Redbooks

ibm.com/redbooks

Implementing a VersaStack Solution by Cisco and IBM with IBM FlashSystem 5030, Cisco UCS Mini, Hyper-V, and SQL Server

David Green

Jordan Fincher

Kiran Ghag

Lee J Cockrell

Nitin D Thorve

Paulo Tomiyoshi Takeda

Sreeni Edula

Vasfi Gucer

Storage

IBM

Redbooks

International Technical Support Organization

Implementing a VersaStack Solution by Cisco and IBM with IBM FlashSystem 5030, Cisco UCS Mini, Hyper-V, and SQL Server

November 2017

SG24-8407-00

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

First Edition (November 2017)

This edition applies to IBM Storwize V5000 Gen2 running Version 7.8 and the Cisco Unified Computing System Mini Version 3.2.

Contents

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 http://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®	IBM®	POWER®
C3®	IBM FlashSystem®	Real-time Compression™
DS8000®	IBM Spectrum™	Redbooks®
Easy Tier®	IBM Spectrum Control™	Redbooks (logo) ®
FlashCopy®	IBM Spectrum Protect™	Storwize®
Global Technology Services®	IBM Spectrum Storage™	System Storage®
HyperSwap®	IBM Spectrum Virtualize™	XIV®

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.

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

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Preface

VersaStack, an IBM® and Cisco integrated infrastructure solution, combines computing, networking, and storage into a single integrated system. It combines the Cisco Unified Computing System (Cisco UCS) Integrated Infrastructure with IBM Spectrum Virtualize™, which includes IBM FlashSystem® storage offerings, for quick deployment and rapid time to value for the implementation of modern infrastructures.

This IBM Redbooks® publication covers the preferred practices for implementing a VersaStack Solution with IBM FlashSystem 5030, Cisco UCS Mini, Microsoft Hyper-V 2016, and Microsoft SQL Server.

Cisco UCS Mini is optimized for branch and remote offices, point-of-sale locations, and smaller IT environments. It is the ideal solution for customers who need fewer servers but still want the comprehensive management capabilities provided by Cisco UCS Manager.

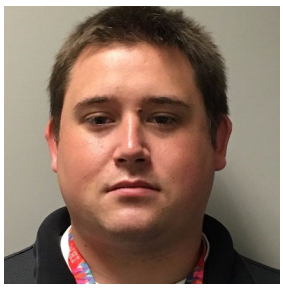
The IBM FlashSystem 5030 delivers efficient, entry-level configurations that are designed to meet the needs of small and midsize businesses. Designed to provide organizations with the ability to consolidate and share data at an affordable price, the IBM IBM FlashSystem 5030 offers advanced software capabilities such as clustering, IBM Easy Tier®, replication and snapshots that are found in more expensive systems.

This book is intended for pre-sales and post-sales technical support professionals and storage administrators who are tasked with deploying a VersaStack solution with Hyper-V 2016 and Microsoft SQL Server.

Authors

This book was produced by a team of specialists from around the world working at the Cisco Raleigh Center.

David Green is an Advisory Software Engineer working in Storage Support at IBM. He received his Bachelor of Science in Computer Information Systems from the University of North Carolina at Greensboro. David joined IBM in 1997 working for the IBM PC Company and supporting IBM PC Server products. In 2001 David moved to the development team that built the IBM line of network appliances. David's primary focus was writing the software to allow a server to provision and re-provision itself after a remote administrator deployed a new image to that server. David is a patent holder for several patents related to provisioning servers across an IP network. Since 2006 David has provided expert-level support of IBM Storage Networking products.



Jordan Fincher is a Product Field Engineer working in Storage Support at IBM. He received his Bachelor of Science in Information Security from Western Governor University. Jordan first started his IBM career in 2012 as a Systems Engineer for the IBM Business Partner e-TechServices doing pre-sales consulting and implementation work for many IBM accounts in Florida. In 2015 Jordan started working in his current role as a Product Field Engineer for IBM Spectrum Virtualize storage products.

Kiran Ghag is an IBM Storage Solution Architect, working with various clients at IBM India. He received his bachelors degree in Computer Engineering from Mumbai University. His current interests include software defined storage using IBM Spectrum™ family. Kiran joined IBM in 2013 as consultant with 10 years of experience in storage systems, currently helping IBM customers with storage solutions and storage infrastructure optimization.

Lee J Cockrell is an IBM Technical Sales Specialist, covering several United States Federal Civilian agencies and Native American Tribal governments for IBM Federal in the Washington D.C. area. He received his B.S. in computer science from the University of Virginia, Charlottesville, VA. His current interests are in storage, cloud, and computer security. Lee joined IBM in 2010 selling storage, primarily IBM Spectrum Virtualize, SAN Volume Controller, IBM FlashSystem, IBM XIV®, and IBM DS8000®. He has worked in the storage industry since 2001, installing and configuring countless storage arrays and co-authoring expert level performance certification tests. Previously, he was a UNIX and firewall administrator in both the public and private sectors.

Nitin D Thorve is an IBM Information Technology Infrastructure Architect, working with Solution Design and Architecture Services, team at IBM India in Pune area. He received his Bachelors degree in computer engineering from MIT Academy of Engineering, Pune. His current interests are in storage, cloud, analytics, AI, and cognitive computing technologies. Nitin joined IBM in 2016 as a Storage subject matter expert with skills in the IBM Spectrum Storage™ family, IBM Flash Storage family, IBM FlashSystem family, IBM Disk Systems DS8000 series, IBM replication technologies, and IBM POWER® hardware, including AIX®, VIOS, and Power virtualization, EMC Storage products, Hitachi Storage products, Netapp NAS products, Cisco, and Brocade SAN Hardware in IBM Pune India. In 2017, Nitin moved to the IBM India Solution Design and Architecture Services team as a Technical Solutions Manager, helping the IBM Global Technology Services® Solutioning team develop new logo solutions for the EMEA region.

Paulo Tomiyoshi Takeda is a SAN and Storage Disk specialist at IBM Brazil. He has over ten years of experience in the IT arena and is an IBM Certified IT Specialist Expert. He holds a bachelors degree in Information Systems from Universidade da Fundação Educacional de Barretos (UNIFEB) and is IBM Certified for Cloud, DS8000, and IBM FlashSystem 7200. His areas of expertise include planning, configuring, and troubleshooting DS8000, IBM Spectrum Virtualize and IBM FlashSystem systems. He works as Level 3 support for IBM global accounts and is involved in storage-related projects such as capacity growth planning, SAN consolidation, storage microcode upgrades, and copy services in the Open Systems environment.

Sreeni Edula is a Technical Marketing Engineer in the Cisco UCS Data Center Solutions Group. He has over 17 years of experience in Information Systems with expertise across Cisco Data Center technology portfolio, including DC architecture design, virtualization, compute, network, storage, and cloud computing. Prior to that he worked as a Solutions Architect at EMC, working in designing, implementing and managing Storage and Virtualization solutions for the customers.

Vasfi Gucer is an IBM Technical Content Services Project Leader with the Digital Services Group. He has more than 20 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 cloud computing, including cloud storage technologies for the last 6 years. Vasfi is also an IBM Certified Senior IT Specialist, Project Management Professional (PMP), IT Infrastructure Library (ITIL) V2 Manager, and ITIL V3 Expert.

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

Jon Tate, Debbie Willmschen, Erica Wazewski
Digital Services Group, Technical Content Services

Warren Hawkins
IBM UK

Karl Hohenauer
IBM Austria

Bernd Albrecht, Hartmut Lonzer
IBM Germany

Chenghui Lv
IBM China

Chris O'Brien, Jawwad Memon
Cisco, Raleigh Center

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 ITSO 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, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:

  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- Stay current on recent Redbooks publications with RSS Feeds:

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

1

Introduction

This chapter introduces VersaStack and the specific VersaStack design used in this book. It includes the following topics:

1.1 Overview

VersaStack is an innovative, validated design combining IBM FlashSystem and the Cisco Unified Computing System (UCS). It allows customers and business partners to create solutions that transform their businesses and reduce risk. VersaStack is an easy, efficient, versatile converged infrastructure that can be configured flexibly to meet the size and performance needs of nearly any business.

Working together, IBM and Cisco have documented VersaStack with a series of Cisco Validated Design (CVD) and IBM Redbooks publications. These validated designs are documented thoroughly to provide faster delivery of applications, greater reliFlashSystem 5030ability, and confidence for customers and business partners.

The VersaStack solution by IBM and Cisco can help to accelerate data center infrastructure deployment, to efficiently manage information and resources, and to adapt to business change. VersaStack is supported by a broad range of services from IBM Business Partners and IBM Global Services.

1.2 The VersaStack solution described in this book

This book covers a validated design with the Cisco UCS Mini and IBM FlashSystem 5030.The Cisco UCS Mini is a medium performance version of the UCS. The IBM FlashSystem 5030 is a mid-range storage array. The hypervisor installed is Hyper-V, and the software installed includes Microsoft SQL Server.

Note on the Storwize rebranding: On 02/11/2020 IBM rebranded IBM Storwize storage systems as IBM FlashSystem, so for example IBM Storwize V5030 is now called IBM FlashSystem 5030. This book been updated to use the new terminology., but you might still see the “Storwize” name in some of the screenshots.

In this design, the Cisco UCS Mini and IBM FlashSystem 5030 together create a small- to mid-sized converged infrastructure that is ideal for a remote office or small data center and that is running applications with medium capacity and performance requirements. The IBM FlashSystem 5030 that is used for this book consists of a single-control enclosure of 2.5-inch form factor drives, including three 400 GB solid-state drives (SSDs), four 900 GB 10 k RPM hard disk drives (HDDs), and 10 2 TB 7.2 k RPM HDDs.

The following design elements distinguish this version of VersaStack from previous models:

- Validation of the Cisco UCS Mini with Cisco Nexus 9000 switches and IBM Storwize V5000 Gen2 storage array with Hyper-V 2016 and Microsoft SQL 2016
- Support for Cisco UCS M5 servers
- Support for the Cisco UCS 3.2(1d) release and Cisco UCS Mini with secondary chassis support
- Support for IBM Spectrum Virtualize V7.8.1.3

1.3 VersaStack synopsis

Other valid VersaStack configurations can include a wide range of Cisco UCS, and the IBM Storwize V5010, V5020, V5030F, V7000, V7000F, IBM FlashSystem 900 and A9000 storage

arrays, or the IBM SAN Volume Controller. The IBM Storwize storage arrays provide features, such as Data Virtualization, IBM Real-time Compression™, and Easy Tier, that complement and enhance virtual environments.

The VersaStack solution includes networking components that consist of Cisco Nexus and MDS switches. These components allow IP, storage, and management networks to be combined on a single converged physical network. The converged infrastructure of compute (Cisco UCS), storage (IBM Storwize), and network is managed by Cisco UCS Director.

1.4 Common VersaStack use cases

As a versatile, converged infrastructure, VersaStack is ideal for small- to mid-sized data centers, where the simple and flexible configuration allows for easy management of virtual and physical assets.

1.4.1 Remote and branch office

VersaStack can be sized to fulfill the entire compute, storage, and networking needs of remote offices, often in a single or partial rack. This configuration allows for a single management interface of the entire office's IT assets and a verified design of an integrated, supported, converged infrastructure, as shown in Figure 1-1.

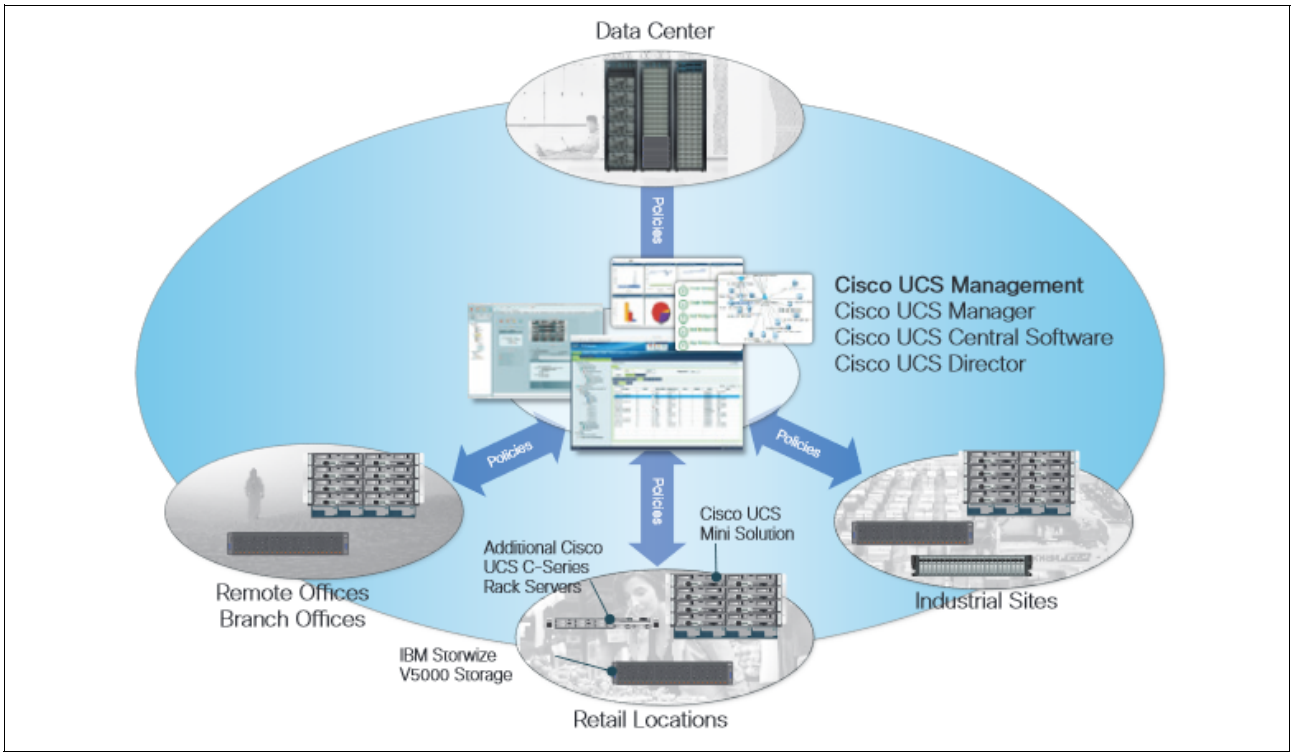


Figure 1-1 VersaStack as a remote and branch office solution

For more information about this use case, see *VersaStack Solution for Remote- and Branch-Office Deployments*.

1.4.2 Data center

VersaStack is ideal for customers who want to simplify the physical and virtual management of their data centers. The converged network infrastructure and single management pane can ease the complexity that many businesses' operating data centers endure.

Customers can choose from a wide array of network, servers, and storage options to build an ideal data center design.

Figure 1-2 shows the components of VersaStack as a data center solution.

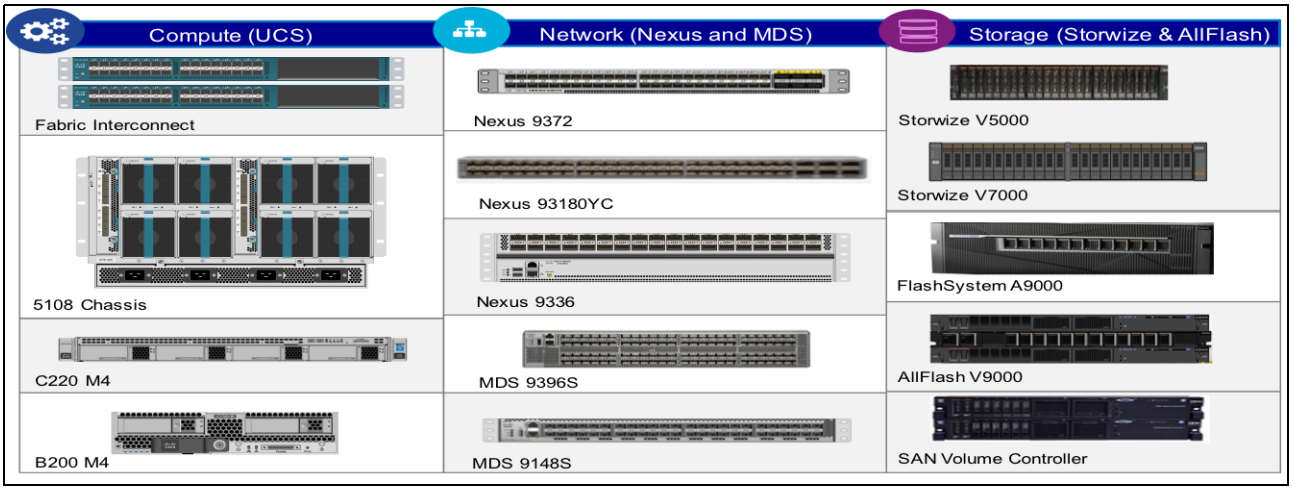


Figure 1-2 VersaStack as a data center solution

For more information about this use case, see *VersaStack Solutions*.

1.4.3 Private cloud

Combined with a hypervisor, such as Hyper-V or VMware, VersaStack becomes a converged private cloud that is capable of supporting a wide variety of operating systems, applications (such as SAP HANA, SQL Server, or Oracle), and small or large performance loads.

Figure 1-3 shows an example of a VersaStack design that is ready for a hypervisor for the private cloud.

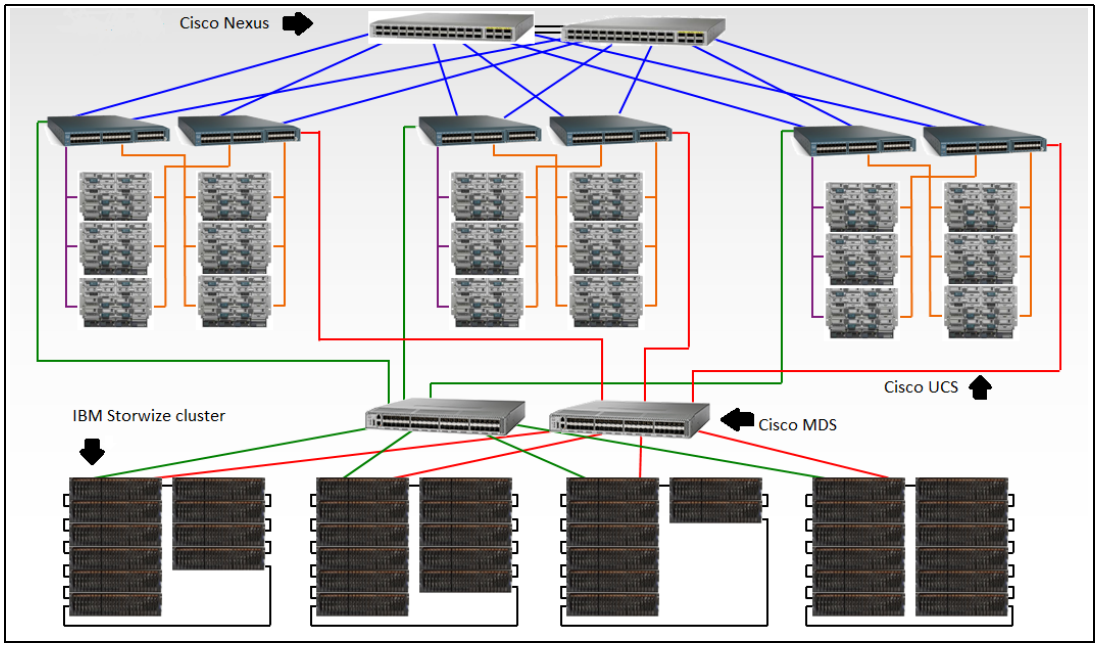


Figure 1-3 VersaStack design ready for a hypervisor for the private cloud

For more information about this use case, see *VersaStack Solution for Private Cloud*.

1.4.4 Hybrid cloud

Implementations with Cisco ONE Enterprise Cloud Suite and IBM Spectrum Copy Data Management create VersaStack for hybrid cloud, which enables orchestration, deployment, management, and migration of applications across the data center, the public cloud, and private cloud environments.

Figure 1-4 shows an overview of the VersaStack Hybrid Cloud architecture.

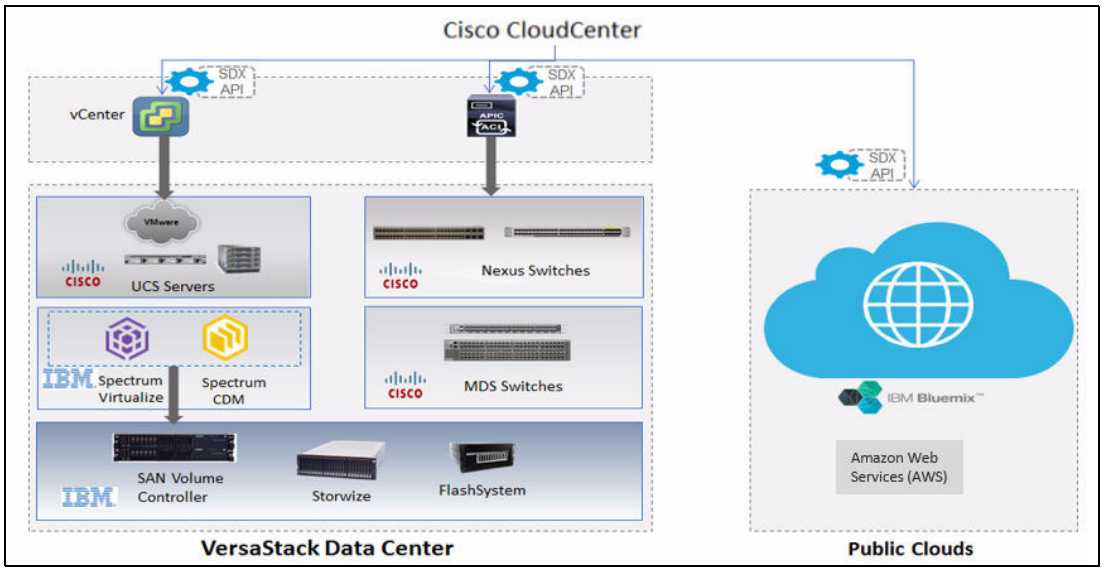


Figure 1-4 VersaStack hybrid cloud architecture

For more information about this use case, see *Top 5 Reasons to Deploy Hybrid Cloud on Versa Stack Solutions*.

1.5 Optional and complementary products

A wide array of optional and complementary products, while beyond the scope of this book, are available for use with VersaStack.

