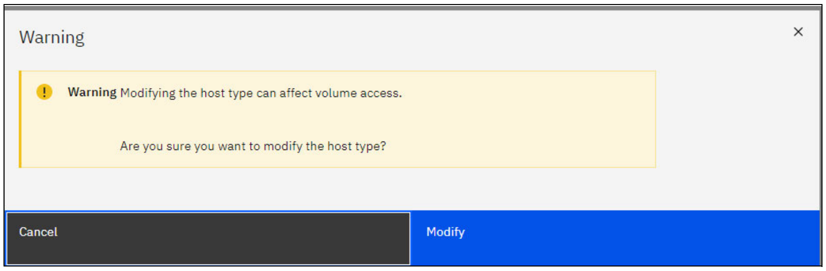
Modify Host Type

This will change the host type of every host within Test_Cluster_vs70

Select New Type: VVOL

Figure 8-27 Clicking Modify

A warning is displayed (Figure 8-28 on page 201).



Warning

Warning Modifying the host type can affect volume access.

Are you sure you want to modify the host type?

Figure 8-28 Warning message

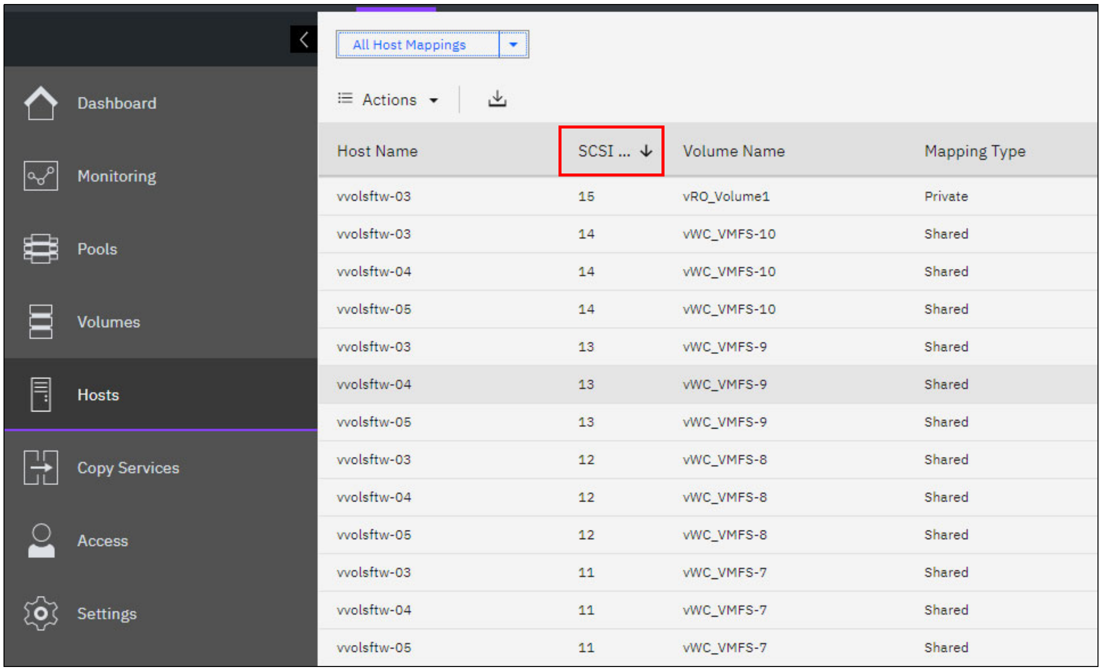
Hosts with a generic host-type allow volumes to be mapped with a Small Computer System Interface (SCSI) ID of 0–2048. However, ESXi detects only SCSI IDs 0–1023.

> **Note:** Hosts with a vVol or `adminlun` host type are limited to SCSI IDs 0–511. This warning refers to existing volumes that might be mapped with a SCSI ID that is greater than 511 that are lost when changing the host type to support vVols.

Normally, the lowest available SCSI ID is used when a volume is mapped to a host. Therefore, it is only in rare circumstances where either more than 511 volumes are mapped to a host or host cluster or a SCSI ID above 511 is specified when a previous mapping was created.

7. Verify the existing SCSI IDs by reviewing the existing host mappings for a host or host cluster:

   a. Select **Hosts** → **Mappings** in the navigation menu, and select **All host mappings**. Sort the mappings in descending order by the SCSI ID column to show the highest SCSI IDs in use (Figure 8-29).



Host Name	SCSI ... ↓	Volume Name	Mapping Type
vvolsftw-03	15	vRO_Volume1	Private
vvolsftw-03	14	vWC_VMFS-10	Shared
vvolsftw-04	14	vWC_VMFS-10	Shared
vvolsftw-05	14	vWC_VMFS-10	Shared
vvolsftw-03	13	vWC_VMFS-9	Shared
vvolsftw-04	13	vWC_VMFS-9	Shared
vvolsftw-05	13	vWC_VMFS-9	Shared
vvolsftw-03	12	vWC_VMFS-8	Shared
vvolsftw-04	12	vWC_VMFS-8	Shared
vvolsftw-05	12	vWC_VMFS-8	Shared
vvolsftw-03	11	vWC_VMFS-7	Shared
vvolsftw-04	11	vWC_VMFS-7	Shared
vvolsftw-05	11	vWC_VMFS-7	Shared

Figure 8-29 Sorting the mappings in descending order

   b. Ensure that SCSI IDs above 511 are not in use before you change the host type.

8. Confirm the identifiers for the PEs by connecting to the CLI of the storage-system management interface by using ssh and run the CLI command **`svcinfo lsadminlunv`** (Example 8-1):

Example 8-1 The svcinfo lsadminlun command

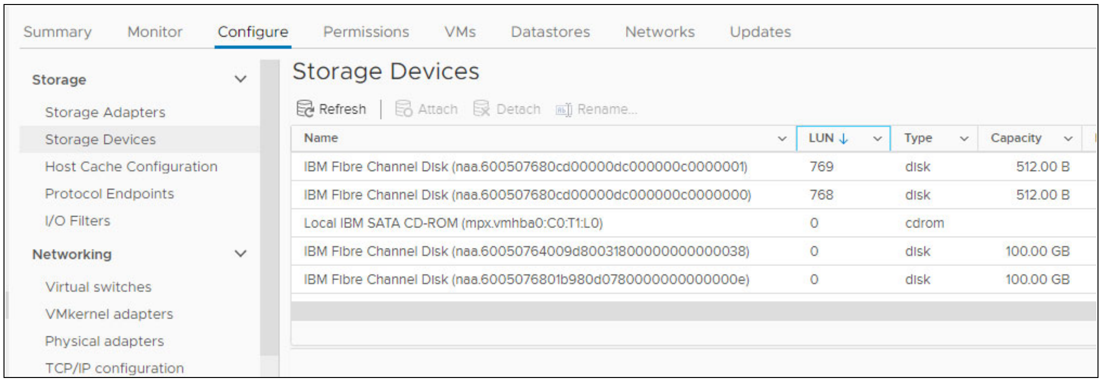
```
IBM_FlashSystem:FS9200-CL:superuser>svcinfo lsadminlun

id SCSI_id          UID
0  0300000000000000 600507680CD00000DC000000C0000000
1  0301000000000000 600507680CD00000DC000000C0000001
```

> **Note:** In Example 8-1:
>
> - The `SCSI_id` column contains the SCSI ID as a hexadecimal value.
>
>   The corresponding value, as reported by either vSphere or the ESXi, is a decimal number.
>
> - The `UID` column appears similar to a traditional LUN UUID. However, the `C` character distinguishes it from a traditional volume.

c. Rescan the HBAs of the hosts to detect the PEs.

d. Verify that the PEs are visible from the ESXi servers. In vSphere, select a host from the inventory and select **Configure** → **Storage Devices** (Figure 8-30).



Storage Devices

Name	LUN ↓	Type	Capacity
IBM Fibre Channel Disk (naa.600507680cd00000dc000000c0000001)	769	disk	512.00 B
IBM Fibre Channel Disk (naa.600507680cd00000dc000000c0000000)	768	disk	512.00 B
Local IBM SATA CD-ROM (mpx.vmhba0:C0:T1:L0)	0	cdrom	
IBM Fibre Channel Disk (naa.60050764009d80031800000000000038)	0	disk	100.00 GB
IBM Fibre Channel Disk (naa.6005076801b980d0780000000000000e)	0	disk	100.00 GB

Figure 8-30 Storage Devices

e. Sort the LUN column in descending order and confirm that a PE exists for each node in the storage system.

In a standard two-node, single I/O-group cluster, two PEs are presented. SCSI IDs that are used for the first PEs start at 768–769, and increase for each additional node in the storage system.

8.3.3 Configuring IBM Spectrum Connect

VASA Credentials, which vCenter uses to connect to the IBM Spectrum Connect server, must be defined.

To define VASA credentials, complete the following steps:

1. Log in to the management interface of IBM Spectrum Connect.
2. Select **VASA Provider settings** from the **Settings** menu (Figure 8-31 on page 203).

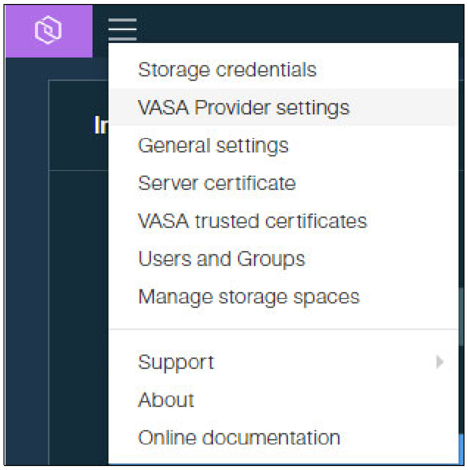
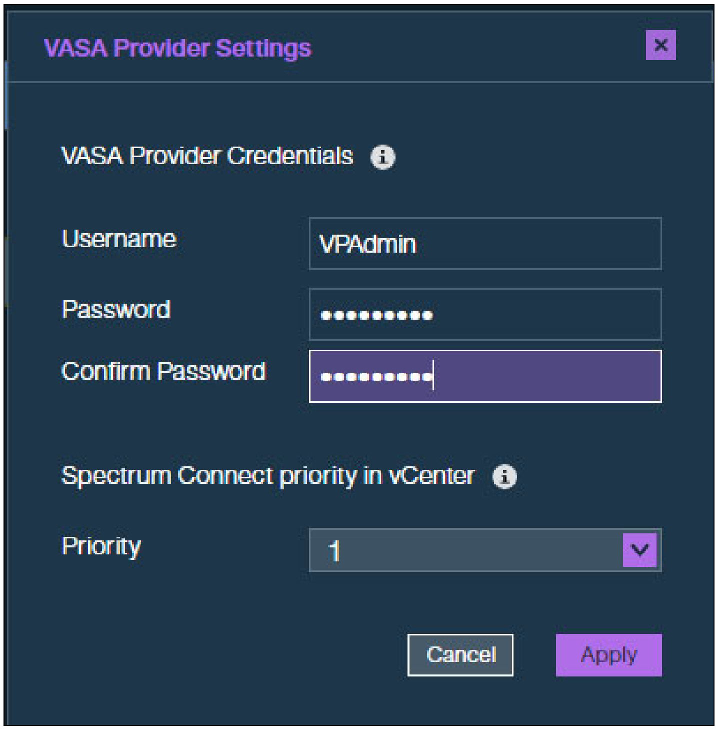


Figure 8-31 VASA Provider settings

3. Define the credentials that vCenter uses to connect to IBM Spectrum Connect when the storage provider is registered (Figure 8-32).



VASA Provider Settings

VASA Provider Credentials

Username VPAdmin

Password ●●●●●●●●●

Confirm Password ●●●●●●●●●

Spectrum Connect priority in vCenter

Priority 1

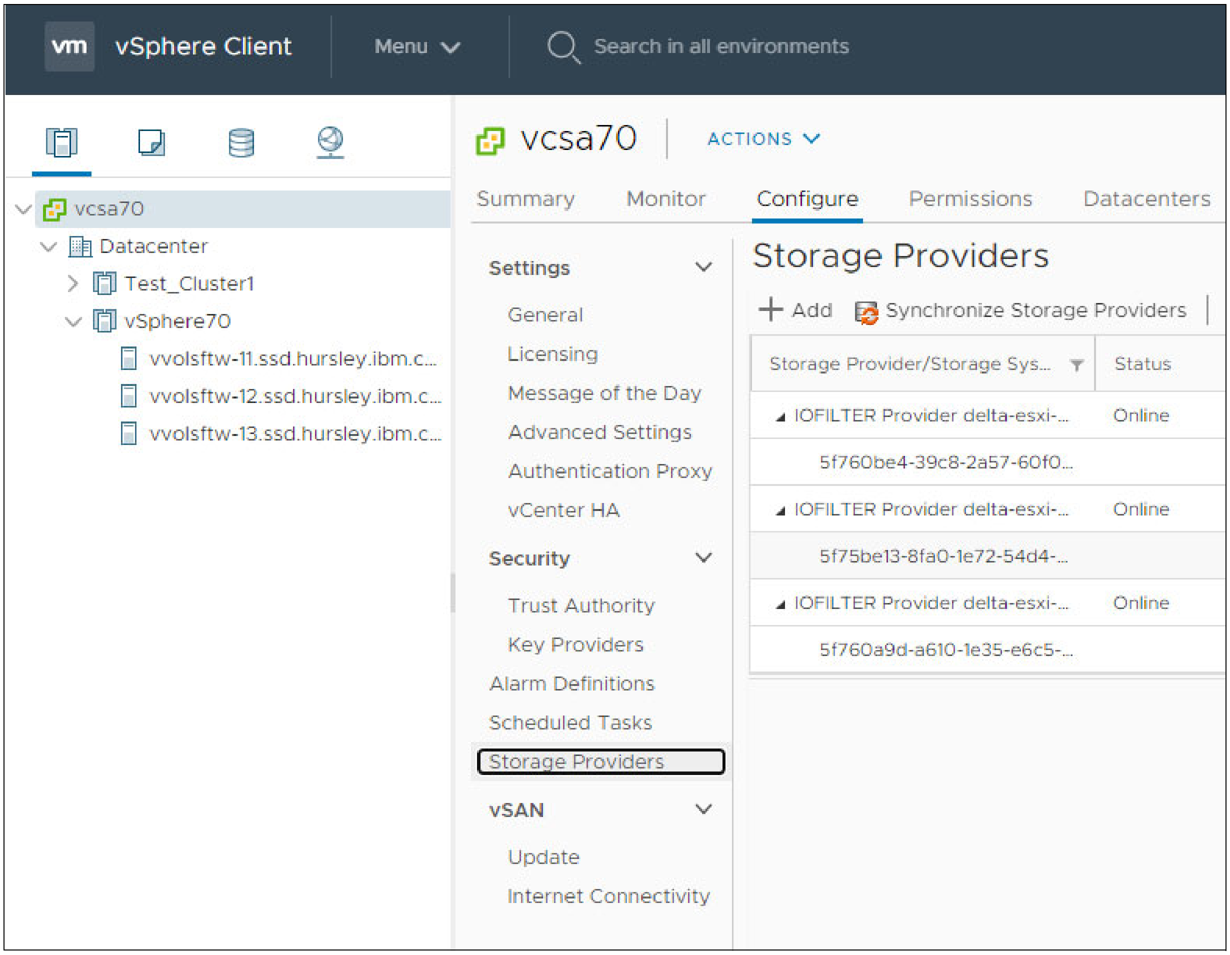
Figure 8-32 VASA Provider Credentials

4. Click **Apply**.

8.3.4 Configuring VMware vSphere vCenter

To register the IBM Spectrum Connect server in vSphere as a Storage Provider, complete the following steps:

1. In the vSphere client, select the vCenter server in the inventory on the left pane, click the **Configure** tab, and select **Storage Providers** under **Security** (Figure 8-33).



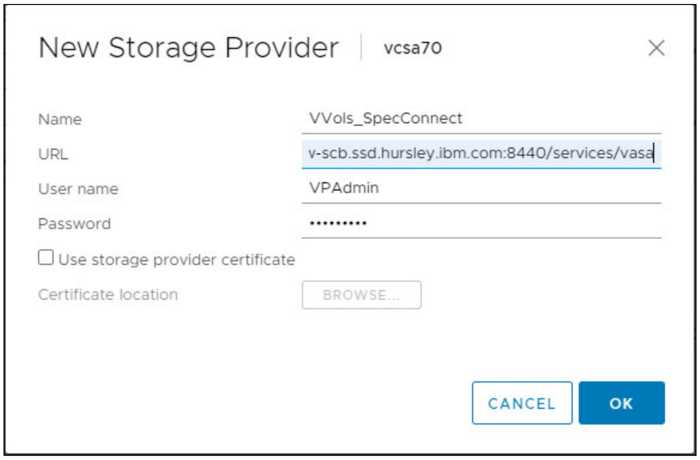
Storage Provider/Storage Sys...	Status
IOFILTER Provider delta-esxi-...	Online
5f760be4-39c8-2a57-60f0...	
IOFILTER Provider delta-esxi-...	Online
5f75be13-8fa0-1e72-54d4-...	
IOFILTER Provider delta-esxi-...	Online
5f760a9d-a610-1e35-e6c5-...	

Figure 8-33 Storage Providers

2. Click **Add** to register a new Storage Provider.

3. Enter the name, URL of the IBM Spectrum Connect server, and the VASA Provider credentials (Figure 8-34 on page 205) as configured in the “Configuring IBM Spectrum Connect” on page 202.

> **Note:** The URL must be in the format of `https://<IP or FQDN of Spectrum Connect server>:8440/services/vasa`.



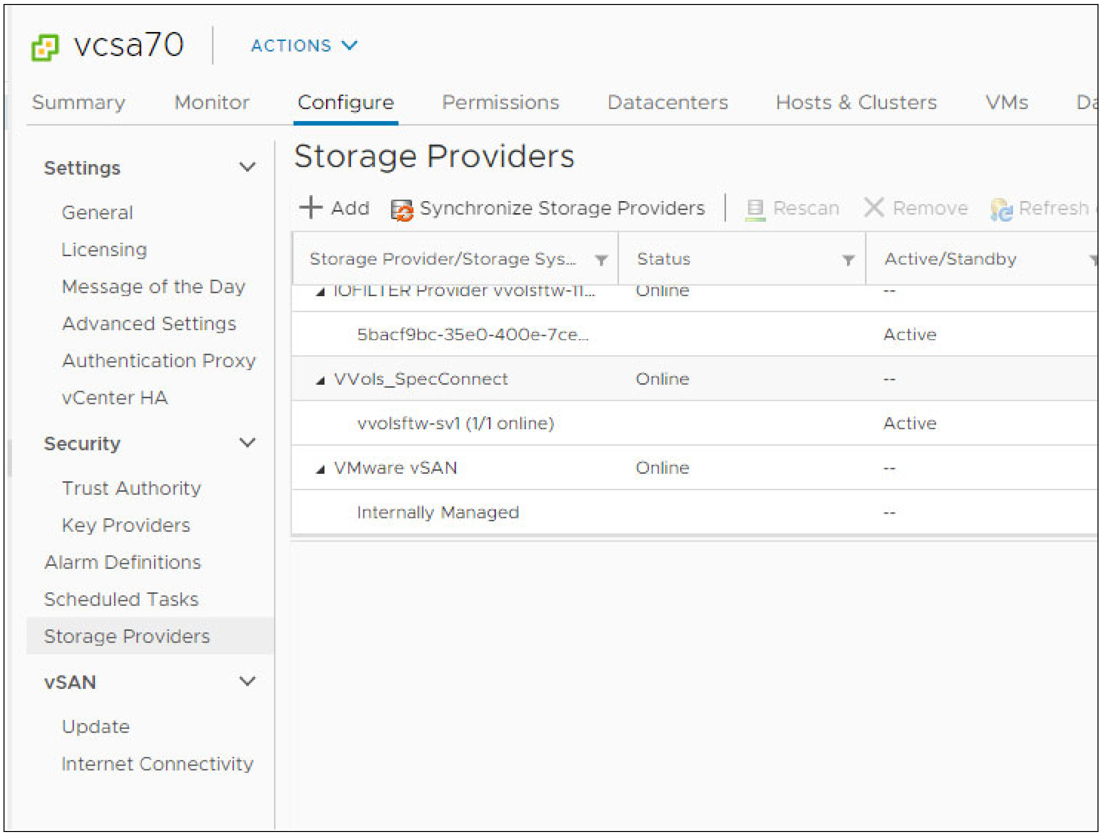
Name	VVols_SpecConnect
URL	v-scb.ssd.hursley.ibm.com:8440/services/vasa
User name	VPAdmin
Password	•••••••••

□ Use storage provider certificate

Certificate location BROWSE...

Figure 8-34 New Storage Provider

4. Click **OK**. The Storage Providers list includes the newly registered storage provider (Figure 8-35).



Storage Provider/Storage Sys...	Status	Active/Standby
IOFILTER Provider vvolsftw-fl...	Online	--
5bacf9bc-35e0-400e-7ce...		Active
VVols_SpecConnect	Online	--
vvolsftw-sv1 (1/1 online)		Active
VMware vSAN	Online	--
Internally Managed		--

Figure 8-35 A newly registered storage provider is shown

8.3.5 Creating a vVol datastore

Before you create a vVol datastore, you must ensure that you created vVol-enabled Storage Services as described in 8.2.1, “Creating Storage Services” on page 189.

In this example, various vVol-enabled storage services are created and delegated in the following environments:

- Production systems and applications
- Development or test environments
- An application environment that requires encryption or extra security considerations and must be isolated from other applications

Each storage service can be configured with specific capabilities such as Space Efficiency, Encryption, and Storage Tier (Figure 8-36).

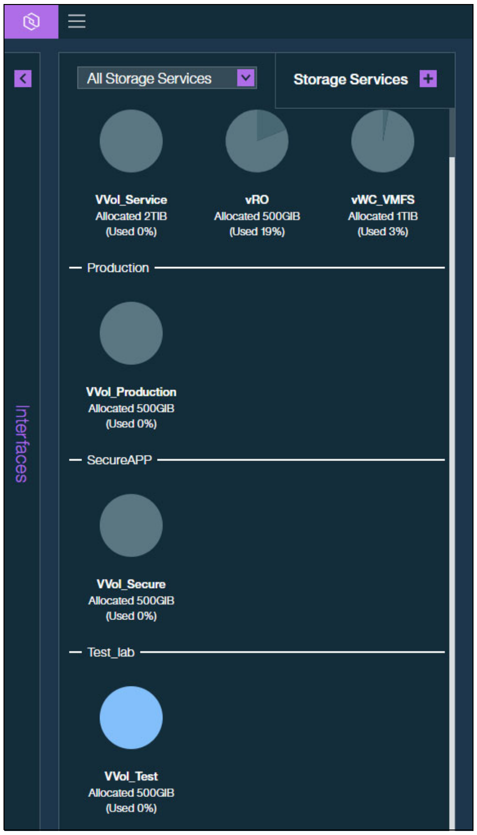


Figure 8-36 vVol-enabled Storage Services

Each Storage Services was allocated a storage resource and associated to the vCenter interface (Figure 8-37 on page 207). See 8.2.3, “Delegating Storage Services to vCenter” on page 194.

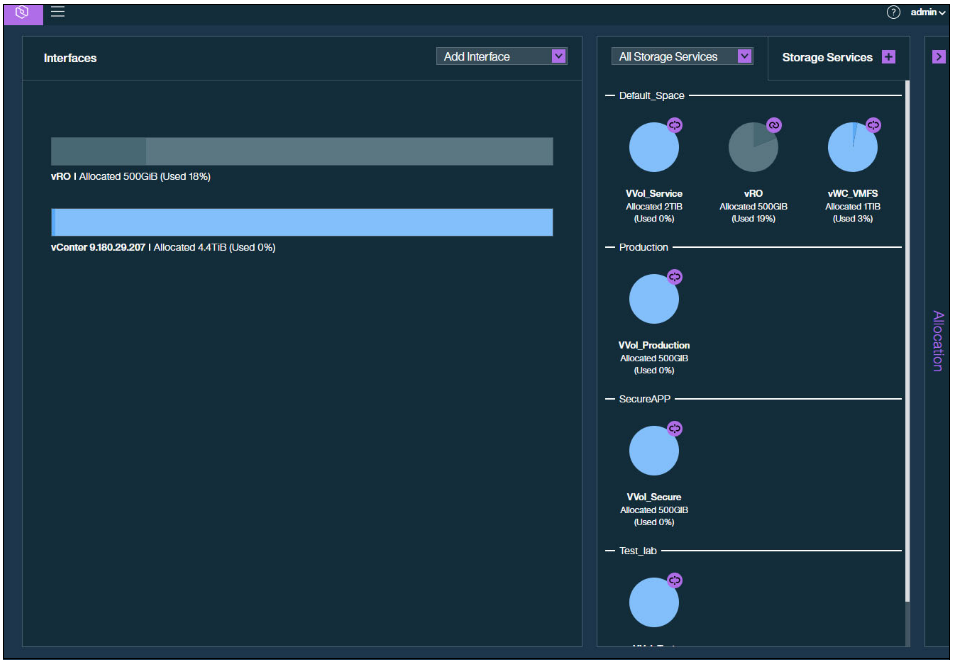


Figure 8-37 vVol-enabled Storage Services delegated to a vCenter interface

After the Storage Containers are configured, create the vVol datastore by completing the following steps:

1. In the vSphere Client window, identify the host or host-cluster for which you want to configure the vVol datastore by right-clicking the object in the vSphere inventory and selecting **Storage** → **New Datastore** (Figure 8-38 on page 208).
2. Select **vVol**, and click **NEXT** (Figure 8-39 on page 208).
3. Select the hosts that require access to the datastore (Figure 8-41 on page 209) and click **NEXT**. Review the summary and click **FINISH**.
4. Enter a name for the VVol datastore, select the related Storage Container from the list, and click **NEXT** (Figure 8-40 on page 209).
5. Repeat this process for any additional vVol datastores (Figure 8-42 on page 210). When the process is finished, the datastores are ready for use.