1.5.1 Cisco application centric infrastructure

Cisco ACI is a new data center architecture designed to address the requirements of today's traditional networks and to meet emerging demands that new computing trends and business factors are placing on the network. Software-defined networking (SDN) has garnered much attention in the networking industry over the past few years due to its promise of a more agile and programmable network infrastructure. Cisco ACI helps to address the challenges of agility and network programmability that software-based overlay networks are trying to address. It also presents solutions to the new challenges that SDN technologies are currently unable to address.

Cisco ACI uses a network fabric that employs industry-proven protocols coupled with innovative technologies to create a flexible, scalable, and highly available architecture of low-latency, high-bandwidth links. This fabric delivers application instantiations using profiles that house the requisite characteristics to enable end-to-end connectivity. The ACI fabric is designed to support the industry trends of management automation, programmatic policies, and dynamic workload provisioning. The ACI fabric accomplishes this support with a combination of hardware, policy-based control systems and closely-coupled software to provide advantages not possible in other architectures.

The ACI switching architecture is presented in a leaf-and-spine topology where every leaf connects to every spine using 40G Ethernet interface or interfaces. At a high level. the Cisco ACI fabric consists of the following major components:

- The Cisco Application Policy Infrastructure Controller (APIC)
- Spine switches
- Leaf switches

Cisco Nexus 9000-based VersaStack design with Cisco ACI consists of Cisco Nexus 9336 PQ-based spine and Cisco 9372 PX-based leaf switching architecture that is controlled using a cluster of three Cisco APICs.

Figure 1-5 depicts the Cisco ACI Fabric design.

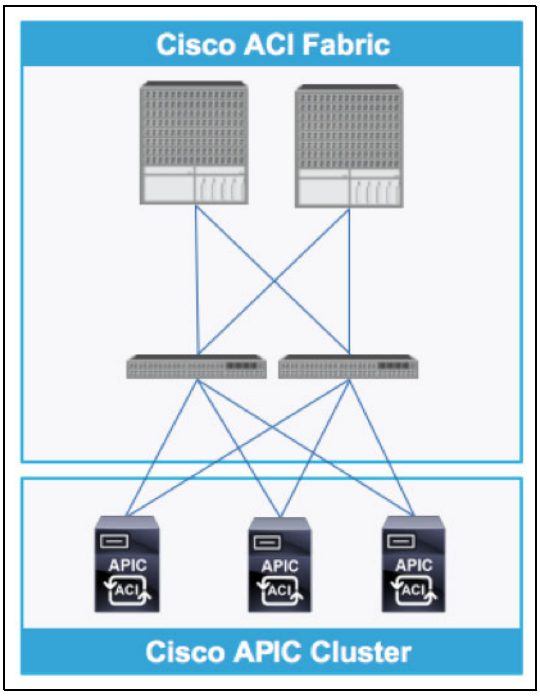


Figure 1-5 Cisco ACI Fabric high-level design

You can find more information about the Cisco Application Centric Infrastructure online.

1.5.2 IBM Spectrum Control Storage Insights

IBM Spectrum Control™ Storage Insights allows for better visibility into the storage infrastructure. It provides improved capacity planning, increased storage utilization, simpler reporting, and enhanced performance monitoring, all leading to reduced costs.

You can find more information about this IBM solution online in the IBM Marketplace.

1.5.3 IBM Spectrum Protect and IBM Spectrum Protect Plus

IBM Spectrum Protect™ is a server and client backup application. IBM Spectrum Protect can simplify data protection where data is hosted in physical, virtual, software-defined, or cloud environments. IBM Spectrum Protect integrates with IBM Spectrum Protect Plus for virtual machine protection with searchable catalog and role-based administration.

IBM Spectrum Protect Plus focuses on protection and recovery of virtual machines and applications and also focuses on disaster recovery and data reuse cases, such as testing and development.

You can find more information about this IBM solution online in the IBM Marketplace.

1.5.4 IBM Spectrum Copy Data Management

IBM Spectrum Copy Data Management manages copies, replicas, and snapshots of enterprise-wide copies of your data. It can help to streamline the creation, management, and use of these copies.

You can find more information in IBM Knowledge Center or on the Cisco website.

1.6 Assumptions made in this book

This book assumes that the IBM Storwize and Cisco UCS products, any Fibre Channel or Ethernet switches, and any other necessary infrastructure in your data center are configured prior to implementing the Hyper-V and Microsoft SQL solution that is described in this book.

The VersaStack configuration used in this book includes the IBM FlashSystem 5030 and a Cisco UCS Mini that uses the embedded Fabric Interconnects (FI) on the UCS Mini chassis for a direct connection to the V5030. The FIs can be in either pass through (NPV) or switch mode. The V5030 is direct-connected to the UCS Mini chassis. As such, the FIs are configured for full-switch mode so as to provide fabric services, such as zoning.

Any UCS configuration examples in this book use the features of the UCS to automatically configure the necessary zoning on the FIs. If your solution uses the FIs in pass through mode to an external Fibre Channel switch, you need to implement the zoning such that the host world wide port names (WWPNs) for the hosts that are created on the UCS are properly zoned to the IBM Storwize storage product. Because there are many different SAN switch vendors and switches, a guide to implementing the required zoning is beyond the scope of this book.

You can find an implementation overview for the Cisco UCS Mini direct-connected to the IBM FlashSystem 5030 on the Cisco website.

You also can find information about how to complete the initial setup for the Cisco UCS Mini online. This information includes detailed steps about creating the system policies and templates that are necessary to implement the solution described in this book. If you are using a different IBM Storwize or using the full Cisco UCS Mini chassis, see the setup guides for those products.

You can also find the V5030 configuration guide online (*Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162). You need to complete the steps included in the configuration guide chapters that detail the initial configuration of the V5000 and the chapter that describes how to create storage pools. This book covers how to create the hosts and volumes.

VersaStack solutions can also include other products from the IBM Storwize family, such as:

- IBM Storwize SAN Volume Controller
- IBM Storwize V7000
- IBM Storwize A9000

If you are using any of these products in your solution, see their respective implementation guides for initial setup of the storage cluster and creating the volumes prior to continuing with the information presented in this book.

1.7 For more information

See the following links for more information:

- Cisco and IBM home pages for VersaStack:
  - Cisco VersaStack Solution home page

  - IBM VersaStack home page
- VersaStack Solutions brochure
- Cisco VersaStack Design Zone and Guides
- Video: VersaStack Solution by Cisco and IBM
- Video: High Level Business Value of VersaStack from IBM and Cisco
- Video: IBM and Cisco VersaStack—Introduction
- Video: Modernize Your Data Center with VersaStack All-Flash Converged Infrastructure and VMWare

2

Architecture of the solution

This chapter describes the physical architecture of the VersaStack solution that is discussed in this book. It includes the following sections:

2.1 VersaStack architecture

VersaStack with the Cisco Unified Computing System (UCS) Mini and the IBM Storwize V5000 Gen2 architecture aligns with the converged infrastructure configurations and preferred practices as identified in previous VersaStack releases. The system includes hardware and software compatibility support between all components and aligns to the configuration preferred practices for each of these components. The core hardware components and software releases are listed and supported on the Cisco compatibility list Cisco Technical References list and the IBM System Storage® Interoperation Center (SSIC).

The VersaStack solution supports high availability at the network, compute, and storage layers such that no single point of failure exists in the design. The system uses 10 Gbps Ethernet jumbo-frame based connectivity combined with port aggregation technologies, such as Virtual PortChannel (vPC), for non-blocking LAN traffic forwarding. A dual SAN 8 Gbps environment that are enabled by the Cisco 6324 Fabric Interconnects provides redundant storage access from compute devices to the storage controllers.

2.1.1 Physical topology

VersaStack direct-attached SAN storage design provides a high redundancy, high-performance solution for the deployment of virtualized data center architecture. This solution design uses direct-attached Fibre Channel (FC) storage connectivity for compute, which enables a simple, flexible, and cost-effective solution.

This VersaStack design uses the Cisco UCS Mini platform with Cisco B200 M5 half-width blades and Cisco UCS C220 M5 rack mount servers connected and managed through Cisco UCS 6324 Fabric Interconnects and the integrated UCS manager. These high-performance servers are configured as stateless compute nodes where the Hyper-V 2016 hypervisor is loaded using Fibre Channel SAN boot.

The boot disks to store the Hyper-V hypervisor image and configuration, along with the block data stores to host application virtual machines (VMs), are provisioned on the IBM FlashSystem 5030 storage. The Cisco UCS and Cisco Nexus 9000 platforms support active port channeling using 802.3ad standard Link Aggregation Control Protocol (LACP). *Port channeling* is a link aggregation technique that offers link fault tolerance and traffic distribution (load balancing) for improved aggregate bandwidth across member ports.

Each Cisco UCS Fabric Interconnect is connected to both the Cisco Nexus 9372 switches using vPC-enabled 10GbE uplinks for a total aggregate bandwidth of 20 GBps. The Cisco UCS Mini can be extended by connecting a second Cisco UCS Chassis with eight blades and with two Cisco UCS rack-mount servers using the 40GbE Enhanced Quad SFP (QSFP+) ports available on the Cisco UCS 6324 Fabric Interconnects.

Figure 2-1 depicts the detailed hardware configuration and cabling for the VersaStack solution used in this book.

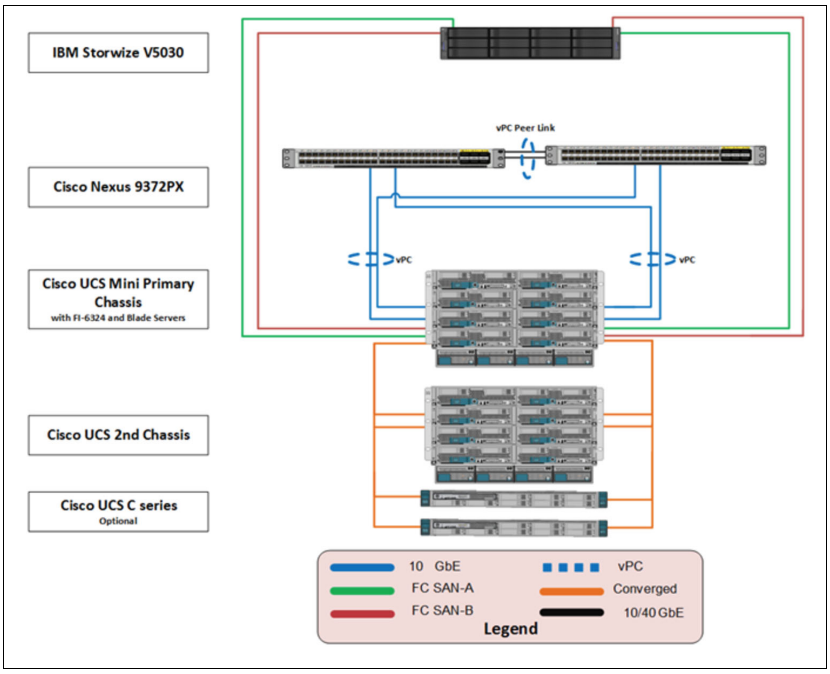


Figure 2-1 Hardware configuration and cabling for the VersaStack solution used in this book

An IBM FlashSystem 5030 is attached directly to the Fabric Interconnects that are embedded in the UCS Mini chassis. The Fabric Interconnects can be configured for full FC switch mode or for N-Port virtualization mode. If the Fabric Interconnects are in N-Port virtualization (NPV) mode, they require connection to an external FC switch to provide zoning and other fabric services. For this book, the Fabric Interconnects are configured in *switch* mode.

The UCS Mini is attached using the Fabric Interconnects to a pair of Cisco Nexus switches. These switches provide Ethernet connectivity for both the blades and any virtual machines in the chassis and provide management of the UCS Mini, the IBM FlashSystem 5030, and any VMs.

Lastly, the UCS Mini primary chassis is connected via the Fabric Interconnects to a second UCS Mini chassis and an external UCS C series blade. Both of these components are optional and are not required for the solution that is detailed in this book.

The reference architecture discussed in this book uses the following components:

- Two Cisco Nexus 9372PX switches
- Two Cisco UCS 6324 Fabric Interconnects
- Support for two Cisco UCS C series servers without any additional networking components
- Support for up to 16 Cisco UCS B series servers with an additional blade server chassis
- An IBM FlashSystem 5030 server
- Support for 16 Gb FC, 12 Gb SAS, 10 Gb iSCSI/FCoE, and 1 Gb iSCSI for additional I/O connectivity
- Support for 760 drives per system and 1,520 drives with a two-way clustered configuration

This book guides you through the low-level steps for deploying the base architecture. These procedures cover everything from physical cabling to network, compute, and storage device configurations.

2.2 Software versions

For current supported versions, see the following IBM and Cisco support matrix links:

- IBM System Storage Interoperability Center
- IBM Spectrum Control Interoperability Matrix
- IBM Spectrum Protect Supported Operating Systems
- Hardware and Software Requirements: IBM FlashCopy® Manager
- Cisco UCS Hardware and Software Compatibility

Table 2-1 lists the software revisions used in this book.

Table 2-1 Software versions

Layer	Device	Version or Release	Details
Compute	Cisco UCS fabric interconnect	3.2(1d)	Embedded management
	Cisco UCS C 220 M4/M5	3.2(1d)	Software bundle release
	Cisco UCS C 220 M4/M5	3.2(1d)	Software bundle release
	Cisco eNIC	4.0.0.3	Ethernet driver for Cisco VIC
	Cisco fNIC	3.0.0.8	FCoE driver for Cisco VIC
Network	Cisco Nexus 9372PX	7.0(3)I4(7)	Operating system version
Storage	IBM FlashSystem 5030	7.8.1.3	Software version
Software	Windows Server 2016 Data Center	Hyper-V 2016	Operating system version
Software	SCVMM	2016	Systems Center Virtual Machine Manager
Software	Microsoft SQL	2016	Microsoft SQL database

2.3 Configuration guidelines

This book provides information about how to configure a fully-redundant, highly-available infrastructure. Therefore, with each step, reference is made to which component is being configured, either 01 or 02 or A and B. For example, the Cisco UCS Fabric Interconnects are identified as *FI-A* or *FI-B*. This information in this book is intended to enable you to fully configure the environment. During the process, various steps require that you insert customer-specific naming conventions, IP addresses, and virtual local area network (VLAN) schemes and that you record appropriate MAC addresses.

Because the design of this deployment is a point of delivery (POD), the architecture in this document uses private networks and only the in-band management VLAN traffic routes through the Cisco 9k switches. Other management traffic is routed through a separate out-of-band management switch. The architecture can vary based on the deployment objectives.

Terminology note: In this context, a POD (or *point of delivery*) is a module of network, compute, storage, and application components that work together to deliver networking services. The POD is a repeatable design pattern, and its components maximize the modularity, scalability, and manageability of data centers.

2.3.1 List of tables

The tables in this section describe the systems, VLANs, virtual storage area networks (VSANs), and virtual machines (VMs) that are necessary for deployment. The networking architecture can be unique to each environment.

Table 2-2 lists the VLANs that are used to validate the solution in this book.

Table 2-2 VLANs used in this solution

VLAN name	VLAN purpose	ID used in validating
Native	VLAN to which untagged frames are assigned	N/A
Cluster	VLAN for cluster communication	3172
LVMN	VLAN designated for Live Migration	3173
VM traffic	VLAN for VM application traffic	3174
Mgmt in band	VLAN for in-band management interfaces	11
VSAN A	VSAN for Fabric A traffic. ID matches FCoE-A VLAN	101
VSAN B	VSAN for Fabric A traffic. ID matches FCoE-B VLAN	102

Table 2-3 lists the host names for the Windows hosts that are used in this solution. The Active Directory Server was installed and configured for this solution. If you have an existing server, you can use your own.

Table 2-3 Host names used in this solution

VM description	Host name
Active Directory	WIN2016DC01
Hyper-V Host 1	WIN-HYPERV-N1
Hyper-V Host 2	WIN-HYPERV-N2
Virtual Cluster Node 1	WIN-MSSQL-N1
Virtual Cluster Node 2	WIN-MSSQL-N2

Table 2-4 provides a place to record the values of each of the listed variables that you use when implementing the solution in this book.

Table 2-4 Recorded variables

Variable	Description	Implementation value
<<var_node01_mgmt_ip>>	Out-of-band management IP for V5000 node 01	
<<var_node01_mgmt_mask>>	Out-of-band management network netmask	
<<var_node01_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_node02_mgmt_ip>>	Out-of-band management IP for V5000 node 02	
<<var_node02_mgmt_mask>>	Out-of-band management network netmask	
<<var_node02_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_cluster_mgmt_ip>>	Out-of-band management IP for V5000 cluster	
<<var_cluster_mgmt_mask>>	Out-of-band management network netmask	
<<var_cluster_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_password>>	Global default administrative password	
<<var_dns_domain_name>>	DNS domain name	
<<var_nameserver_ip>>	DNS server IP or IPs	
<<var_timezone>>	VersaStack time zone (for example, *America/New_York*)	
<<var_global_ntp_server_ip>>	NTP server IP address	
<<var_email_contact>>	Administrator email address	
<<var_admin_phone>>	Local contact number for support	
<<var_mailhost_ip>>	Mail server host IP	
<<var_country_code>>	Two-letter country code	
<<var_state>>	State or province name	
<<var_city>>	City name	
<<var_org>>	Organization or company name	
<<var_unit>>	Organizational unit name	
<<var_street_address>>	Street address for support information	
<<var_contact_name>>	Name of contact for support	
<<var_admin>>	Secondary Admin account for storage login	
<<var_nexus_A_hostname>>	Cisco Nexus A host name	
<<var_nexus_A_mgmt0_ip>>	Out-of-band Cisco Nexus A management IP address	
<<var_nexus_A_mgmt0_netmask>>	Out-of-band management network netmask	

Variable	Description	Implementation value
<<var_nexus_A_mgmt0_gw>>	Out-of-band management network default gateway	
<<var_nexus_B_hostname>>	Cisco Nexus B host name	
<<var_nexus_B_mgmt0_ip>>	Out-of-band Cisco Nexus B management IP address	
<<var_nexus_B_mgmt0_netmask>>	Out-of-band management network netmask	
<<var_nexus_B_mgmt0_gw>>	Out-of-band management network default gateway	
<<var_ib-mgmt_vlan_id>>	In-band management network VLAN ID	
<<var_native_vlan_id>>	Native VLAN ID	
<<var_lvmn_vlan_id>>	Windows Live Migration VLAN ID	
<<var_cluster_vlan_id>>	Windows Cluster VLAN ID	
<<var_vm-traffic_vlan_id>>	VM traffic VLAN ID	
<<var_nexus_vpc_domain_id>>	Unique Cisco Nexus switch VPC domain ID	
<<var_ucs_clustername>>	Cisco UCS Manager cluster host name	
<<var_ucsa_mgmt_ip>>	Cisco UCS Fabric Interconnect A out-of-band management IP address	
<<var_ucs_mgmt_mask>>	Out-of-band management network netmask	
<<var_ucs_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_ucs_cluster_ip>>	Cisco UCS Manager cluster IP address	
<<var_ucsb_mgmt_ip>>	Cisco UCS Fabric Interconnect B out-of-band management IP address	
<<var_cimc_mask>>	Out-of-band management network netmask	
<<var_cimc_gateway>>	Out-of-band management network default gateway	
<<var_ftp_server>>	IP address for FTP server	
<<var_UTC_offset>>	UTC time offset for your area	
<<var_vsan_a_id>>	VSAN ID for FC FI-A (101 is used)	
<<var_vsan_b_id>>	VSAN ID for FC FI-B (102 is used)	
<<var_fabric_a_fcoe_vlan_id>>	Fabric ID for FCoE A (101 is used)	
<<var_fabric_b_fcoe_vlan_id>>	Fabric ID for FCoE B (102 is used)	
<<var_In-band_mgmtblock_net>>	Block of IP addresses for KVM access for UCS	
<<var_hyperv_host_infra_01_ip>>	Windows Hyper-V host 01 in-band Mgmt IP	
<<var_lvmn_ip_host-01>>	LVMN VLAN IP address for Hyper-V host 01	
<<var_lvmn_mask_ host-01>>	LVMN VLAN netmask for Hyper-V host 01	
<<var_hyperv_hos t_infra_02_ip>>>	VMware Hyper-V host 02 in-band Mgmt IP	

Variable	Description	Implementation value
<<var_lvmn_vlan_id_ip_host-02>>	LVMN VLAN IP address for Hyper-V host 02	
<<var_csv_vlan_id_mask_host-02>>	LVMN VLAN netmask for Hyper-V host 02	
<<var_cluster_ip_ host-01>>	Cluster VLAN IP address for Hyper-V host 01	
<<var_cluster_mask_host-01>>	Cluster VLAN netmask for Hyper-V host 01	
<<var_cluster_ip_host-02>>	CSV VLAN IP address for Hyper-V host 02	
<<var_cluster_mask_host-02>>	CSV VLAN netmask for Hyper-V host 02	

Table 2-5 provides a place to record values for additional variables.

Table 2-5 Record values for additional variables

Source	Switch/Port	Variable	WWPN
FC_NodeA-fabricA	Switch A FC3	<<var_wwpn_FC_NodeA-fabricA>>	
FC_NodeA-fabricB	Switch B FC3	<<var_wwpn_FC_NodeA-fabricB>>	
FC_NodeB-fabricA	Switch A FC4	<<var_wwpn_FC_NodeB-fabricA>>	
FC_NodeB-fabricB	Switch B FC4	<<var_wwpn_FC_NodeB-fabricB>>	
HyperV-Host-infra-01-A	Switch A	<<var_wwpn_VM-Host-Infra-01-A>>	
HyperV-Host-infra-01-B	Switch B	<<var_wwpn_VM-Host-Infra-01-B>>	
HyperV-Host-infra-02-A	Switch A	<<var_wwpn_VM-Host-Infra-02-A>>	
HyperV-Host-infra-02-B	Switch B	<<var_wwpn_VM-Host-Infra-02-B>>	

2.3.2 VersaStack build process

Figure 2-2 depicts the process used to build the solution detailed in this book. The process starts with physical infrastructure and cabling, then moves to configuring the Nexus switches and the V5030 storage, and then configuring the UCS. The final step is installing Windows and creating the infrastructure (Hyper-V, VMs, and Microsoft SQL Server cluster) used in this solution.

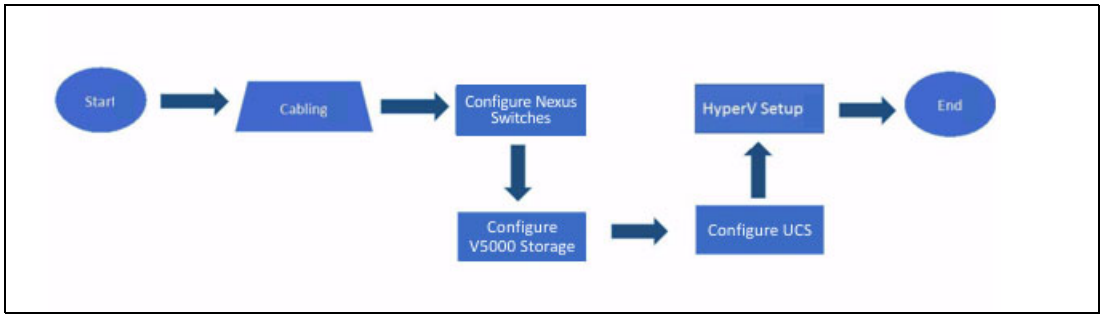


Figure 2-2 The process used to build the solution detailed in this book

2.4 VersaStack cabling

The information in this section is provided as a reference for cabling the equipment in a VersaStack environment. To simplify cabling requirements, the tables include both local and remote device and port locations.

The tables in this section contain details for the prescribed and supported configuration of the IBM FlashSystem 5030 running V7.8.1.3.

This book assumes that out-of-band management ports are plugged in to an existing management infrastructure at the deployment site. These interfaces are used in various configuration steps.

Important: Be sure to follow the cabling directions in this section. Failure to do so will result in changes to the deployment procedures that follow, because specific port locations are mentioned.

You can order IBM FlashSystem 5030 systems in a different configuration from that presented in the tables in this section. Before starting, be sure that the configuration matches the descriptions in the tables and diagrams in this section.

Figure 2-3 on page 20 illustrates the cabling diagrams for VersaStack configurations using the Cisco Nexus 9000 and IBM FlashSystem 5030. For SAS cabling information, connect the IBM FlashSystem 5030 control enclosure and expansion enclosure according to the cabling guide listed in IBM Knowledge Center.

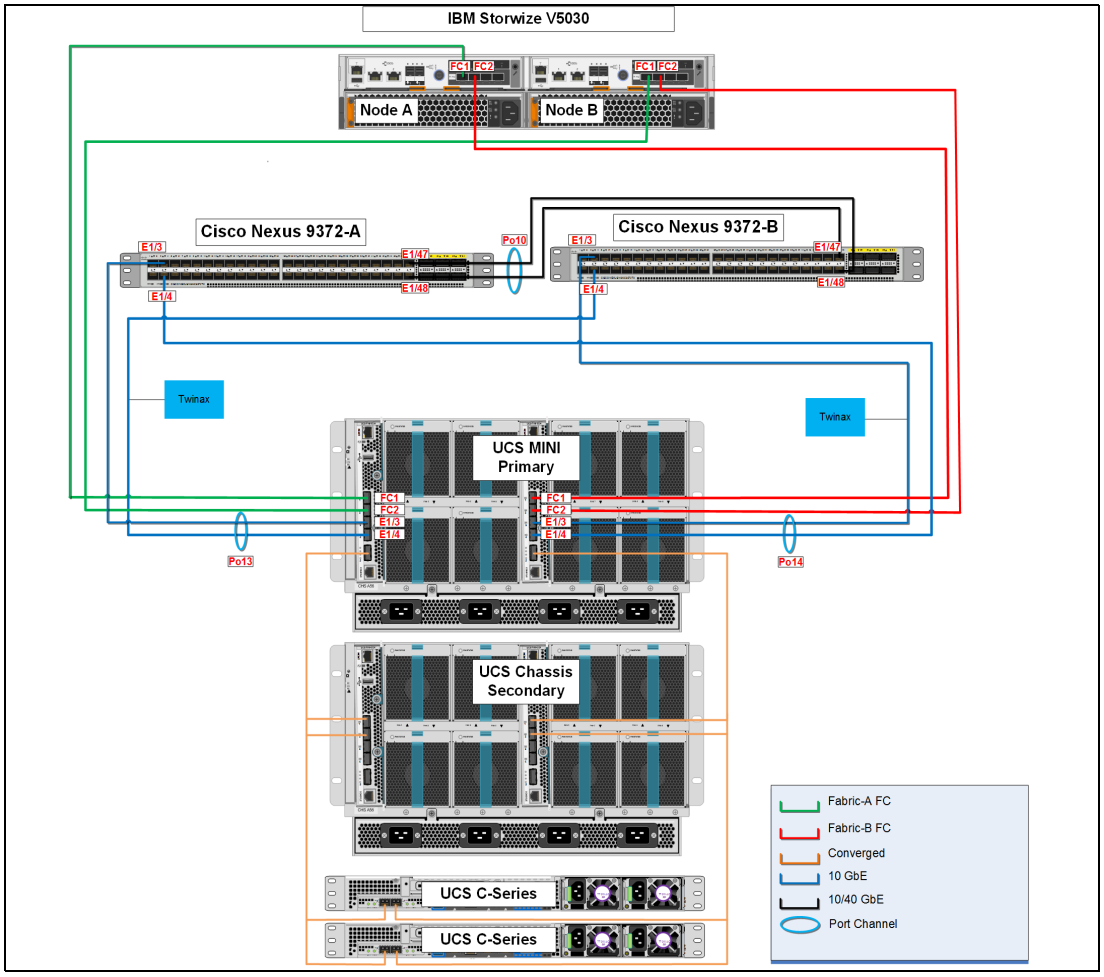


Figure 2-3 VersaStack cabling diagram

Table 2-6 lists the cabling for the Cisco Nexus 9000-A that is used in the solution described in this book.

Table 2-6 Cabling for the Cisco Nexus 9000-A used in this solution

Local port	Connection	Remote device	Remote port
Eth1/3	10GbE	Cisco UCS FI-A	Eth1/3
Eth1/4	10GbE	Cisco UCS FI-B	Eth1/4
Eth1/47[a]	40GbE	Cisco Nexus 9000-B	Eth1/47
Eth1/48[a]	40GbE	Cisco Nexus 9000-B	Eth1/48
Eth1/36	10GbE	Management switch	Any

a. For Quad Small Form Factor (QSFP) port

Table 2-7 lists the cabling for Node A of the IBM FlashSystem 5030 storage system that is used in the solution that is described in this book.

Table 2-7 Cabling for Node A of the IBM FlashSystem 5030 storage system used in this solution

Local port	Connection	Remote device	Remote port
E1	GbE	Management switch	Any
E2 (optional)	GbE	Management switch	Any
FC1	8gbps	Cisco UCS FI-A	FC1/1
FC2	8gbps	Cisco UCS FI-B	FC1/1

Table 2-8 lists the cabling for Node B of the IBM FlashSystem 5030 storage system that is used in the solution that is described in this book.

Table 2-8 Cabling for Node B of the IBM FlashSystem 5030 storage system used in this solution

Local port	Connection	Remote device	Remote port
E1	GbE	Management switch	Any
E2 (optional)	GbE	Management switch	Any
FC1	8gbps	Cisco UCS FI-A	FC1/2
FC2	8gbps	Cisco UCS FI-B	FC1/2

Table 2-9 lists the connections for the Cisco UCS FI-A that is used in the solution that is described in this book.

Table 2-9 Connections for the Cisco UCS FI-A used in this solution

Local port	Connection	Remote device	Remote port
Mgmt0	GbE	Management switch	Any
FC1/1	8 Gbps	V5000 Node-A	FC1/1
FC1/2	8 Gbps	V5000 Node-B	FC1/1
Eth1/3	10GbE	Cisco Nexus 9000-A	Eth 1/3
Eth1/4	10GbE	Cisco Nexus 9000-B	Eth 1/4
Scalability 1	40GbE	2nd UCS Chassis	IOM 2208XP

Table 2-10 lists the connections for the Cisco UCS FI-B that is used in the solution that is described in this book.

Table 2-10 Connections for the Cisco UCS FI-B used in this solution

Local port	Connection	Remote device	Remote port
Mgmt0	GbE	Management switch	Any
FC1/1	8 Gbps[a]	V5000 Node-A	FC1/2
FC1/2	8 Gbps[a]	V5000 Node-B	FC1/2
Eth1/3	10GbE	Cisco Nexus 9000-B	Eth 1/3
Eth1/4	10GbE	Cisco Nexus 9000-A	Eth 1/4
Scalability 1	40GbE	2nd UCS Chassis	IOM 2208XP

a. 16 Gbps is also possible.

2.5 Microsoft SQL Server on the VersaStack architecture

Figure 2-4 illustrates the design of the Microsoft SQL Server on VersaStack architecture that is used in this book. This design is extremely flexible. All of the required components fit in one data center rack or can accommodate a customer's data center design requirements. Port density enables the networking components to accommodate multiple configurations.

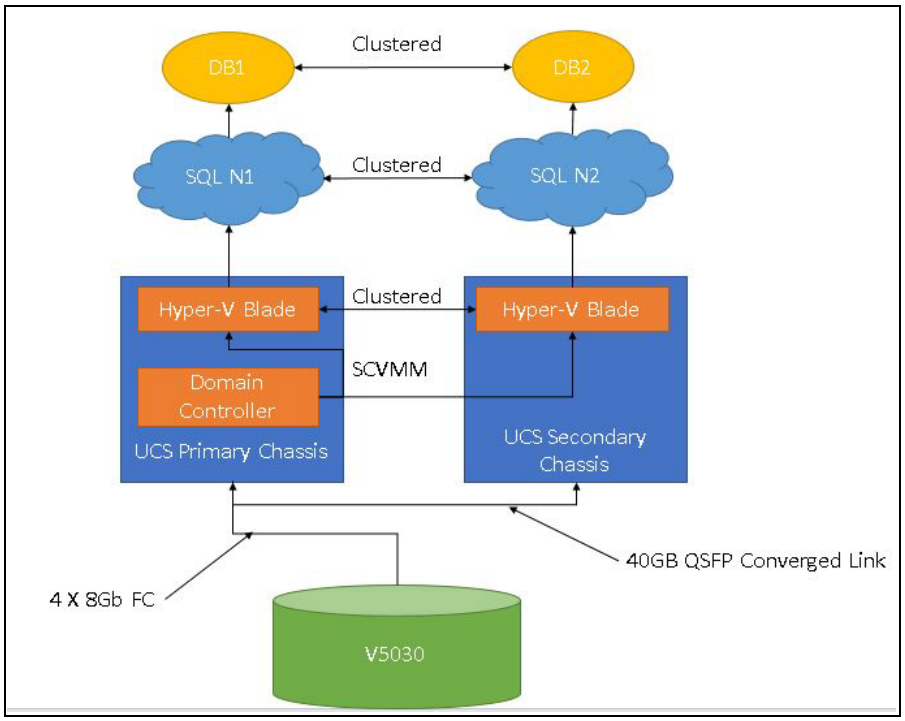


Figure 2-4 High-level architecture diagram of Microsoft SQL Server on VersaStack

Figure 2-4 depicts two Cisco UCS B series blade servers running Microsoft Windows Server with Hyper-V. Microsoft SQL Server is running on virtual machines created on the Hyper-V environment.

The VersaStack solution in this book uses the Cisco UCS-Mini chassis and embedded Fabric Interconnects Cisco UCS blades with Cisco UCS virtual interface card (VIC) and an IBM FlashSystem 5030 storage controller. The UCS chassis is direct connected to the FlashSystem 5030 with the embedded Fabric Interconnects, providing FC switching and zoning. The UCS blades have SAN-boot hosts with block-level access to both their boot LUNs and shared storage data stores.

The reference hardware configuration includes the following items:

- Cisco UCS-Mini with three B series blade servers (two to virtualize the SQL Servers and one as a Windows Domain Controller)
- Two Cisco UCS 6324 embedded Fabric Interconnects
- One IBM FlashSystem 5030 system, which is composed of an IBM FlashSystem 5030 control enclosure and expansion enclosures

The base VersaStack design is used in this book. However, all of the components can be scaled as required to support business needs. For example, the UCS Mini can be upgraded to a full UCS with stand-alone Fabric Interconnects to greatly increase port density.

Other possibilities for expansion include more (or different) servers or additional disk shelves to increase disk space and I/O capacity and additional UCS chassis to increase compute capacity. You can also add special hardware or software features to introduce new capabilities to the solution.

This book guides you through the low-level steps for deploying the base architecture. These procedures cover everything from physical cabling to network, compute and storage device configurations, and Microsoft 2016 Server and Microsoft SQL Cluster deployment.

For more information about the design of VersaStack, see the Versa Stack for Data Center Design Guide.

3

Design considerations for Microsoft Hyper-V and SQL Server

Previous publications have covered general resiliency and fault tolerance guidance for the Cisco UCS and IBM Spectrum Virtualize storage (V7000, V9000, San Volume Controller, and so on). This chapter focuses on design considerations and preferred practices for using Microsoft Hyper-V as a hypervisor and running Microsoft SQL Server as a tenant virtual machine.

Other resources: For design guidance about the Cisco UCS Mini and IBM Storwize V5000 Gen2, see the *VersaStack Design Guide*.

This chapter includes the following topics:

3.1 Microsoft Hyper-V considerations

Microsoft Hyper-V is a type 1 hypervisor. Thus, the Hyper-V server owns and virtualizes all of the physical resources (processor, memory, I/O adapters, and so on) within a root partition and then shares these resources to child partitions (virtual machines).

3.1.1 Root partition considerations

When planning your Hyper-V deployment, it is important to prepare for some additional overhead in compute, networking, and storage resources that the hypervisor adds in addition to the normal workload of the child partitions. To minimize the resources that are required by the hypervisor, it is suggested that the root partition be dedicated to Hyper-V. Keep additional software applications and features to a minimum on the root partition to avoid resource contention within the hypervisor itself.

Microsoft recommends using the Windows Server Core installation for Hyper-V root partitions as a way to minimize the amount of compute resources that the root partition requires to serve virtual machines. For ease of use and management in the installation that is used for this book, Windows Server 2016 Datacenter edition is used for the Hyper-V root partition.

The network interfaces on the root partition serve as a bridge between the upstream network infrastructure and the child partitions. Because of this, all of the virtual local area networks (VLANs) for the child partitions that need to be accessed outside the physical server must be configured and allowed on the physical interfaces that are owned by the root partition.

The root partition generally is responsible for managing multipathing to the storage. As such, you need to install the IBM Subsystem Device Driver Device Specific Module (SDDDSM) software on the root partition. You can find more information about SDDDSM on the IBM Support SDDDSM web page.

3.1.2 Child partition considerations

When sizing how much memory capacity a child partition needs, use the same guidelines as though you were sizing a physical Windows operating system installation. Optionally, for memory, you can opt to enable Dynamic Memory and allow Windows to size the memory for you. For more information about using Dynamic Memory, see the online Microsoft TechNet documentation.

When configuring a child partition's storage, you can use a virtual hard disk (VHD) that sits as a file accessible to the root partition, or you can configure a virtual host bus adapter (vHBA) to access the storage controller LUN directly.

Using VHD storage includes the following qualities:

- Maximum 64 terabyte size
- Protection against data loss during a power failure
- Alignment format that is optimized for large sector disks
- A 4 KB logical sector for improved performance on applications designed for 4 KB transactions
- The ability to be snapshot by the hypervisor for data protection

When using a VHDX-format disk, the following formats are available:

- The *fixed disk* pre-allocates the full capacity of the disk on creation. As a result, this format typically has a lower CPU, is less likely to fragment, and results in a lower I/O rate when compared to a dynamic disk.
- *Dynamic disks* are provisioned such that space is allocated on demand. As a result, you have the capability to save on used storage space. However, when a write request to this disk type comes in and if new blocks are used, the block must be allocated before the host write is processed. This configuration results in higher CPU and storage bandwidth overhead when compared to fixed disks.

In contrast, configuring a vHBA to access a controller directly has the following benefits:

- The file system of the root partition is bypassed, which reduces CPU usage for storage I/O in the root partition.
- A larger disk size is supported.

When using vHBAs for storage access, note that the HBA driver of the root partition and the connected SAN devices must support N_Port ID Virtualization (NPIV). Additionally, if more than one HBA is installed on the physical server, configure multiple vHBAs in the child partition to more effectively use available bandwidth. This method for storage access also requires additional configuration on the storage controller being accessed to present volumes to the child partition and creates the need to configure multipathing on the child partition.

3.2 Microsoft SQL Server design considerations

This section describes various design considerations for Microsoft SQL Server and installing the Failover Clustering feature.

Specific business requirements can drive each solution and can require changes to accommodate the goals. This section provides an overview of design aspects that you need to consider and further reading that is required in each direction.

3.2.1 Sizing and design planning for Microsoft SQL Server

Consider the following information when sizing and planning the design for software and hardware for Microsoft SQL Server:

- Starting with Microsoft SQL Server 2012, use an New Technology File System (NTFS) formatted file system to store SQL installation binaries and other files. Installing Microsoft SQL Server on a computer with FAT32 file system is supported but not recommended, because it is less secure than the NTFS.
- Microsoft SQL Server setup blocks installations on read-only, mapped, or NTFS compressed drives.
- SQL Server requires a minimum of 6 GB of free disks space for storing installation binaries. More capacity might be required based on additional Microsoft SQL Server components chosen for installation. Ensure that you reserve at least 1 GB of free disk space for the operational and data warehouse database. This space is required at the time of the database creation.
- The following storage types for data files are supported:
  - Local disk
  - Shared storage

  - Storage spaces direct (S2D)
  - SMB file share
- Microsoft SQL Server 2016 requires .NET Framework 4.6 for the Database Engine, Master Data Services or Replication. Microsoft SQL Server 2016 setup automatically installs .NET Framework.

See Hardware and Software Requirements for Installing SQL Server for more information.

3.2.2 Database applications and workload

The following typical database design types are available:

- *Online transaction processing (OLTP) database applications* are optimal for managing changing data. These applications typically have many users who are performing transactions while change in real-time data. In other words, online transaction processing (OLTP) is a live database (accommodates inserts, deletes, updates, and so on).
- *Decision-support System (DSS) database applications* are optimal for data queries that do not change data. This database is the database from which data is extracted and analyzed statistically (but not modified) to inform business or other decisions and is exactly opposite to the *operational database*, which is continuously updated. For example, a decision support database might provide data to determine the average salary of distinct types of employees. Often, decision-support data is extracted from operational databases. The tables in a decision-support database are heavily indexed, and the raw data is frequently preprocessed and organized to support the several types of queries to be used.

The entire architecture is designed to suit several high-performance workload patterns, including an OLTP, DSS, and various other workloads that are characterized by small number of random I/Os. Log I/O is the most critical component, because it directly affects the transaction latency. Memory mitigates the I/O pressure on the storage subsystem. However, beyond a certain threshold, increasing memory might not yield any noticeable benefit.

There are certain OLTP workloads that have a reporting or End of Day consolidation (EOD) job in the mix. For this kind of reporting and EOD job, I/O capacity must be carefully evaluated to ensure that such workloads are not affecting regular production OLTP transactions. Many of the reporting and batch jobs use temporary database space. To provide optimal performance for this kind of workloads, you can employ solid-state drives (SSDs) or all flash storage to store temporary database (`tempdb`) files.

3.2.3 Storage, RAID type and disk selection

Redundant Array of Independent Disks (RAID) is used to improve the performance characteristics of individual disks (by striping data across several disks) and to provide protection from individual disk failures. Most of the RAID types are supported for various applications and input output (IO) intensive workloads on various servers.

Although RAID is not a part of Microsoft SQL Server, implementing RAID can directly affect the way Microsoft SQL Server performs. RAID levels 0, 1, and 5 are typically used with Microsoft SQL Server. However, we have striped our disks with RAID 5 in our design, which gives an equivalent performance.

The IBM standard recommendation for the IBM Storwize V5000 is to use a distributed RAID 6 (DRAID 6) solution all the time. DRAID 6 is tested to show that the I/O performance of DRAID 6 is faster than traditional RAID 5 in almost all workloads. You can find more information about DRAID 6 can in IBM Knowledge Center.

The capacity use of Microsoft SQL Server internally can be segregated into sub-areas, and each sub area can benefit from different a RAID type and cache settings. The following sub-areas are available:

- *System Database*: Stores system information about the Microsoft SQL Server instance, database templates, and job schedules.
- *TempDB files*: Stores intermediate query results. SSD disks are recommended for this type of data.
- *Database DB files*: Stores user data from database tables. A single database can span across multiple storage volumes to provide higher performance. Capacity can be determined based on parameters such as record sizes or record count and expected growth.
- *Database log files*: Stores database transaction logs during server operation. Low latency disks, such as SSDs, are highly recommended for this area.

3.2.4 IOPS requirements for Microsoft SQL Server

It is important to calculate the desired theoretical I/O operations per second (IOPS) requirement for a given database. Larger number of disks with faster revolutions per minute (RPM) or storage arrays provide sufficient IOPS while maintaining low latency and queuing on all disks.

Planning for minimal latency before deployment, and regular monitoring helps avoiding serious issues. Most of the time, it is not good to use other types of resources, such as CPU or memory, to compensate for slow response from the I/O subsystem.

3.2.5 Server virtualization

The database deployment is built on server virtualization by using Microsoft Hyper-V technology. This design provides an efficient and flexible back end for hosting Microsoft SQL Server transactional workloads. Each of the virtual machines hosting the Microsoft SQL Server database instances should be configured with the optimal computational and storage resources to suit the workload. Typical OLTP workloads are not CPU-intensive. For a virtualized database platform, you can start with four vCPUs and scale when the aggregate utilization of those vCPUs crosses the threshold that is set by the internal IT practices.

3.2.6 Database availability

The configuration is designed to have the cluster level availability by using Windows Server Failover Cluster (WSFC) feature. The Hyper-V technology also provides a rich medium to have database instance highly available and optimal performance by using the high availability (HA), database recovery (DRS) and live migration features enabled. However, in this configuration for Microsoft SQL Server, Hyper-V uses the Microsoft Windows Failover Cluster feature to provide high availability.

3.2.7 Quality of service and network segregation

The network traffic within the proposed architecture is segregated to ensure maximum bandwidth availability. Each of the network interfaces that are defined is designed to follow a certain quality of service (QoS) policy, which is assumed to give intended performance and functions.