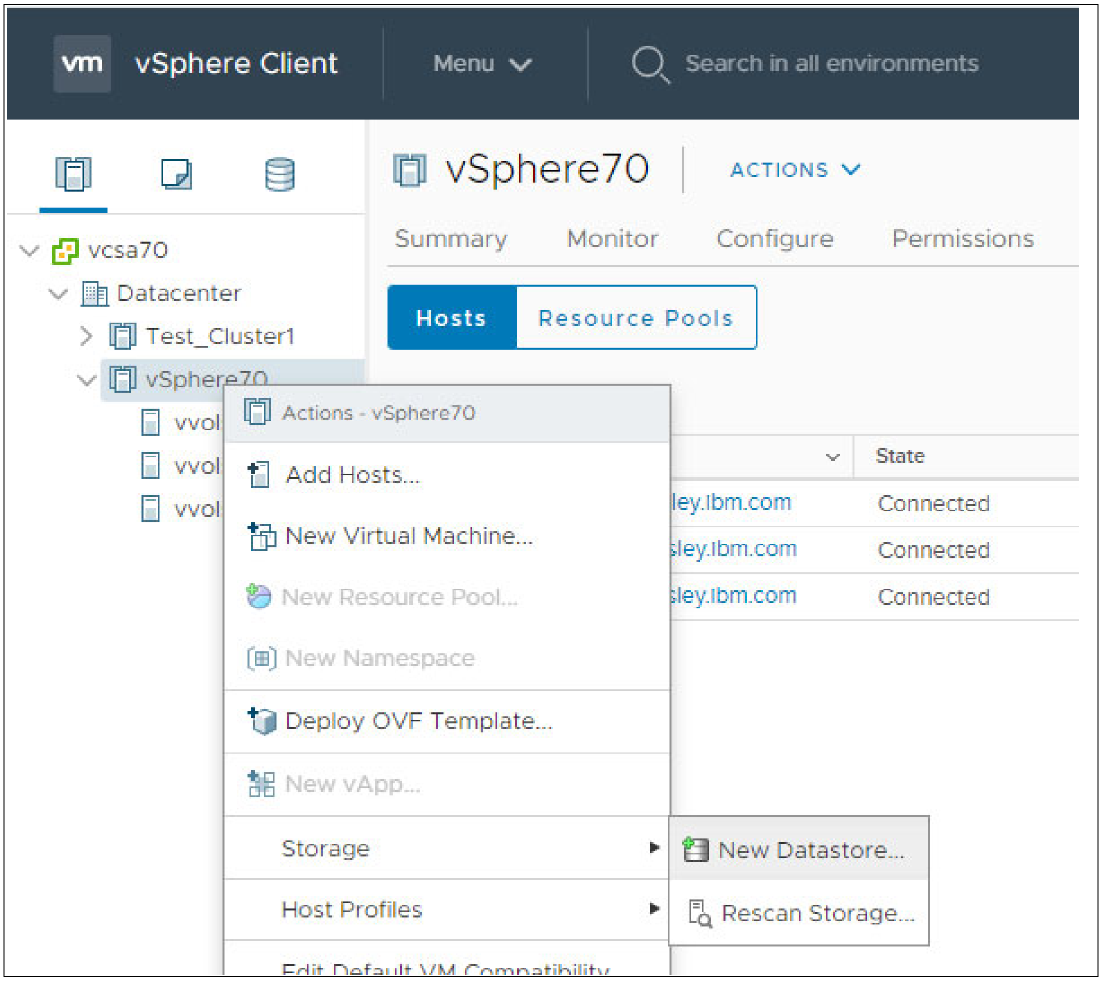
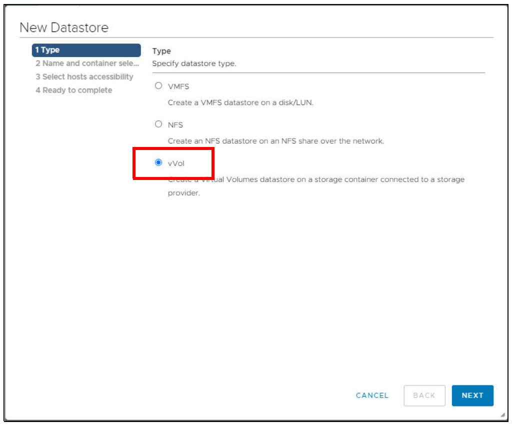


Figure 8-38 New Datastore:1



New Datastore

1 Type
2 Name and container sele...
3 Select hosts accessibility
4 Ready to complete

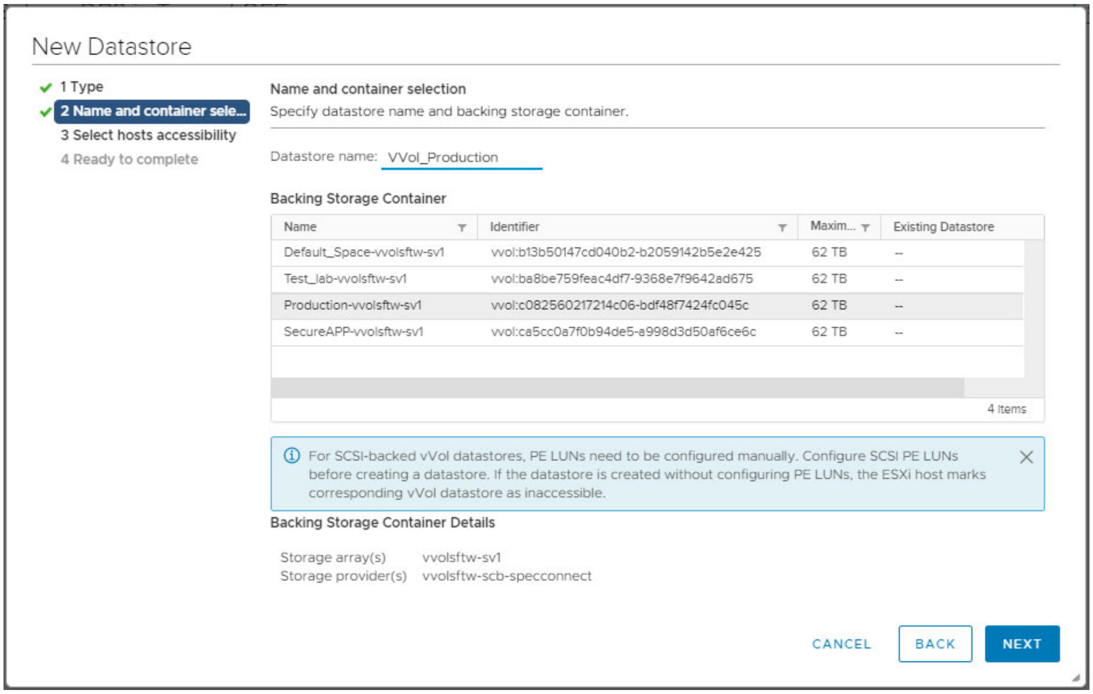
Type
Specify datastore type.

○ VMFS
Create a VMFS datastore on a disk/LUN.

○ NFS
Create an NFS datastore on an NFS share over the network.

● vVol
Create a Virtual Volumes datastore on a storage container connected to a storage provider.

Figure 8-39 New Datastore: 2



New Datastore

Name and container selection

Specify datastore name and backing storage container.

Datastore name: VVol_Production

Backing Storage Container

Name	Identifier	Maxim...	Existing Datastore
Default_Space-vvolsftw-sv1	vvol:b13b50147cd040b2-b2059142b5e2e425	62 TB	--
Test_lab-vvolsftw-sv1	vvol:ba8be759feac4df7-9368e7f9642ad675	62 TB	--
Production-vvolsftw-sv1	vvol:c082560217214c06-bdf48f7424fc045c	62 TB	--
SecureAPP-vvolsftw-sv1	vvol:ca5cc0a7f0b94de5-a998d3d50af6ce6c	62 TB	--

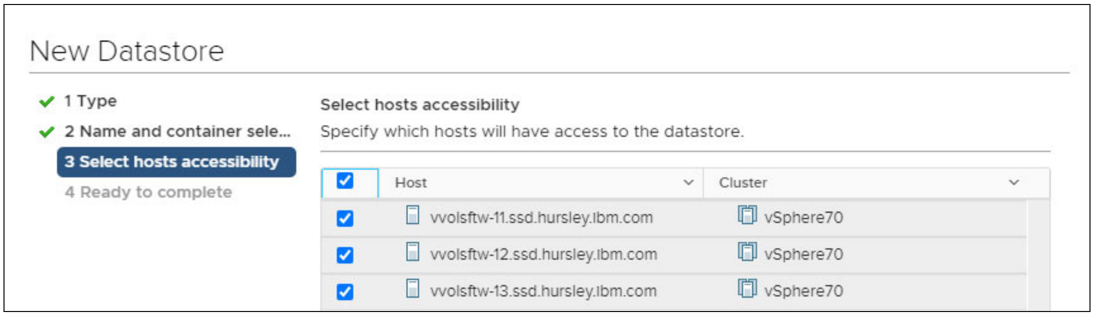
4 Items

For SCSI-backed vVol datastores, PE LUNs need to be configured manually. Configure SCSI PE LUNs before creating a datastore. If the datastore is created without configuring PE LUNs, the ESXi host marks corresponding vVol datastore as inaccessible.

Backing Storage Container Details

Storage array(s) vvolsftw-sv1
Storage provider(s) vvolsftw-scb-specconnect

Figure 8-40 New Datastore: 3



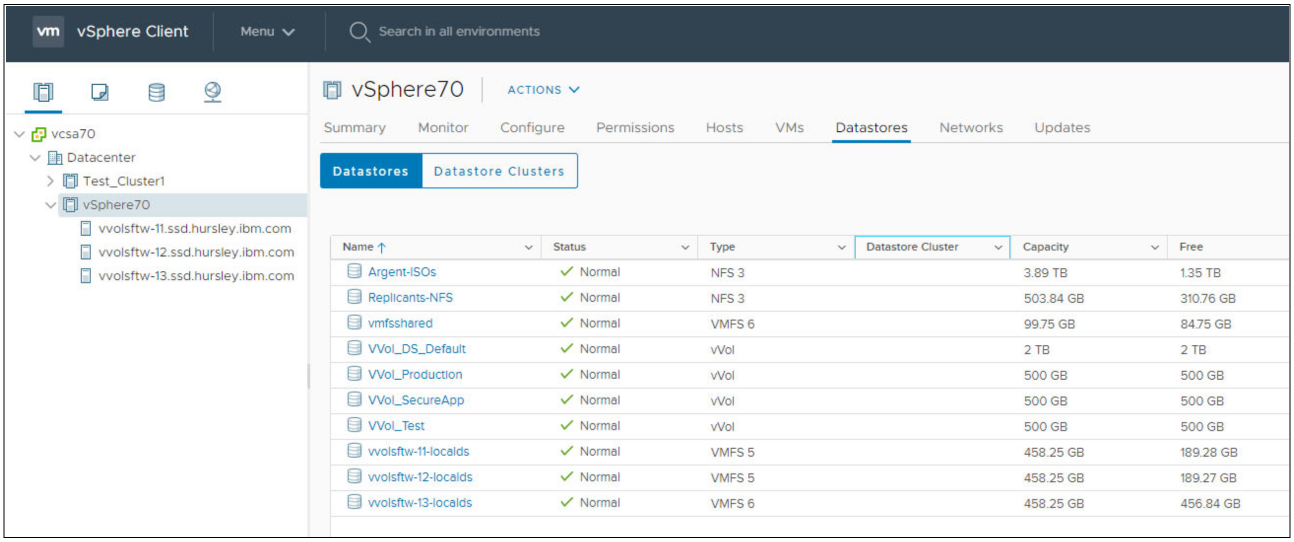
New Datastore

Select hosts accessibility

Specify which hosts will have access to the datastore.

☑	Host	Cluster
☑	vvolsftw-11.ssd.hursley.ibm.com	vSphere70
☑	vvolsftw-12.ssd.hursley.ibm.com	vSphere70
☑	vvolsftw-13.ssd.hursley.ibm.com	vSphere70

Figure 8-41 New Datastore: 4



Name ↑	Status	Type	Datastore Cluster	Capacity	Free
Argent-ISOs	✓ Normal	NFS 3		3.89 TB	1.35 TB
Replicants-NFS	✓ Normal	NFS 3		503.84 GB	310.76 GB
vmfsshared	✓ Normal	VMFS 6		99.75 GB	84.75 GB
VVol_DS_Default	✓ Normal	vVol		2 TB	2 TB
VVol_Production	✓ Normal	vVol		500 GB	500 GB
VVol_SecureApp	✓ Normal	vVol		500 GB	500 GB
VVol_Test	✓ Normal	vVol		500 GB	500 GB
vvolsftw-11-localds	✓ Normal	VMFS 5		458.25 GB	189.28 GB
vvolsftw-12-localds	✓ Normal	VMFS 5		458.25 GB	189.27 GB
vvolsftw-13-localds	✓ Normal	VMFS 6		458.25 GB	456.84 GB

Figure 8-42 Repeating the process for any additional vVol datastores

8.4 Best-practice considerations and troubleshooting

This section describes best-practice considerations and troubleshooting tips.

8.4.1 Protecting the IBM Spectrum Connect server

The IBM Spectrum Connect server is the key component in facilitating integration between multiple VMware platforms and IBM Storage Virtualize storage systems.

Therefore, it is a best practice to protect the IBM Spectrum Connect server to enable optimal functions:

- Where possible, use VMware vSphere Fault Tolerance (FT) to ensure that if there is an outage to the ESXi host that is running the IBM Spectrum Connect server, then the wider infrastructure is still able to access the IBM Spectrum Connect integrations. If FT is not available, then ensure that vSphere HA is used to minimize downtime of the server hosting the IBM Spectrum Connect application.
- Allocate appropriate compute resources to the IBM Spectrum Connect VM. Because the applications run as a conduit between the multiple VMware interfaces and multiple storage systems, performance of the end-to-end system is impacted if resources are limited.
- Most importantly, ensure that all VMs associated with providing the vVol infrastructure are not stored on a VMware vSphere Virtual Volume datastore, which includes the vCenter Service Appliance (vCSA), the IBM Spectrum Connect server, and other servers that these applications require to function.

  If an outage occurs, the IBM Spectrum Connect server must start before any vVol operations function.

  If the IBM Spectrum Connect server depends on an external LDAP or NFS server that is on a vVol datastore, then it fails to successfully start IBM Spectrum Connect services. If IBM Spectrum Connect services fail to start, then vVol datastores are inaccessible and VMs on the vVol datastore are unavailable. If this situation occurs, contact IBM Support.

8.4.2 Viewing the relationships between vVol and VM

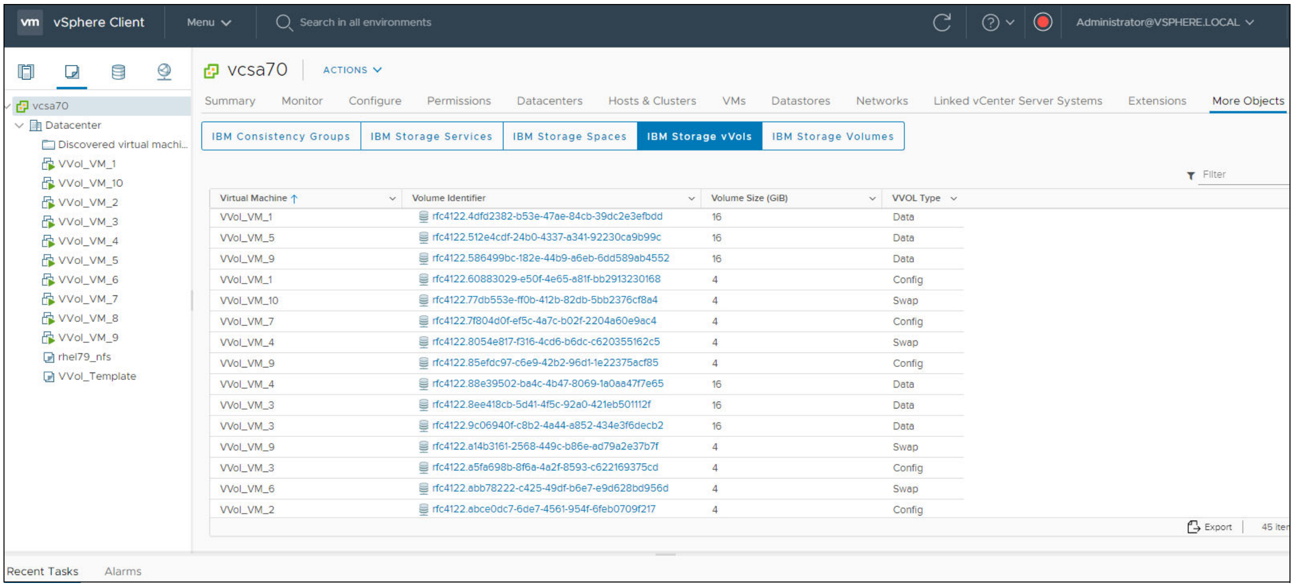
Because the vVols are created with a unique identifier, it can be difficult to establish to which VM a vVol belongs and to which vVols a VM is associated.

By creating the association between the vVol-enabled storage service and the vCenter interface in IBM Spectrum Connect, the IBM Storage Enhancements plug-in can assimilate information from both systems.

The relationships between vVols and VMs can then be displayed for the vSphere administrator.

To access display of vVol and VM relationships, complete the following steps:

1. Locate the top-level vCenter object in the vSphere Client inventory, and select the **More Objects** tab (Figure 8-43).



Virtual Machine	Volume Identifier	Volume Size (GiB)	VVOL Type
VVol_VM_1	rfc4122.4dfd2382-b53e-47ae-84cb-39dc2e3efbdd	16	Data
VVol_VM_5	rfc4122.512e4cdf-24b0-4337-a341-92230ca9b99c	16	Data
VVol_VM_9	rfc4122.586499bc-182e-44b9-a6eb-6dd589ab4552	16	Data
VVol_VM_1	rfc4122.60883029-e50f-4e65-a81f-bb2913230168	4	Config
VVol_VM_10	rfc4122.77db553e-ff0b-412b-82db-5bb2376cf8a4	4	Swap
VVol_VM_7	rfc4122.7f804d0f-ef5c-4a7c-b02f-2204a60e9ac4	4	Config
VVol_VM_4	rfc4122.8054e817-f316-4cd6-b6dc-c620355162c5	4	Swap
VVol_VM_9	rfc4122.85efdc97-c6e9-42b2-96d1-1e22375acf85	4	Config
VVol_VM_4	rfc4122.88e39502-ba4c-4b47-8069-1a0aa47f7e65	16	Data
VVol_VM_3	rfc4122.8ee418cb-5d41-4f5c-92a0-421eb501112f	16	Data
VVol_VM_3	rfc4122.9c06940f-c8b2-4a44-a852-434e3f6decb2	16	Data
VVol_VM_9	rfc4122.a14b3161-2568-449c-b86e-ad79a2e37b7f	4	Swap
VVol_VM_3	rfc4122.a5fa698b-8f6a-4a2f-8593-c622169375cd	4	Config
VVol_VM_6	rfc4122.abb78222-c425-49df-b6e7-e9d628bd956d	4	Swap
VVol_VM_2	rfc4122.abce0dc7-6de7-4561-954f-6feb0709f217	4	Config

Figure 8-43 Selecting IBM Storage vVols

2. Click **IBM Storage vVols** to list the detected vVols on the storage array and the vVols size and type.
3. If required, export the list as a CSV file to generate a report.

   For more information about the IBM Storage Enhancements plug-in, see 8.5, “IBM Storage Enhancements for VMware vSphere Web Client plug-in” on page 218.

8.4.3 Mirroring the utility volume

A utility volume is created on the storage system as part of the configuration of vVols. IBM Spectrum Connect creates and manages a database on the utility volume. The VM metadata that is stored in this database is critical to both IBM Spectrum Connect operations and the vVols environment.

Because the availability and integrity of the utility volume is fundamental to the vVols environment, store a mirrored copy of the volume for redundancy. If possible, store the mirrored copy in a second storage pool that is in a separate failure domain. For example, use a storage pool that is created with managed disks (MDisks) that are from different storage systems or separate I/O groups.

8.4.4 Performing an upgrade on a storage system with vVols enabled

During a code upgrade, the storage system intentionally limits the tasks that a user can run from both the GUI and CLI. This measure is a protective one to ensure that the upgrade is not disrupted. Because managing VMs on vVols datastores requires the running of CLI commands on the system, the same restrictions apply in the vVols environment.

Therefore, VM-management tasks (for example, powering off a VM) fail when an upgrade is running on the storage system. Automated services, such as VMware HA and Distributed Resource Scheduler (DRS), also are affected because they send system commands by using IBM Spectrum Connect.

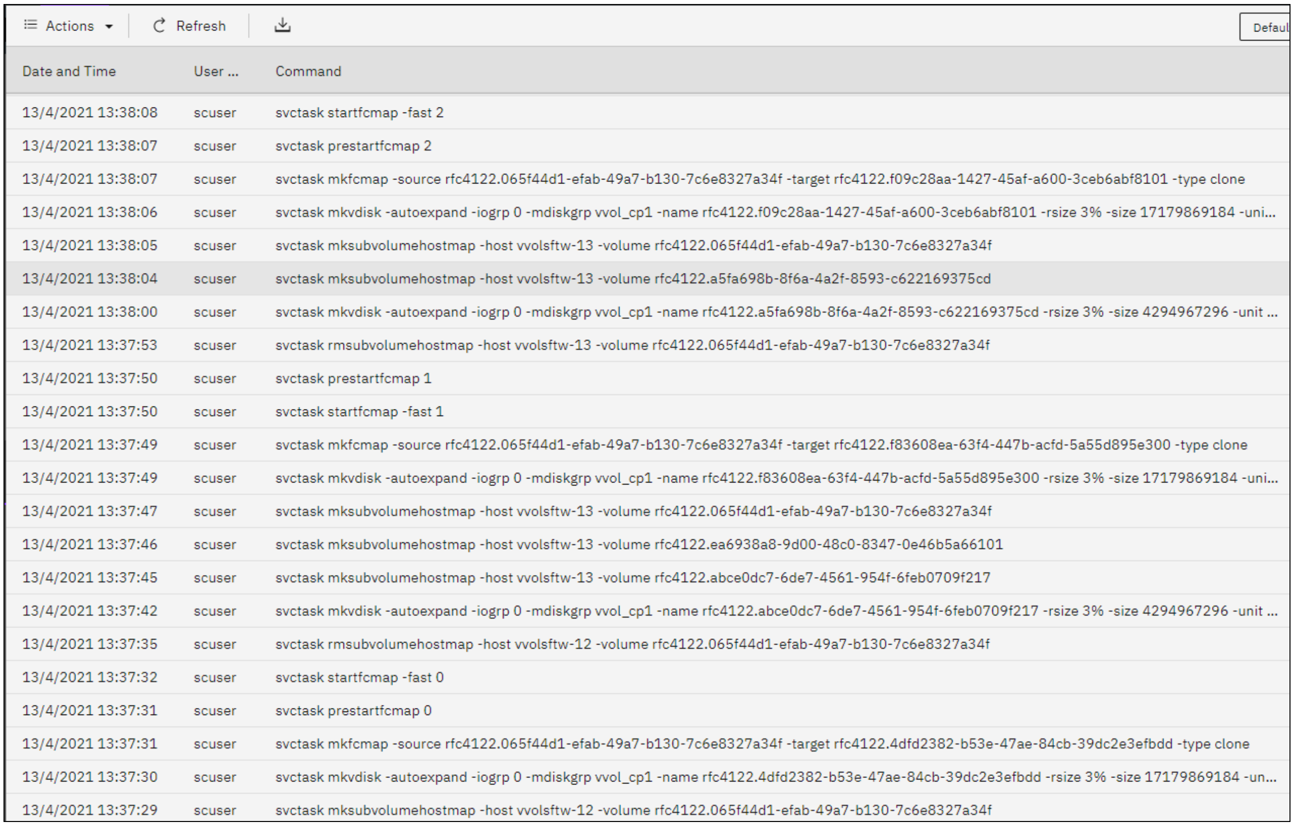
Therefore, it is important to plan an upgrade with your vSphere administrator. To ensure a smooth upgrade in your vVols environment, consider the following suggestions:

- Plan your upgrade for a time when VM management is not required.
- Warn your vSphere administrator not to run management tasks on VMs stored on vVols datastores during an upgrade because it results in task failures on the vSphere Client.
- Be aware of automated backup schedules that use VM snapshots.

> **Tip:** After you perform an upgrade, it is possible that the vSphere Web Client will mark cold VMs as *inaccessible*, which means that ESXi hosts were unable to start a new binding to these VMs. This is expected during a code upgrade.
>
> To recover management of these VMs, the vSphere administrator removes the affected VMs from the inventory and then adds them again.

8.4.5 Understanding audit log entries

For illustration purposes, a VM template on a vVol datastore is created, and 10 VMs are created from this template. Figure 8-44 on page 213 shows a section of the audit log of the storage system where you can see the CLI commands that are issued from the IBM Spectrum Connect server.