In Microsoft SQL Server 2016 release, Cluster Shared Volumes (CSV) are supported for hosting the database files, which allows storage traffic to be routed through the cluster interconnect between the primary and standby nodes if the primary loses connectivity to the storage. For this purpose, jumbo frames are enabled on the interface, which can carry CSV traffic.

3.2.8 Network availability and topology requirements

Plan network connections within and between farms in large data center environments and server cluster to provide redundant connectivity. Configure network paths to ensure aggregated bandwidth requirements of client access are met.

In a bigger database solution, where web servers and application servers are used, it is recommended practice to have two network adapters:

- One to handle user traffic
- One to handle communication with the servers that are running Microsoft SQL Server

4

VersaStack Cisco Nexus 9000 network configuration

This chapter provides a description of the initial configuration steps for the setup of the Cisco Nexus 9000 Series switches in a VersaStack deployment. After the procedures are complete, the configuration provides higher throughput and redundant Layer 2 network connectivity for the Cisco UCS Mini environment to the upstream switches.

The Cisco Nexus 9000 Series switches are Cisco Application Centric Infrastructure (Cisco ACI) ready, which provides a foundation for automating application deployments and delivers simplicity, agility, and flexibility. These deployment procedures are customized to include the environment variables.

This chapter includes the following topics:

4.1 Initial terminal connection

The configuration for the solution described in this book is set up using a Cisco 2901 Terminal Server that is connected using the console port on the switch shown in Figure 4-1.

Figure 4-1 Console port

4.2 Configuring the Cisco Nexus switch A

To set up the initial configuration for the Cisco Nexus switch A, complete the steps shown in Example 4-1.

Note: On initial boot and connection to the serial or console port of the switch, the NX-OS setup automatically starts and attempts to enter Power on Auto Provisioning.

Example 4-1 Configuring the Cisco Nexus switch A

```
Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: y
   ---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:
   Enter the password for "admin":
   Confirm the password for "admin":

   ---- Basic System Configuration Dialog VDC: 1 ----
This setup utility will guide you through the basic configuration of the system.
Setup configures only enough connectivity for management of the system.

Please register Cisco Nexus9000 Family devices promptly with your supplier.
Failure to register may affect response times for initial service calls. Nexus9000
devices must be registered to receive entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the
remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): y
   Create another login account (yes/no) [n]: n
   Configure read-only SNMP community string (yes/no) [n]:
   Configure read-write SNMP community string (yes/no) [n]:
   Enter the switch name : <<var_nexus_A_hostname>>
   Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
   Mgmt0 IPv4 address : <<var_nexus_A_mgmt0_ip>>
   Mgmt0 IPv4 netmask : <<var_nexus_A_mgmt0_netmask>>
   Configure the default gateway? (yes/no) [y]:
   IPv4 address of the default gateway : <<var_nexus_A_mgmt0_gw>>
   Configure advanced IP options? (yes/no) [n]:
   Enable the telnet service? (yes/no) [n]:
   Enable the ssh service? (yes/no) [y]:
```

```
   Type of ssh key you would like to generate (dsa/rsa) [rsa]:
   Number of rsa key bits <1024-2048> [1024]: 2048
   Configure the ntp server? (yes/no) [n]: y
   NTP server IPv4 address : <<var_global_ntp_server_ip>>
   Configure default interface layer (L3/L2) [L2]:
   Configure default switchport interface state (shut/noshut) [noshut]:
   Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:
password strength-check
switchname <<var_nexus_A_hostname>>
vrf context management
 ip route 0.0.0.0/0 <<var_nexus_A_mgmt0_gw>>
exit
 no feature telnet
ssh key rsa 2048 force
 feature ssh
ntp server <<var_global_ntp_server_ip>>
system default switchport
 no system default switchport shutdown
 copp profile strict
interface mgmt0 ip address <<var_nexus_A_mgmt0_ip>> <var_nexus_A_mgmt0_netmask>>
no shutdown
Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
[########################################] 100% Copy complete
```

4.3 Configuring the Cisco Nexus switch B

To set up the initial configuration for the Cisco Nexus switch B, complete the steps shown in Example 4-2.

Note: On initial boot and connection to the serial or console port of the switch, the NX-OS setup automatically starts and attempts to enter Power on Auto Provisioning.

Example 4-2 Configuring the Cisco Nexus switch B

```
Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: y
         ---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:
   Enter the password for "admin":
   Confirm the password for "admin":
         ---- Basic System Configuration Dialog VDC: 1 ---
This setup utility will guide you through the basic configuration of the system.
Setup configures only enough connectivity for management of the system.

Please register Cisco Nexus9000 Family devices promptly with your supplier.
Failure to register may affect response times for initial service calls. Nexus9000
devices must be registered to receive entitled support services.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the
re-maining dialogs.

Would you like to enter the basic configuration dialog (yes/no): y
```

```
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : <<var_nexus_B_hostname>>
  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
    Mgmt0 IPv4 address : <<var_nexus_B_mgmt0_ip>>
    Mgmt0 IPv4 netmask : <<var_nexus_B_mgmt0_netmask>>
Configure the default gateway? (yes/no) [y]:
    IPv4 address of the default gateway : <<var_nexus_B_mgmt0_gw>>
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]:
    Type of ssh key you would like to generate (dsa/rsa) [rsa]:
    Number of rsa key bits <1024-2048> [1024]: 2048
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_global_ntp_server_ip>>
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut) [noshut]:
  Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:
The following configuration will be applied:
password strength-check
switchname <<var_nexus_B_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_nexus_B_mgmt0_gw>>
exit
 no feature telnet
ssh key rsa 2048 force
 feature ssh
ntp server <<var_global_ntp_server_ip>>
system default switchport
 no system default switchport shutdown
 copp profile strict
interface mgmt0 ip address <<var_nexus_B_mgmt0_ip>> <<var_nexus_B_mgmt0_netmask>>
no shutdown
Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
[########################################] 100% Copy complete.
```

4.4 Enabling the Cisco Nexus 9000 features and settings

On *both* the Cisco Nexus 9000 Series switches, you need to enable the IP switching feature and set the default spanning tree behaviors.

Complete the following steps on each of the Cisco Nexus 9000 Series switches:

1. Enter configuration mode by running the following command:

   ```
   config terminal
   ```

2. To enable the necessary features, run the following commands:

   ```
   feature lacp
   feature vpc
   feature interface-vlan
   ```

3. Configure the spanning tree and save the running configuration to start:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
copy run start
```

4.5 Creating the VLANs for the VersaStack traffic

To create the virtual local area networks (VLANs) for the VersaStack traffic for the Cisco Nexus switch A and Cisco Nexus switch B, run the commands shown in Example 4-3 on *both* switches in configuration mode.

Example 4-3 Creating the necessary VLANs

```
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
vlan <<var_native_vlan_id>>
name Native-VLAN
vlan <<var_cluster_vlan_id>>
name MS-Cluster-VLAN
vlan <<var_vm_traffic_vlan_id>>
name VM-Traffic-VLAN
vlan <<var_csv_vlan_id>>
name MS-CSV-VLAN
exit
copy run start
```

4.6 Configuring the Virtual PortChannel domain

This section describes how to create the Virtual PortChannels (vPCs) domain.

4.6.1 Configure the vPC for the Cisco Nexus switch A

To configure Virtual PortChannels (vPCs) for the Cisco Nexus switch A, complete the following steps:

1. From the global configuration mode, create a vPC domain by running the following command:

   ```
   vpc domain <<var_nexus_vpc_domain_id>>
   ```

2. Make the Cisco Nexus switch A the primary vPC peer by defining a low priority value by running the following command:

   ```
   role priority 10
   ```

3. Use the management interfaces on the supervisors of the Cisco Nexus switch A to establish a keepalive link by running the following command:

   ```
   peer-keepalive destination <<var_nexus_B_mgmt0_ip>>  source
   <<var_nexus_A_mgmt0_ip>>
   ```

4. Enable the features for this vPC domain by running the following commands:

```
peer-switch
delay restore 150
peer-gateway
ip arp synchronize
auto-recovery
copy run start
```

4.6.2 Configure the vPC for the Cisco Nexus switch B

To configure vPCs for the Cisco Nexus switch B, complete the following steps:

1. From the global configuration mode, create a vPC domain by running the following command:

```
vpc domain 101
```

2. Make the Cisco Nexus switch B, the primary vPC peer by defining a low priority value by running the following command:

```
role priority 20
```

3. Use the management interfaces on the supervisors of the Cisco Nexus switch B to establish a keepalive link by running the following command:

```
peer-keepalive destination <<var_nexus_A_mgmt0_ip>> source
<<var_nexus_B_mgmt0_ip>>
```

4. Enable the features for this vPC domain by running the following commands:

```
peer-switch
delay restore 150
peer-gateway
ip arp synchronize
auto-recovery
copy run start
```

4.7 Configuring the network interfaces for the vPC peer links

This section describes how to configure the network interfaces for the vPC peer links.

4.7.1 Configure the network interface for the Cisco Nexus switch A

To configure the network interfaces for the vPC peer links for the Cisco Nexus switch A, complete the following steps:

1. Define a port description for the interfaces connecting to vPC Peer by using the following commands:

```
<var_nexus_B_hostname>>
interface Eth1/47
description VPC Peer <<var_nexus_B_hostname>>:1/47
interface Eth1/48
description VPC Peer <<var_nexus_B_hostname>>:1/48
```

2. Apply a port channel to both vPC peer links and start the interfaces by running the following commands:

```
interface Eth1/47,Eth1/48
channel-group 10 mode active
no shutdown
```

3. Define a description for the port channel connecting to the N9K-B by running the following commands:

```
<<var_nexus_B_hostname>>
interface Po10
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, Cluster, CSV and the native VLAN by running the following commands:

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_cluster_vlan_id>>,<<var_vm_traffic_vlan_id>>,<<var_csv_vlan_id>>
```

5. Make this port channel the vPC peer link and start it by running the following commands:

```
vpc peer-link
no shutdown
copy run start
```

4.7.2 Configure the network interface for the Cisco Nexus switch B

To configure the network interfaces for the vPC peer links for the Cisco Nexus switch B, complete the following steps:

1. Define a port description for the interfaces connecting to the vPC Peer N9K-A by running the following commands:

```
<var_nexus_A_hostname>>
interface Eth1/47
description VPC Peer <<var_nexus_A_hostname>>:1/47
interface  Eth1/48
description VPC Peer <<var_nexus_A_hostname>>:1/48
```

2. Apply a port channel to both vPC peer links and start the interfaces by running the following commands:

```
interface Eth1/47,Eth1/48
channel-group 10 mode active
no shutdown
```

3. Define a description for the port channel connecting to the N9K-A by running the following commands:

```
interface Po10
description vPC peer-link
```

4. Make the port channel a switchport and configure a trunk to allow all VLANs by running the following commands:

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_cluster_vlan_id>>, <<var_vm_traffic_vlan_id>>,<<var_csv_vlan_id>>
```

5. Make this port channel the vPC peer link and start it by running the following commands:

```
vpc peer-link
no shutdown
copy run start
```

4.8 Configuring network interfaces to the Cisco UCS Fabric Interconnects

This section describes how to configure the network interfaces to the Cisco UCS Fabric Interconnects.

4.8.1 Configure the Cisco Nexus switch A to FI-A

To configure the network interfaces to the Cisco UCS Fabric Interconnect for Cisco Nexus switch A, complete the following steps:

1. Define a description for the port channel that connects to FI-A by running the following commands:

```
interface Po13
description <<var_ucs_clustername>>-A
```

2. Make the port channel a switchport and configure a trunk to allow all VLAN traffic by running the following commands:

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_cluster_vlan_id>>, <<var_vm_traffic_vlan_id>>,<<var_csv_vlan_id>>
```

3. Make the port channel and associated interfaces into spanning tree edge ports by running the following command:

```
spanning-tree port type edge trunk
```

4. Set the MTU to be 9216 to support jumbo frames by running the following command:

```
mtu 9216
```

5. Make a vPC and start it by running the following commands:

```
vpc 13
no shutdown
```

6. Define a port description for the interface that connects to FI-A by running the following commands:

```
interface eth1/3
description FI-A:1/3
```

7. Start the interface by running the following commands:

```
channel-group 13 mode active
no shutdown
```

8. Define a description for the port channel connecting to FI-B by running the following commands:

```
Po14
description <<var_ucs_clustername>>-B
```

9. Make the port channel a switchport and configure a trunk to allow all VLAN traffic by running the following commands:

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,<<var_cluster_vlan_id>>,
<<var_vm_traffic_vlan_id>>,<<var_csv_vlan_id>>
```

10. Make the port channel and associated interfaces into spanning tree edge ports by running the following command:

```
spanning-tree port type edge trunk
```

11. Set the MTU to be 9216 to support jumbo frames by running the following command:

```
mtu 9216
```

12. Make a vPC and bring it up by running the following commands:

```
vpc 14
no shutdown
```

13. Define a port description for the interface connecting to `<<var_ucs_clustername>>-B` as follows:

```
interface Eth1/4
description <<var_ucs_clustername>>-B:1/4
```

14. Apply it to a port channel and open the interface by running the following commands:

```
channel-group 14 force  mode active
no shutdown
copy run start
[########################################] 100%
Copy complete.
```

4.8.2 Configure the Cisco Nexus switch B to FI-B

To configure the network interfaces to the Cisco UCS Fabric Interconnect for Cisco Nexus switch B, complete the following steps:

1. Define a description for the port channel that connects to FI-B by running the following commands:

```
interface Po14
description <<var_ucs_clustername>>-B
```

2. Make the port channel a switchport and configure a trunk to allow all VLAN traffic by running the following commands:

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_cluster_vlan_id>>,
<<var_vm_traffic_vlan_id>>,<<var_csv_vlan_id>>
```

3. Make the port channel and associated interfaces into spanning tree edge ports by running the following command:

```
spanning-tree port type edge trunk
```

4. Set the MTU to be 9216 to support jumbo frames by running the following command:

```
mtu 9216
```

5. Make a vPC and start it by running the following commands:

```
vpc 14
no shutdown
```

6. Define a port description for the interface that connects to FI-B by running the following commands:

```
interface Eth1/3
description <<var_ucs_clustername>>-B:1/3
```

7. Start the interface by running the following commands:

```
channel-group 14 mode active
no shutdown
```

8. Define a description for the port channel that connects to FI-A by running the following commands:

```
interface Po13
description <<var_ucs_clustername>>-A
```

9. Make the port channel a switchport and configure a trunk to allow all VLAN traffic by running the following commands:

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,<<var_cluster_vlan_id>>,
<<var_vm_traffic_vlan_id>>,<<var_csv_vlan_id>>
```

10. Make the port channel and associated interfaces into spanning tree edge ports by running the following command:

```
spanning-tree port type edge trunk
```

11. Set the MTU to be 9216 to support jumbo frames by running the following command:

```
mtu 9216
```

12. Make a vPC and start it by running the following commands:

```
vpc 13
no shutdown
```

13. Define a port description for the interface that connects to FI-A by running the following commands:

```
interface eth1/4
description <<var_ucs_clustername>>-A:1/4
```

14. Start the interface by running the following commands:

```
channel-group 13 mode active
no shutdown
copy run start
[########################################] 100%
Copy complete.
```

5

The Cisco Unified Computing System Mini configuration

This chapter describes how to set up and optimize the Cisco Unified Computing System (UCS) Mini to for use in a VersaStack environment. By using the configuration described in this chapter, the Cisco UCS Mini can provide fault tolerance platform for a virtual environment.

This chapter includes the following sections:

5.1 Completing the initial setup of the Cisco UCS 6324 Fabric Interconnects

This section provides the detailed procedures for configuring the Cisco UCS 6324 Fabric Interconnects for use in a VersaStack environment.

Each chassis of the Cisco UCS Mini supports one or two Fabric Interconnects. For resiliency purposes, two Fabric Interconnects are ideal for optimized deployments of a Cisco UCS Mini chassis. The Fabric Interconnects are modular components that attach into the Cisco UCS Mini blade server chassis. A midplane connects the blade servers to the Fabric Interconnects. The Cisco UCS 6324 Fabric Interconnects support direct-attached storage (DAS) array and the IBM FlashSystem 5030 is directly attached to the UCS 6324 Fabric Interconnects.

Important: The steps are necessary to provision the Cisco UCS C-Series and B-Series servers. Follow these steps precisely to avoid improper configuration.

5.1.1 Cisco UCS Fabric Interconnects 6324 A

To configure the Cisco UCS 6324 A server for use in a VersaStack environment, complete the following steps:

1. Connect to the console port on the first Cisco UCS 6324 Fabric Interconnects, and complete the following prompts with the provided information:

```
Enter the configuration method: console
Enter the setup mode; setup newly or restore from backup.(setup/restore)? Setup
You have choosen to setup a a new fabric interconnect? Continue? (y/n): y
Enforce strong passwords? (y/n) [y]: y
Enter the password for "admin": <<var_password>>
Enter the same password for "admin": <<var_password>>
Is this fabric interconnect part of a cluster (select 'no' for standalone)?
(yes/no) [n]: y
Which switch fabric (A|B): A
Enter the system name: <<var_ucs_clustername>>
Physical switch Mgmt0 IPv4 address: <<var_ucsa_mgmt_ip>>
Physical switch Mgmt0 IPv4 netmask: <<var_ucsa_mgmt_mask>>
IPv4 address of the default gateway: <<var_ucsa_mgmt_gateway>>
Cluster IPv4 address: <<var_ucs_cluster_ip>>
Configure DNS Server IPv4 address? (yes/no) [no]: y
DNS IPv4 address: <<var_nameserver_ip>>
Configure the default domain name? y
Default domain name: <<var_dns_domain_name>>
Join centralized management environment (UCS Central)? (yes/no) [n]: Enter
```

2. Review the settings that are output to the console. If they are correct, answer `yes` to apply and save the configuration.
3. Wait for the login prompt and make sure that the configuration process has completed before proceeding.

5.1.2 Cisco UCS Fabric Interconnects 6324 B

To configure the Cisco UCS 6324 B server for use in a VersaStack environment, power on the second module and connect to the console port on the second Cisco UCS 6324 Fabric Interconnects. Then, complete the following prompts with the provided information:

```
Enter the configuration method: console
Installer has detected the presence of a peer Fabric interconnect. This Fabric
interconnect will be added to the cluster. Do you want to continue {y|n}? y
Enter the admin password for the peer fabric interconnect: <<var_password>>
Physical switch Mgmt0 IPv4 address: <<var_ucsb_mgmt_ip>>
Apply and save the configuration (select 'no' if you want to reenter)? (yes/no): y
```

5.2 VersaStack Cisco UCS base setup

This section describes the steps to set up the VersaStack Cisco UCS Mini that has an IBM FlashSystem 5030 attached over Fibre Channel protocol.

This document assumes the use of Cisco UCS Manager Software version 3.2(1d). To upgrade the Cisco UCS Manager software and the Cisco UCS 6324 Fabric Interconnects software to version 3.2(1d), see the Cisco UCS Manager Install and Upgrade Guides.

5.2.1 Logging in to the Cisco UCS Manager

To log in to the Cisco UCS Manager environment, complete the following steps:

1. Open a web browser and navigate to the Cisco UCS 6324 Fabric Interconnects cluster address.
2. Select the HTML **Launch UCS Manager** option. The examples in this book use HTML options.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter `admin` as the user name and then enter the administrative password.
5. Click **Login** to log in to the Cisco UCS Manager.

6. As shown in Figure 5-1, enter the information for Anonymous Reporting if you want, and then click **OK**.

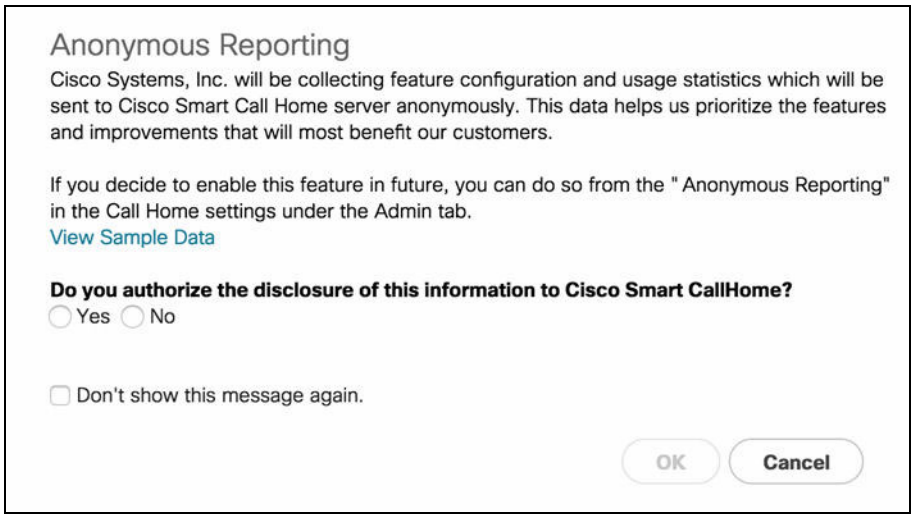


Figure 5-1 Anonymous reporting to Cisco

5.2.2 Adding a block of IP addresses for access to a kernel-based virtual machine console

The kernel-based virtual machine (KVM) console is an virtual interface that is accessible from the Cisco UCS Manager GUI or the KVM Launch Manager that emulates a direct connection to each KVM using a web-browser. Also, the KVM console interface allows system administrators to connect to the server from a remote location across the network.

IP addresses: This block of IP addresses should be in the same subnet as the management IP addresses for the Cisco UCS Manager.

To create a block of IP address for server Keyboard, Video, Mouse (KVM) access in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. As shown in Figure 5-2 on page 47, click **Pools** → **root** → **IP Pools ext-mgmt**. Then, in the Actions pane, select **Create Block of IPv4 Addresses**.