Date and Time	User ...	Command
13/4/2021 13:38:08	scuser	svctask startfcmap -fast 2
13/4/2021 13:38:07	scuser	svctask prestartfcmap 2
13/4/2021 13:38:07	scuser	svctask mkfcmap -source rfc4122.065f44d1-efab-49a7-b130-7c6e8327a34f -target rfc4122.f09c28aa-1427-45af-a600-3ceb6abf8101 -type clone
13/4/2021 13:38:06	scuser	svctask mkvdisk -autoexpand -iogrp 0 -mdiskgrp vvol_cp1 -name rfc4122.f09c28aa-1427-45af-a600-3ceb6abf8101 -rsize 3% -size 17179869184 -uni...
13/4/2021 13:38:05	scuser	svctask mksubvolumehostmap -host vvolsftw-13 -volume rfc4122.065f44d1-efab-49a7-b130-7c6e8327a34f
13/4/2021 13:38:04	scuser	svctask mksubvolumehostmap -host vvolsftw-13 -volume rfc4122.a5fa698b-8f6a-4a2f-8593-c622169375cd
13/4/2021 13:38:00	scuser	svctask mkvdisk -autoexpand -iogrp 0 -mdiskgrp vvol_cp1 -name rfc4122.a5fa698b-8f6a-4a2f-8593-c622169375cd -rsize 3% -size 4294967296 -unit ...
13/4/2021 13:37:53	scuser	svctask rmsubvolumehostmap -host vvolsftw-13 -volume rfc4122.065f44d1-efab-49a7-b130-7c6e8327a34f
13/4/2021 13:37:50	scuser	svctask prestartfcmap 1
13/4/2021 13:37:50	scuser	svctask startfcmap -fast 1
13/4/2021 13:37:49	scuser	svctask mkfcmap -source rfc4122.065f44d1-efab-49a7-b130-7c6e8327a34f -target rfc4122.f83608ea-63f4-447b-acfd-5a55d895e300 -type clone
13/4/2021 13:37:49	scuser	svctask mkvdisk -autoexpand -iogrp 0 -mdiskgrp vvol_cp1 -name rfc4122.f83608ea-63f4-447b-acfd-5a55d895e300 -rsize 3% -size 17179869184 -uni...
13/4/2021 13:37:47	scuser	svctask mksubvolumehostmap -host vvolsftw-13 -volume rfc4122.065f44d1-efab-49a7-b130-7c6e8327a34f
13/4/2021 13:37:46	scuser	svctask mksubvolumehostmap -host vvolsftw-13 -volume rfc4122.ea6938a8-9d00-48c0-8347-0e46b5a66101
13/4/2021 13:37:45	scuser	svctask mksubvolumehostmap -host vvolsftw-13 -volume rfc4122.abce0dc7-6de7-4561-954f-6feb0709f217
13/4/2021 13:37:42	scuser	svctask mkvdisk -autoexpand -iogrp 0 -mdiskgrp vvol_cp1 -name rfc4122.abce0dc7-6de7-4561-954f-6feb0709f217 -rsize 3% -size 4294967296 -unit ...
13/4/2021 13:37:35	scuser	svctask rmsubvolumehostmap -host vvolsftw-12 -volume rfc4122.065f44d1-efab-49a7-b130-7c6e8327a34f
13/4/2021 13:37:32	scuser	svctask startfcmap -fast 0
13/4/2021 13:37:31	scuser	svctask prestartfcmap 0
13/4/2021 13:37:31	scuser	svctask mkfcmap -source rfc4122.065f44d1-efab-49a7-b130-7c6e8327a34f -target rfc4122.4dfd2382-b53e-47ae-84cb-39dc2e3efbdd -type clone
13/4/2021 13:37:30	scuser	svctask mkvdisk -autoexpand -iogrp 0 -mdiskgrp vvol_cp1 -name rfc4122.4dfd2382-b53e-47ae-84cb-39dc2e3efbdd -rsize 3% -size 17179869184 -un...
13/4/2021 13:37:29	scuser	svctask mksubvolumehostmap -host vvolsftw-12 -volume rfc4122.065f44d1-efab-49a7-b130-7c6e8327a34f

Figure 8-44 Audit log entries

In Figure 8-44, the following CLI commands are used:

- **`mkvdisk`**. This command is used to create the vVols in the allocated storage pool. vVols are created with a unique identifier, in compliance with Request For Comment (RFC) 4122) to distinguish themselves from traditional volumes. A volume is created for each VMDK on the vVol datastore.

  If VM-level snapshots are created for any VMDK on the vVol datastore, more **`mkvdisk`** commands are issued to create associated volumes on the storage array. Also, if the VM Home folder is stored on a vVol datastore, then more vVols are required to store the VM configuration files or logs. When a VM is powered on, an extra volume is created and dedicated to memory swap. This volume is deleted when a VM is powered off.

- **`mksubvolumehostmap`** and **`rmsubvolumehostmap`**. These commands are used to create and remove the mapping of the vVols to a specific ESXi host. These commands differ from the more traditional **`mkvdiskhostmap`** and **`rmvdiskhostmap`** commands, which are used to map traditional SCSI devices, and require an HBA rescan to detect. The **`subvolumehostmap`** commands are mapped by using the PE and provide a more dynamic environment with vVols being mapped and removed more frequently.

  ESXi periodically requires access to the VM metadata, so you might observe these commands being used frequently, even when active administration or management tasks are not being performed. This situation is normal and can be ignored.

- **`mkfcmap`**, **`prestartfcmap`**, and **`startfcmap`**. FlashCopy is used by vVols to primarily offload VM-level snapshots to the storage system. However, it is also used when you perform storage migrations by using Storage vMotion or when you perform VM-clone operations of a powered-off VM. When a VM is powered on, ESXi uses its own data-copy operator.

8.4.6 IBM Storage Virtualize GUI

It is not expected that a storage administrator needs to interact with vVols individually, but rather rely on the vSphere administrator's actions within vCenter to facilitate management tasks. Therefore, the vVols are not visible through the IBM Storage Virtualize GUI. Instead, they are only visible to the storage administrator by using the CLI over ssh. The Utility Volume (or **metadatavdisk**) is visible in both the GUI and CLI.

To prevent an accidental action in the IBM Storage Virtualize from affecting the IBM Spectrum Connect objects, the storage system prevents manipulation of these objects unless the manipulation is performed by a user with the VASA-Provider role. When a “superuser” or similar account is used to change objects that were created by IBM Spectrum Connect, the following error is reported:

```
CMMVC8652E The command failed as a volume is owned and has restricted use.
```

In some circumstances, there might be a requirement to make manual changes to these objects. Therefore, the storage administrator is advised to log in to the Storage System with a user account that is assigned with the VASA Provider role.

> **Warning:** Do not make manual changes unless advised by a member of IBM Support because it might cause more issues.

8.4.7 Metadata VDisk

The metadata VDisk (or Utility Volume) is a dedicated volume within the IBM Storage Virtualize storage system that is mounted locally onto the configuration node of the cluster. This volume stores the metadata database that is required to maintain awareness of the individual components of the vVols environment.

When configured in an HA configuration, both Active and Standby IBM Spectrum Connect servers use the same database to ensure infrastructure consistency.

> **Tip:** For more information about the HA configuration, see the *IBM Spectrum Connect User Guide* available at IBM Fix Central.

If the IBM Spectrum Connect server is permanently unavailable (and no backup exists), a new IBM Spectrum Connect server can be commissioned to recover the metadata database on the metadata VDisk, and the environment can be resurrected. For more information about this recovery process, contact IBM Support.

To query the active state of the metadata VDisk, connect to the Storage System by using the CLI management interface and run the following command (Example 8-2).

Example 8-2 The svcinfo lsmetadatavdisk command

```
IBM_FlashSystem:FS9200-CL:superuser>svcinfo lsmetadatavdisk
vdisk_id 16
vdisk_name vdisk0
status online
```

If the status of the **metadatavdisk** reports `corrupt`, verify that the underlying VDisk is in an operational state by checking the detailed view of the specific vdisk_id (vdisk_id **16** in Example 8-3 on page 215). Verify that the underlying VDisk is in an operational state.

Example 8-3 Verify that the underlying VDisk is in an operational state

```
IBM_2145:vvolsftw-sv1:superuser> lsvdisk 16 | grep ^status
status online
status online
```

In rare circumstances, the output from the **lsmetadatavdisk** command shows `corrupt`, and there are messages in the IBM Spectrum Connect `hsgsvr.log` file reporting the following error:

```
CMMVC8580E The action failed because the metadata utility volume is corrupt.
```

This error might occur if the configuration node experienced issues when attempting to access the internal mounted volume. To resolve this issue, put the configuration node into service state by using the service assistant. After a few minutes, bring the node back in to the cluster, and retry the **lsmetadatavdisk** command again. The metadata VDisk can now report its online status.

Note: If you are unsure of the status of the metadata VDisk, contact IBM Support.

8.4.8 Enabling debugging in IBM Spectrum Connect

By default, the logging in IBM Spectrum Connect is limited to informational events and does not always provide the user with the necessary information that is required to debug specific issues. More verbose logging is available when required.

To enable the debug logging, complete the following steps:

1. Log in to the IBM Spectrum Connect server by using ssh or console.
2. Locate the `hsgsvr.ini` file located in the `/opt/ibm/ibm_spectrum_connect/conf.d/hsgsvr` directory.
3. Change the `debug=False` setting to `debug=True`.
4. Restart IBM Spectrum Connect Services by running the following command:

   ```
   systemctl restart ibm_spectrum_connect
   ```

5. Wait a few minutes for the services to restart. Additional debug logging is in the file `/var/log/sc/hsgsvr.log`.

8.4.9 Certificates

Certificates are used by vSphere, IBM Spectrum Connect, and IBM Storage Virtualize to secure communication between the separate components. Therefore, ensure that the IBM Spectrum Connect certificate is configured correctly.

A common symptom of certificate issues is where the Storage Provider is registered successfully in vCenter. However, the ESXi hosts might report errors in `vvold.log` citing errors in communicating with the IBM Spectrum Connect server because the hostname does not match the names that are defined in the certificate (Example 8-4).

Example 8-4 The vvold.log file

```
2021-04-13T12:06:20.483Z error vvold[1053651] [Originator@6876 sub=Default] Initialize: Unable
to init session to VP vVols_SpecConnect state: 0
2021-04-13T12:06:25.487Z info vvold[1053615] [Originator@6876 sub=Default]
VasaSession::GetEndPoint: with url https://vvolsftw-scb.ssd.hursley.ibm.com:8440/services/vasa
```

```
2021-04-13T12:06:25.490Z warning vvold[1053615] [Originator@6876 sub=Default]
VasaSession::GetEndPoint: failed to get endpoint, err=SSL Exception: Verification parameters:
--> PeerThumbprint: A1:61:6B:C9:11:72:DF:0B:5D:BA:9D:3B:C2:49:1E:FB:3B:64:84:9D
--> ExpectedThumbprint:
--> ExpectedPeerName: vvolsftw-scb.ssd.hursley.ibm.com
--> The remote host certificate has these problems:
-->
--> * Hostname does not match the subject names in certificate, using default
```

If this certificate-issue occurs, regenerate the certificate in IBM Spectrum Connect with the correct common name and fully qualified domain name, as follows:

1. Go to the IBM Spectrum Connect management interface window and click **Server Certificate** (Figure 8-45).

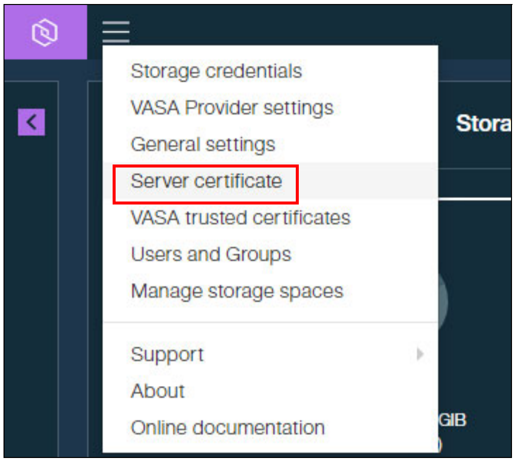
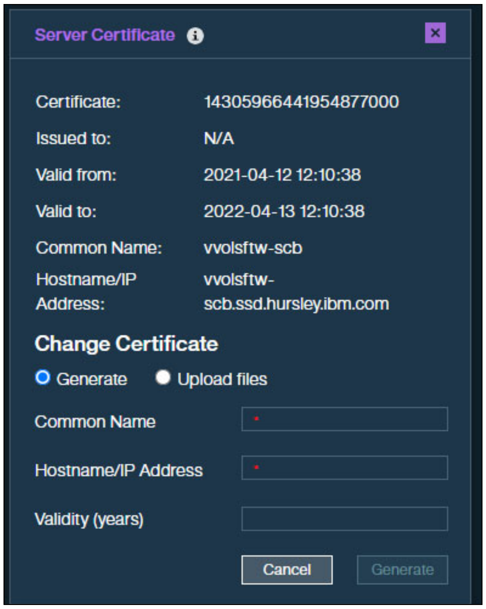


Figure 8-45 Server Certificate: 1

2. In the Server Certificate window, click **Generate** (Figure 8-46).


Server Certificate

Certificate: 14305966441954877000
Issued to: N/A
Valid from: 2021-04-12 12:10:38
Valid to: 2022-04-13 12:10:38
Common Name: vvolsftw-scb
Hostname/IP Address: vvolsftw-scb.ssd.hursley.ibm.com

Change Certificate

● Generate ○ Upload files

Common Name
Hostname/IP Address
Validity (years)

Figure 8-46 Server Certificate: 2

3. After the certificate regenerates, you must remove and reregister the Storage Provider.

8.4.10 Prerequisites, limitations, and restrictions

This section describes the prerequisites, limitations, and restrictions.

Prerequisites

The following items are the prerequisites:

- **NTP**. An NTP client must be configured on the base Linux OS under the IBM Spectrum Connect application, the IBM Storage Virtualize storage system, and vSphere, which includes vCenter and ESXi hosts. Given the multiple components in the end-to-end infrastructure, any time-skew between IBM Spectrum Connect, IBM Storage Virtualize, and the VMware platforms can complicate debugging issues when logs are reviewed.
- **Supported versions**. Check IBM Documentation for the interoperability matrix for supported versions of IBM Spectrum Connect, IBM Storage Virtualize, and vSphere. For IBM Spectrum Connect V3.11, which is the latest version at the time of writing, see Compatibility and requirements.

Restrictions

The following are the restrictions:

- Array-based replication for vVol is not currently supported by IBM Spectrum Connect or IBM Storage Virtualize. This item is planned for a future release.
- vVols are not supported in a HyperSwap configuration.

Limitations

The following are the limitations:

- At the time of writing, The number of vVols in an IBM Storage Virtualize storage system is limited to 10,000 per IBM Storage Virtualize cluster. Depending on the scale of the vSphere environment, the number of VMs might not be suitable for a vVol implementation, especially given the number of volumes that can be consumed by a single VM.

  With traditional VMFS datastores, a single LUN can host thousands of VMs. The best-practice guidance on the number of VMs per datastore is more focused on the workload being generated, rather than the number of VMs.

  In a vVol environment, a single VM requires a minimum of three volumes:

  – Configuration vVol
  – Swap vVol
  – Data vVol

  > **Note:** For more information about the types of vVols, see Virtual Volume Objects.

- If more VMDKs are configured on the VM, then more associated vVols are created. If a VM-level snapshot is taken of the VM, then an additional vVol is created for each VMDK configured on the VM.

  > **Note:** A conservative assumption is to assume that a single VM requires 10 vVols, and so consider the scale of the VMware environment being used to evaluate whether a vVol solution is suitable.

For the specific version of IBM Storage Virtualize, see the Configuration Limits and Restrictions of your hardware in IBM Documentation. For example, see V8.4.0.x Configuration Limits and Restrictions for IBM FlashSystem 9200.

8.5 IBM Storage Enhancements for VMware vSphere Web Client plug-in

The IBM Storage Enhancements for VMware vSphere plug-in integrates directly into the vSphere Client and enables VMware administrators the ability to provision storage resources to hosts or clusters that are registered within vCenter.

The storage administrator can use the Storage Spaces and Storage Services objects in IBM Spectrum Connect to complete the following actions:

- Create a preset of specific storage capabilities.
- Allocate pools of storage capacity, either parent pools or child pools, in which volumes that are created by using the IBM Storage Enhancements vSphere plug-in are located.
- Delegate those presets to vCenter so they can be used by a vSphere administrator as either VMFS datastores or RDMs.

The IBM Storage Enhancements for VMware vSphere Web Client plug-in is automatically deployed and enabled for each vCenter server that is registered in the Interfaces window of IBM Spectrum Connect.

8.5.1 Installing the vSphere plug-in

Before you can use the IBM Storage Enhancements for VMware vSphere plug-in on the vCenter client side, you must define, in IBM Spectrum Connect, the vCenter servers for which you want to provide storage resources. Then, you can attach storage services that you want to make available to each vCenter server.

The storage services that you attach on the IBM Spectrum Connect side are accessible by vSphere Client, and can be used for volume creation by using the IBM Storage Enhancements for vSphere Client.

Before you begin, log out of vSphere Client browser windows on the vCenter server to which you want to add IBM Spectrum Connect. Otherwise, after IBM Spectrum Connect is added, you must log out and log in again before you can use the extension.

Add the vCenter servers to which you can later attach storage services that are visible and accessible on the vSphere Client side. You can add a single vCenter server at a time.

When you enter the vCenter credentials on the IBM Spectrum Connect side, verify that the vCenter user has sufficient access level in vCenter to complete this procedure.

To add a vCenter server, complete the following steps:

1. In the IBM Spectrum Connect UI, click **Add Interface** on the Interfaces window and then select **Add vCenter**. The Add New vCenter Server for vWC window opens (Figure 8-47 on page 219).

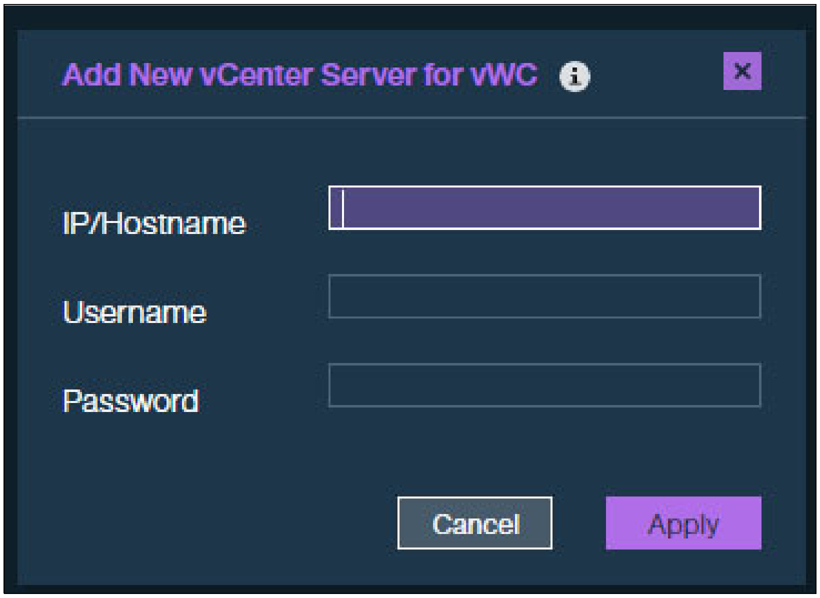
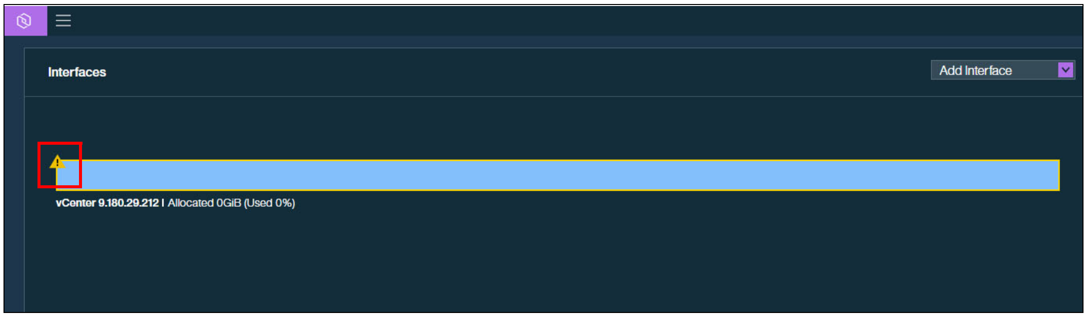


Figure 8-47 Add New vCenter Server for vWC

2. Enter the IP address or FQDN of the vCenter server, and the username and password for that vCenter server (Figure 8-48).



vCenter 9.180.29.212 | Allocated 0GiB (Used 0%)

Figure 8-48 vCenter interface was added to IBM Spectrum Connect

If the provided IP address and credentials are accepted by the vCenter server, it is added to the list of servers in the Interfaces window. The yellow frame and the exclamation mark in Figure 8-48 indicate that storage services are not yet delegated to the interface.

> **Notes:**
>
> - If you want to use the vSphere Web Client extension on all vCenter servers that operate in linked mode, each server instance must be added to IBM Spectrum Connect, which ensures that the extension is registered on all linked servers properly.
> - The same vCenter server cannot be added to more than one IBM Spectrum Connect instance. Any attempt to add an already registered vCenter server to another IBM Spectrum Connect overrides the primary connection.

3. If you need to update the vCenter credentials that are being used by IBM Spectrum Connect or to remove the vCenter interface, right-click the **vCenter** as displayed in the Interfaces window, and click either **Modify** or **Remove** (Figure 8-49).

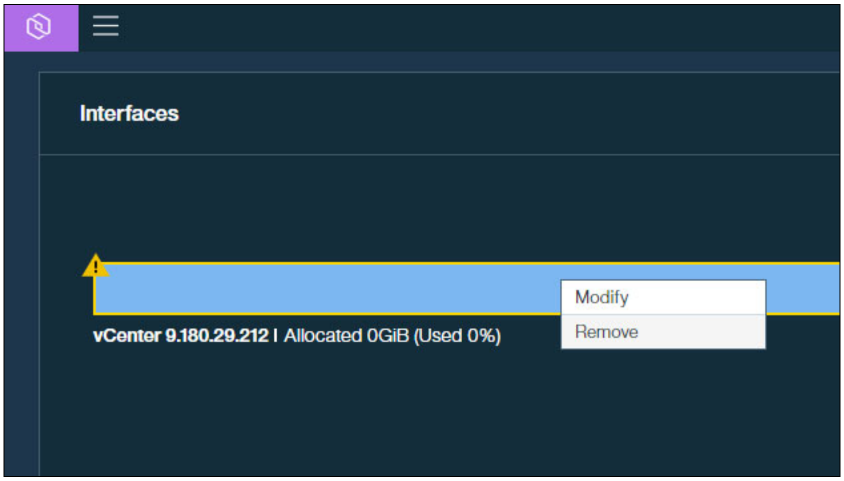


Figure 8-49 Updating the vCenter credentials

8.5.2 Provisioning storage from within vCenter

To enable the provisioning of storage from the vSphere Client, you must first create a Storage Service with an associated storage resource. This Storage Service can then be delegated to the vCenter interface (as described in 8.2.3, “Delegating Storage Services to vCenter” on page 194). Volumes that are created from within the vSphere Client will be created in the associated pool on the IBM Storage Virtualize storage system.

8.5.3 Using the IBM Storage Enhancements vSphere plug-in

When the vCenter interface is registered in IBM Spectrum Connect, the IBM Storage plug-in is automatically installed into vCenter. This plug-in enables the extra UI functions to interact with the IBM Storage Virtualize storage system and perform storage provisioning operations.

To provision volumes by using the IBM Storage Enhancements plug-in, complete the following steps:

1. In the vSphere Client, select the **Hosts & Clusters** tab. Right-click the host or cluster to which you want to provision volumes and select **IBM Storage** → **Create new IBM Storage volume** (Figure 8-50 on page 221).

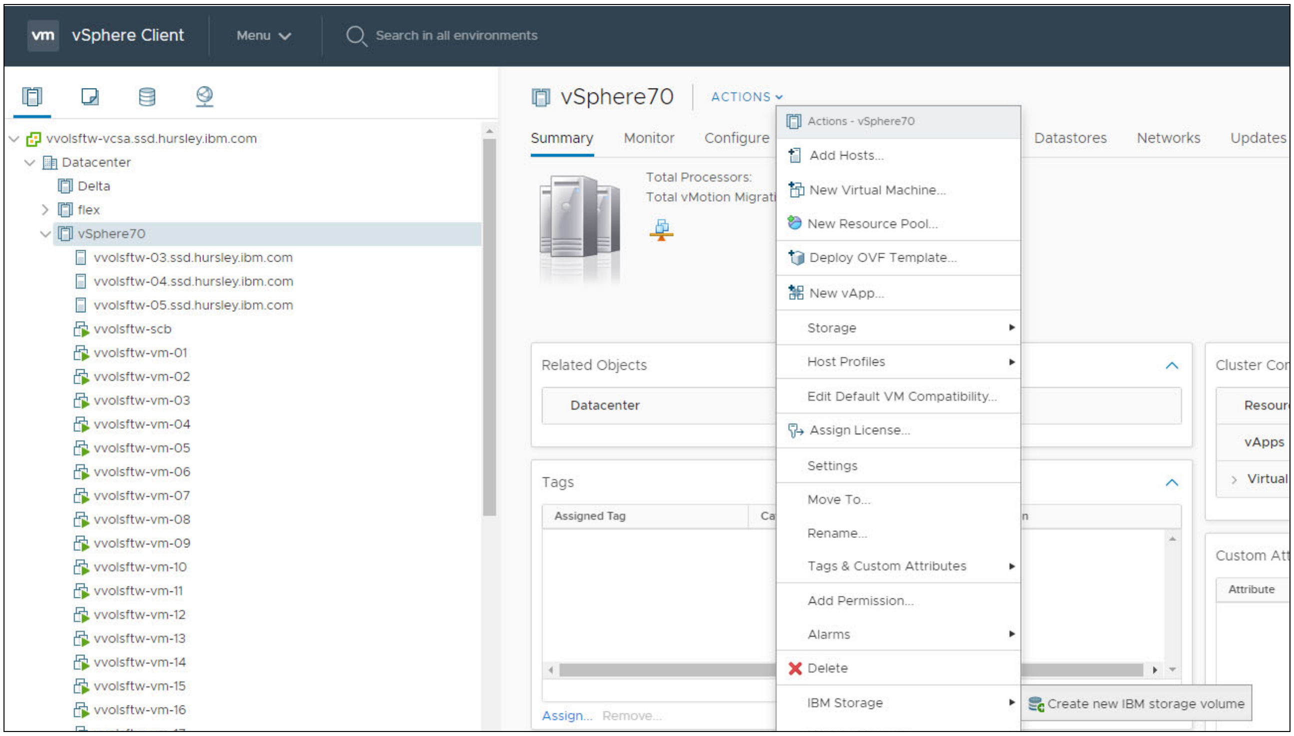
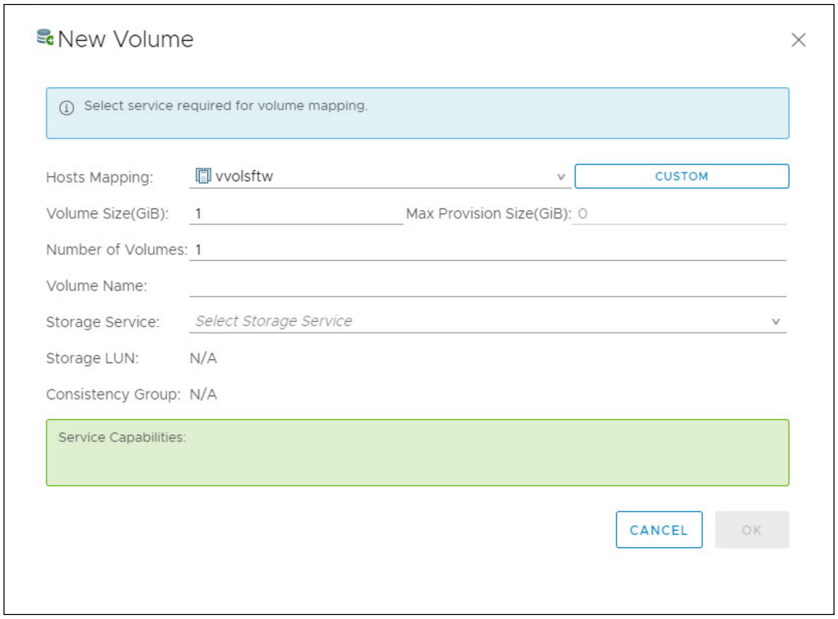


Figure 8-50 Creating an IBM Storage volume

The New Volume window is displayed (Figure 8-51).



New Volume

Select service required for volume mapping.

Hosts Mapping: vvolsftw

Volume Size(GiB): 1

Max Provision Size(GiB): 0

Number of Volumes: 1

Volume Name:

Storage Service: *Select Storage Service*

Storage LUN: N/A

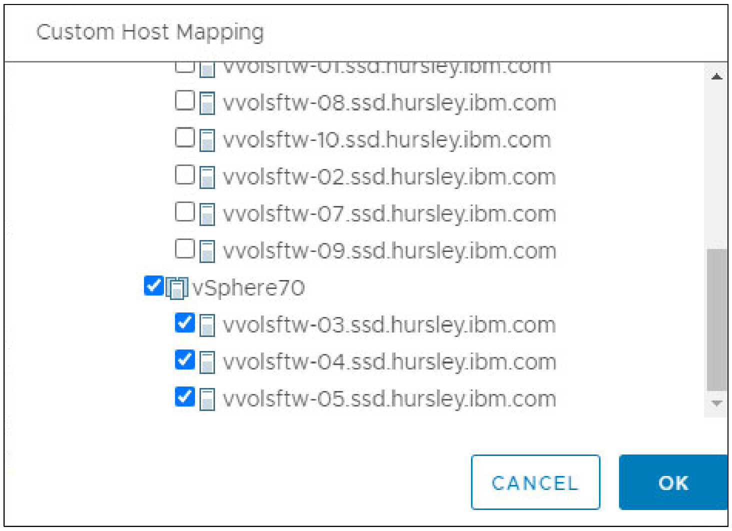
Consistency Group: N/A

Service Capabilities:

Figure 8-51 New Volume window

2. In the Hosts Mapping field, click the arrow and select the hosts to which you want to map the volumes. If you select a vSphere Cluster from the list, the volumes are mapped by using the Host Cluster feature in IBM Storage Virtualize (see 2.1.1, “IBM Storage Virtualize host clusters” on page 8). This mapping ensures that if more hosts are added to the Host Cluster on the IBM Storage Virtualize system, they automatically inherit existing Host Cluster mappings.

3. If a custom-volume mapping is required, click **Custom**, and select the boxes for each ESXi host or cluster to which you want to map the volumes and click **OK** (Figure 8-52).

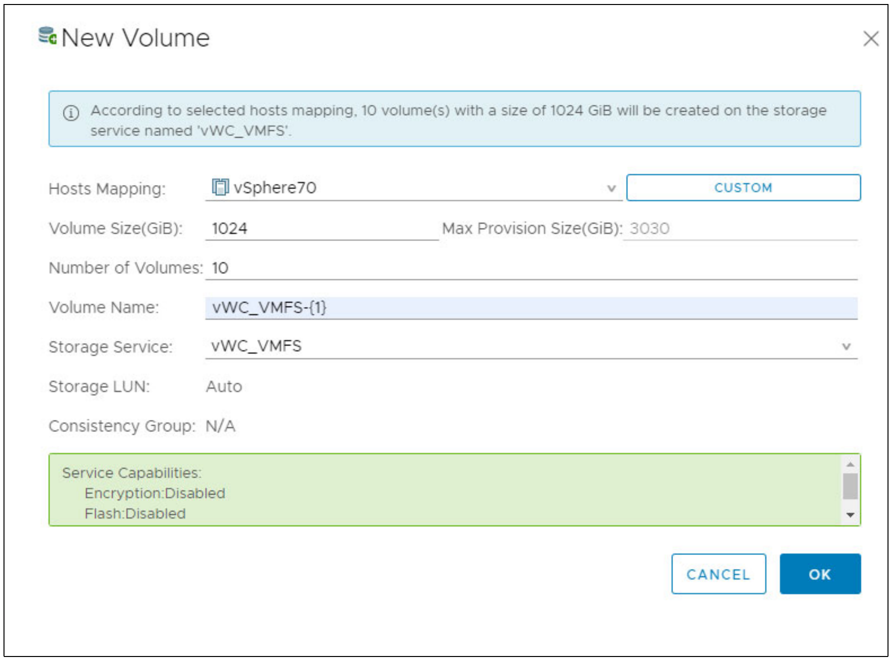


Custom Host Mapping

- □ vvolsftw-01.ssd.hursley.ibm.com
- □ vvolsftw-08.ssd.hursley.ibm.com
- □ vvolsftw-10.ssd.hursley.ibm.com
- □ vvolsftw-02.ssd.hursley.ibm.com
- □ vvolsftw-07.ssd.hursley.ibm.com
- □ vvolsftw-09.ssd.hursley.ibm.com
- ☑ vSphere70
  - ☑ vvolsftw-03.ssd.hursley.ibm.com
  - ☑ vvolsftw-04.ssd.hursley.ibm.com
  - ☑ vvolsftw-05.ssd.hursley.ibm.com

Figure 8-52 Custom Host Mapping

4. Enter the required size, quantity, and name for the volumes to be created. When you create multiple volumes simultaneously, the text box next to the Volume Name entry displays `vol_{1}` by default. The number between the brackets ({ }) is incremented for each volume being created (Figure 8-53).



New Volume

According to selected hosts mapping, 10 volume(s) with a size of 1024 GiB will be created on the storage service named 'vWC_VMFS'.

Hosts Mapping: vSphere70 CUSTOM

Volume Size(GiB): 1024 Max Provision Size(GiB): 3030

Number of Volumes: 10

Volume Name: vWC_VMFS-{1}

Storage Service: vWC_VMFS

Storage LUN: Auto

Consistency Group: N/A

Service Capabilities:
Encryption:Disabled
Flash:Disabled

Figure 8-53 New Volume

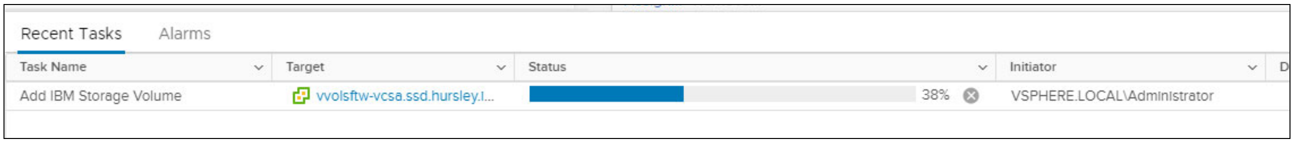
5. Select the Storage Service in which you want to create the volumes. If multiple Storage Services exist, they are included in the list.

   – Storage capabilities that were defined on the Storage Service are listed in the green area of the window.

   – A summary of the task is shown in the blue area of the window.

6. The Storage LUN value defines the SCSI ID to be used when mapping the volume to the host or host cluster. Unless for a specific requirement, select **Auto** for the Storage LUN value so that the SCSI ID can be automatically determined by the system.
7. Click **OK** to begin the storage provisioning task.

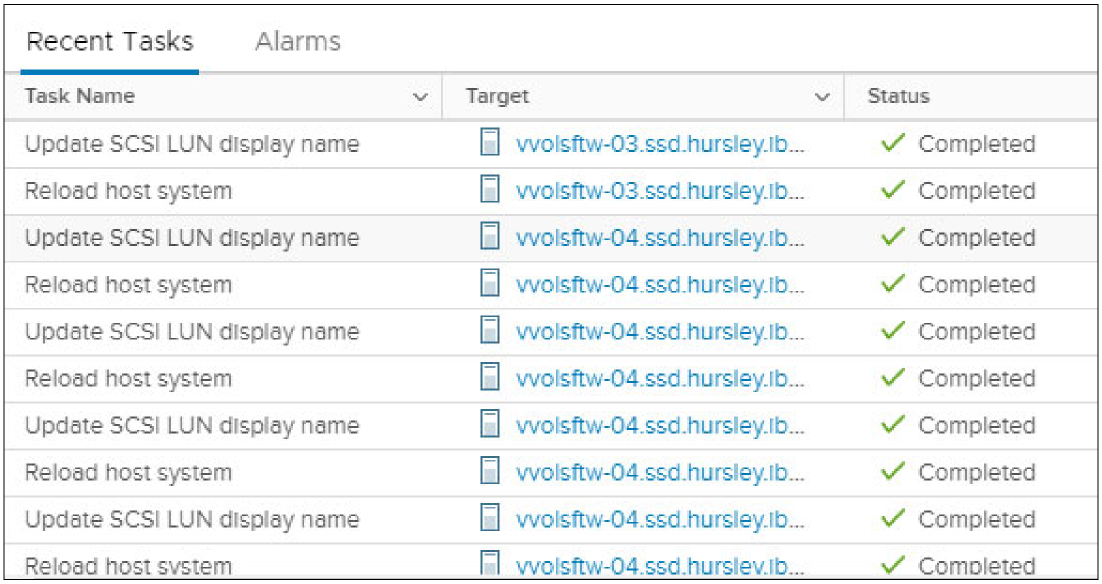
   The status of the operation is displayed in the Recent Tasks tab of the vSphere Client window (Figure 8-54).



Task Name	Target	Status	Initiator	D
Add IBM Storage Volume	vvolsftw-vcsa.ssd.hursley.l...	38%	VSPHERE.LOCAL\Administrator	

Figure 8-54 Status of the operation

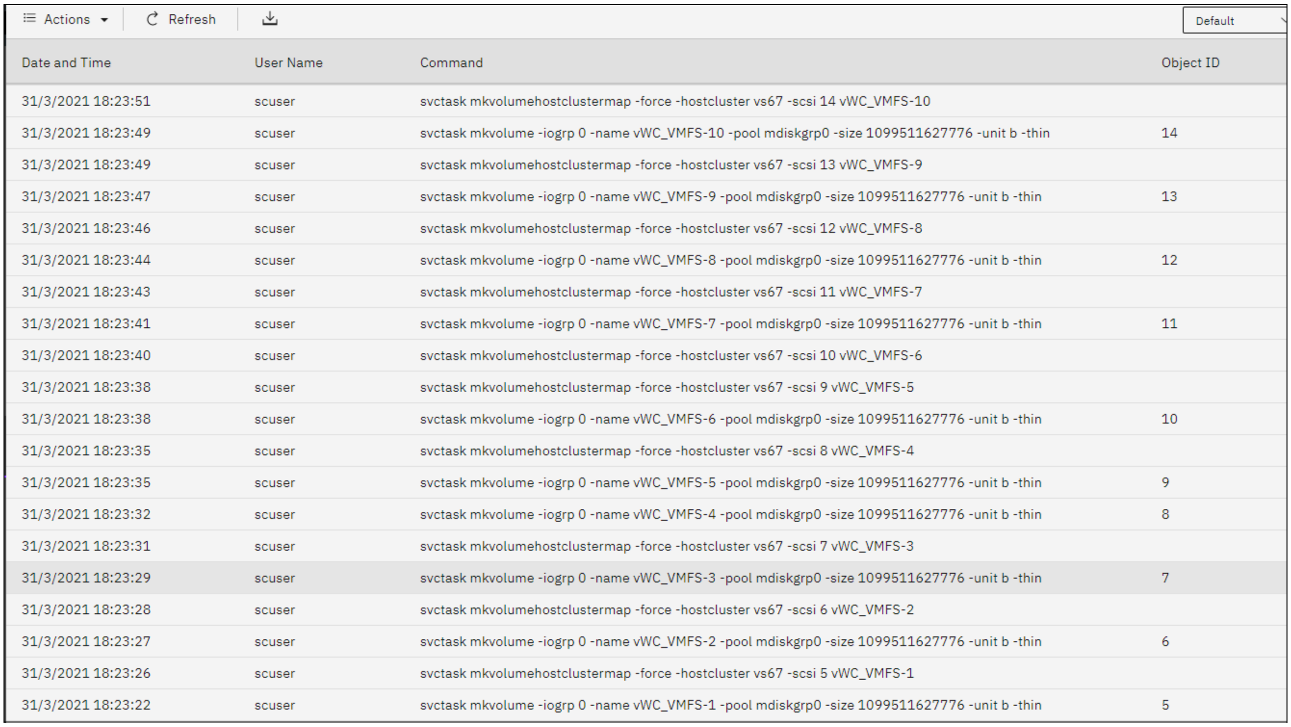
Hosts that were involved in the storage-provisioning operation are automatically scanned for storage changes. Also, the display names for the volumes also reflect the names that are defined in the previous step (Figure 8-55).



Task Name	Target	Status
Update SCSI LUN display name	vvolsftw-03.ssd.hursley.ib...	✓ Completed
Reload host system	vvolsftw-03.ssd.hursley.ib...	✓ Completed
Update SCSI LUN display name	vvolsftw-04.ssd.hursley.ib...	✓ Completed
Reload host system	vvolsftw-04.ssd.hursley.ib...	✓ Completed
Update SCSI LUN display name	vvolsftw-04.ssd.hursley.ib...	✓ Completed
Reload host system	vvolsftw-04.ssd.hursley.ib...	✓ Completed
Update SCSI LUN display name	vvolsftw-04.ssd.hursley.ib...	✓ Completed
Reload host system	vvolsftw-04.ssd.hursley.ib...	✓ Completed
Update SCSI LUN display name	vvolsftw-04.ssd.hursley.ib...	✓ Completed
Reload host system	vvolsftw-04.ssd.hursley.ib...	✓ Completed

Figure 8-55 Recent Tasks

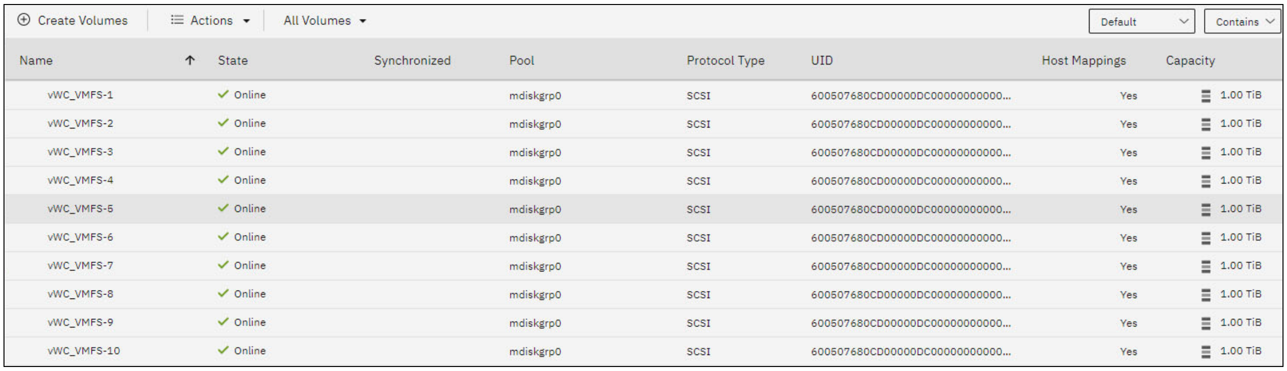
8. Verify that the commands were issued correctly by checking the Audit Log (Figure 8-56 on page 224) in the IBM Storage Virtualize storage system. To access the Audit Log, log in to the web interface of the Storage System and select **Access** → **Audit Log**. You can also use the CLI to run the `cataudit1og` command when you are logged in using ssh.



Date and Time	User Name	Command	Object ID
31/3/2021 18:23:51	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 14 vWC_VMFS-10	
31/3/2021 18:23:49	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-10 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	14
31/3/2021 18:23:49	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 13 vWC_VMFS-9	
31/3/2021 18:23:47	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-9 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	13
31/3/2021 18:23:46	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 12 vWC_VMFS-8	
31/3/2021 18:23:44	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-8 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	12
31/3/2021 18:23:43	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 11 vWC_VMFS-7	
31/3/2021 18:23:41	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-7 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	11
31/3/2021 18:23:40	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 10 vWC_VMFS-6	
31/3/2021 18:23:38	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 9 vWC_VMFS-5	
31/3/2021 18:23:38	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-6 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	10
31/3/2021 18:23:35	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 8 vWC_VMFS-4	
31/3/2021 18:23:35	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-5 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	9
31/3/2021 18:23:32	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-4 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	8
31/3/2021 18:23:31	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 7 vWC_VMFS-3	
31/3/2021 18:23:29	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-3 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	7
31/3/2021 18:23:28	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 6 vWC_VMFS-2	
31/3/2021 18:23:27	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-2 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	6
31/3/2021 18:23:26	scuser	svctask mkvolumehostclustermap -force -hostcluster vs67 -scsi 5 vWC_VMFS-1	
31/3/2021 18:23:22	scuser	svctask mkvolume -iogrp 0 -name vWC_VMFS-1 -pool mdiskgrp0 -size 1099511627776 -unit b -thin	5

Figure 8-56 Audit Log

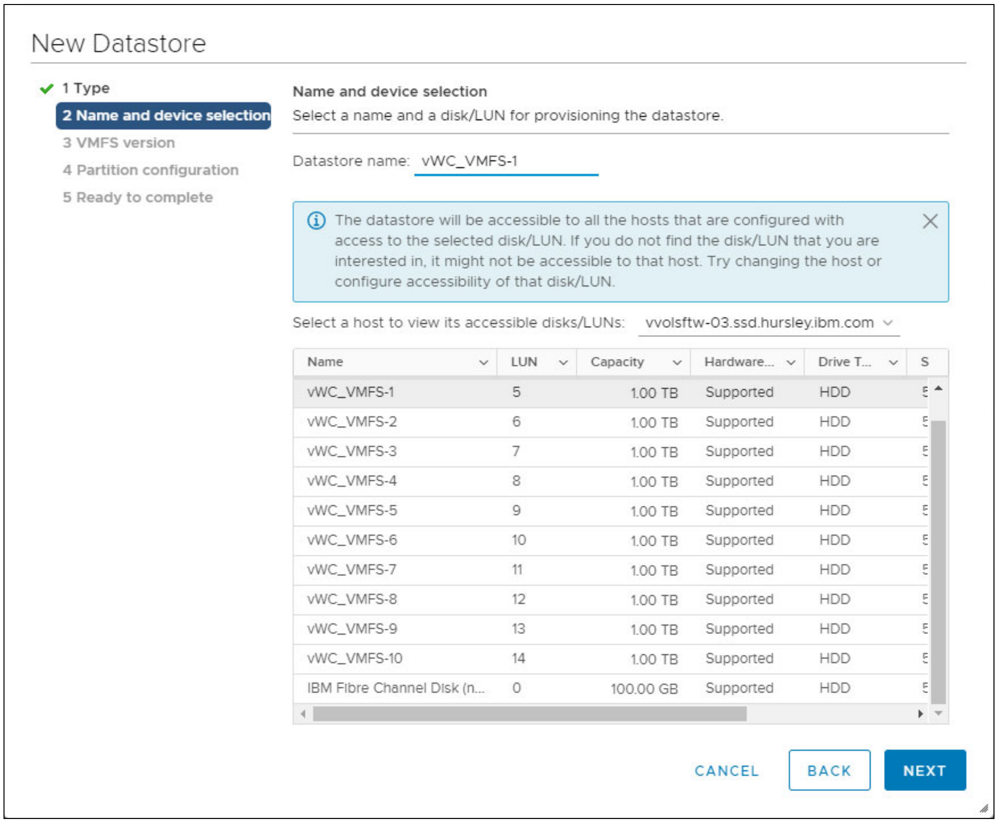
The names of the created volumes were carried through from the previous New Volume step (Figure 8-57).



Name	State	Synchronized	Pool	Protocol Type	UID	Host Mappings	Capacity
vWC_VMFS-1	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-2	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-3	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-4	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-5	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-6	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-7	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-8	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-9	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB
vWC_VMFS-10	✓ Online		mdiskgrp0	SCSI	600507680CD00000DC00000000000...	Yes	1.00 TiB

Figure 8-57 Notice the names of the created volumes

The volumes are created and mapped to the selected Hosts or Clusters, and the vSphere administrator is now able to create VMFS datastores or RDMs from these volumes by using the normal vSphere workflow (Figure 8-58 on page 225).



New Datastore

✓ 1 Type
2 Name and device selection
3 VMFS version
4 Partition configuration
5 Ready to complete

Name and device selection
Select a name and a disk/LUN for provisioning the datastore.

Datastore name: vWC_VMFS-1

The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN.

Select a host to view its accessible disks/LUNs: vvolsftw-03.ssd.hursley.ibm.com

Name	LUN	Capacity	Hardware...	Drive T...	S
vWC_VMFS-1	5	1.00 TB	Supported	HDD	5
vWC_VMFS-2	6	1.00 TB	Supported	HDD	5
vWC_VMFS-3	7	1.00 TB	Supported	HDD	5
vWC_VMFS-4	8	1.00 TB	Supported	HDD	5
vWC_VMFS-5	9	1.00 TB	Supported	HDD	5
vWC_VMFS-6	10	1.00 TB	Supported	HDD	5
vWC_VMFS-7	11	1.00 TB	Supported	HDD	5
vWC_VMFS-8	12	1.00 TB	Supported	HDD	5
vWC_VMFS-9	13	1.00 TB	Supported	HDD	5
vWC_VMFS-10	14	1.00 TB	Supported	HDD	5
IBM Fibre Channel Disk (n...	0	100.00 GB	Supported	HDD	5

Figure 8-58 New Datastore

8.5.4 Viewing more storage information from within the vSphere Client

When logged in to the vSphere Client, the vSphere administrator can use the IBM Storage Enhancements plug-in to view additional information about the storage objects that were delegated to the vCenter Interface.

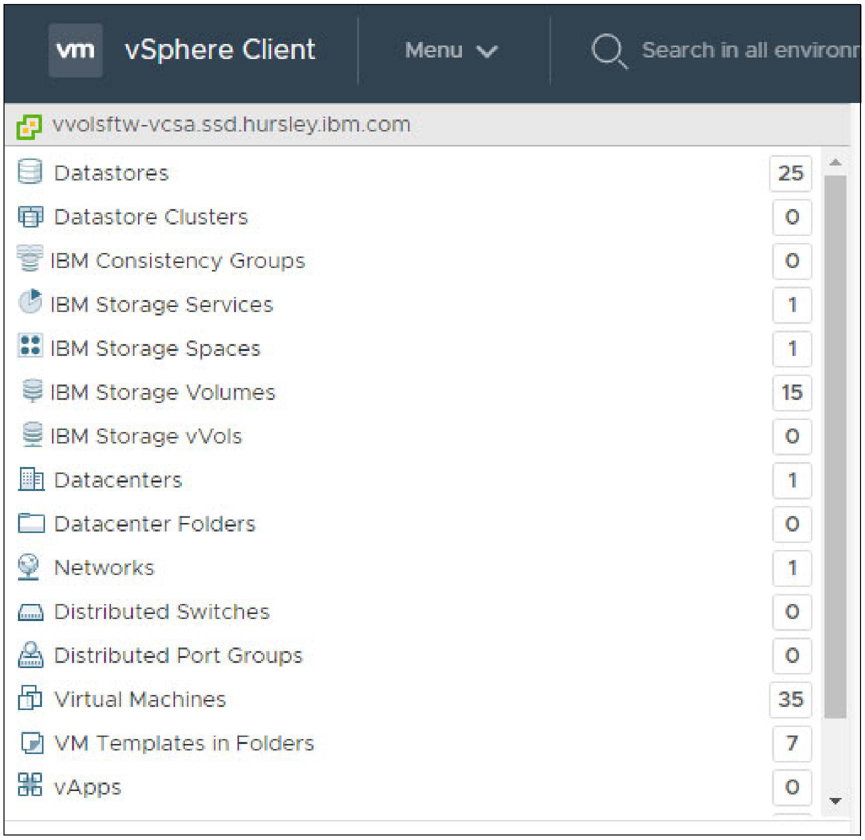
For each vCenter server, the following IBM Storage categories are available to view for IBM Storage Virtualize platforms:

- Storage services
- Storage spaces
- Storage volumes
- Storage vVols

> **Important:** You might notice references to IBM consistency groups. However, this integration applies only to IBM FlashSystem A9000/R storage systems.

To view additional information about the storage objects, complete the following steps:

1. Go to the vCenter Server under the Resources list from the Global Inventory Lists view in the vSphere Client. Open an IBM Storage category to view additional information about the objects that are currently delegated to the selected vCenter server (Figure 8-59 on page 226).