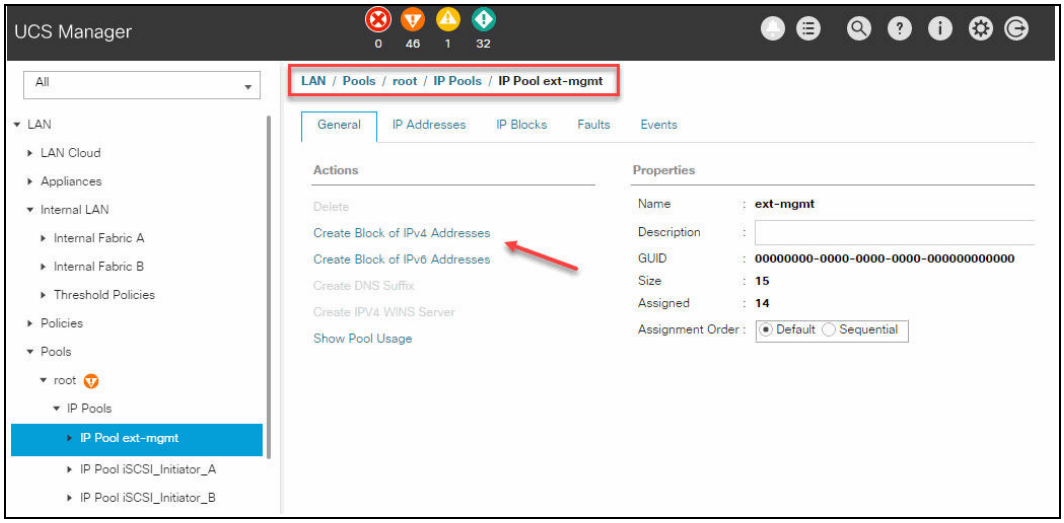


Figure 5-2 Creating IP block addresses for KVM management

3. Enter the starting IP address of the block, the number of IP addresses required, the subnet, and the gateway information.
4. Click **OK** to create the IP block, and then click **OK** in the confirmation message.

5.2.3 Synchronizing the Cisco UCS Mini chassis to NTP

Network Time Protocol (NTP) synchronization can be crucial from the management, security, and troubleshooting aspect. NTP synchronization can provide unique time frame of reference between all components in the Cisco UCS Mini chassis. Without a synchronized date and time, accurately correlating log files can be extremely difficult or even impossible.

To configure NTP synchronization of your Cisco UCS Mini, complete the following steps:

1. In the Cisco UCS Manager, go to the Admin tab in the navigation pane.

2. Select **Admin** → **Time Zone Management**, as shown in Figure 5-3.

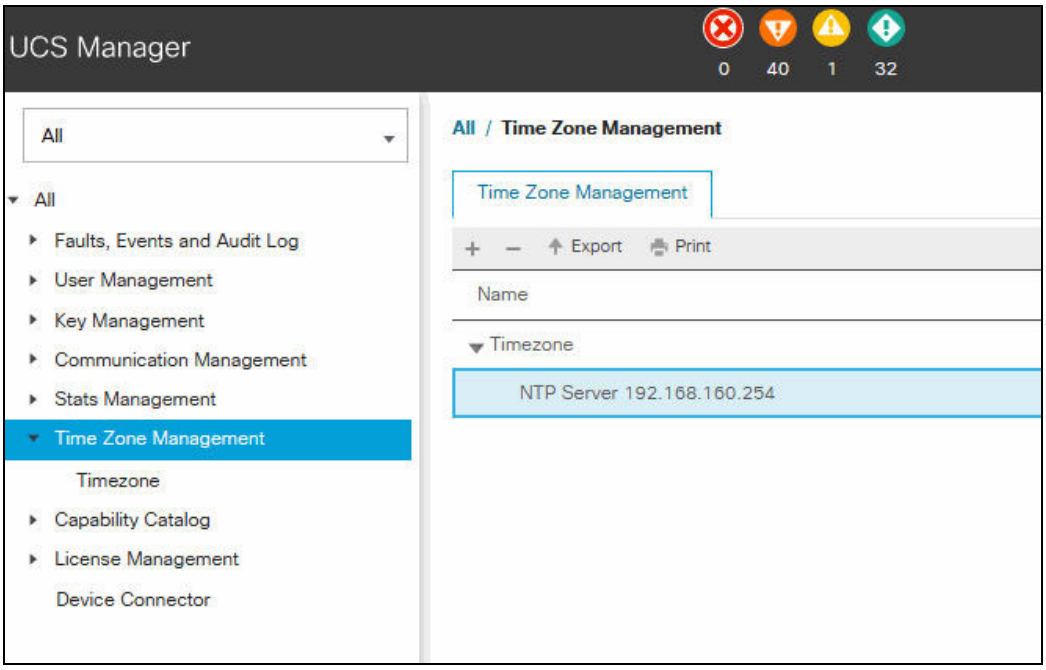


Figure 5-3 Time Zone Management

3. Click **Add** to include the appropriate NTP server IP information or the fully qualified domain name (FQDN), and then click **OK**, as shown in Figure 5-4.

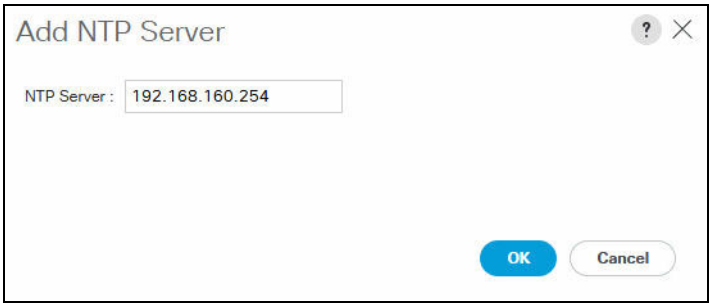


Figure 5-4 Configuring the NTP Server

4. Click **OK** to complete the setup of NTP Server for the Cisco UCS Mini.

5.2.4 Configuring the UCS Servers discovery policy

To configure the UCS Servers, you need to edit the chassis discovery policy. Setting the discovery policy simplifies the extension of the Cisco UCS Mini chassis. To modify the chassis discovery policy, complete the following steps:

1. In the Cisco UCS Manager, go to the Equipment tab in the navigation pane and select **Equipment** in the list on left under the pull-down menu.
2. In the right pane, go to the Policies tab.

3. Under Global Policies, set the Chassis/FEX Discovery Policy to mach the number of uplink ports that can be cabled between the Primary chassis to the Secondary Chassis. Set the Rack Server Discovery Policy to *Immediate*. Leave the other settings as is or change if appropriate for your environment. See Figure 5-5. Click **Save Changes**.

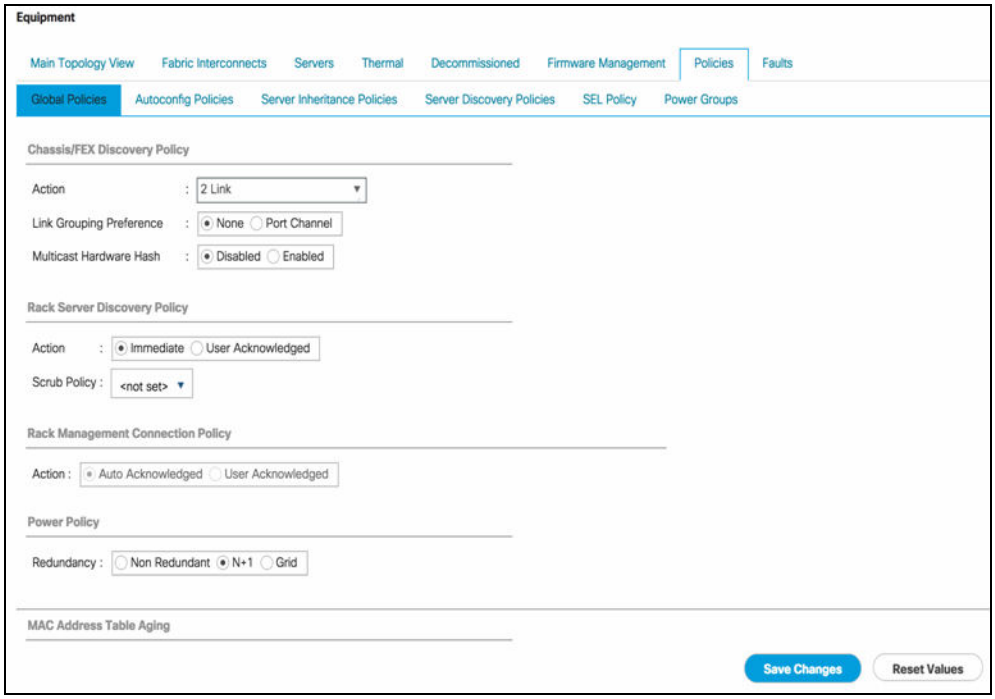


Figure 5-5 Configuring discovery policy for UCS Servers

5.2.5 Acknowledging the Cisco UCS Mini chassis

To acknowledge all Cisco UCS Mini chassis, complete the following steps:

1. In Cisco UCS Manager, go to the Equipment tab in the navigation pane.
2. Expand Chassis and select each chassis that is listed.

3. Right-click the both the primary and extended secondary chassis, and select **Acknowledge Chassis,** as shown in Figure 5-6.

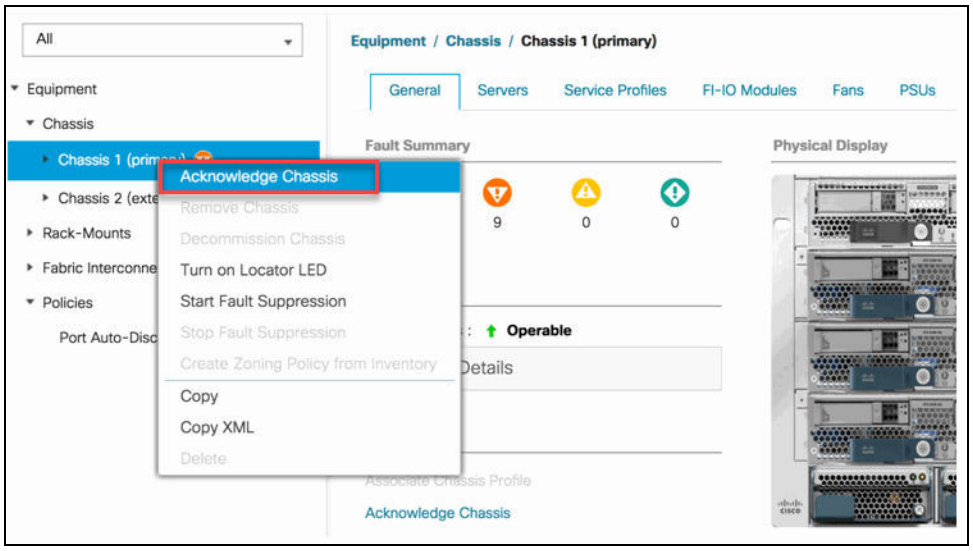


Figure 5-6 Acknowledge the UCS Mini chassis

4. Click **Yes** and then click **OK**.

5.3 Enabling the server and uplink ports in the Fabric Interconnects

The Cisco Fabric Interconnects is built to provide a unified connection for LAN and SAN combined into a single I/O module. The unified ports allow the Fabric Interconnects to support multiple and direct connections from the Cisco UCS Mini to Fibre Channel, Fibre Channel over Ethernet (FCoE), and Internet Small Computer System Interface (iSCSI) over IP.

To enable the server and uplink ports, complete the following steps:

1. In the Cisco UCS Manager, go to the Equipment tab in the navigation pane.
2. Click **Equipment** → **Fabric Interconnects** → **Fabric Interconnect A (primary)** → **Fixed Module**.
3. Expand **Ethernet Ports**.

4. Select the ports that are connected to the chassis, right-click them, and select **Configure as Uplink Port**, as shown in Figure 5-7.

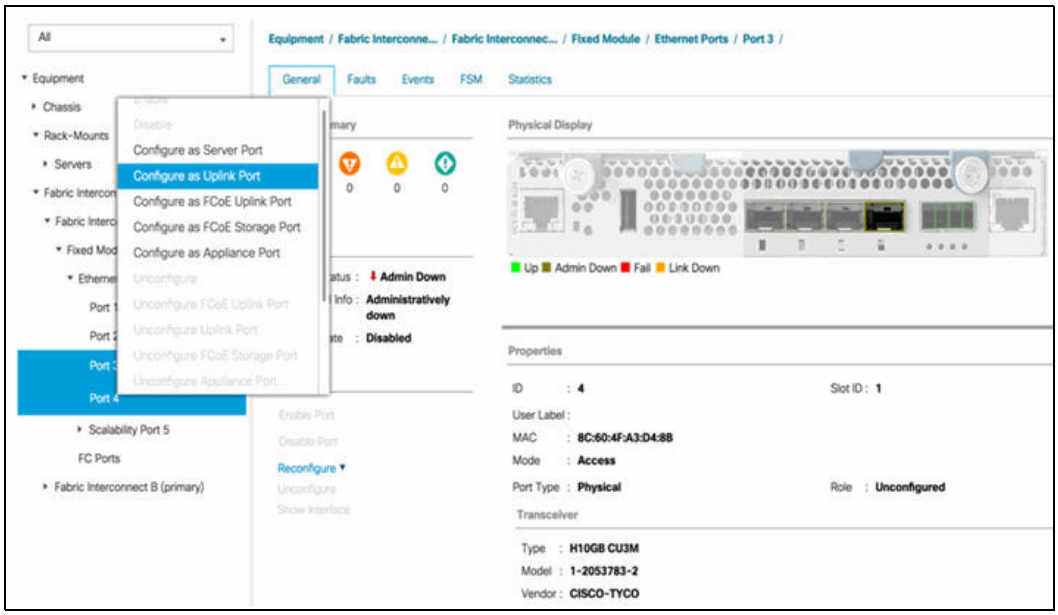


Figure 5-7 Configure as a server port

5. Click **Yes** to confirm the uplink ports, and then click **OK**.

5.3.1 Creating an UUID suffix pool

To configure the necessary Universally Unique Identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In the Cisco UCS Manager, go the Servers tab in the navigation pane.
2. Click **Pools** → **root**.

3. Right-click **UUID Suffix Pools** and then select **Create UUID Suffix Pool**, as shown in Figure 5-8.

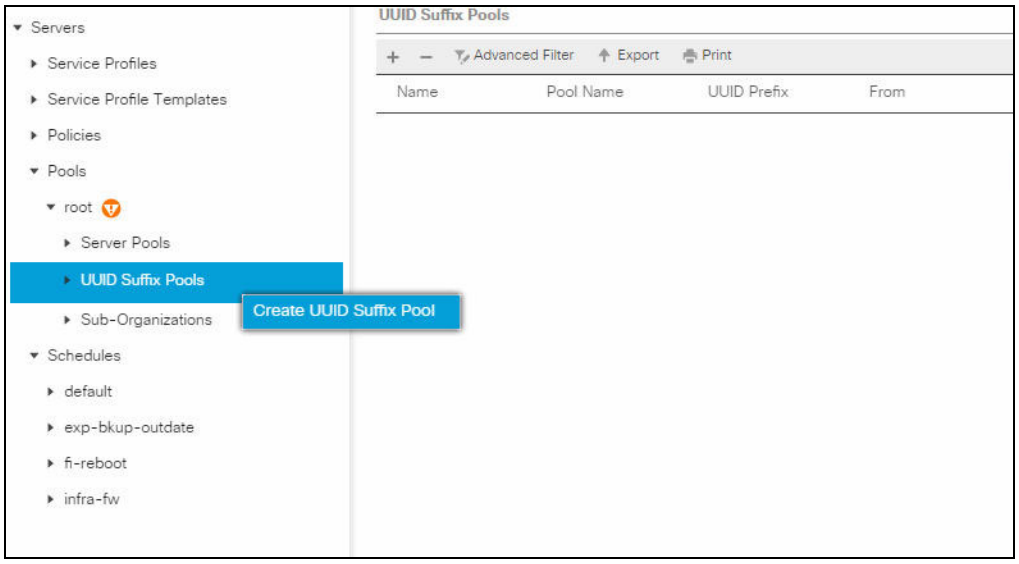


Figure 5-8 Create UUID Suffix Pool

4. Enter `UUID_Pool` as the name of the UUID suffix pool.
5. (Optional) Enter a description for the UUID suffix pool.
6. Keep the prefix at the derived option.
7. Click **Next**.
8. Click **Add** to add a block of UUIDs.
9. Keep the From field at the default setting.
10. Specify a size for the UUID block that is sufficient to support the available blade or server resources, as shown in Figure 5-9.

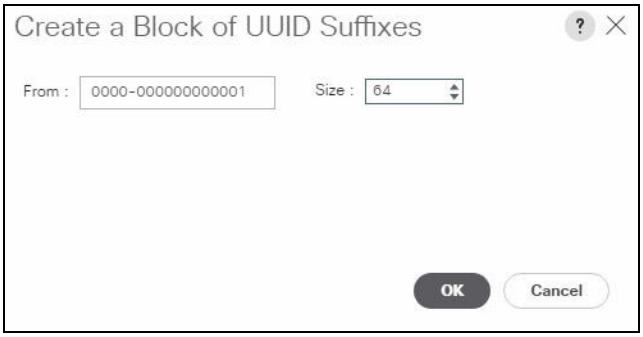


Figure 5-9 Add a block of UUIDs

11. Click **OK**.

12. Click **Finish** and **OK**. Figure 5-10 shows the new UUID.

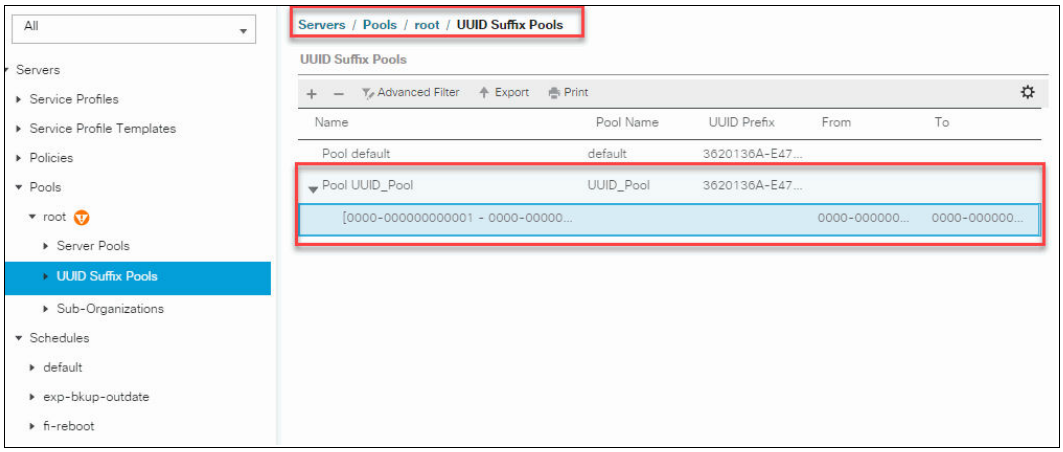


Figure 5-10 Add UUID blocks

5.3.2 Creating a server pool

Unique server pools: Consider creating unique server pools to achieve the granularity that is required in your environment.

To configure the necessary server pool for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Pools** → **root**.
3. Right-click **Server Pools** and select **Create Server Pool**, as shown in Figure 5-11.

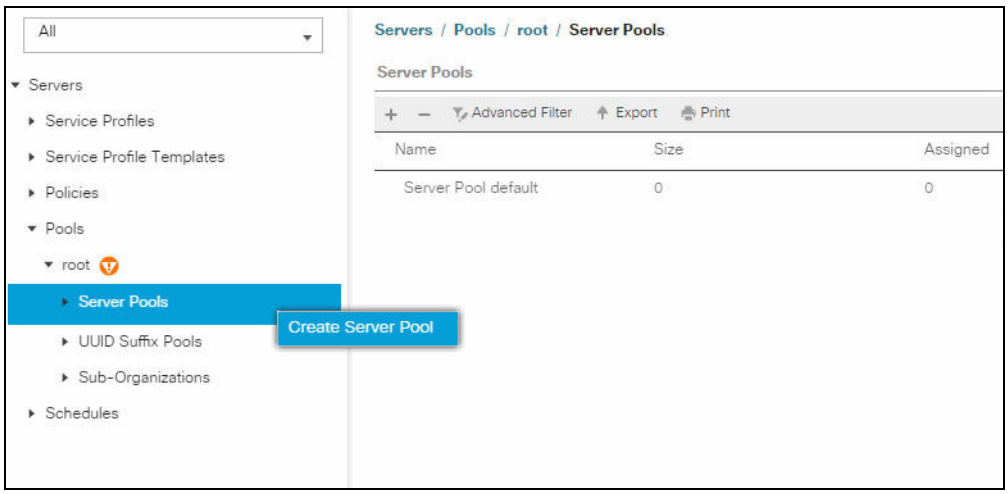


Figure 5-11 Create server pool

4. Enter `Infra_Pool` as the name of the server pool.
5. (Optional) Enter a description for the server pool.
6. Click **Next**.

7. Select two (or more) servers to be used for the Infra_Pool cluster and click **>>** to add them to the Infra_Pool server pool.
8. Click **Finish**, and then click **OK**.

5.3.3 Creating a host firmware package

The administrator can use firmware management policies to select the corresponding packages for a server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a server configuration in the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Policies** → **root**.
3. Right-click **Host Firmware Packages** and select **Create Host Firmware Package**, as shown in Figure 5-12.

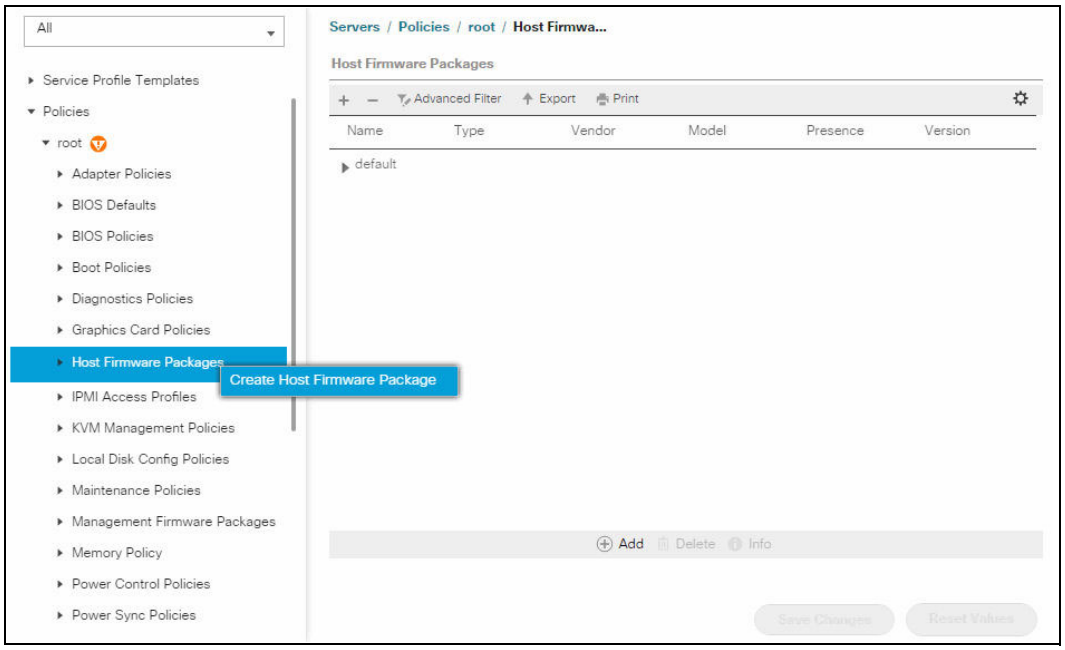


Figure 5-12 Create host firmware package

4. Enter `HyperV-Hosts` as the name of the host firmware package.
5. Leave **Simple** selected.
6. Select the Version 3.2(1d) for both Blade Servers and Rack Package.

7. Leave Excluded Components with only Local Disk selected, and click **OK** to create the host firmware package, as shown in Figure 5-13.

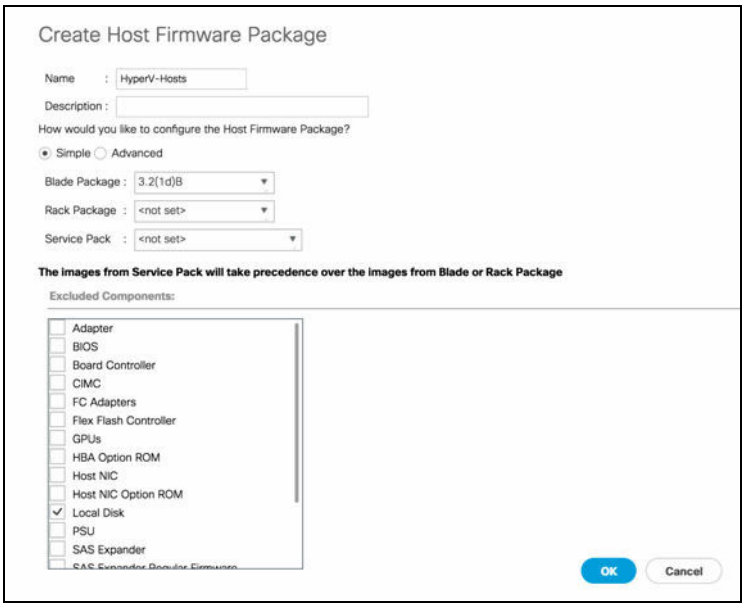


Figure 5-13 Creating host package

8. Click **OK** again.

5.3.4 Creating a local disk configuration policy

The procedure in this section creates a SAN boot disk policy. A local disk configuration for the Cisco UCS environment is necessary if the servers in the environment do not have a local disk.

Important: Do not use this policy on servers that contain local disks.

To create a local disk configuration policy for SAN boot, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Policies** → **root**.

3. Right-click **Local Disk Config Policies** and select **Create Local Disk Configuration Policy**, as shown in Figure 5-14.

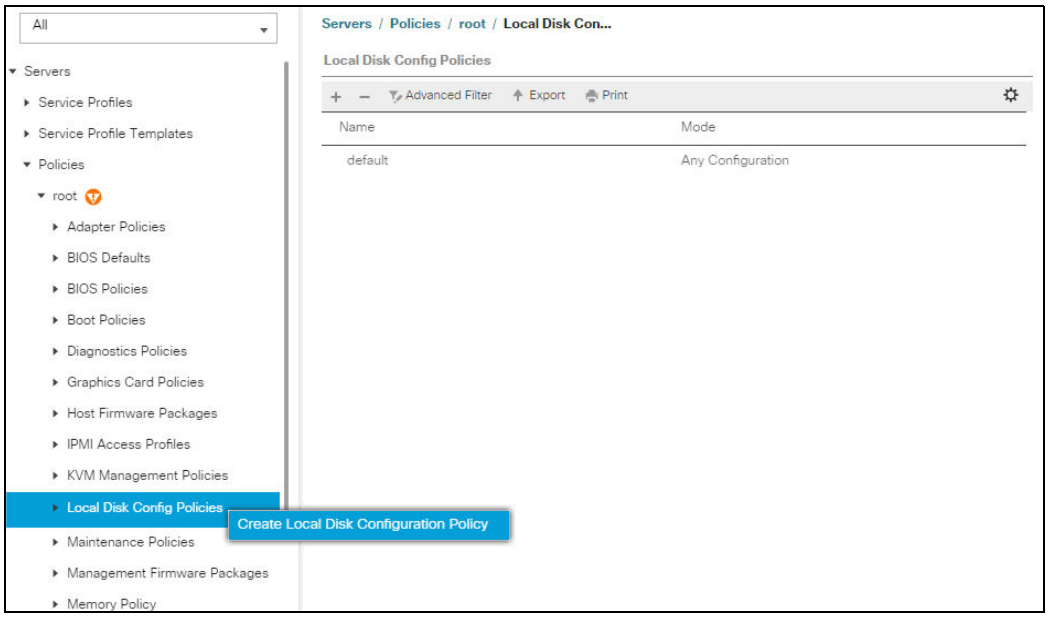


Figure 5-14 Create Local Disk Configuration Policy

4. Enter `SAN-Boot` as the local disk configuration policy name. Change the mode to **No Local Storage**, and click **OK** to create the local disk configuration policy. See Figure 5-15.

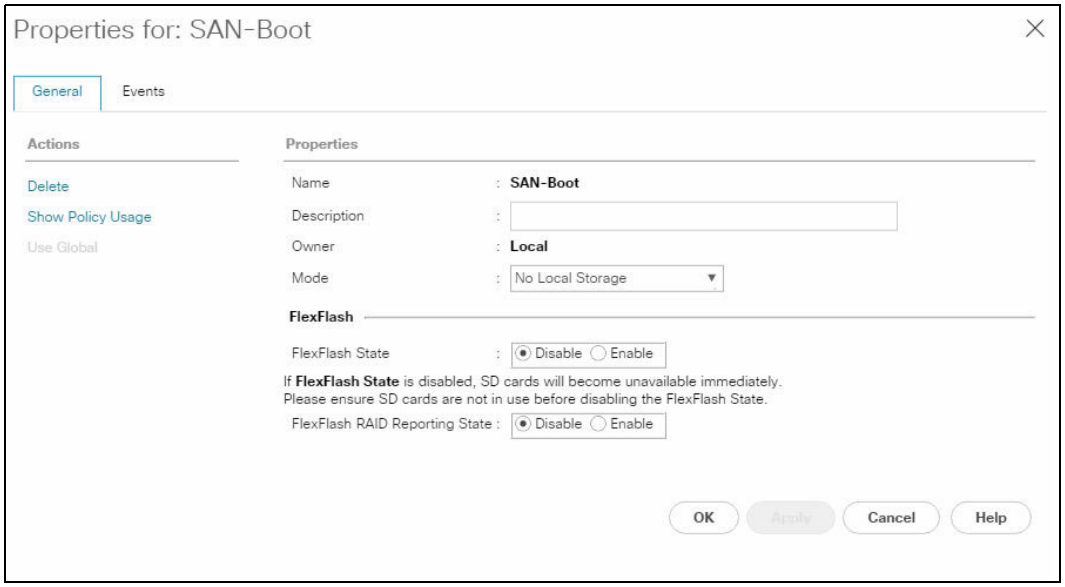


Figure 5-15 Create the policy

5. Click **OK** again.

5.3.5 Creating a power control policy

To create a power control policy for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Policies** → **root**.
3. Right-click **Power Control Policies**, and select Create Power Control Policy.
4. Enter `No-Power-Cap` as the power control policy name. Change the Power Capping setting to **No Cap**, and then click **OK** to create the power control policy. See Figure 5-16.

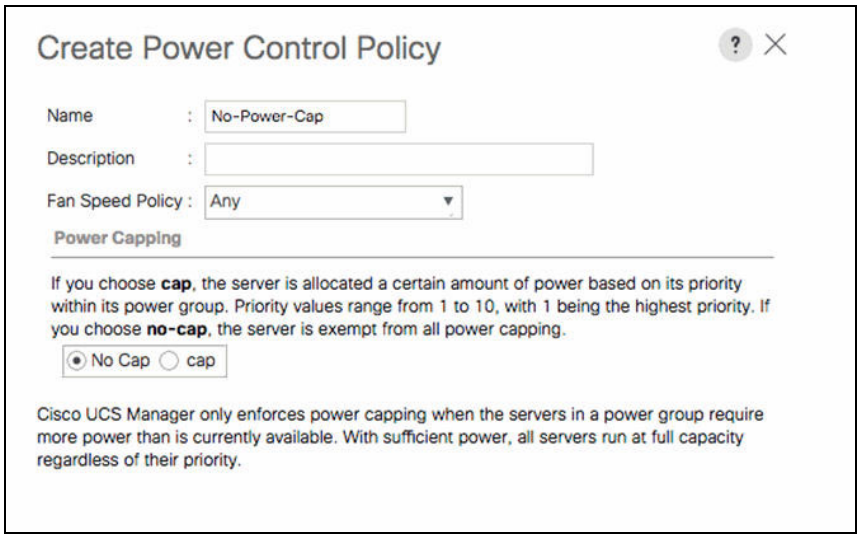


Figure 5-16 Create Power Control Policy

5. Click **OK** again.

5.3.6 Creating a server pool qualification policy (optional)

To create an optional server pool qualification policy for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Policies** → **root**.
3. Right-click **Server Pool Policy Qualifications** and select **Create Server Pool Policy Qualification**.

4. Enter `UCSB-B200-M5` as the name for the policy. Select **Create Server PID Qualifications**, and then enter `UCSB-B200-M5` as the PID. Click **OK** to create the server pool qualification policy. See Figure 5-17.

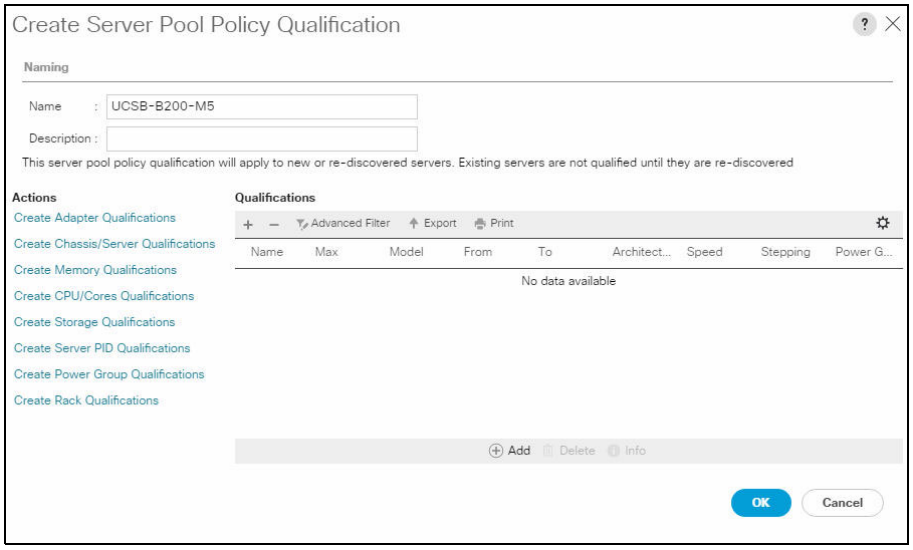


Figure 5-17 Create Server PID Qualifications

5. Click **OK** again.

5.3.7 Creating a Server BIOS policy

The following policies are for optimal performance for the Hyper-V. Depending on your requirements, you can change the settings as needed. For more information, see your Cisco UCS documentation.

To create a server BIOS policy for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Policies** → **root**.

3. Right-click **BIOS Policies** and select **Create BIOS Policy**. Enter `HyperV-Hosts` as the BIOS policy name, and click **OK**. See Figure 5-18.

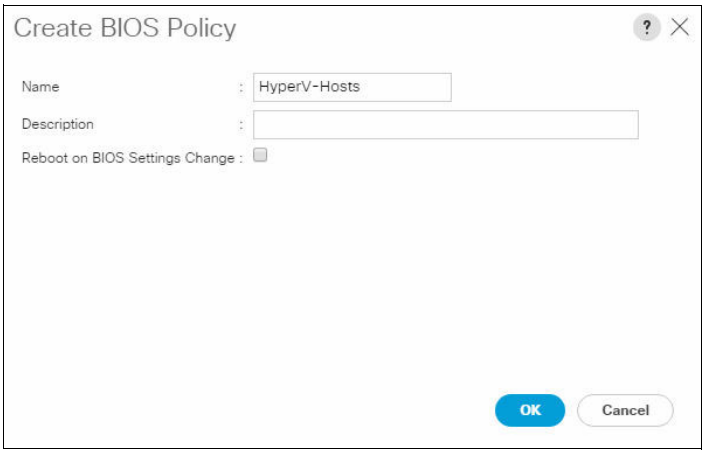


Figure 5-18 Creating the BIOS policy

4. Using the Main tab of the Policy (Figure 5-19), make the following changes:
   - Change CDN Control to *Enabled*
   - Change the Quiet Boot setting to *Disabled*

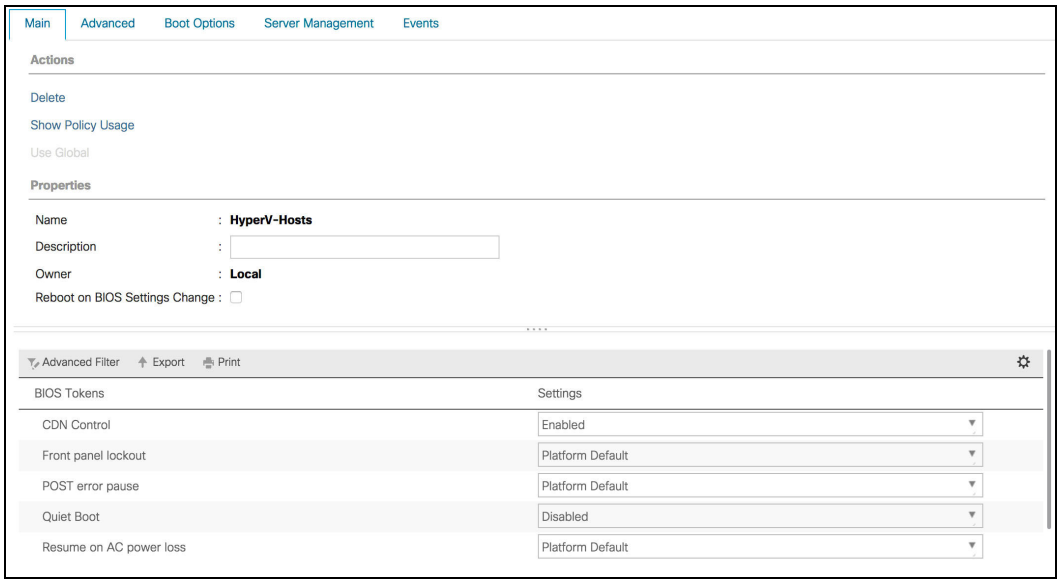


Figure 5-19 Main properties of BIOS policy

5. Select the options **Advanced** → **Processor**, as shown in Figure 5-20, and make the following changes:
   a. Change DRAM Clock Throttling to *Performance*.
   b. Change Frequency Floor Override to *Enabled*.
   c. Change Processor C State to *Disabled*.

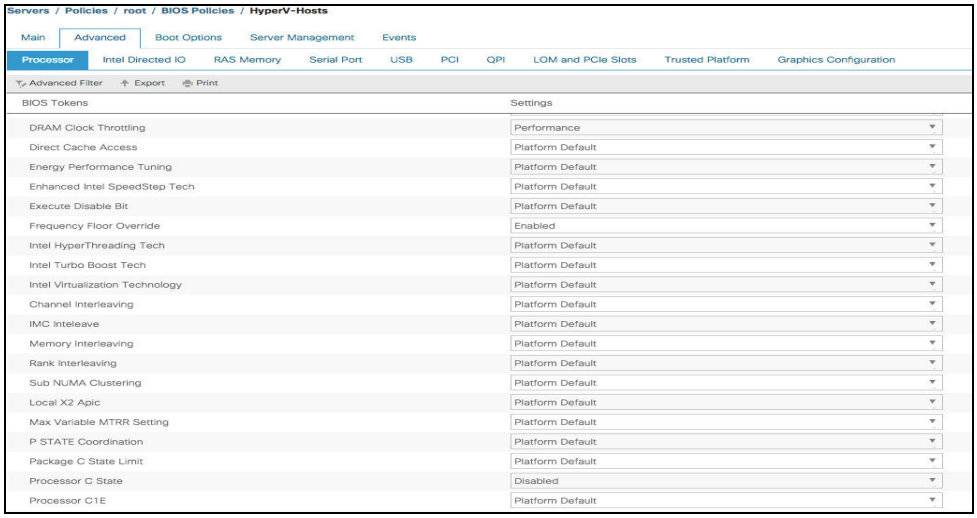


Figure 5-20 Advanced properties options

6. Scroll down and continue to update the following information, as shown in Figure 5-21:
   a. Change Processor C1E to *Disabled*.
   b. Change Processor C3 Report to *Disabled*.
   c. Change Energy Performance to *Performance*.

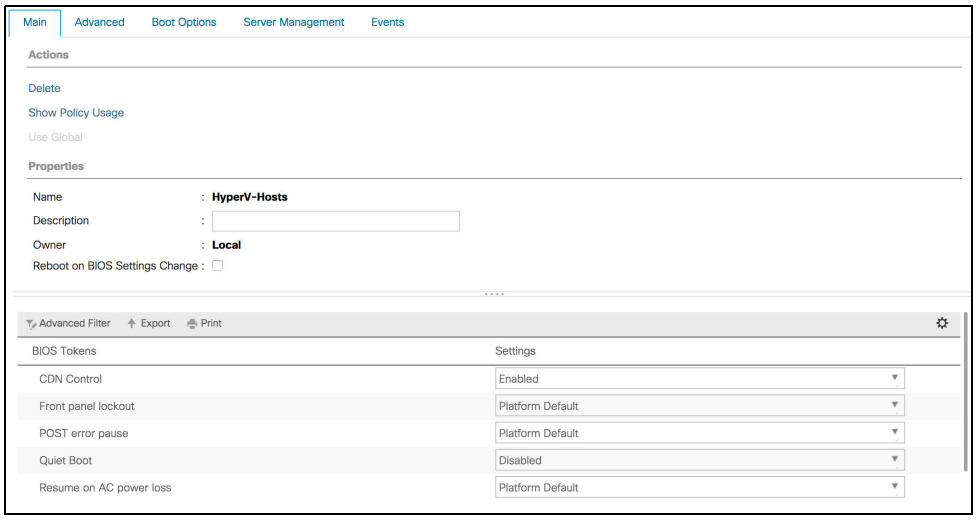


Figure 5-21 Advanced processor options

7. In the RAS Memory tab, change LV DDR Mode to *Performance Mode*.
8. Click **Save Change** to commit the changes, and then click **OK**.

9. Click **Next** and go to the RAS Memory tab. Change LV DDR Mode to *Performance Mode*, As shown in Figure 5-22.

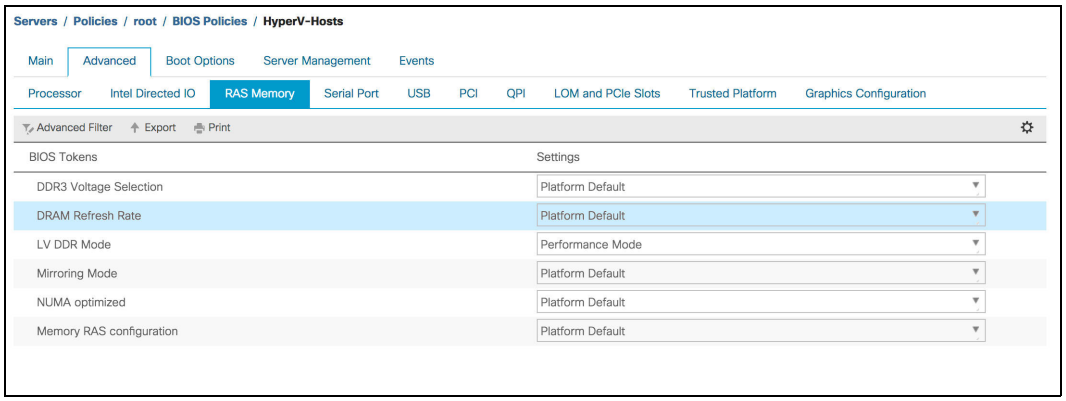


Figure 5-22 RAS Memory

10. Click **Finish** to create the BIOS policy, and then click **OK**.

5.3.8 Creating a vNIC/vHBA placement policy for the VM infrastructure hosts

To create a vNIC/vHBA placement policy for the VM infrastructure hosts, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Policies** → **root**.
3. Right-click **vNIC/vHBA Placement Policies** and select **Create Placement Policy**.
4. Enter `HyperV-Host` as the name of the placement policy. Click **1** and select **Assigned Only**, as shown in Figure 5-23. Click **OK**.

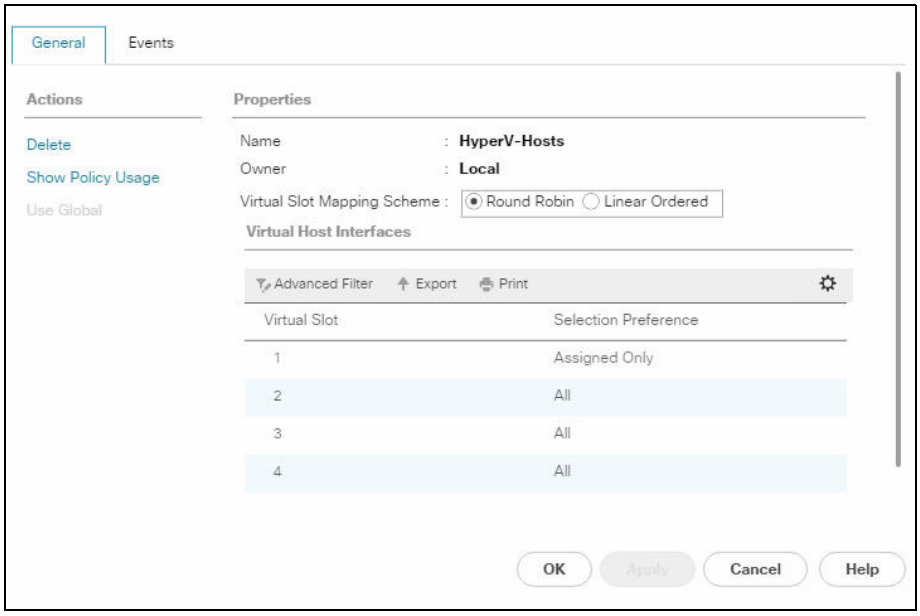


Figure 5-23 vNIC and vHBA placement policy

5. Click **OK** again.

5.3.9 Updating the default Maintenance Policy

To update the default Maintenance Policy, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Policies** → **root**.
3. Click **Maintenance Policies** → **default**.
4. Change the Reboot Policy to **User Ack**. See an example in Figure 5-24.