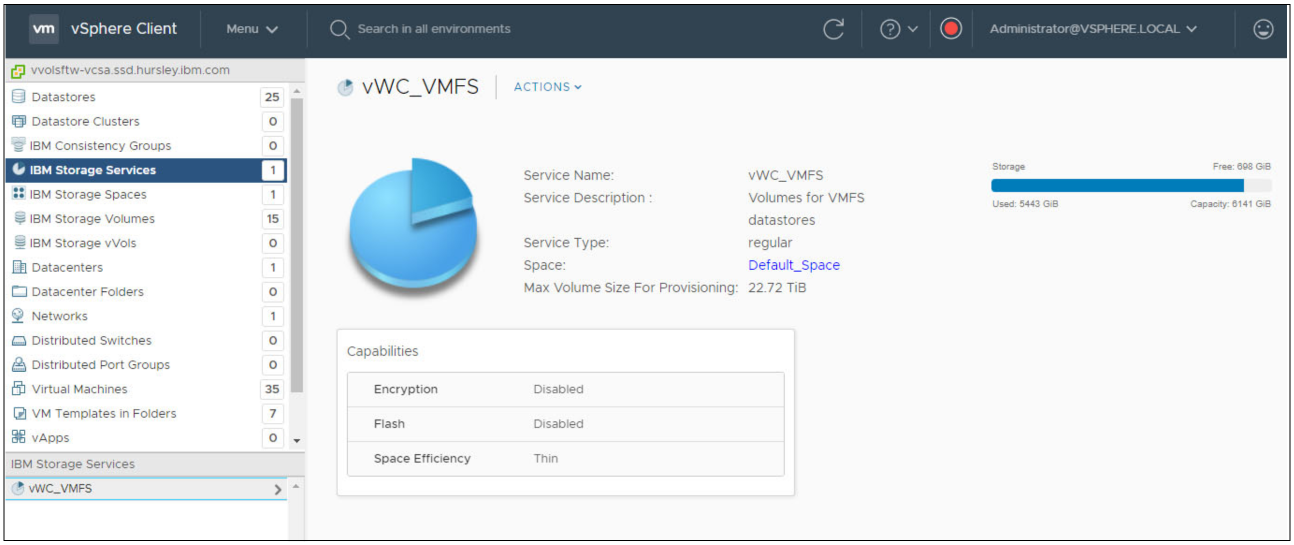


vvolsftw-vcsa.ssd.hursley.ibm.com

Datastores	25
Datastore Clusters	0
IBM Consistency Groups	0
IBM Storage Services	1
IBM Storage Spaces	1
IBM Storage Volumes	15
IBM Storage vVols	0
Datacenters	1
Datacenter Folders	0
Networks	1
Distributed Switches	0
Distributed Port Groups	0
Virtual Machines	35
VM Templates in Folders	7
vApps	0

Figure 8-59 Global Inventory Lists

2. To view the capabilities names that are defined on a Storage Service, select **IBM Storage Services** in the menu on the left. Beneath the menu, select the required Storage Service (Figure 8-60).



vvolsftw-vcsa.ssd.hursley.ibm.com

Datastores	25
Datastore Clusters	0
IBM Consistency Groups	0
IBM Storage Services	1
IBM Storage Spaces	1
IBM Storage Volumes	15
IBM Storage vVols	0
Datacenters	1
Datacenter Folders	0
Networks	1
Distributed Switches	0
Distributed Port Groups	0
Virtual Machines	35
VM Templates in Folders	7
vApps	0

IBM Storage Services

vWC_VMFS

vWC_VMFS

Service Name:	vWC_VMFS
Service Description :	Volumes for VMFS datastores
Service Type:	regular
Space:	Default_Space
Max Volume Size For Provisioning:	22.72 TiB

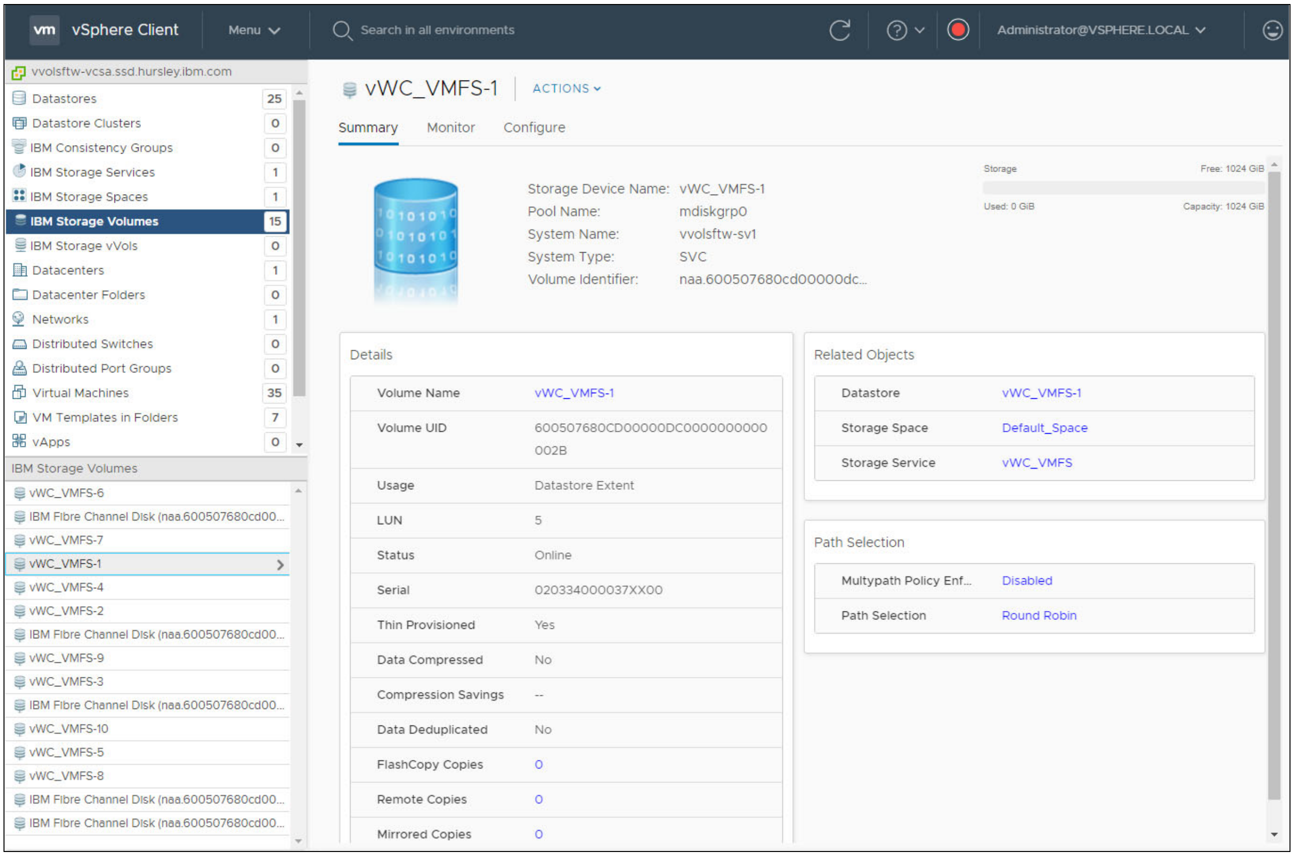
Storage Free: 698 GiB
Used: 5443 GiB Capacity: 6141 GiB

Capabilities

Encryption	Disabled
Flash	Disabled
Space Efficiency	Thin

Figure 8-60 Viewing the capabilities that are defined on a Storage Service

3. To find specific information about a particular volume, select **IBM Storage Volumes** from the menu in the left panel. Beneath the menu, select the specific storage volume (Figure 8-61 on page 227).



vvolsftw-vcsa.ssd.hursley.ibm.com

Datastores	25
Datastore Clusters	0
IBM Consistency Groups	0
IBM Storage Services	1
IBM Storage Spaces	1
IBM Storage Volumes	15
IBM Storage vVols	0
Datacenters	1
Datacenter Folders	0
Networks	1
Distributed Switches	0
Distributed Port Groups	0
Virtual Machines	35
VM Templates in Folders	7
vApps	0

IBM Storage Volumes

vWC_VMFS-6
IBM Fibre Channel Disk (naa.600507680cd00...
vWC_VMFS-7
vWC_VMFS-1
vWC_VMFS-4
vWC_VMFS-2
IBM Fibre Channel Disk (naa.600507680cd00...
vWC_VMFS-9
vWC_VMFS-3
IBM Fibre Channel Disk (naa.600507680cd00...
vWC_VMFS-10
vWC_VMFS-5
vWC_VMFS-8
IBM Fibre Channel Disk (naa.600507680cd00...
IBM Fibre Channel Disk (naa.600507680cd00...

Storage Device Name:	vWC_VMFS-1
Pool Name:	mdiskgrp0
System Name:	vvolsftw-sv1
System Type:	SVC
Volume Identifier:	naa.600507680cd00000dc...

Storage Free: 1024 GiB
Used: 0 GiB Capacity: 1024 GiB

Details

Volume Name	vWC_VMFS-1
Volume UID	600507680CD00000DC0000000000002B
Usage	Datastore Extent
LUN	5
Status	Online
Serial	020334000037XX00
Thin Provisioned	Yes
Data Compressed	No
Compression Savings	--
Data Deduplicated	No
FlashCopy Copies	0
Remote Copies	0
Mirrored Copies	0

Related Objects

Datastore	vWC_VMFS-1
Storage Space	Default_Space
Storage Service	vWC_VMFS

Path Selection

Multypath Policy Enf...	Disabled
Path Selection	Round Robin

Figure 8-61 Finding specific information about a particular volume

8.6 Performing more storage volume management tasks

When viewing the additional information for a storage volume by using the Global Inventory List view in the vSphere Client, the vSphere Administrator can perform more tasks, such as:

- Rename the volume.
- Delete the volume.
- Define the Multipath Policy.
- Create more host mappings.
- Remove existing host mappings.
- Extend the volume size.

8.6.1 Considerations

Volume protection is an IBM Storage Virtualize feature that prevents volumes from being inadvertently deleted or unmapped from a host or host cluster. When attempting to delete a volume or remove existing host mappings, this task might fail if volume protection is enabled on the storage system, and the volume recently processed I/O operations. When this setting is enabled, volumes must be idle before they can be deleted from the system or unmapped from a host or host cluster. Volumes can be deleted only if they have been idle for the specified interval. By default this interval is set to 15 minutes.

When volume protection is disabled, volumes can be deleted even if they recently processed I/O operations. In the management GUI, select **Settings** → **System** → **Volume Protection** to manage volume protection values on the system and on specific pools. You must have the SecurityAdmin or Administrator role to change volume protection settings.

The Extend volume size task might fail if a thick-provisioned (fully allocated) volume is created on the storage system, and a fast-format task is still in progress. If this situation occurs, wait for the fast-formatting process to complete, and then run the command again.

When the Extend volume size task successfully finishes, the LUN that is backing the datastore increases in size but the VMFS file system does not change. Rescan the HBA for each host that accesses the datastore so that the host can detect the change in volume size. Then, you must expand the VMFS file system by right-clicking a datastore and selecting **Increase Datastore Capacity** to take advantage of the additional capacity.

8.7 IBM Storage Plug-in for VMware vRealize Orchestrator

The IBM Storage Plug-in for VMware vRO allows VMware administrators to include IBM storage discovery and provisioning in their vRO-automation workflows. The plug-in package can be downloaded from IBM Spectrum Connect, and then deployed on the vRO server. The deployment includes the matching of a unique token key that is set on both servers. Through vRO Client, dedicated IBM Storage control elements become available, which allows the issuing of workflows with storage volumes that are attached to the vRO server. Rather than issuing volume operations manually and being limited to one manual operation at a time, VMware administrators can plan and automate storage operations in their virtualized cloud environments.

8.7.1 Configuring IBM Spectrum Connect for VMware vRealize Orchestrator

The IBM Storage Plug-in for the VMware vRO is used for discovery of the IBM storage resources and provisioning automation workflows in the vRO.

To access the vRO management options, go to the Interfaces window of the IBM Spectrum Connect server and add the vRO server interface, as shown in Figure 8-62.

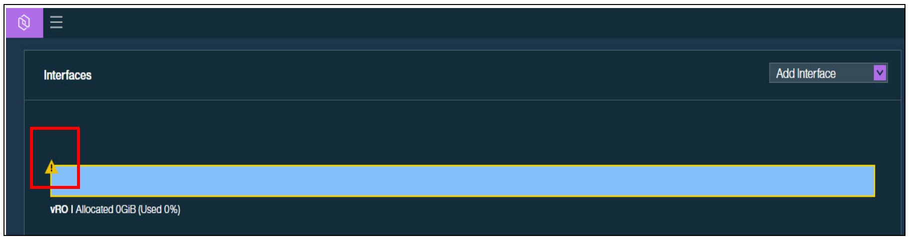


Figure 8-62 Interfaces window

The yellow frame and the exclamation mark (Figure 8-62) indicate that Storage Services are not yet delegated to the interface. You can then manage the integration with vRO as described in the following sections.

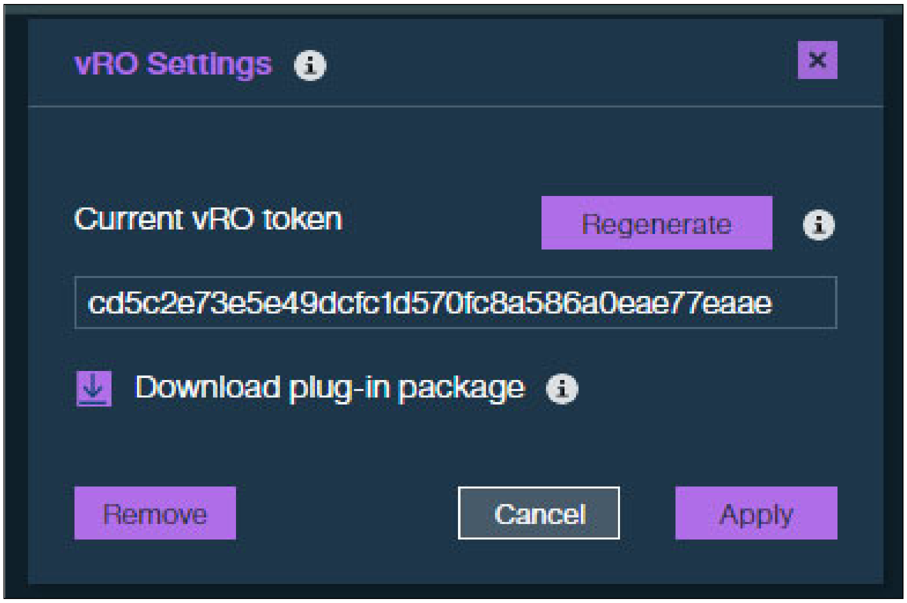
Downloading and installing the plug-in package for vRO

To enable the IBM Storage workflows in the vRO, you must first download the IBM Storage plug-in package from IBM Spectrum Connect and install it on the vRO server.

To download and install the IBM Storage plug-in package, complete the following steps:

1. On the Interfaces window, right-click the vRO server, and then select **Modify**.

2. In the vRO Settings dialog, click **Download plug-in package** to save the package to your local computer (Figure 8-63).



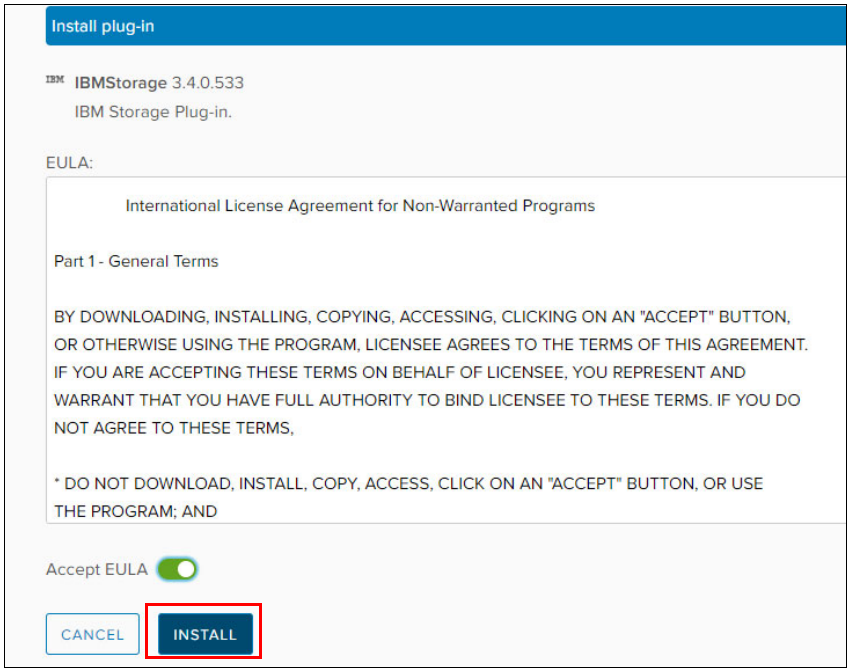
Current vRO token

cd5c2e73e5e49dcfc1d570fc8a586a0eae77eaae

Figure 8-63 Downloading the plug-in package

Alternatively, you can download the package from Downloading and installing the plug-in package for vRO.

3. Copy the current vRO token key from the Current vRO token input box. The current vRO token key is used in step 11 on page 231.
4. In the vSphere Client, select the **Configure** tab.
5. Click **Manage Plug-Ins** in the Plug-Ins category. Select **Browse** → **Install**.
6. Locate and choose the downloaded plug-in file.
7. Accept the license agreement and click **INSTALL** (Figure 8-64 on page 230).


Install plug-in

IBMStorage 3.4.0.533

IBM Storage Plug-in.

EULA:

International License Agreement for Non-Warranted Programs

Part 1 - General Terms

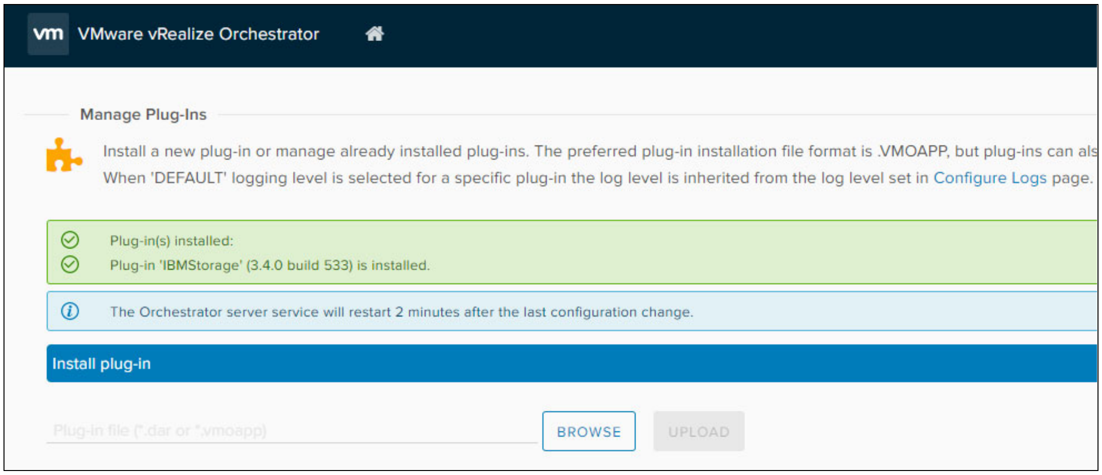
BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND

Accept EULA

Figure 8-64 Installing the plug-in

The `Plug-in IBMStorage (3.x.x build xxx) is installed` message is displayed (Figure 8-65).



Manage Plug-Ins

Install a new plug-in or manage already installed plug-ins. The preferred plug-in installation file format is .VMOAPP, but plug-ins can als

When 'DEFAULT' logging level is selected for a specific plug-in the log level is inherited from the log level set in Configure Logs page.

Plug-in(s) installed:

Plug-in 'IBMStorage' (3.4.0 build 533) is installed.

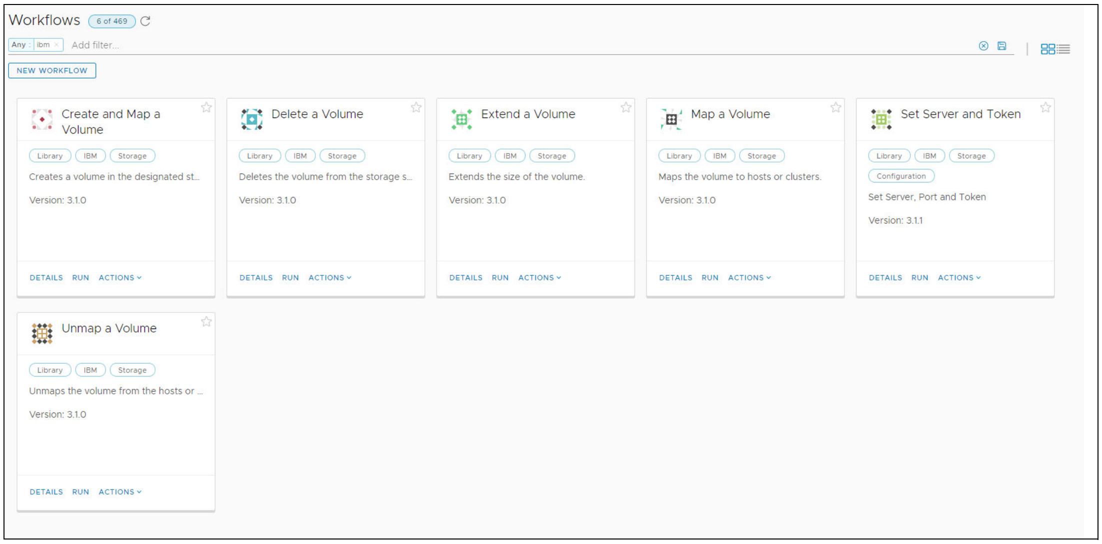
The Orchestrator server service will restart 2 minutes after the last configuration change.

Install plug-in

Figure 8-65 Confirmation message

Installation is completed, and the IBM Storage plug-in is displayed in the list of vRO plug-ins.

8. Start the VRO Client, and go to the **Workflows** tab.
9. On the **Workflows** tab, add a search filter for **IBM** to list the new workflows available that are using IBM Spectrum Connect (Figure 8-66 on page 231).



Workflows 6 of 469

Any ibm Add filter...

NEW WORKFLOW

Create and Map a Volume
Library IBM Storage
Creates a volume in the designated st...
Version: 3.1.0
DETAILS RUN ACTIONS

Delete a Volume
Library IBM Storage
Deletes the volume from the storage s...
Version: 3.1.0
DETAILS RUN ACTIONS

Extend a Volume
Library IBM Storage
Extends the size of the volume.
Version: 3.1.0
DETAILS RUN ACTIONS

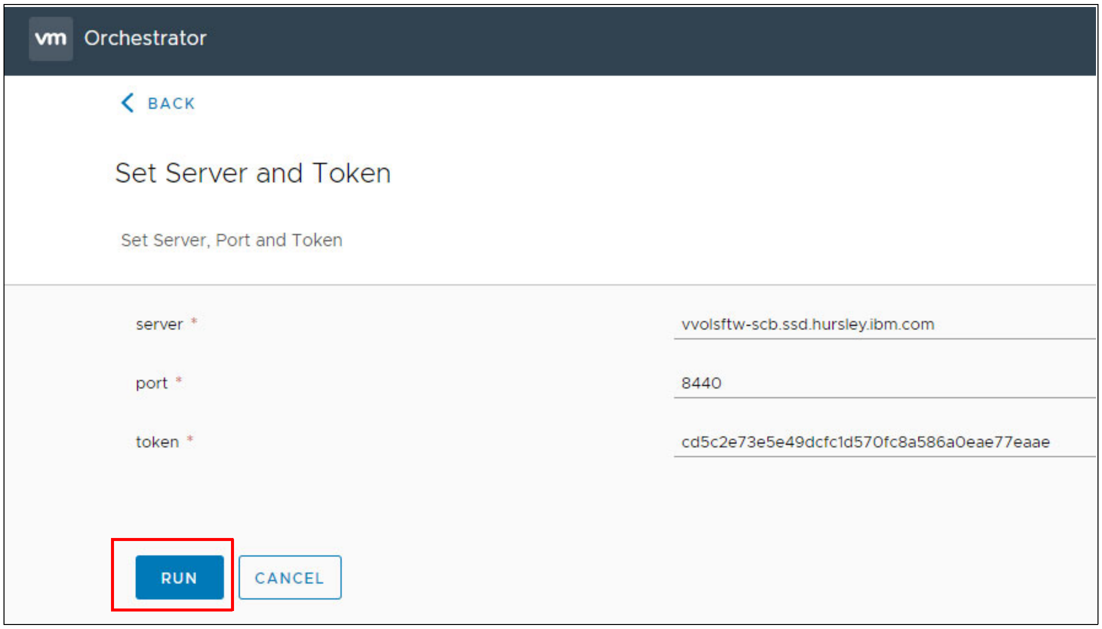
Map a Volume
Library IBM Storage
Maps the volume to hosts or clusters.
Version: 3.1.0
DETAILS RUN ACTIONS

Set Server and Token
Library IBM Storage Configuration
Set Server, Port and Token
Version: 3.1.1
DETAILS RUN ACTIONS

Unmap a Volume
Library IBM Storage
Unmaps the volume from the hosts or ...
Version: 3.1.0
DETAILS RUN ACTIONS

Figure 8-66 Listing the new workflows

10. Locate the Set Server and Token workflow and click **Run**.
11. Enter the following information in the correct fields in Figure 8-67:
    – In the server field, enter the FQDN.
    – In the port field, enter the port of the IBM Spectrum Connect server.
    – In the token field paste the token from step 3 on page 229, and click **Run**.



Set Server and Token

Set Server, Port and Token

server * vvolsftw-scb.ssd.hursley.ibm.com

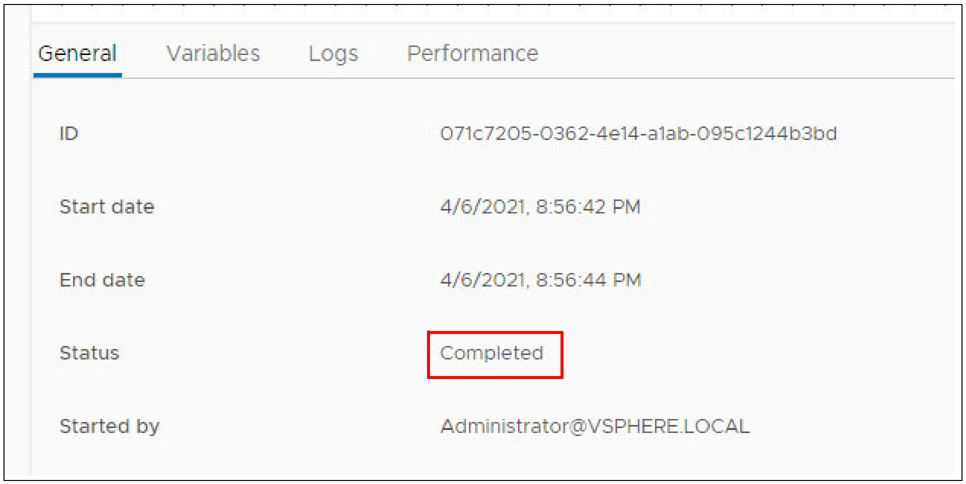
port * 8440

token * cd5c2e73e5e49dcfc1d570fc8a586a0eae77eaae

Figure 8-67 Set Server and Token screen

Tip: If you experience issues running the Set Server and Token workflow, retry the procedure with a web browser in Incognito or Private Browsing modes.

The workflow starts and a completion status is returned (Figure 8-68 on page 232).



ID	071c7205-0362-4e14-a1ab-095c1244b3bd
Start date	4/6/2021, 8:56:42 PM
End date	4/6/2021, 8:56:44 PM
Status	Completed
Started by	Administrator@VSPHERE.LOCAL

Figure 8-68 Workflow completed

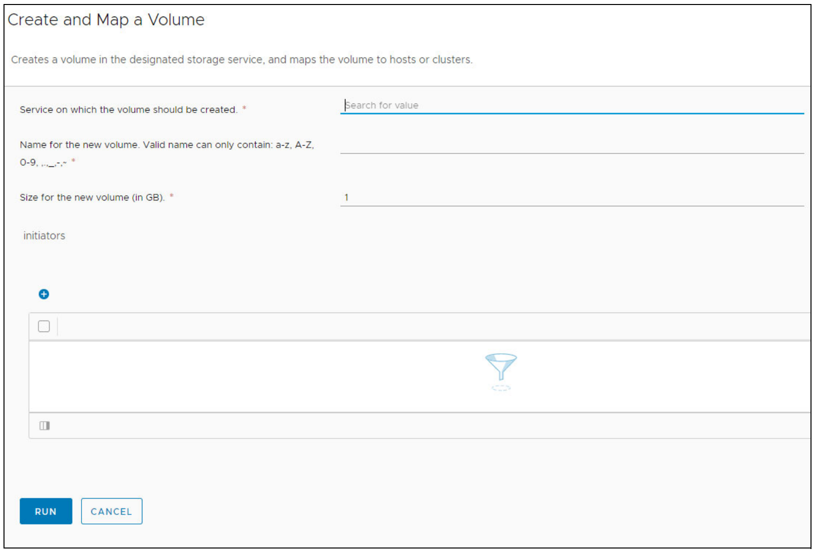
The initial configuration of the vRO plug-in is complete.

8.7.2 Using vRealize Automation and VMware vRealize Orchestrator

If a Storage Service with an allocated storage resource is not already provisioned, you must now create one and delegate it to the vRO interface (as described in 8.2.1, “Creating Storage Services” on page 189) before any volumes can be created by using vRO workflows.

After a Storage Service is created and allocated, complete the following steps:

1. Run the Create and Map a Volume workflow (Figure 8-69).



Create and Map a Volume

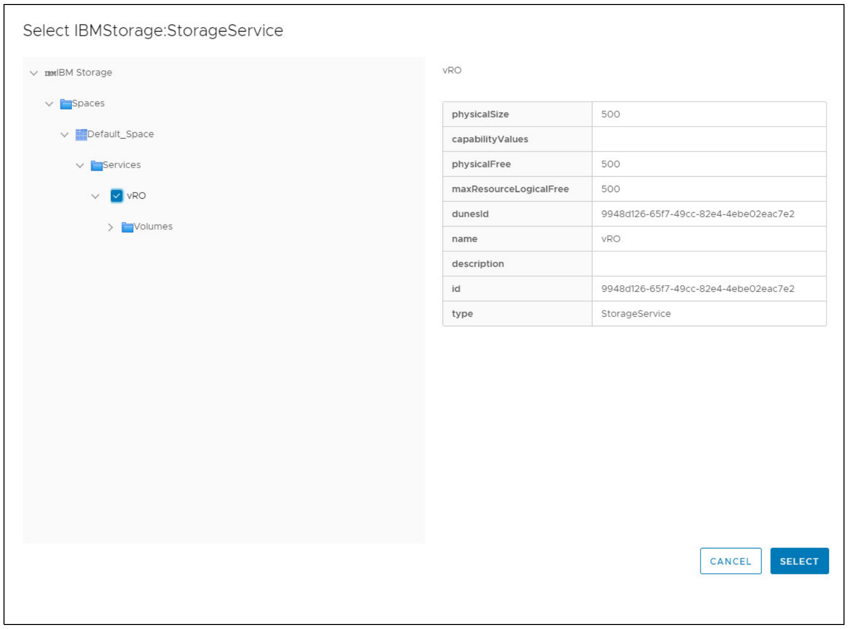
Creates a volume in the designated storage service, and maps the volume to hosts or clusters.

Service on which the volume should be created. *	Search for value
Name for the new volume. Valid name can only contain: a-z, A-Z, 0-9, .,_,-,~ *	
Size for the new volume (in GB). *	1

initiators

Figure 8-69 Create and Map a Volume workflow

2. Click in the “Service on which the volume should be created” window and search for a Storage Service (Figure 8-70).



Select IBMStorage:StorageService

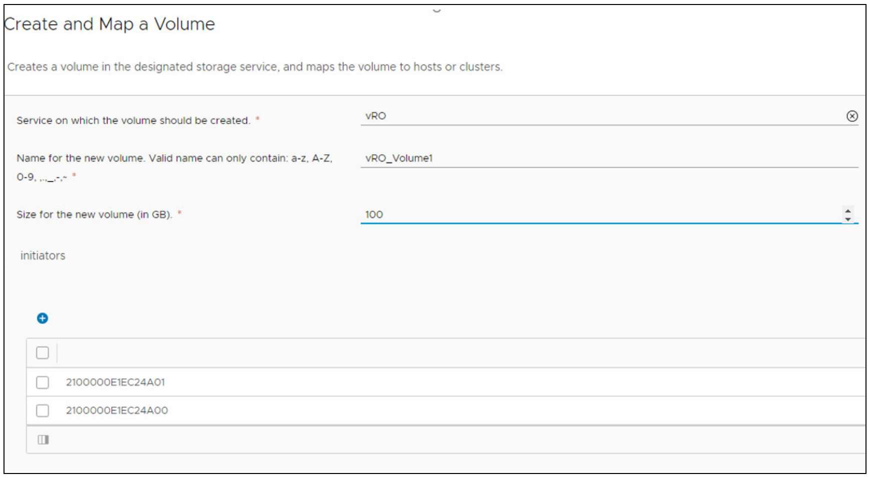
- IBM Storage
  - Spaces
    - Default_Space
      - Services
        - ☑ vRO
          - Volumes

vRO

physicalSize	500
capabilityValues	
physicalFree	500
maxResourceLogicalFree	500
dunesId	9948d126-65f7-49cc-82e4-4ebe02eac7e2
name	vRO
description	
id	9948d126-65f7-49cc-82e4-4ebe02eac7e2
type	StorageService

Figure 8-70 Selecting a Storage Service

3. Enter the following information:
   – Name for the new volume: Enter a volume name.
   – Size for the new volume (in GB): Enter the capacity for the new volume.
   – Click the plus icon (**+**) at the bottom of the window and enter the worldwide port name (WWPN), Fibre Channel (FC), or iSCSI qualified name (iqn) for the hosts to which you want the volume mapped. Click **Run** (Figure 8-71).



Create and Map a Volume

Creates a volume in the designated storage service, and maps the volume to hosts or clusters.

Service on which the volume should be created. *	vRO
Name for the new volume. Valid name can only contain: a-z, A-Z, 0-9, .,.._,-,~ *	vRO_Volume1
Size for the new volume (in GB). *	100

initiators

+

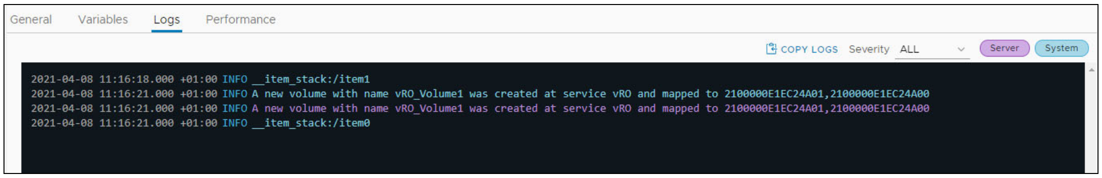
□

□ 2100000E1EC24A01

□ 2100000E1EC24A00

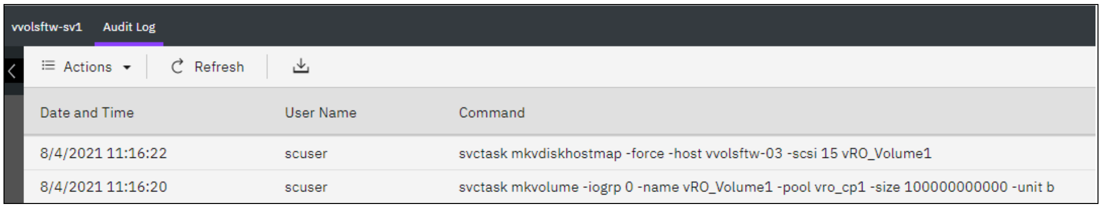
Figure 8-71 Create and Map a Volume

4. After the task is complete, review the Logs workflow (Figure 8-72) and the Audit Log (Figure 8-73) of the Storage System.



```
2021-04-08 11:16:18.000 +01:00 INFO __item_stack:/item1
2021-04-08 11:16:21.000 +01:00 INFO A new volume with name vRO_Volume1 was created at service vRO and mapped to 2100000E1EC24A01,2100000E1EC24A00
2021-04-08 11:16:21.000 +01:00 INFO A new volume with name vRO_Volume1 was created at service vRO and mapped to 2100000E1EC24A01,2100000E1EC24A00
2021-04-08 11:16:21.000 +01:00 INFO __item_stack:/item0
```

Figure 8-72 Logs workflow



Date and Time	User Name	Command
8/4/2021 11:16:22	scuser	svctask mkvdiskhostmap -force -host vvolsftw-03 -scsi 15 vRO_Volume1
8/4/2021 11:16:20	scuser	svctask mkvolume -iogrp 0 -name vRO_Volume1 -pool vro_cp1 -size 100000000000 -unit b

Figure 8-73 Audit Log

8.8 IBM Storage Management Pack for VMware vRealize Operations Manager

The IBM Storage Management Pack for VMware vROps Manager allows vROps Manager users to obtain comprehensive monitoring information about the IBM storage resources that are used in their virtualized environment.

Connectivity to VMware vRealize Operations Manager can be provided either by using IBM Spectrum Connect to act as the middle-ware between vROps and IBM Storage Virtualize, or by using the dedicated storage plug-in that is provided by VMware that communicates directly with the storage system.

The VMware plug-in is available through the VMware Marketplace and is published as “vRealize Operations Management Pack for IBM SAN Volume Controller and IBM Storwize 4.0.0”. For more information, see IBM Storage Management Pack for VMware vRealize Operations Manager.

When using IBM Spectrum Connect for vROps integration, the management pack can be downloaded from the IBM Spectrum Connect GUI and then deployed on the vROps Manager server. After a VMware vROps Manager server is registered on an instance of IBM Spectrum Connect that is configured with storage systems, storage spaces, services, and vRealize servers, the storage-related data is pushed to the vROps Manager server in 5-minute intervals by default.

The dedicated IBM storage system adapter that is deployed on the vROps Manager server enables monitoring of the supported IBM storage system by using the vROps Manager. This adapter reports the storage-related information, such as monitoring data of all logical and physical elements, covering storage systems, storage domains, storage pools, volumes, hosts, modules, target ports, disks, health status, events, thresholds, and performance. It also provides the dashboards that display detailed status, statistics, metrics, and analytics data alongside hierarchical flowcharts with graphic representation of IBM storage system elements.

Relationships between the IBM storage system elements (storage systems, ports, storage pools, volumes, host, host initiator, modules, domain) and datastores, VMs, and hosts are displayed graphically in a drill-down style. This display provides VMware administrators with a complete and up-to-date picture of their used storage resources.

8.8.1 Configuring IBM Spectrum Connect for VMware vRealize Operations Manager

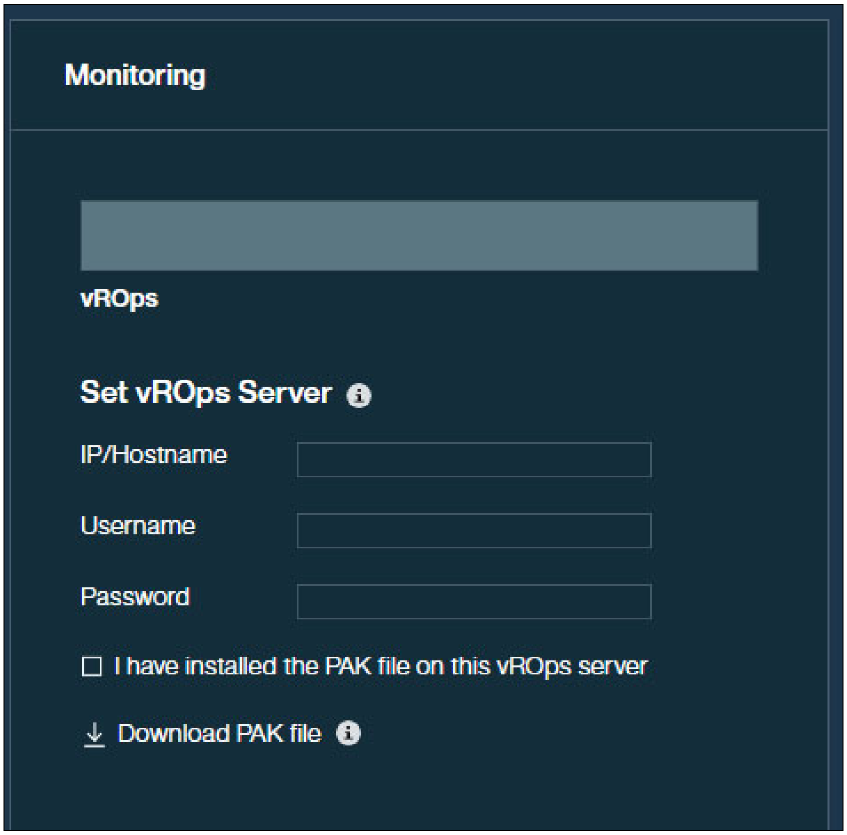
Before you can use the IBM Storage Management Pack for VMware vROps Manager, you must set a connection to at least one vROps Manager server, and then define which storage systems should be monitored in vROps.

Downloading the vROps management package

IBM Spectrum Connect provides a management package in the form of a PAK file, which can be deployed on the vROps Manager.

To download the PAK file from IBM Spectrum Connect, complete the following steps:

1. Go to the Monitoring window of the IBM Spectrum Connect GUI. The Set vROps Server dialog is displayed (Figure 8-74).



Monitoring

vROps

Set vROps Server

IP/Hostname

Username

Password

□ I have installed the PAK file on this vROps server

Figure 8-74 Set vROps Server dialog

2. On the bottom of the Monitoring window, click **Download PAK file** to save the file to your local computer. Alternatively, you can access the PAK file by using ssh or Secure Copy Protocol (SCP) by copying the package from the following directory on the IBM Spectrum Connect server:

   `/opt/ibm/ibm_spectrum_connect/downloads/static/IBM_Storage_Adapter-3.`*`x.xxxx`*`_signed.pak`

   – *`x.x`* is the release and mod number.
   – *`xxx`* is the current build number.

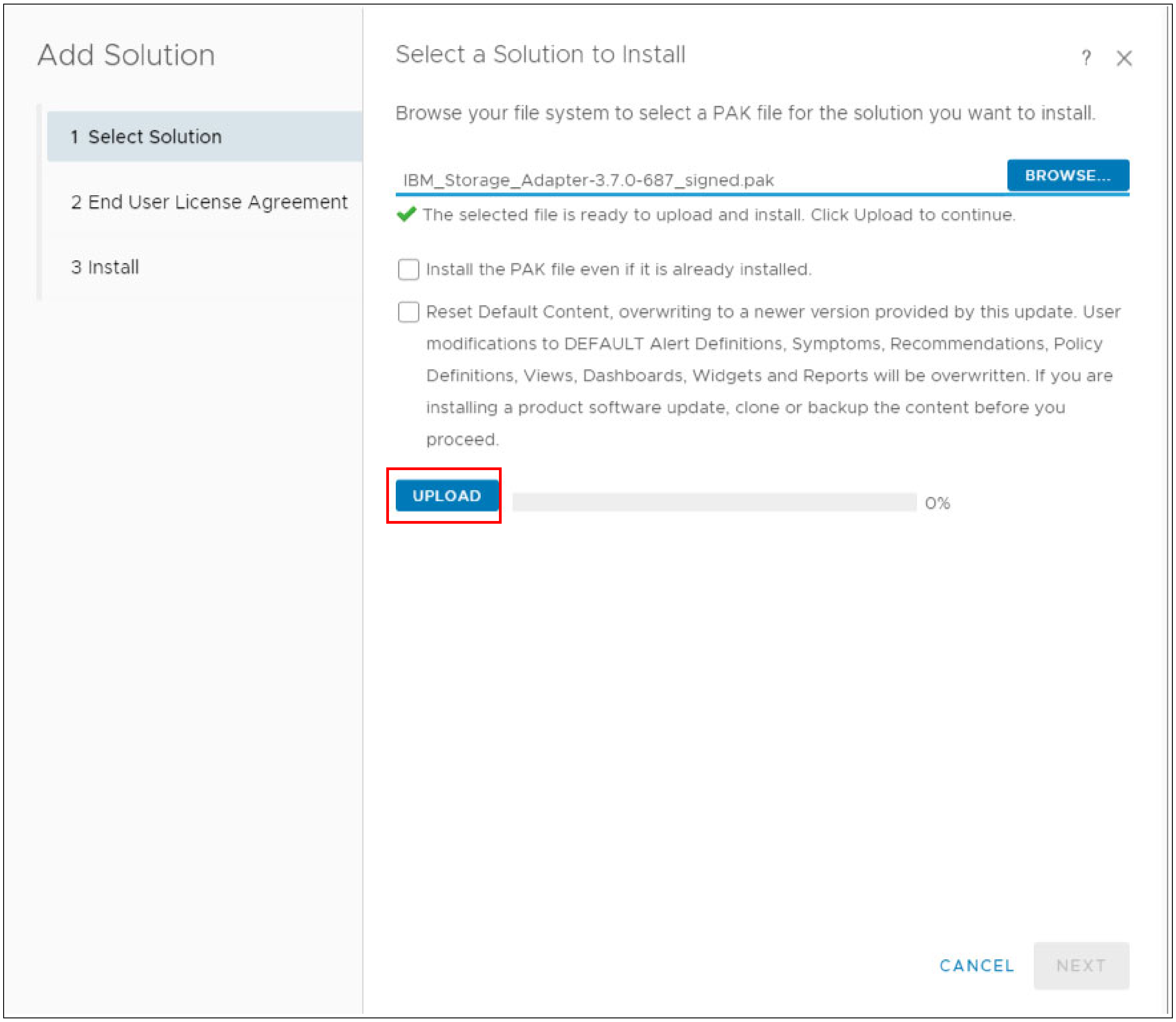
3. Save the file to your computer to later upload it to the vROps Manager.

8.8.2 Installing Management Pack in VMware vRealize Operations Manager

After the management package is downloaded to the computer, it must be deployed on the vROps Manager.

To deploy the management package on the vROps, complete the following steps:

1. Access the vROps Manager administrative web console by using `https://<hostname or IP address of the vROps UI>`.
2. Select **Administration** → **Solutions** → **Repository**.
3. In the Repository window, click **ADD/UPGRADE** to add a management package. The Add Solution dialog is displayed.
4. In the Add Solution dialog, click **Browse** and select the management package that is downloaded from IBM Spectrum Connect (Figure 8-75 on page 237). Click **UPLOAD** to start deployment.



Browse your file system to select a PAK file for the solution you want to install.

IBM_Storage_Adapter-3.7.0-687_signed.pak

✓ The selected file is ready to upload and install. Click Upload to continue.

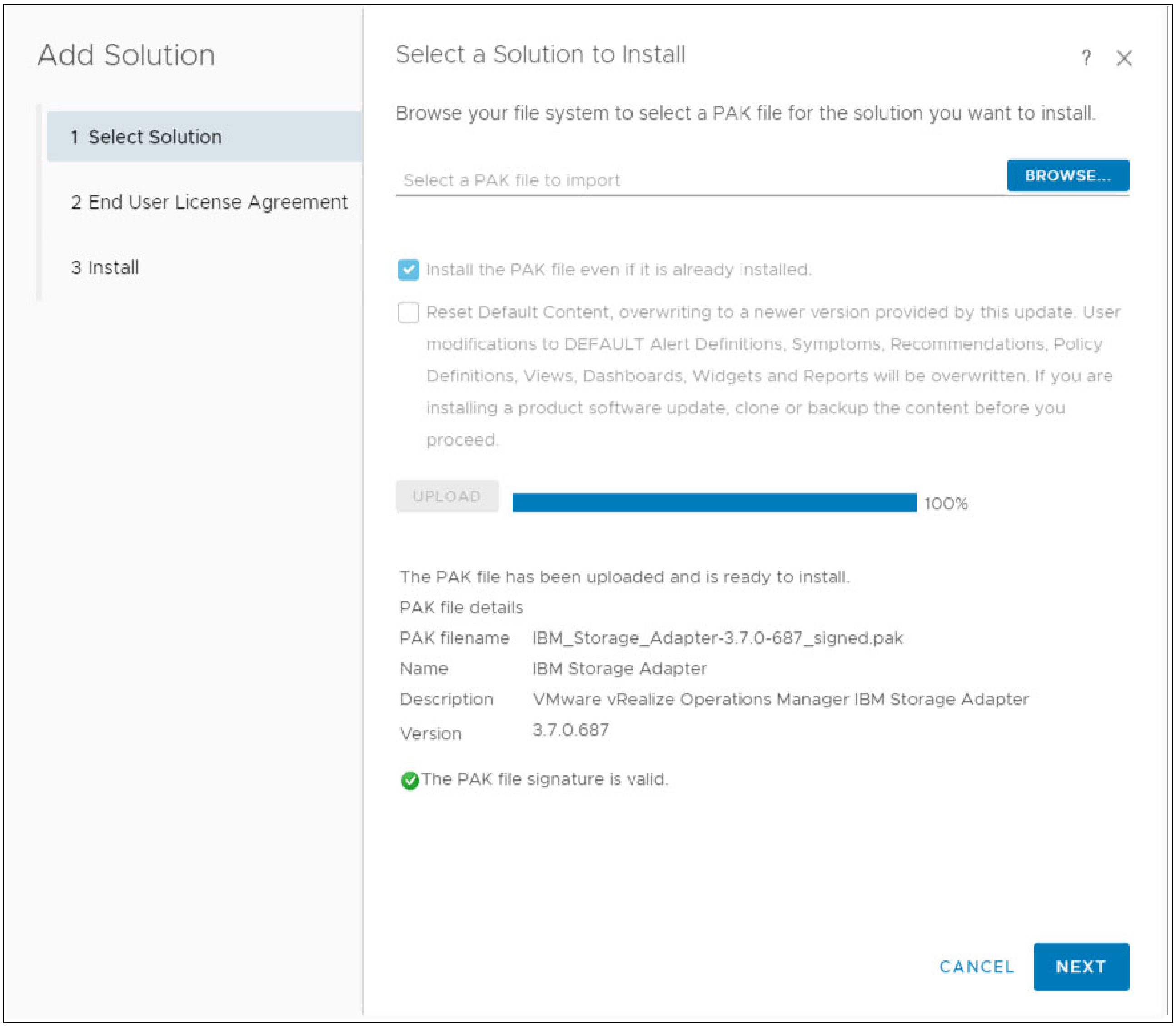
□ Install the PAK file even if it is already installed.

□ Reset Default Content, overwriting to a newer version provided by this update. User modifications to DEFAULT Alert Definitions, Symptoms, Recommendations, Policy Definitions, Views, Dashboards, Widgets and Reports will be overwritten. If you are installing a product software update, clone or backup the content before you proceed.

Figure 8-75 Starting a deployment

After the package is uploaded, the package information is displayed (Figure 8-76 on page 238).

5. Click **NEXT**. The IBM license agreement is displayed.
6. Accept the IBM license agreement and click **NEXT** to continue. The Installation Solution progress is displayed.
7. Click **FINISH** to complete the installation. More configuration of the management package is not required on the vROps. Under certain conditions, the package’s status might appear as `Not configured on the vROps`. You can disregard this information.


Add Solution
1 Select Solution
2 End User License Agreement
3 Install
Select a Solution to Install
? ×

Browse your file system to select a PAK file for the solution you want to install.

Select a PAK file to import
BROWSE...

☑ Install the PAK file even if it is already installed.

□ Reset Default Content, overwriting to a newer version provided by this update. User modifications to DEFAULT Alert Definitions, Symptoms, Recommendations, Policy Definitions, Views, Dashboards, Widgets and Reports will be overwritten. If you are installing a product software update, clone or backup the content before you proceed.

The PAK file has been uploaded and is ready to install.

PAK file details

PAK filename	IBM_Storage_Adapter-3.7.0-687_signed.pak
Name	IBM Storage Adapter
Description	VMware vRealize Operations Manager IBM Storage Adapter
Version	3.7.0.687

✓ The PAK file signature is valid.

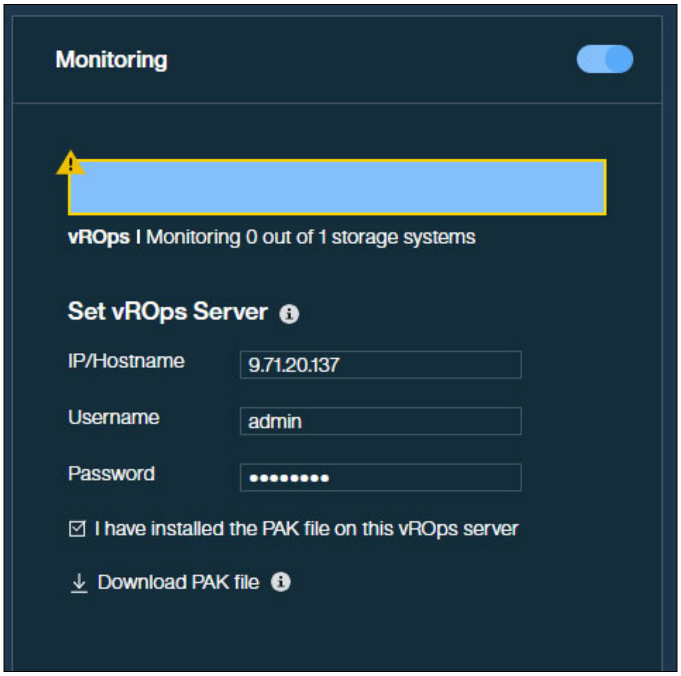
Figure 8-76 Package information

Connecting the vROps server to IBM Spectrum Connect

After the management package is successfully deployed, you must add the vROps Manager server to IBM Spectrum Connect. Then, the vROps Manager server must be connected to IBM Spectrum Connect.