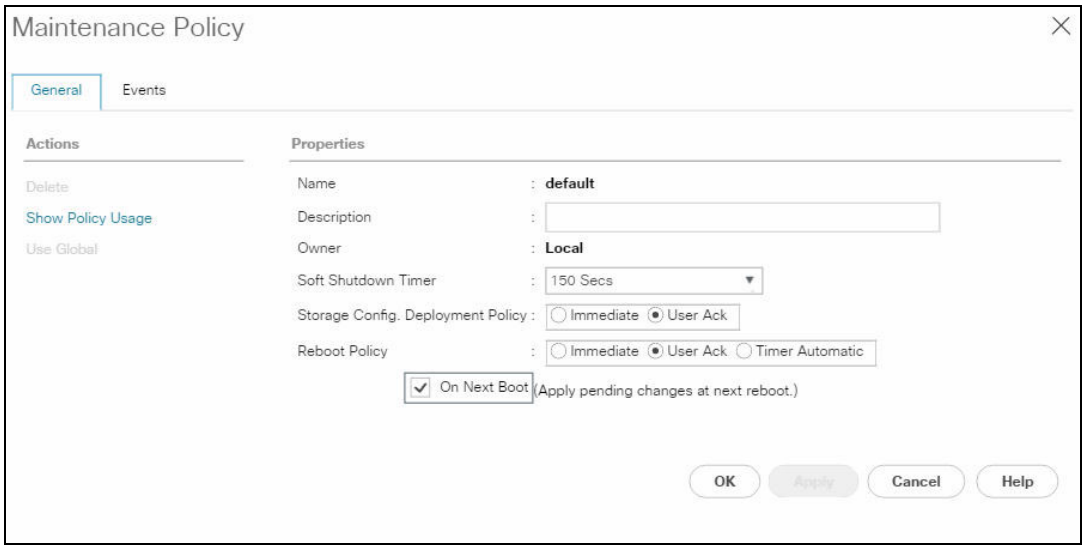


Figure 5-24 Maintenance Policy

5. Click **OK** to accept the change.
6. Click **Save Changes**.

5.4 Configuring UCS SAN connectivity

The next sections show the steps that are required to enable SAN connectivity for your VersaStack UCS environment.

5.4.1 Configuring unified ports

Important: Ensure that you reconfigure on the subordinate switch to save time before you begin this process.

To enable the server and FC uplink ports, complete the following steps:

1. On the Equipment tab, select **Fabric Interconnect A or B**, which should be the subordinate Fabric Interconnects, and then select **Configure Unified Ports** as shown in Figure 5-25 on page 63. Click **Yes**.

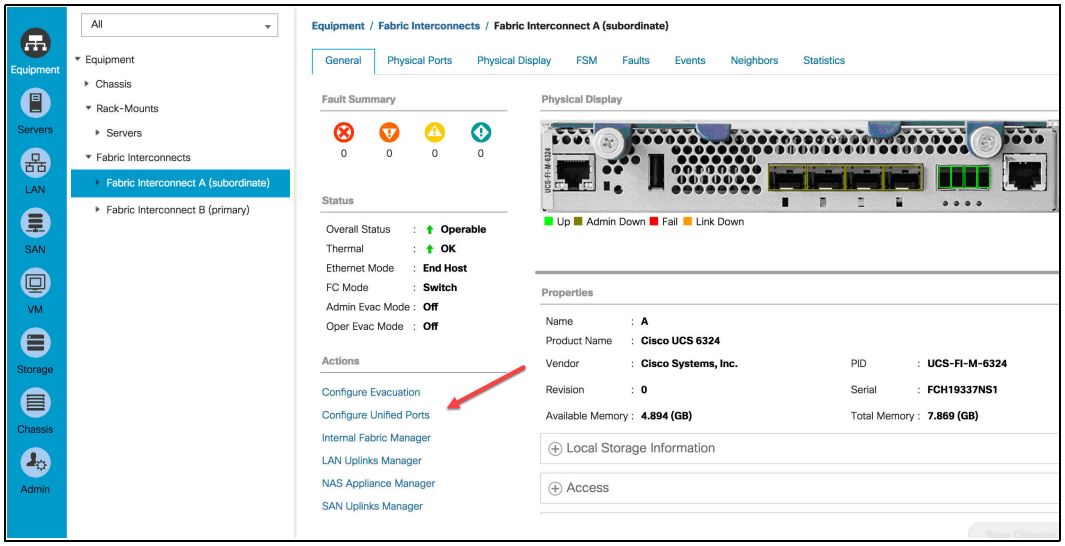


Figure 5-25 Configure Unified Ports

2. Slide the lever to change the ports 1-2 to change the ports to FC. Click **Finish** and then click **Yes** to the reboot message. Click **OK** to commit the changes. See an example in Figure 5-26.

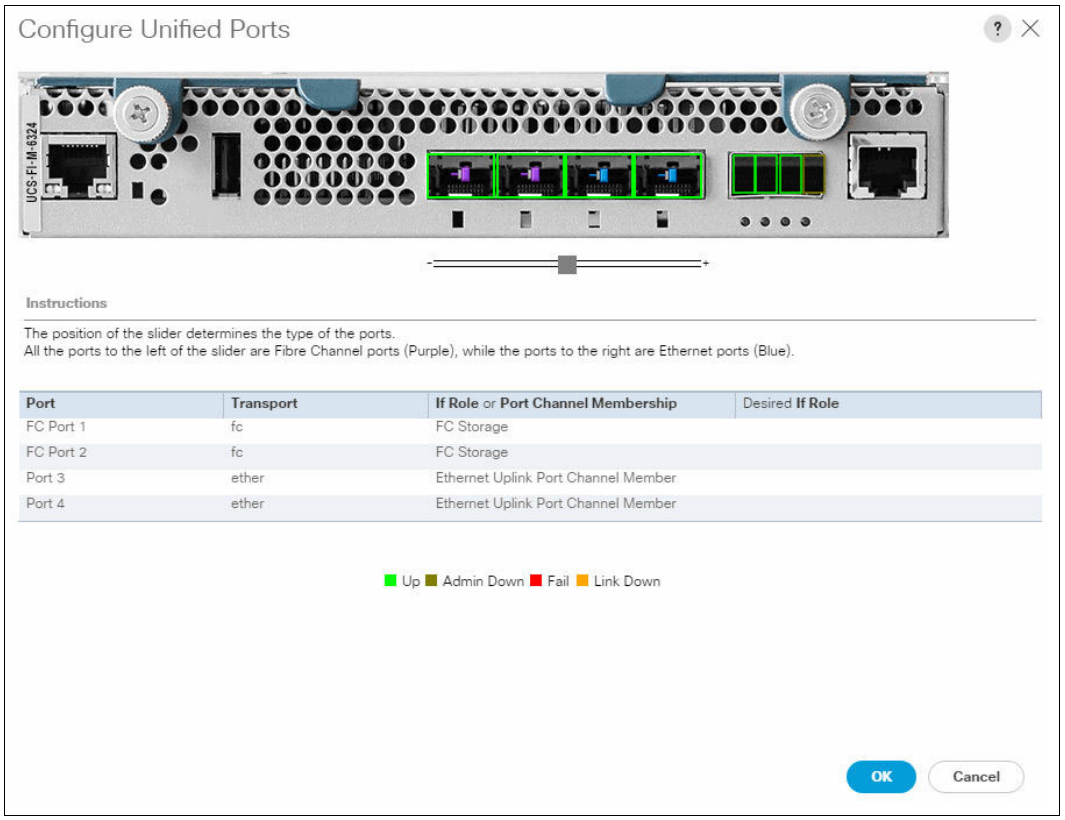


Figure 5-26 Configuring Unified Ports 1 and 2

3. When the subordinate has completed the reboot, select the Primary Fabric Interconnect (A or B), and then select **Configure Unified Ports**. Then, click **Yes**.

4. Slide the bar to the left to select ports 1-2 for FC (purple), click **Finish**, and click **Yes** in response to the restart message. You must log in to the client again after the restart of the Fabric Interconnects complete.

5.4.2 Configure Fabric Interconnects in FC switching mode

Switching FC modes requires the Fabric Interconnects to restart. The restart takes place automatically. When the Fabric Interconnects complete the restart process, a new management session must be established to continue with management and configuration.

Complete the following steps to configure Fabric Interconnects in FC switching mode:

1. Go to the Equipment tab in the left pane, as shown in Figure 5-27, and expand the **Fabric Interconnects** object.

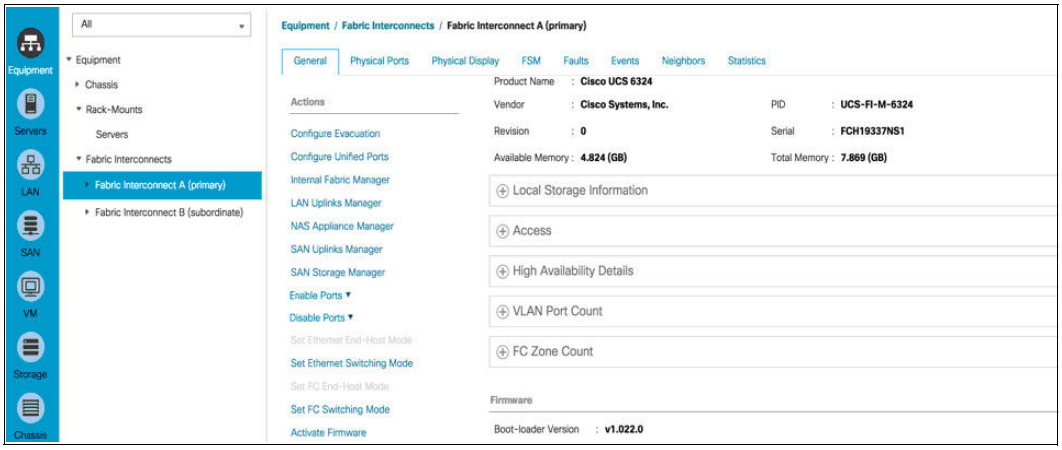


Figure 5-27 Check fabric interconnects

2. Select **Fabric Interconnect A**, in the left pane. Then, go to the General tab, and click **Set FC Switch Mode** in the left pane.
3. Click **Yes** and then **OK**.
4. Repeat step 2 for **Fabric Interconnect B**.
5. Wait for the Fabric Interconnects to restart before proceeding. This process can take approximately 5 minutes for the restart of both nodes.

5.4.3 Creating storage virtual storage area networks

To configure the necessary virtual storage area networks (VSANs) and FC port channels for the Cisco UCS Mini environment, complete the following steps:

1. Go to the SAN tab and expand the **Storage Cloud** tree.
2. Right-click **VSANs** and choose **Create Storage VSAN**. In the window shown in Figure 5-28 on page 65, complete the following information:
   a. Enter `VSAN_A` as the VSAN name for Fabric A opens.
   b. Select **Fabric A**.
   c. Enter the VSAN ID 101 for Fabric A.
   d. Enter the FCoE VLAN ID 101 for Fabric A.
3. Click **OK**.

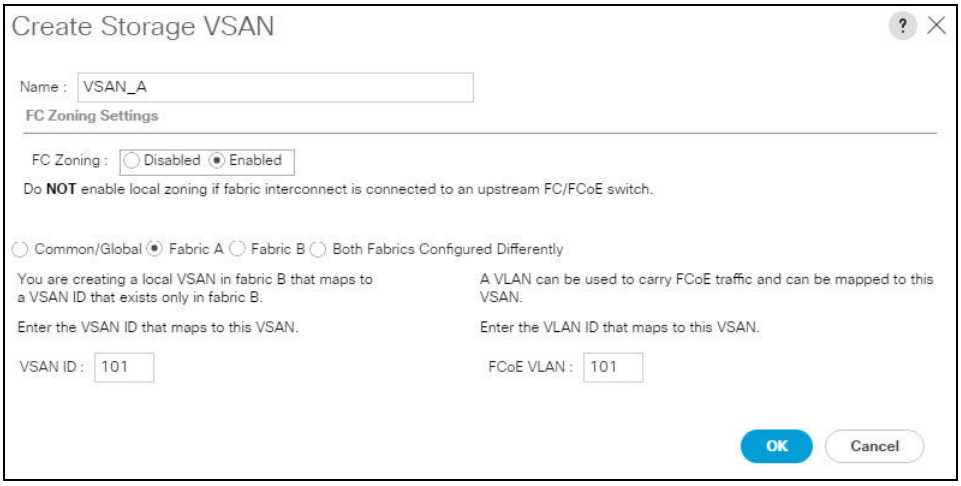


Figure 5-28 Create storage VSAN-A

4. Click **OK** again to create the VSAN.
5. Right-click **VSANs** and select **Create Storage VSAN** to create a VSAN for Fabric B. Then, enter the following information, as shown in Figure 5-29:
   a. Enter `VSAN_B` as the VSAN name for Fabric B.
   b. Select **Enabled** under the FC Zoning Settings.
   c. Select **Fabric B**.
   d. Enter the VSAN ID 102 for Fabric B.
   e. Enter the FCoE VLAN ID 102 for Fabric B.
   f. Click **OK**.

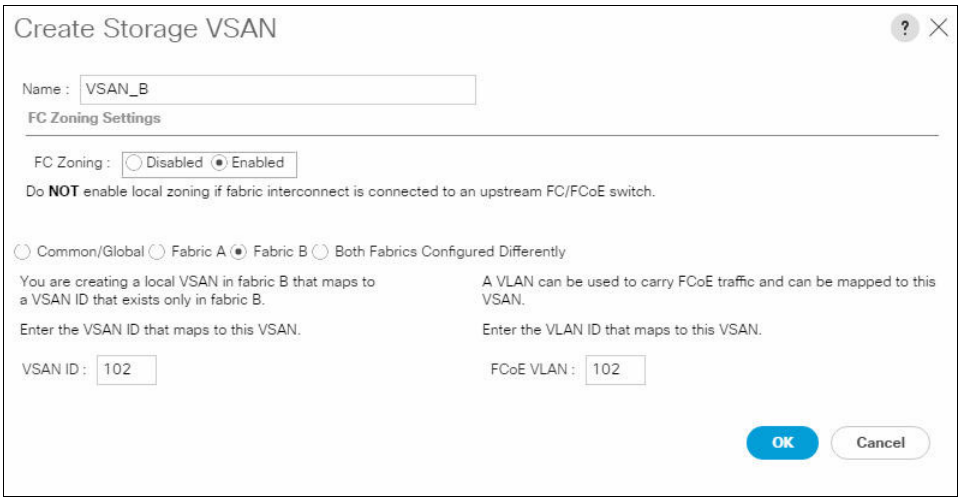


Figure 5-29 Create storage VSAN-B

6. Click **OK** again to create the VSAN.

5.4.4 Configuring the FC storage ports

To configure the FC storage ports, complete the following steps:

1. Go to the Equipment tab and click **Equipment** → **Fabric Interconnects** → **Fabric Interconnect B (primary)** → **Fixed Module**.
2. Expand the **FC Ports** object.
3. Select **FC Ports 1 and 2**, which is connected to the IBM storage array, and click **Configure as FC Storage Port** as shown in Figure 5-30.

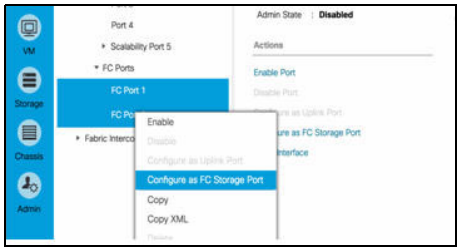


Figure 5-30 Configuring as FC ports

4. Click **Yes**, and then click **OK**.
5. Assign the `VSAN_B` (102) that you created to FC1 and FC2 storage ports on the General tab, and click **Save Changes**. Then click **OK**.
6. Repeat the steps for FC ports 1-2 in Fabric Interconnects A, and be sure to assign `VSAN_A` (101).

5.4.5 Creating WWNN pools

To configure the necessary worldwide node name (WWNN) pools for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the SAN tab in the navigation pane.
2. Click **Pools** → **root**.
3. Right-click **WWNN Pools** and select **Create WWNN Pool**.
4. Enter `WWNN_Pool` as the name of the WWNN pool.
5. (Optional) Add a description for the WWNN pool.
6. Click **Next**.
7. Click **Add** to add a block of WWNNs.
8. Keep the default block of WWNNs, or specify a base WWNN.
9. Specify a size for the WWNN block that is sufficient to support the available blade or server resources, as shown in Figure 5-31 on page 67. Then, click **OK**.

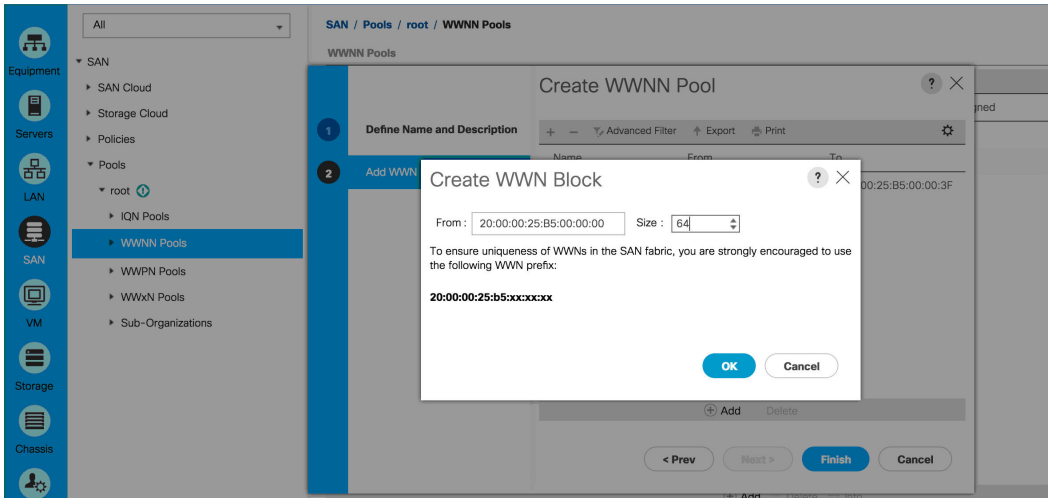


Figure 5-31 Create WWNN block

10. Click **Finish**.

    Figure 5-32 shows the properties of WWNN created.

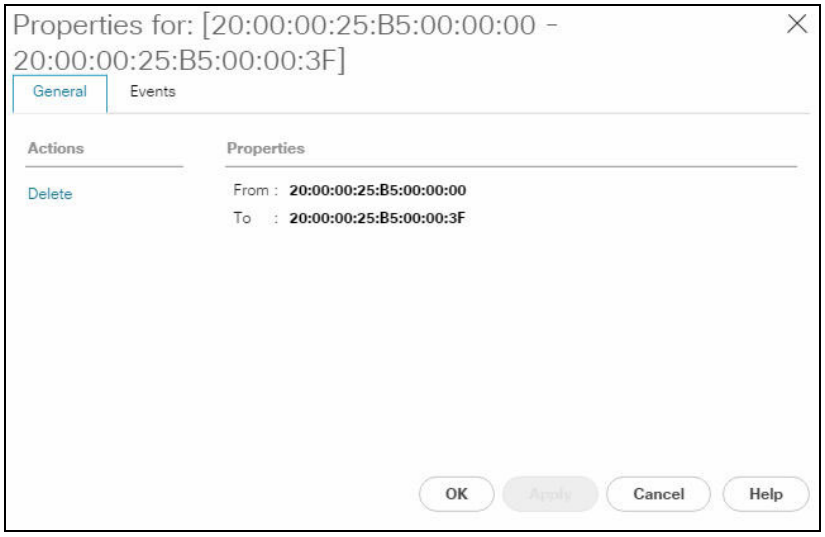


Figure 5-32 Create the WWNN pool

11. Click **OK**.

5.4.6 Creating WWPN pools

Terminology note: The worldwide port name (WWPN) is the name that is assigned to a port in a Fibre Channel fabric. This name is used on storage area networks and performs a function equivalent to the MAC address in Ethernet protocol as a unique identifier in the network.

To configure the necessary WWPN pools for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the SAN tab in the navigation pane.
2. Click **Pools** → **root**.
3. Right-click **WWPN Pools** and select **Create WWPN Pool**.

Note: This procedure creates the following WWPN pools:

- One for fabric A
- One for fabric B

4. Enter `WWPN_Pool_A` as the name of the WWPN pool for Fabric A. See Figure 5-33.

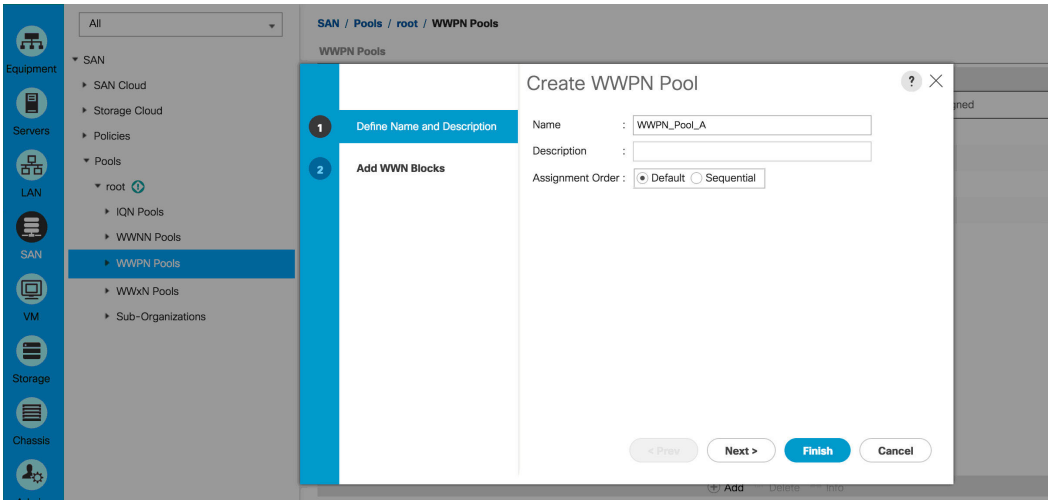


Figure 5-33 Creating WWPN Pool

5. (Optional) Enter a description for this WWPN pool.
6. Click **Next**.
7. Click **Add** to add a block of WWPNs.