To add the VROps Manager server to IBM Spectrum Connect, complete the following steps:

1. Go to the Monitoring window of the IBM Spectrum Connect GUI (Figure 8-77 on page 239).
2. Enter the following information:
   - IP/Hostname. IP address or FQDN of the vROps Manager server
   - Username
   - Password
3. Select the checkbox to confirm you installed the PAK file on the vROps Manager server.


Monitoring

vROps I Monitoring 0 out of 1 storage systems

Set vROps Server

IP/Hostname 9.71.20.137

Username admin

Password ●●●●●●●●

☑ I have installed the PAK file on this vROps server

Figure 8-77 Monitoring window

Controlling storage system monitoring on the vROps server

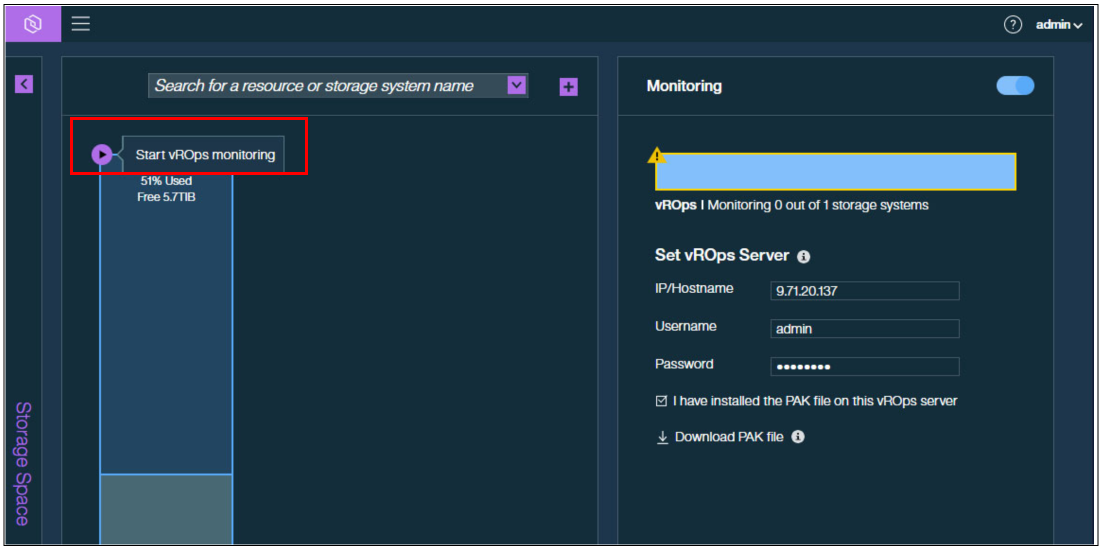
When a single IBM Spectrum Connect instance is managing multiple IBM Storage Virtualize storage systems, you can select which systems to monitor and which to ignore.

To enable monitoring, complete the following steps:

1. Go to the Monitoring window of the IBM Spectrum Connect GUI.
2. In the Storage Systems window, right-click a storage system that you intend to monitor, and select **Start vROps monitoring**, or click **Start Monitoring** on the storage system (Figure 8-78 on page 240). The monitored system color changes to indicate the connection to the vROps server. IBM Spectrum Connect starts pushing the information to vROps Manager by using RESTful API requests.

   To stop monitoring a storage system, click **Stop Monitoring** on the monitored system.

   After a vROps server connection is defined and storage systems are associated with the vROps server, detailed monitoring information for these storage systems becomes available in vROps.



vROps I Monitoring 0 out of 1 storage systems

Set vROps Server

IP/Hostname 9.71.20.137

Username admin

Password ••••••••

☑ I have installed the PAK file on this vROps server

Download PAK file

Figure 8-78 Start vROps monitoring

9

Troubleshooting

This chapter provides information to troubleshoot common problems that can occur in an IBM FlashSystem and VMware vSphere environment. It also explains how to collect the necessary problem determination data.

This chapter includes the following sections:

- 9.1, “Collecting data for support” on page 242
- 9.2, “Common support cases” on page 245

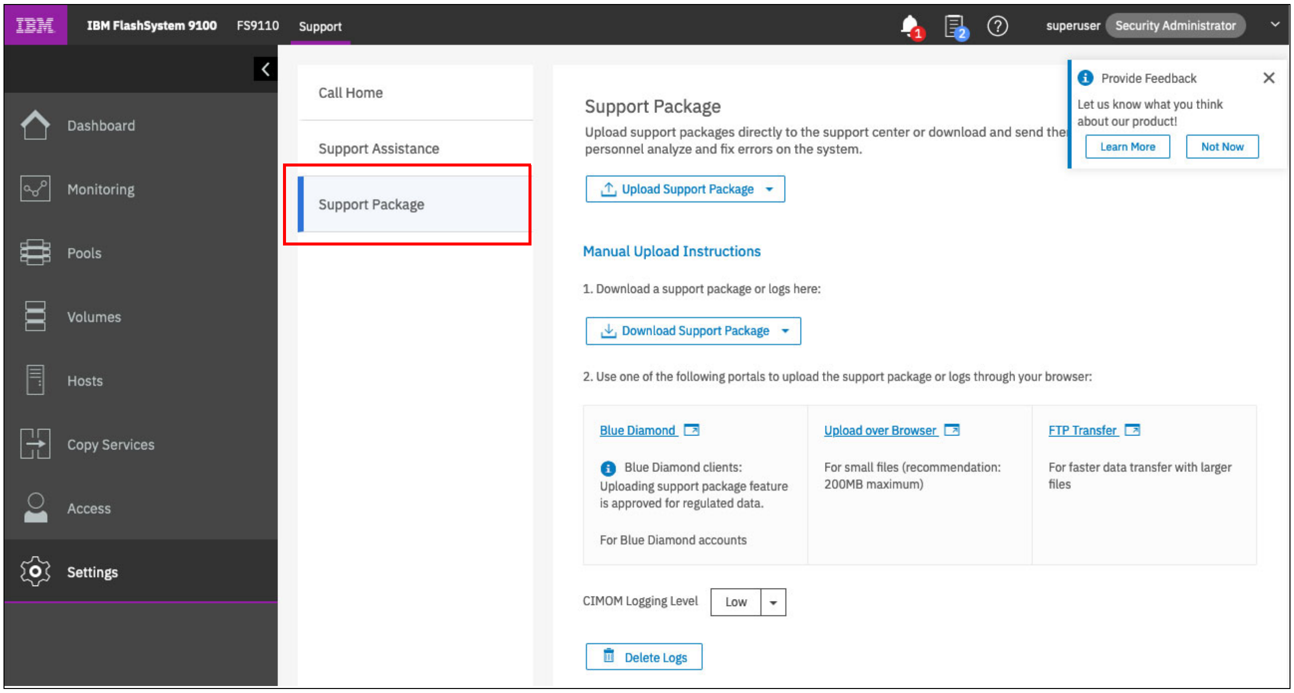
9.1 Collecting data for support

This section discusses the data that needs to be collected before contacting support for assistance. When interacting with support, it is important to provide a clear problem description, so the support engineers can help resolve the issue. A good problem description includes the following information:

- What was expected?
- What was not expected?
- What are the resources that are involved (volumes, hosts, and so forth)?
- When did the problem take place?

9.1.1 Data collection guidelines for SAN Volume Controller and IBM FlashSystem

On SAN Volume Controller (SVC) and IBM FlashSystem, system logs can be collected in the product GUI by selecting **Settings** → **Support Package** (Figure 9-1).



Support Package

Upload support packages directly to the support center or download and send the personnel analyze and fix errors on the system.

Let us know what you think about our product!

Manual Upload Instructions

1. Download a support package or logs here:

2. Use one of the following portals to upload the support package or logs through your browser:

Blue Diamond clients: Uploading support package feature is approved for regulated data.

For Blue Diamond accounts

For small files (recommendation: 200MB maximum)

For faster data transfer with larger files

CIMOM Logging Level: Low

Figure 9-1 Collecting a support package in the GUI

For more information about the level of logs to collect for various issues, see What Data Should You Collect for a Problem on IBM Storage Virtualize systems?

For the topics covered in the scope of this document, you typically need to gather a snap (option) 4, which contains standard logs plus new statesaves. Because this data often takes a long time to collect, it might be advantageous to manually create the statesaves, and then collect the standard logs afterward. This task can be done by using the `svc_livedump` command-line interface (CLI) utility, which is available in the product command-line interface (Example 9-1 on page 243).

Example 9-1   Using svc_livedump to manually generate statesaves

```
IBM_FlashSystem:Cluster_9.42.162.160:superuser>svc_livedump -nodes all -y
Livedump - Fetching Node Configuration
Livedump - Checking for dependent VDisks
Livedump - Check Node status
Livedump - Preparing specified nodes  - this may take some time...
Livedump - Prepare node 1
Livedump - Prepare node 2
Livedump - Trigger specified nodes
Livedump - Triggering livedump on node 1
Livedump - Triggering livedump on node 2
Livedump - Waiting for livedumps to complete dumping on nodes 1,2
Livedump - Waiting for livedumps to complete dumping on nodes 2
Livedump - Successfully captured livedumps on nodes 1,2
```

After you generate the necessary statesaves, collect standard logs and the latest statesaves (option 3), and use the GUI to create a support package including the manually generated livedumps. Alternatively, you can create the support package by using the CLI (Example 9-2).

Example 9-2   Using svc_snap to generate a support package in the CLI

```
IBM_FlashSystem:Cluster_9.42.162.160:superuser>svc_snap -gui3
Collecting data
Packaging files
Snap data collected in /dumps/snap.78E35HW-2.210329.170759.tgz
```

When the support package is generated by using the command line, you can download it by using the GUI or using a Secure Copy Protocol (SCP) client.

9.1.2 Data collection guidelines for VMware ESXi

For issues involving VMware ESXi hypervisor, which includes storage access errors, it is vital to ensure that the logs from the host-side of the connection are collected in addition to the storage subsystem. For the VMware instructions about collecting ESXi log packages, see Collecting diagnostic information for VMware ESXi (653).

When downloading a package for an ESXi host, the default settings provide the information that is needed to analyze most problems.

9.1.3 Data collection guidelines for VMware Site Recovery Manager

Troubleshooting problems that involve VMware Site Recovery Manager usually requires the analyzing of data from the following sources:

1. The storage systems associated in all related sites as shown in 9.1.1, “Data collection guidelines for SAN Volume Controller and IBM FlashSystem” on page 242.
2. The IBM Storage Replication Adapter (SRA) appliance logs in all related sites.
3. The VMware Site Recovery Manager logs.

IBM SRA log collection

Current versions of the IBM SRA are deployed inside of the VMware Site Recovery Manager (SRM) server. By default, the SRA application logs all data in `/var/log/vmware/srm` on the SRM server where SRA is deployed.

VMware SRM log collection

For the VMware instructions for creating and downloading SRM logs, see Collecting diagnostic information for Site Recovery Manager (1009253).

> **Important:** When collecting data for problems that are related to SRM, make sure to collect data from all sites associated with the problem.

9.1.4 Data collection guidelines for IBM Spectrum Connect (VASA or vVols)

For troubleshooting issues associated with VASA or VMware vSphere Virtual Volume (vVol), the following sets of data are required for troubleshooting:

1. A support package from the storage system as shown in 9.1.1, “Data collection guidelines for SAN Volume Controller and IBM FlashSystem” on page 242
2. A support package from IBM Spectrum Connect
3. A support package from the management application interfacing with IBM Spectrum Connect
4. If the problem includes access to the data, ESXi logs as shown in 9.1.2, “Data collection guidelines for VMware ESXi” on page 243

Collecting Data for IBM Spectrum Connect

IBM Spectrum Connect logs can be collected in the following two ways:

1. Using the Operating System Shell

   IBM Spectrum Connect stores data in `/var/log/sc` by default. Copy the contents of this directory off the system for use.

2. Using the IBM Spectrum Connect User Interface

   In the IBM Spectrum Connect User Interface, select **Settings** → **Support** → **Collect log** to gather and download the log files (Figure 9-2).

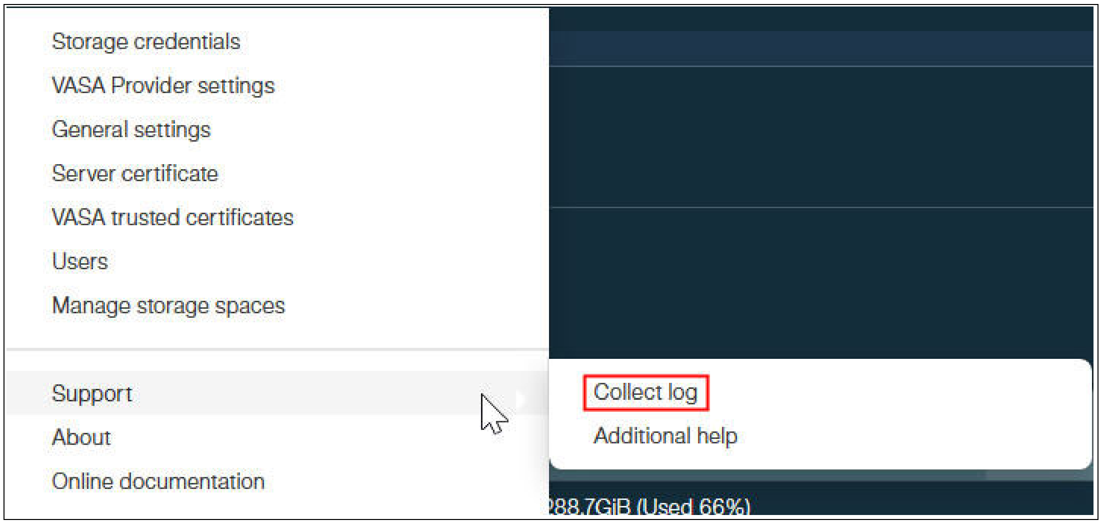


Figure 9-2 Collecting IBM Spectrum Connect logs

Collecting data for VMware vCenter

vCenter logs can be collected by using the same process as ESXi hosts, as described in 9.1.2, “Data collection guidelines for VMware ESXi” on page 243. The difference is when selecting resources for which to collect logs, select the vCenter server instead of (or in addition to) an ESXi host.

Collecting data for VMware vRealize Orchestrator

For the VMware data collection instructions for the VMware vRealize Orchestrator (vRO), see Generating a log bundle from command line for a vRealize Orchestrator 7.x appliance (2150664).

Collecting data for VMware vRealize Operations Manager

For the VMware data collection instructions for the VMware vRealize Operations (vROps) Manager, see Collecting diagnostic information from vRealize Operations (2074601).

9.2 Common support cases

This section describes topics that are commonly raised to the support center. This section is not meant to be a comprehensive guide on debugging interoperability issues between SVC, IBM FlashSystem, and VMware products.

9.2.1 Storage loss of access

When troubleshooting the loss of access to storage, it is important to properly classify how access was lost and what resources are involved.

The three general categories of storage loss of access events in VMware products are:

- All paths down (APD)
- Permanent device loss (PDL)
- Virtual machine (VM) crash

All Paths Down

An APD event takes place when all the paths to a datastore are marked offline. Example 9-3 shows the `vmkernel` log signature for an APD event.

Example 9-3 ESXi All Paths Down log signature

```
cpu1:2049)WARNING: NMP: nmp_IssueCommandToDevice:2954:I/O could not be issued to
device "naa.600507681081025a1000000000000003" due to Not found
cpu1:2049)WARNING: NMP: nmp_DeviceRetryCommand:133:Device
"naa.600507681081025a1000000000000003": awaiting fast path state update for
failover with I/O blocked. No prior reservation exists on the device.
cpu1:2049)WARNING: NMP: nmp_DeviceStartLoop:721:NMP Device
"naa.600507681081025a1000000000000003" is blocked. Not starting I/O from device.
cpu1:2642)WARNING: NMP: nmpDeviceAttemptFailover:599:Retry world failover device
"naa.600507681081025a1000000000000003" - issuing command 0x4124007ba7c0
cpu1:2642)WARNING: NMP: nmpDeviceAttemptFailover:658:Retry world failover device
"naa.600507681081025a1000000000000003" - failed to issue command due to Not found
(APD), try again...
cpu1:2642)WARNING: NMP: nmpDeviceAttemptFailover:708:Logical device
"naa.600507681081025a1000000000000003": awaiting fast path state update...
```

When all paths are lost, if there is no path update lasting through the `Misc.APDTimeout` value (default of 140 seconds), then the APD condition is latched. Example 9-4 shows the log signature in the `vobd.log` file for a latched APD state.

Example 9-4 ESXi All Paths Down timeout

```
[APDCorrelator] 2682686563317us: [esx.problem.storage.apd.timeout] Device or
filesystem with identifier [11ace9d3-7bebe4e8] has entered the All Paths Down
Timeout state after being in the All Paths Down state for 140 seconds. I/Os will
now be fast failed.
```

These issues are typically the result of errors in path recovery. Corrective actions include:

- Validating the best practice multipathing configuration is in use as shown in 2.3, “Multi-path considerations” on page 18.
- Validate all server driver and firmware levels are at the latest supported level.
- Validate the network infrastructure connecting the host and storage is operating correctly.

Permanent device loss

A PDL event is the response to an unrecoverable I/O error that is returned by a storage controller. Example 9-5 shows the `vmkernel` log signature for a PDL event.

Example 9-5 ESXi permanent device loss log signature

```
cpu17:10107)WARNING: Vol3: 1717: Failed to refresh FS
4beb089b-68037158-2ecc-00215eda1af6 descriptor: Device is permanently unavailable
cpu17:10107)ScsiDeviceIO: 2316: Cmd(0x412442939bc0) 0x28, CmdSN 0x367bb6 from
world 10107 to dev "naa.600507681081025a1000000000000003" failed H:0x0 D:0x2 P:0x0
Valid sense data: 0x2/0x3e/0x1
cpu17:10107)Vol3: 1767: Error refreshing PB resMeta: Device is permanently
unavailable
```

For a list of I/O errors that trigger PDL, see Permanent Device Loss (PDL) and All-Paths-Down (APD) in vSphere 6.x and 7.x (2004684).

These types of events are often the result of a hardware failure or low-level protocol error in the server host bus adapter (HBA), storage area network (SAN), or the storage array. If hardware errors are found that match the time in which the PDL happens, PDL is likely the cause.

Virtual machine crash

If a VM fails in the absence of an APD or PDL event, then treat this scenario as an operating system or application failure inside the VM. If the analysis of the guest VM points to a storage I/O timeout, then this analysis might point to latency in processing VM I/O requests. In such situations, it is important to review the following sets of data:

- The `vmkernel` log of the ESXi host that houses the VM that failed. Specifically, look for events that are related to the physical device backing the datastore that houses the VM.
- The storage array’s performance data. Specifically, check for peak read-and-write latency during the time when the VM failed.
- Operating System and application logs for the VM that failed. Specifically, identify key timeout values and the time of the crash.

9.2.2 VMware migration task failures

This section discusses the failures for two types of migrations:

1. *vMotion* is a migrate task that is used to move the running state of the VM (for example, memory and compute resource) between ESXi hosts.
2. *Storage vMotion* is a migrate task that is used to move the VM storage resources between datastores, for example VMDK files datastores.

vMotion tasks

vMotion tasks are largely dependent on the Ethernet infrastructure between the ESXi hosts. The only real storage interaction is at the end when file locks must move from one host to another. In this phase, it is possible for SCSI Reservation Conflicts or file lock contention to result in the failing of the migration task. The following articles describe the most frequent issues:

- Investigating virtual machine file locks on ESXi hosts (10051)
- Resolving SCSI reservation conflicts (1002293)
- IBM Spectrum Virtualize APAR HU01894

Storage vMotion tasks

Storage vMotion tasks are primarily dependent on storage throughput.

Migrating virtual machines between datastores within the same storage controller uses the storage array's capabilities for faster performance. This is achieved through a technology such as Extended Copy (XCOPY) or VAAI Hardware Accelerated Move, which offloads the copy operation to the storage array itself.

The default timeout for the task to complete is 100 seconds. If the migration takes longer than 100 seconds to complete, then the task fails with a timeout, as shown in Example 9-6.

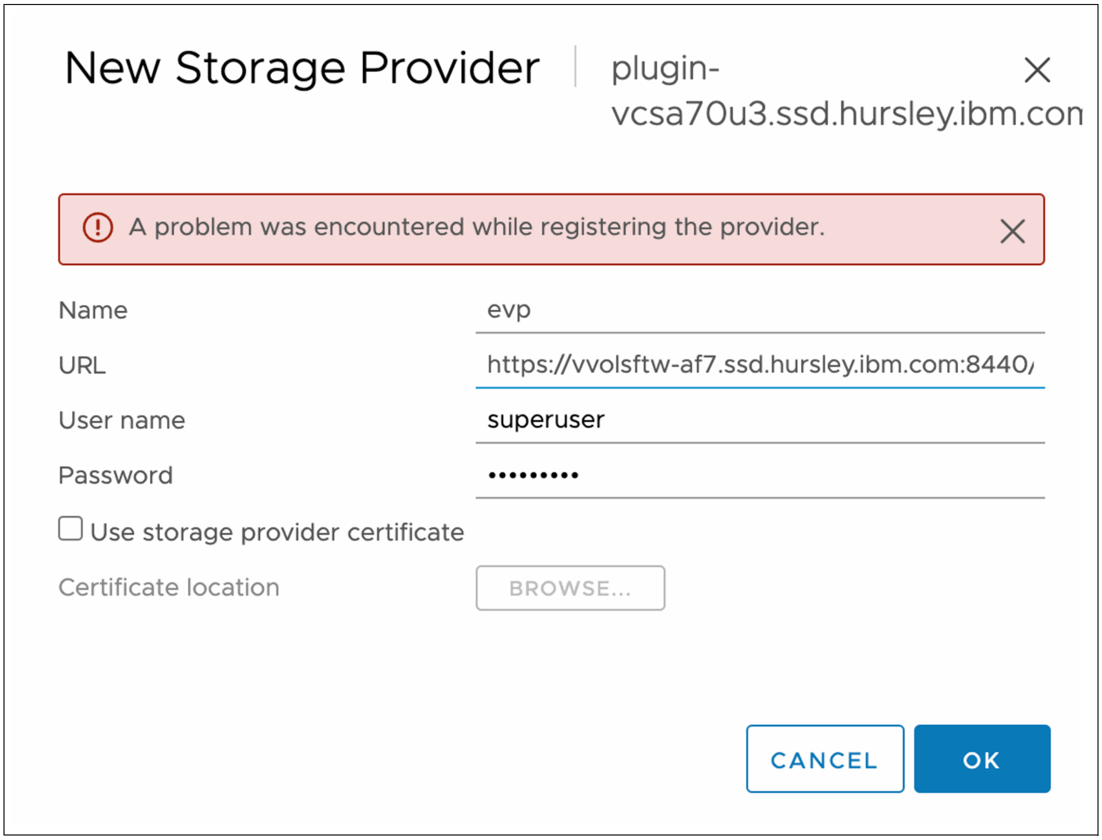
Example 9-6 VMware Log Storage vMotion timeout

```
vmkernel: 114:03:25:51.489 cpu0:4100)WARNING: FSR: 690: 1313159068180024 S:
Maximum switchover time (100 seconds) reached. Failing migration; VM should resume
on source.
vmkernel: 114:03:25:51.489 cpu2:10561)WARNING: FSR: 3281: 1313159068180024 D: The
migration exceeded the maximum switchover time of 100 seconds. ESX has
preemptively failed the migration to allow the VM to continue running on the
source host.
vmkernel: 114:03:25:51.489 cpu2:10561)WARNING: Migrate: 296: 1313159068180024 D:
Failed: Maximum switchover time for migration exceeded(0xbad0109) @0x41800f61cee2
```

The task is generic by nature and the root cause behind the timeout typically requires performance analysis of the storage arrays that are involved and a detailed review of the ESXi logs for the host performing the task. In some circumstances, it might be appropriate to increase the default timeout, as described at Using Storage Motion to migrate a virtual machine with many disks fails without timeout (1010045).

9.2.3 Registration of vVol/VASA Storage Provider failures

There can be several reasons why an attempt to register the Storage Provider into vSphere might fail. Some failure cases provide a generic error message such as `A problem was encountered while registering the provider`. See Figure 9-3 on page 248.



New Storage Provider | plugin-vcsa70u3.ssd.hursley.ibm.con

A problem was encountered while registering the provider.

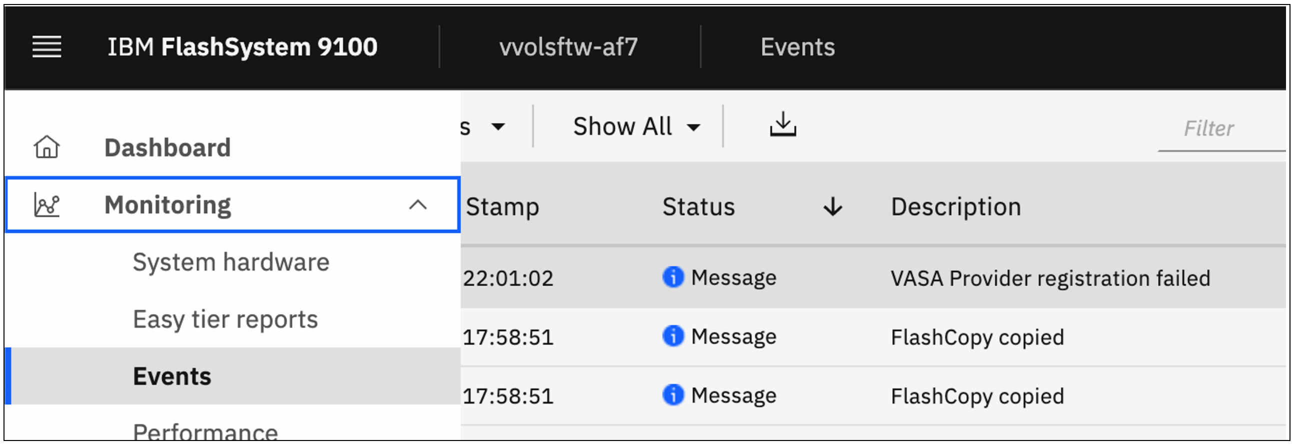
Name	evp
URL	https://vvolsftw-af7.ssd.hursley.ibm.com:8440/
User name	superuser
Password	•••••••••

□ Use storage provider certificate

Certificate location

Figure 9-3 Generic error message

Assuming the VASA Provider URL is correctly defined and is accessible from vSphere, registration failure cases can generate an event log entry detailing the reason for the failure. In situations with connectivity issues, no further debug information is generated on the storage system. See Figure 9-4.



Stamp	Status	Description
22:01:02	Message	VASA Provider registration failed
17:58:51	Message	FlashCopy copied
17:58:51	Message	FlashCopy copied

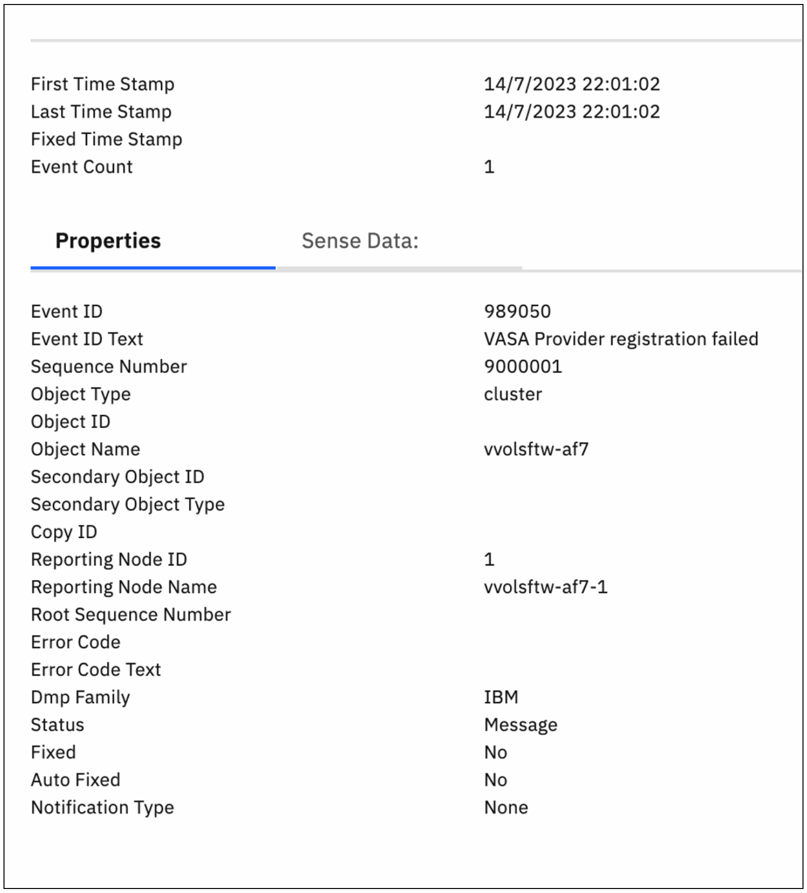
Figure 9-4 Vasa Provider registration failed message

Review the event log by selecting **Monitoring** → **Events** from the storage system GUI.

Review any event log entries titled `VASA provider registration failed`. Double-click the failure message, or right-click and select properties to view additional context.

The following example and Figure 9-5 provide some context about the error:

```
Event ID989050
Event ID TextVASA provider registration failed
ExplanationAn attempt to register the VASA provider within a vCenter console
failed
```

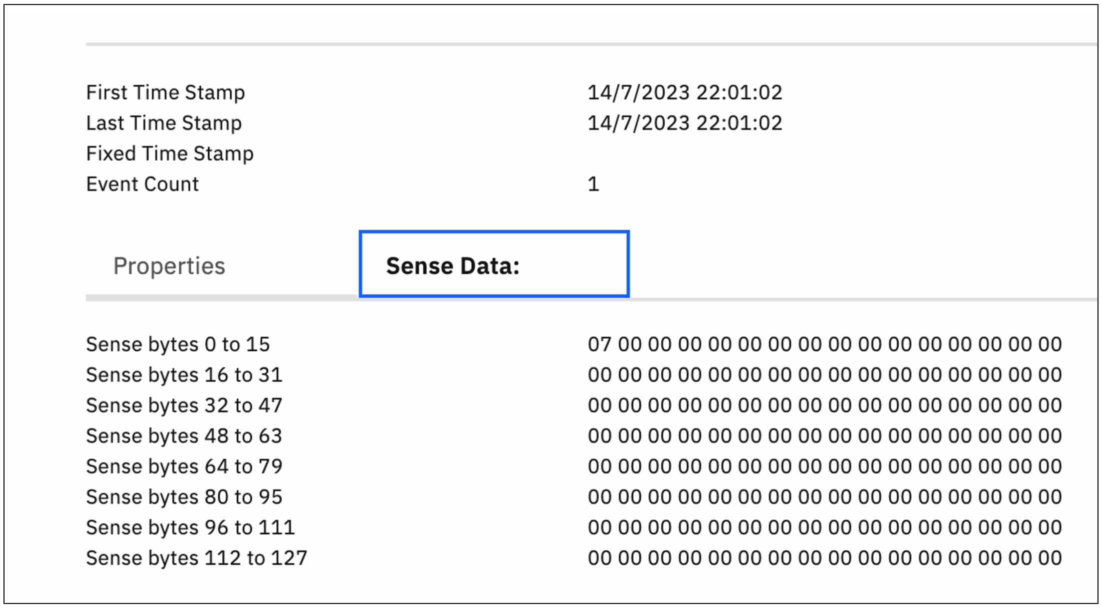


First Time Stamp	14/7/2023 22:01:02
Last Time Stamp	14/7/2023 22:01:02
Fixed Time Stamp	
Event Count	1

Event ID	989050
Event ID Text	VASA Provider registration failed
Sequence Number	9000001
Object Type	cluster
Object ID	
Object Name	vvolsftw-af7
Secondary Object ID	
Secondary Object Type	
Copy ID	
Reporting Node ID	1
Reporting Node Name	vvolsftw-af7-1
Root Sequence Number	
Error Code	
Error Code Text	
Dmp Family	IBM
Status	Message
Fixed	No
Auto Fixed	No
Notification Type	None

Figure 9-5 Event properties

Review the error log entry and associated sense data, and make note of the value for `Sense byes 0 to 15`. See Figure 9-6 on page 250.



```
First Time Stamp        14/7/2023 22:01:02
Last Time Stamp         14/7/2023 22:01:02
Fixed Time Stamp
Event Count             1
```

```
Sense bytes 0 to 15       07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sense bytes 16 to 31      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sense bytes 32 to 47      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sense bytes 48 to 63      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sense bytes 64 to 79      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sense bytes 80 to 95      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sense bytes 96 to 111     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sense bytes 112 to 127    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Figure 9-6 Sense Data

This information is also available within the detailed view of the specific eventlog entry. See Example 9-7.

Example 9-7 Detailed view of the specific eventlog entry

```
IBM_FlashSystem:vvolsftw-af7:superuser>lseventlog 9000001
sequence_number 9000001
...
object_name vvolsftw-af7
status message
event_id 989050
event_id_text VASA Provider registration failed
...
sense1 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
sense8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

The value associated with sense1 will indicate the reason for the registration failure. Provide this information when dealing with IBM Support. The logged failure cases can be summarized by Table 9-1.

Table 9-1 Logged failure cases.

Sense Code Value	Reason for failure
01	Failed to authenticate username and password.
02	An existing user account exists with a configured cert_uid.
04	The specified user account on the storage system is "Locked".
05	The creation of a truststore has failed.
05 01	Certificate bundle is too large to be stored in a single truststore.

Sense Code Value	Reason for failure
06	Failed to add the vCenter IP to the certuid field on the user account.
07	The usergroup ownership is invalid for the specified user.

The following sections include some common reasons for registration failures and some suggested recovery actions.

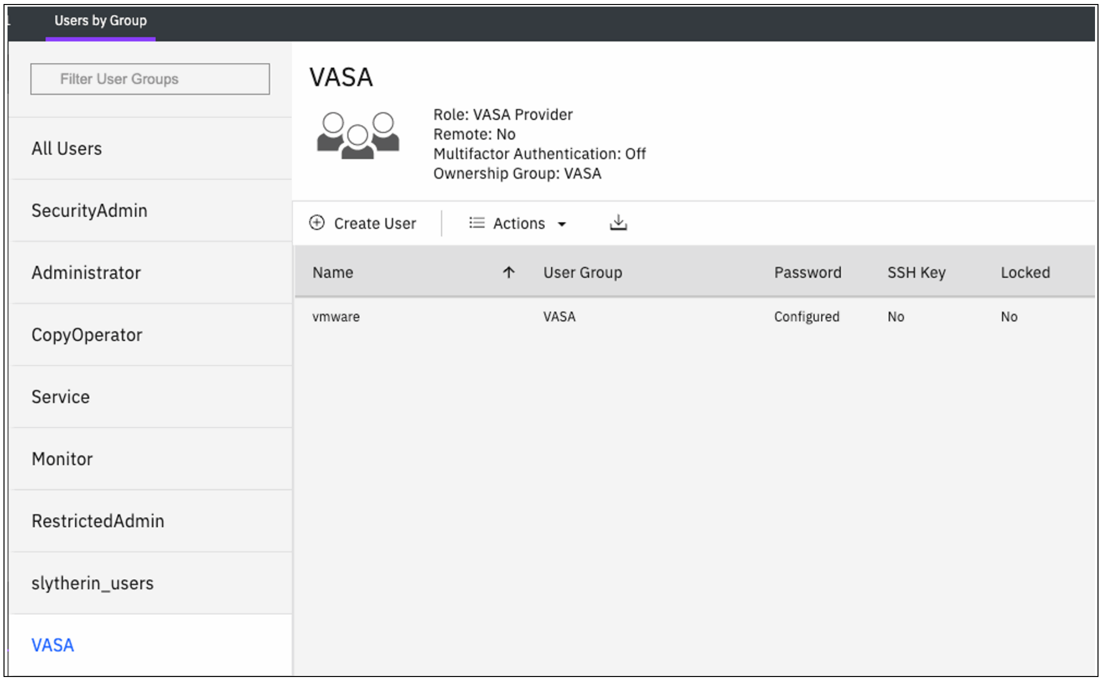
Incorrect credentials being specified (Sense 01, 02, 04, 06)

Ensure that the credentials are entered as defined in the **Settings** → **vVol** page when enabling vVol. This should not be the superuser or other administrative account, and must be for a user account within, for example, the VASA usergroup, assigned with the VASAProvider role.

Additionally, if a previous attempt to register the storage provider has failed for another reason, the password authentication capability might have been removed from the user account.

To check the user account status on the storage system locate the user account and ensure the Password authentication is `Configured` before attempting registration.

Figure 9-7 shows an example of a system ready to be registered.



VASA

Role: VASA Provider
Remote: No
Multifactor Authentication: Off
Ownership Group: VASA

Name	User Group	Password	SSH Key	Locked
vmware	VASA	Configured	No	No

Figure 9-7 An example of a system ready to be registered

If the Password value is displayed as `No`, it suggests password authentication has been disabled for the user account in favor of certificate authentication.

To verify, use the storage system CLI to identify the user account. Run the **`lsuser`** command and specify the username or id. See Example 9-8 on page 252.

Example 9-8 lsuser vmware command

```
IBM_FlashSystem:vvolsftw-af7:superuser>lsuser vmware
id 1
name vmware
password no
ssh_key no
remote no
usergrp_id 6
usergrp_name VASAUsers
owner_id 0
owner_name VASA
locked no
locked_until
password_expiry_time
password_change_required no
certuid 9.71.20.191
```

In the CLI example, as shown in Example 9-8, the values for `password=no` and `certuid=9.71.20.191` suggests that a partial registration was triggered in vSphere and has caused the removal of password authentication for the user account. Additionally, the IP address of the vCenter appliance that is used for registration is defined in the certuid field.

To reconfigure the user account, run the following **`chuser`** command:

```
chuser -password <new password> -nocertuid <username>
```

For the user ID, vmware, the command might look like the following:

```
chuser -password C0mpl3xPasswd -nocertuid vmware
```

After completing the preceding task, verify that the output of the **`lsuser`** command correctly reflects the changes and then reattempt the Storage Provider registration with the new credentials.

The maximum number of truststores defined on the storage system (Sense 05)

The storage system supports a maximum number of 7 truststores, and any attempt to register the Storage Provider within vSphere also attempts to store the vSphere certificate bundle on the storage system. Repeated failed attempts to register a Storage Provider within vSphere can cause duplicated truststore entries and eventually reaches the maximum limit.

To validate this, connect to the storage system management CLI and run the **`lstruststore`** command, as shown in Example 9-9.

Example 9-9 lstruststore command

```
IBM_FlashSystem:vvolsftw-af7:superuser>lstruststore
id name               percent_used space restapi ipsec vasa email
0  common_CA_database 100          0     off     off   off  off
1  store0             45           6.5KB off     off   on   off
2  store1             45           6.5KB off     off   on   off
3  store2             45           6.5KB off     off   on   off
4  store3             45           6.5KB off     off   on   off
```

Review the VASA column in the lstruststore output. Any truststores that show `vasa=on` will have been created by an attempted registration of the Storage Provider in vCenter. If the

Storage Provider has not been successfully registered in vSphere, and you have multiple or duplicated entries displayed in the output of **lstruststore** where vasa=on. Remove each truststore using the **rmtruststore <id>** command and retry Storage Provider registration.

The certificates being too large for the truststore (Sense 05 01)

In certain situations with environments with complex certificate configurations, vSphere attempts to submit multiple certificates within a single file, which cannot be added in a single truststore because of the large size. The truststore within IBM Storage Virtualize has a limit of 12 KB per truststore, so any certificate file must not exceed 12 KB.

To workaround this limitation, the certificate file can be split in to multiple, smaller files that individually are less than the 12 KB limit.

After an attempted registration, the certificates are temporarily stored within the configuration node in the file /dumps/vmware-vasa-cert. The following command can be run from an external machine to securely copy the certificate file to a local /tmp directory:

```
scp superuser@<Cluster_IP>:/dumps/vmware-vasa-certs /tmp
```

This certificate file must be split manually into two or more smaller files with a different name, such as vmware-vasa-certs-1, vmware-vasa-certs-2. The final size of each file must be less than 12 KiB and must include one entire certificate, which includes the line having the text BEGIN CERTIFICATE and the line having the text END CERTIFICATE.

These multiple certificate files must then be securely copied back to the Storage Virtualize config node:

```
scp /tmp/vmware-vasa-certs-* superuser@<Cluster_IP>:/dumps/
```

Create multiple truststores by using the split certificate files copied to the storage system by running the **mktruststore** command:

```
svctask mktruststore -file /dumps/vmware-vasa-certs-1 -vasa on
svctask mktruststore -file /dumps/vmware-vasa-certs-2 -vasa on
```

Also create a file /dumps/bypass-truststore to trigger the VASA provider to bypass the truststore creation as it has already been manually created. On a local system, create an empty file with the name bypass-truststore and copy it to the /dumps directory on the configuration node.

```
/tmp # touch /tmp/bypass-truststore
/tmp # scp /tmp/bypass-truststore superuser@<Cluster_IP>:/dumps
```

Register the VASA Provider again within vCenter, and verify that it registered successfully.

The incorrect user role being assigned to the user's usergroup (Sense 07)

By default, when enabling the vVol function on the system, a VASA usergroup is created, and assigned the VASAProvider role, which allows manipulation of vVol objects. No other user role is permitted for the VASA provider user. If configuring vVol bu using the CLI, ensure that the appropriate VASAProvider role is assigned to the user group that contains the user account.

The Root certificate not being registered into vSphere

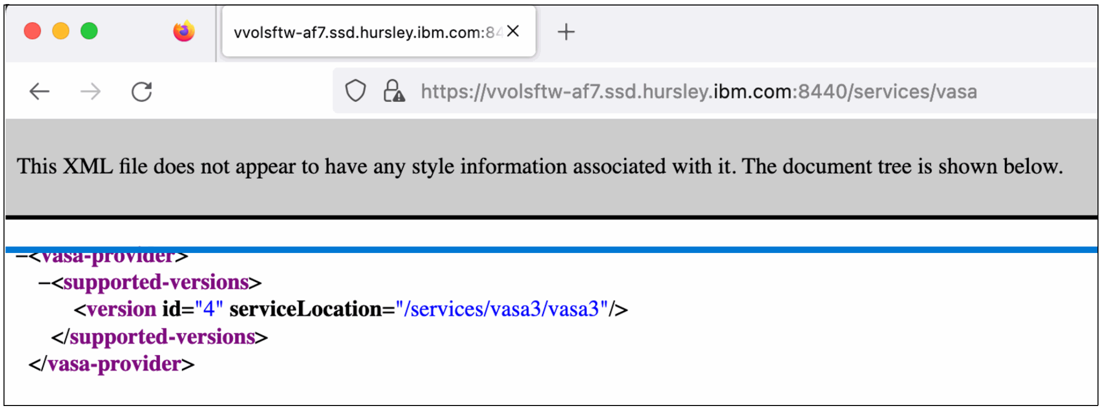
If a user attempts to register a Storage Provider into vCenter without previously adding the root certificate to the vCenter trust store, an error is returned stating The signing certificate of the provider has not been added to the truststore. However, despite this error, the vSphere certificate was stored in the storage system's truststore, and the password was removed from the user account. If after correcting this by exporting the storage root certificate and importing into vSphere, then any subsequent attempts to register the storage provider fail until the user account is reconfigured. Also, see the sections “Incorrect credentials being specified (Sense 01, 02, 04, 06)” on page 251, and “The maximum number of truststores defined on the storage system (Sense 05)” on page 252.

Incorrect VASA URL being used or network connectivity issues

Make sure that the URL is copied from the **Settings** → **vVol** page in the storage system management interface. The following URL is an example of the syntax::

```
https://<IP or FQDN of the system>:8440/services/vasa
```

For additional validation, verify that the URL is visible in a web browser before continuing to register the Storage Provider. You should be able to see the following information, as shown in Figure 9-8.


vvolsftw-af7.ssd.hursley.ibm.com:84
https://vvolsftw-af7.ssd.hursley.ibm.com:8440/services/vasa

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
–<vasa-provider>
  –<supported-versions>
      <version id="4" serviceLocation="/services/vasa3/vasa3"/>
    </supported-versions>
  </vasa-provider>
```

Figure 9-8 XML file style information error

Furthermore, consider testing IP connectivity from the vCenter Appliance console by running a curl request to the VASA provider URL from an ssh or console session that is similar to the following example:

```
curl -i -k https://vvolsftw-af7.ssd.hursley.ibm.com:8440/services/vasa
```

Example 9-10 Failed response

```
url: (7) Failed connect to vvolsftw-fab1.ssd.hursley.ibm.com:8440; Connection timed out
```

Example 9-11 Successful response

```
/tmp $ curl -i -k https://vvolsftw-af7.ssd.hursley.ibm.com:8440/services/vasa
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 14 Jul 2023 16:32:49 GMT
Content-Type: text/xml; charset=utf-8
Content-Length: 130
Connection: keep-alive
Vary: Cookie
Set-Cookie: sessionid=n1axvojsrcv5rvbchamnadbnjfj6tyjz; HttpOnly; Path=/; SameSite=Lax; Secure
Strict-Transport-Security: max-age=63072000; includeSubDomains
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Pragma: no-cache
```

```
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'none'; img-src 'self'; script-src 'self'; style-src
'self';
<vasa-provider><supported-versions><version id="4" serviceLocation="/services/vasa3/vasa3"
/></supported-versions></vasa-provider>
```

> **Note:** To determine the accessibility of the VASA URL, consider testing the preceding command from the vCenter Server Appliance (vCSA) CLI or other machines in the same subnet as the storage system.

If the information shown in Example 9-11 on page 254 is not being returned, either by using the browser or curl query, verify that network connectivity is available to the storage system on TCP port 8440. If the issue persists, it might be necessary to restart the VASA Provider services on the storage system. To do this, access the cluster management CLI through an ssh connection and run the following command:

```
satask restartservice -service nginx
```

Be aware that it can take approximately 5 minutes for all VASA provider services to become functional. After issuing the **`restartservice`** command, wait for approximately 5 minutes and retry the previous diagnostics steps.

> **Note:** The VASA Provider processes and services are supported by the nginx service and so forcing a **`nginx restart`** will subsequently trigger a restart of all VASA provider services on the node. All VASA provider services run on only the configuration node of the system at any one time. In the event of a configuration node failover, for example, during firmware upgrade or maintenance procedure, the VASA provider services will be started on the newly definde configuration node.

If after 5–-10 minutes there is still no response from the VASA Provider URL, contact IBM support.

Storage system certificate misconfiguration

As mentioned in Chapter 6.2.3 Configuring a storage system certificate, it is required that the IP address or FQDN as used in the VASA Provider URL must be defined in the Subject Alternative Name field in the system certificate. Ensure that the same value appears in both the VASA Provider URL and the Subject Alternative Name field within the system certificate.

9.2.4 vVol Metadata migration before upgrading to 8.6.1.x or newer

Because of architectural changes around how the vVol metadata is being stored and to support vVol enhancements in future releases, a new method of storing vVol metadata is implemented in systems running 8.6.0.0 or later.

Any systems that enabled vVol by using the storage system management GUI on firmware versions 8.5.4 or earlier are configured with the legacy version1 metadata model.

Any system that enables vVols by using the storage system management GUI on firmware versions 8.6.0.0 or later is automatically configured with the version2 metadata model.

Firmware levels 8.6.1 and later of IBM Storage Virtualize do not support the legacy metadata model, so 8.6.0 firmware is the final stream that supports configurations with legacy metadata. Any system upgrade after the 8.6.0 LTS release, for example to 8.6.1.0 or later, requires the version2 metadata model.

How to verify the version of vVol metadata

Connect to the CLI of the storage system by using ssh and use the **`lsmetadatavdisk`** command to view details about the configured metadata vdisk.

Example 9-12 shows the output as seen on a system running 8.5.4.x or earlier, although a version number is not displayed, this presents as a version1 metadata vdisk:

Example 9-12 lsmetadatavdisk - Output as seen on a system running 8.5.4.x or earlier

```
IBM_2145:vvolsftw-sv1:superuser>lsmetadatavdisk
vdisk_id 87
vdisk_name vdisk58
status online
```

Upgrading a system that has a version1 metadatavdisk to 8.6.0.x firmware updates the CLI output.

Example 9-13 lsmetadatavdisk - After upgrading a system with a version1 metadatavdisk to 8.6.0. firmware*

```
IBM_FlashSystem:vvolsftw-af7:superuser>lsmetadatavdisk
vdisk_id vdisk_name status version
0        vdisk0     online 1
```

Code upgrade from version1 to version2 metadata

Storage systems using version1 metadata must first upgrade to an 8.6.0.x release, and then complete a metadata migration process to migrate all existing vVol metadata to a new version2 metadata format. Before upgrading to an 8.6.1.x release, the Software Update Test Utility will check for the existence of version1 metadata and, if detected, prevent the upgrade until this migration has been completed.

During the Software Upgrade Test process, the following message will appear:

```
******************** Error found ********************

The system identified that a version 1 metadata volume exists for VMware Virtual
Volumes (vVols). Please see the following web page for the actions that must be
completed before this upgrade can be performed:
https://www.ibm.com/support/pages/node/6983196.
```

Refer to the listed support page for the most recent information on the migration process.

Migration procedure

The version2 metadatavdisk will be created as a 4 TB space-efficient (thin-provisioned) volume. However, the metadata consumes a fraction of this capacity.

The actual consumption depends on the size of the vSphere configuration, such as the number of Virtual Machines and the associated number of Virtual Machine Disks being stored on vVol storage.

For planning and capacity management within the metadatavdisk, account for approximately 1 MB per vVol.

Note: During the metadata migration process, the embedded VASA provider services are temporarily inaccessible, and the Storage Provider is listed as offline in vSphere. Subsequently, any vVol datastores presented from this storage system are inaccessible and although any existing I/O requests from VMs are serviced normally, any management tasks performed on virtual machines within these datastores fails.

Procedure

Identify the parent pool in which to store the new version2 metadatavdisk.

Use the **`mkmetadatavdisk`** command specifying the `<parent pool id>` and the **`-migrate`** flag as shown in the following example:

```
mkmetadatavdisk -mdiskgrp 0 -migrate
Virtual Disk, id [51], successfully created
```

A new metadatavdisk is initially displayed in the output of **`lsmetadatavdisk`** command. See Example 9-14.

Example 9-14 lsmetadatavdisk command

```
IBM_FlashSystem:vvolsftw-af7:superuser>lsmetadatavdisk
vdisk_id vdisk_name      status version
0        vdisk0          online    1
51       metadatavolume0 online    2
```

The creation of the second metadatavdisk prompts the migration process to begin. After successful completion, the original version1 metadatavdisk is removed and an event log entry is posted. This process might take approximately 1 hr though it depends on the size of the vVol configuration and number of vVols.

```
Event ID 989055
Event ID Text Metadata migration complete
```

if the migration fails, a message will be reported in the system event log:

```
Event ID 009220
Event ID Text Metadata migration failed
```

If the metadata migration process fails, contact IBM support.

After the process finishes, the output of **`lsmetadatavdisk`** is updated to reflect the new metadata volume. See Example 9-15.

Example 9-15 lsmetadatavdisk - Output reflecting the new metadata volume

```
IBM_FlashSystem:vvolsftw-af7:superuser>lsmetadatavdisk
vdisk_id vdisk_name      status version
51       metadatavolume0 online 2
```

Revalidate the system configuration by using the Software Update Test Utility and proceed with the upgrade as instructed.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- *Implementation Guide for IBM Storage FlashSystem and IBM SAN Volume Controller: Updated for IBM Storage Virtualize Version 8.6*, SG24-8542
- *Performance and Best Practices Guide for IBM Storage FlashSystem and IBM SAN Volume Controller: Updated for IBM Storage Virtualize Version 8.6,* SG24-8543
- *IBM FlashSystem Safeguarded Copy Implementation Guide*, REDP-5654

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- IBM Storage Virtualize Family Storage Replication Adapter documentation

  https://www.ibm.com/docs/en/spectrumvirtual-sra
- VMware Reference Architectures

  https://core.vmware.com/reference-architectures
- V8.6.0.x Configuration Limits and Restrictions for IBM FlashSystem 9100 and 9200

  https://www.ibm.com/support/pages/v860x-configuration-limits-and-restrictions-ibm-flashsystem-9100-and-9200

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Redbooks

IBM Storage Virtualize and VMware: Integrations, Implementation

SG24-8549-00

ISBN DocISBN

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

SG24-8549-00

ISBN 0738425281

Printed in U.S.A.