8. Specify the starting WWPN in the block for Fabric A, as shown in Figure 5-34.

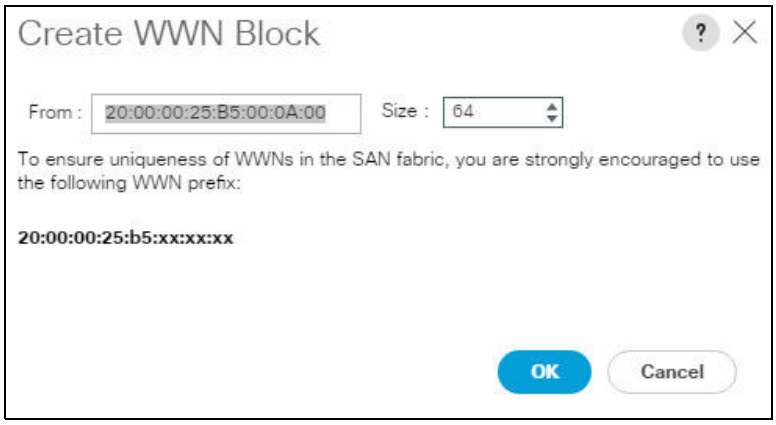


Figure 5-34 Creating the WWN Block

Note: For the VersaStack solution, place 0A in the next-to-last octet of the starting WWPN to identify all the WWPNs in this pool as Fabric A addresses.

9. Specify a size for the WWPN block that is sufficient to support the available blade or server resources.
10. Click **OK**.
11. Click **Finish** to create the WWPN pool, as shown in Figure 5-35.

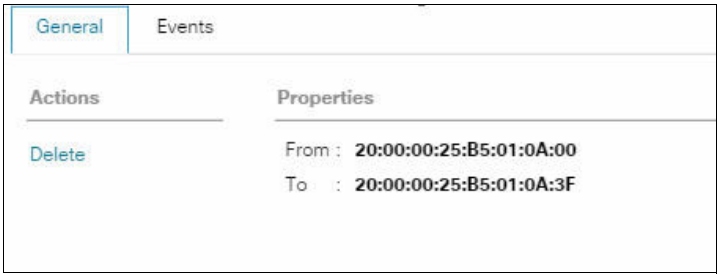


Figure 5-35 Create the WWPN pool

12. Click **OK** to proceed with WWPN Pools for Fabric B.
13. Right-click **WWPN Pools**, and then click **Create WWPN Pool**.
14. Enter `WWPN_Pool_B` as the name for the WWPN pool for Fabric B.
15. (Optional) Enter a description for this WWPN pool.
16. Click **Next**.
17. Click **Add** to add a block of WWPNs.
18. Enter the starting WWPN address in the block for Fabric B.

Note: For the VersaStack solution, place 0B in the next to last octet of the starting WWPN to identify all the WWPNs in this pool as Fabric B addresses.

19. Specify a size for the WWPN block that is sufficient to support the available blade or server resources.

20. Click **OK**.
21. Click **Finish**.
22. Click **OK**.

Figure 5-36 shows successful pool creation.

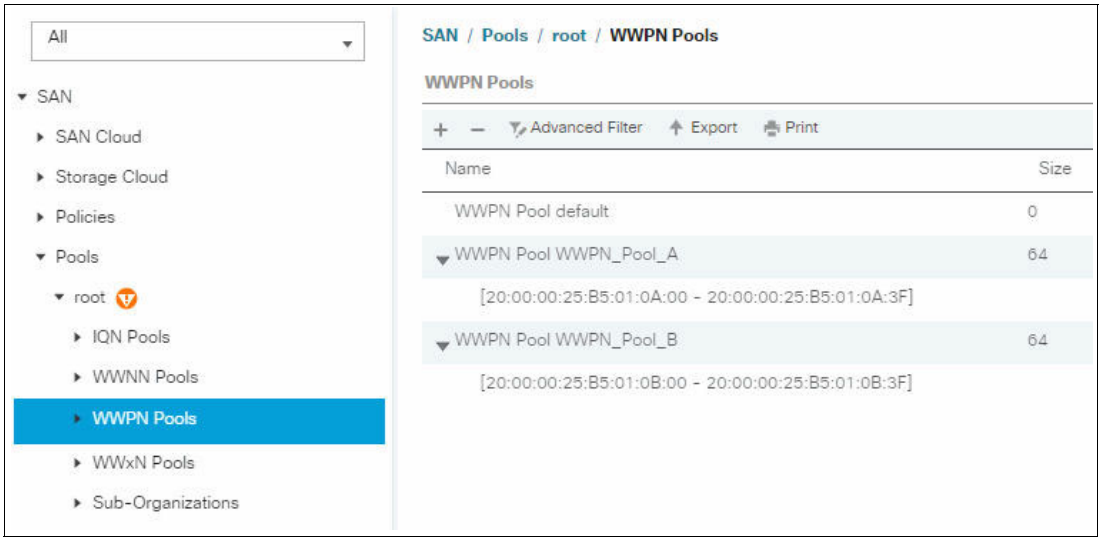


Figure 5-36 Check pool creation

5.4.7 Creating virtual HBA templates for Fabric A and Fabric B

To create multiple virtual host bus adapter (HBA) templates for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the SAN tab in the navigation pane.
2. Click **Policies** → **root**.
3. Right-click **vHBA Templates** and select **Create vHBA Template**. Then, to create the first virtual HBA template, complete the following information, as shown in Figure 5-37 on page 71:
   a. Enter `vHBA_Template_A` as the virtual HBA template name.
   b. Select **A** for Fabric ID.
   c. In the Select VSAN list, select **VSAN_A**.
   d. In the WWPN Pool list, select **WWPN_Pool_A**.
   e. Click **OK** to create the virtual HBA template.

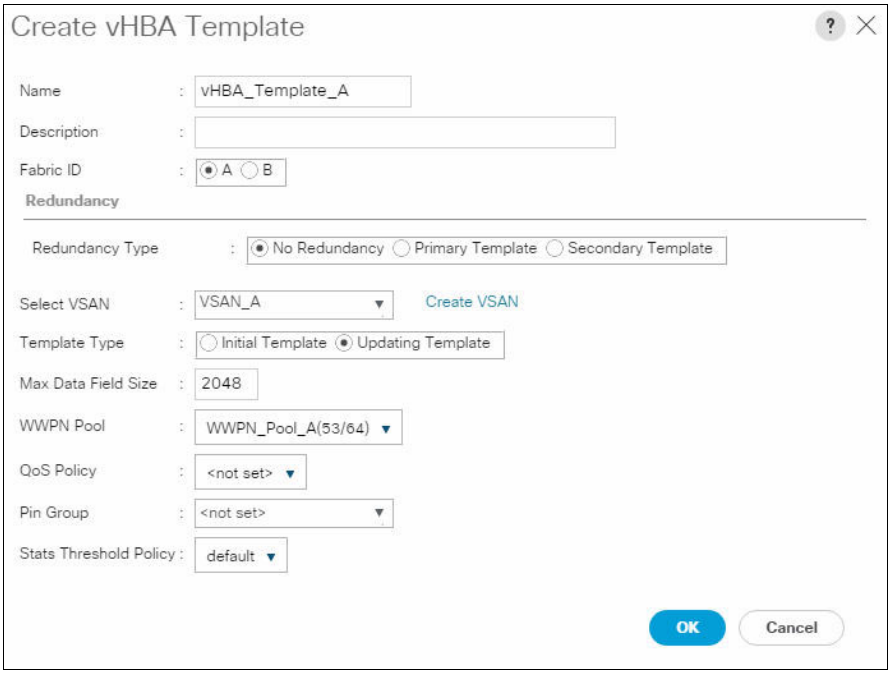


Figure 5-37 Creating the first virtual HBA template

4. Click **OK** again.
5. In the navigation pane, go back to the SAN tab.
6. Click **Policies** → **root**, and right-click **vHBA Templates**.
7. Select **Create vHBA Template**. To create the second virtual HBA template, complete the following information, as shown in Figure 5-38 on page 72:
   a. Enter `vHBA_Template_B` as the virtual HBA template name.
   b. Select **B** for Fabric ID.
   c. In the Select VSAN list, select **VSAN_B**.
   d. In the WWPN Pool, select **WWPN_Pool_B**.
   e. Click **OK** to create the virtual HBA template.

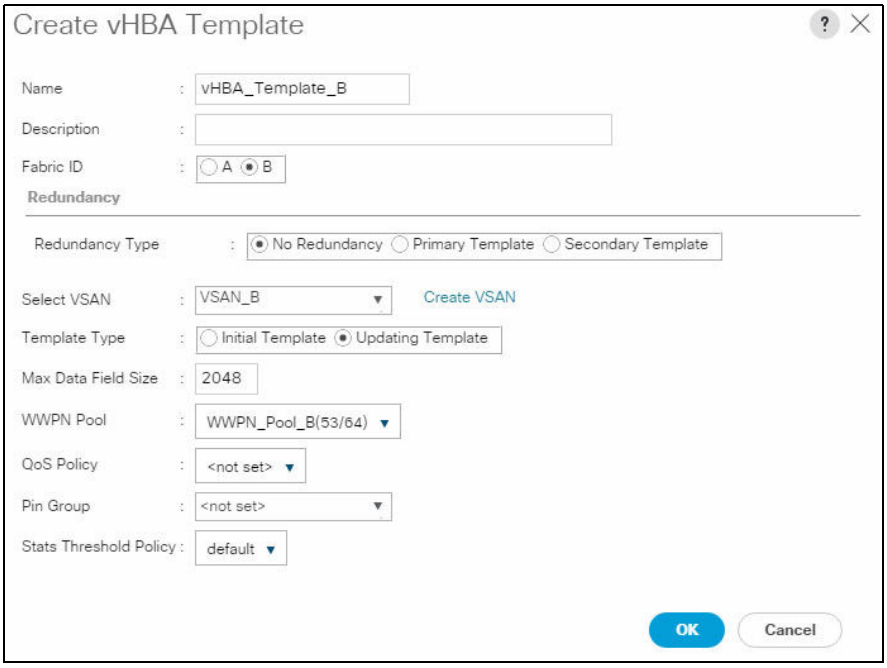


Figure 5-38 Creating the second virtual HBA template

8. Click **OK** again.

5.4.8 Creating boot policies

This procedure applies to a Cisco UCS Mini environment in which two FC interfaces are used on the IBM FlashSystem 5030 Node 1 and two FC Interfaces are used on Node 2. This procedure captures a single boot policy that defines Fabric-A as the primary fabric. You can choose to create a second boot policy, which uses Fabric-B as the primary fabric, to spread the boot-from-SAN traffic load on both nodes in case of disaster recovery.

You need the WWPN from the IBM FlashSystem 5030 to complete the example in this section. You can find this number by logging in to the IBM Storwize GUI and then hovering the mouse over the FC ports, as shown in the Figure 5-39.

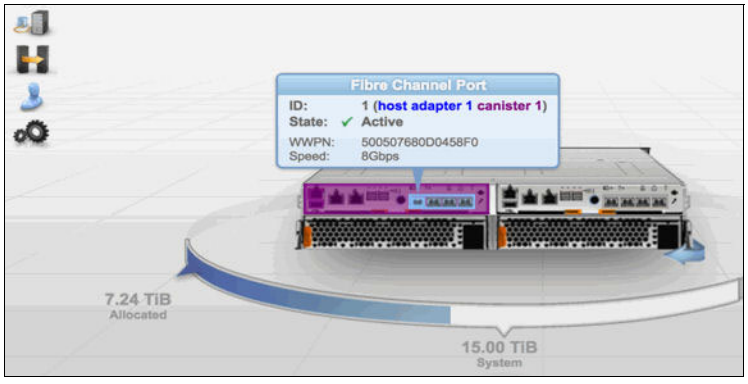


Figure 5-39 Visualizing WWPN of IBM Storwize FC ports

Use Table 5-1 to record the WWPN information.

Table 5-1 IBM FlashSystem 5030 WWPN information

Node	Port ID	WWPN	Variable
Node 1	1		WWPN-Node1-Fabric-A
Node 1	2		WWPN-Node1-Fabric-B
Node 2	1		WWPN-Node2-Fabric-A
Node 2	2		WWPN-Node2-Fabric-B

The initial boot policy provides a single path to the SAN. If more than one path is defined to the boot volume and if there is no multipath software available, as is the case for an initial installation of Windows Server 2016, data corruption can occur on the disk. After installing the operating system and enabling the MPIO feature, you can define the secondary boot path.

WWPN variables: Use the WWPN variables that you noted in Table 5-1.

To create boot policies for the Cisco UCS Mini environment, complete the following steps.

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Policies** → **root**.
3. Right-click **Boot Policies** and select **Create Boot Policy**. Then, complete the following information, as shown in Figure 5-40:
   a. Enter `Boot-Fabric-A` as the name of the boot policy.
   b. (Optional) Enter a description for the boot policy.
   c. Keep the **Reboot on Boot Order Change** option clear.

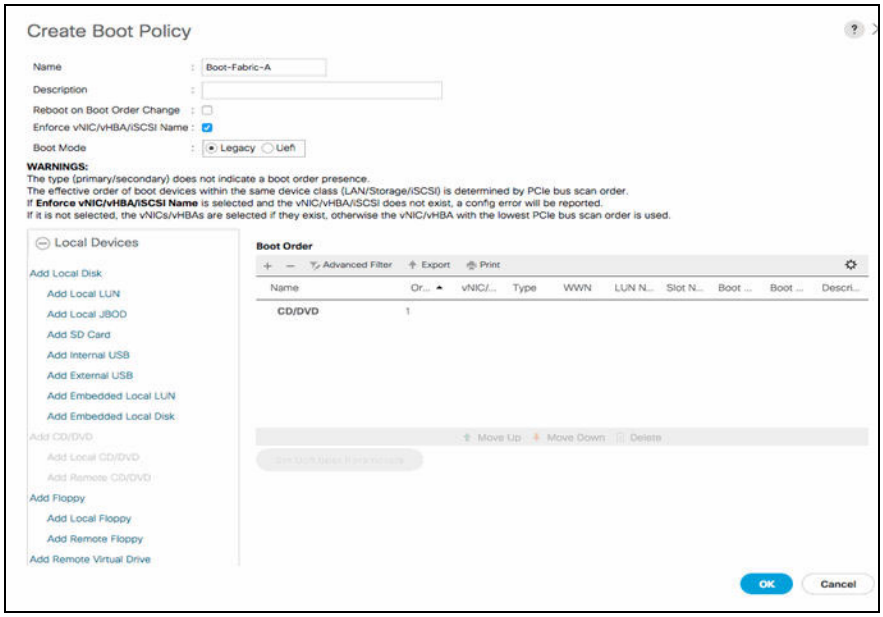


Figure 5-40 Creating a boot policy: Boot order

4. Expand the **Local Devices** drop-down menu, and click **Add CD/DVD**. The Local and Remote options are disabled.

5. Scroll down on the left side, expand the **vHBAs** drop-down menu, and click **Add SAN Boot**. Complete the following information, as shown in Figure 5-41:
   - Enter Fabric-A in the vHBA field.
   - Make sure that the **Primary** option is selected as the SAN boot type.
   - Click **OK** to add the SAN boot initiator.

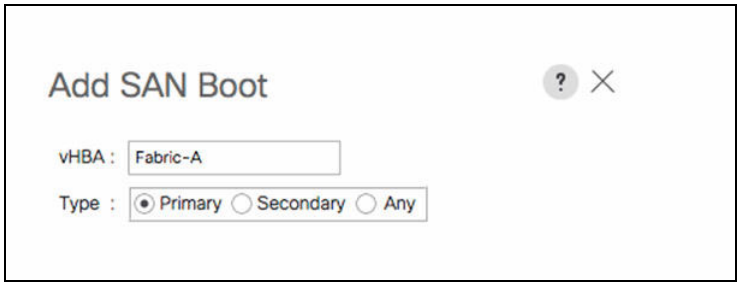


Figure 5-41 Adding the SAN boot initiator

6. From the **vHBA** drop-down menu, select **Add SAN Boot Target**. Then, complete the following information, as shown in Figure 5-42:
   - Keep 0 as the value for Boot Target LUN.
   - Enter the WWPN for node 1 going to switch A.
   - Keep the **Primary** option selected as the SAN boot target type.
   - Click **OK** to add the SAN boot target.

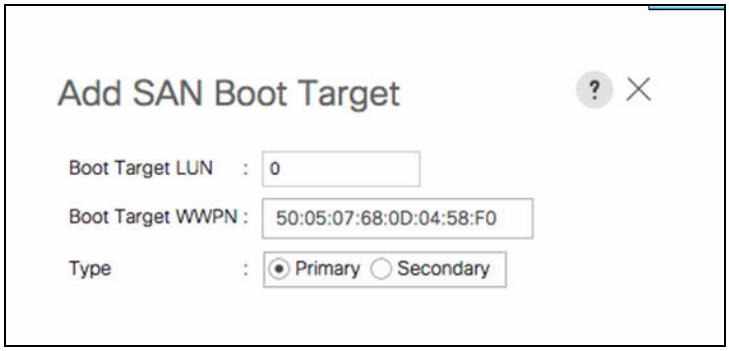


Figure 5-42 Adding the primary SAN boot target

5.5 Configuring UCS LAN connectivity

This section describes the LAN connectivity aspects for your VersaStack Cisco UCS solution.

5.5.1 Creating uplink port channels to Cisco Nexus switches

To configure the necessary port channels out of the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the LAN tab in the navigation pane.

Port channels: This procedure creates the following port channels:

- One from fabric A to both Cisco Nexus switches
- One from fabric B to both Cisco Nexus switches

2. Click **LAN** → **LAN Cloud** and expand **Fabric A** tree. Then, right-click **Port Channels** and select **Create Port Channel**.
3. Enter `13` as the unique ID of the port channel, and enter `vPC-13-Nexus` as the name of the port channel. (See Figure 5-43.) Click **Next**.

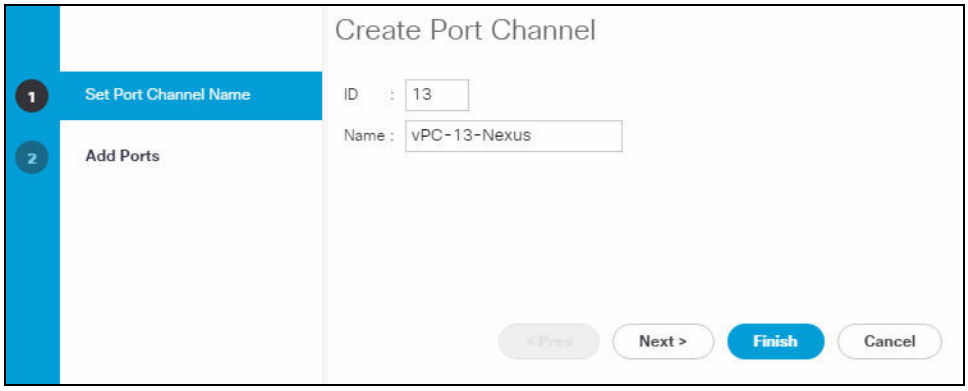


Figure 5-43 Setting the port channel name

4. Select the following ports to be added to the port channel, as shown in Figure 5-44:
   - Slot ID 1 and port 3
   - Slot ID 1 and port 4
5. Click **>>** to add the ports to the port channel. Then, click **Finish** to create the port channel.

Figure 5-44 Adding ports

6. Click **OK**.

Complete the next items to create a port channel for Fabric B.

1. In the navigation pane, click **LAN** → **LAN Cloud** and expand **Fabric B**.
2. Right-click **Port Channels** and select **Create Port Channel**. Enter `14` as the unique ID of the port channel.

3. Enter `vPC-14-Nexus` as the name of the port channel, as shown in Figure 5-45. Click **Next**.

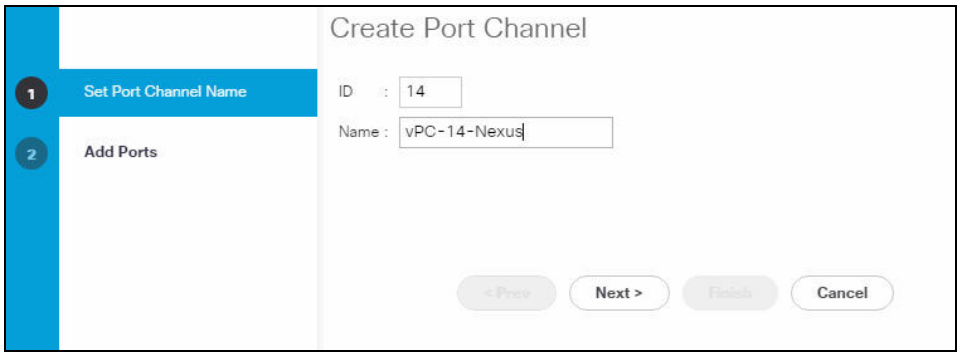


Figure 5-45 Set Port Channel Name

4. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 3
   - Slot ID 1 and port 4
5. Click **>>** to add the ports to the port channel, and then click **Finish** to create the port channel.
6. Click **OK**.

5.5.2 Creating MAC address pools

To configure the necessary MAC address pools for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the LAN tab in the navigation pane.
2. Click **Pools** → **root**.

> **Address pools:** This procedure creates one MAC address pool for each switching fabric.

3. Right-click **MAC Pools** under the root organization, and select **Create MAC Pool** to create the MAC address pool.
4. Enter `MAC_Pool_A` as the name of the MAC pool, and enter a description for the MAC pool (optional), as shown Figure 5-46. Click **Next**.

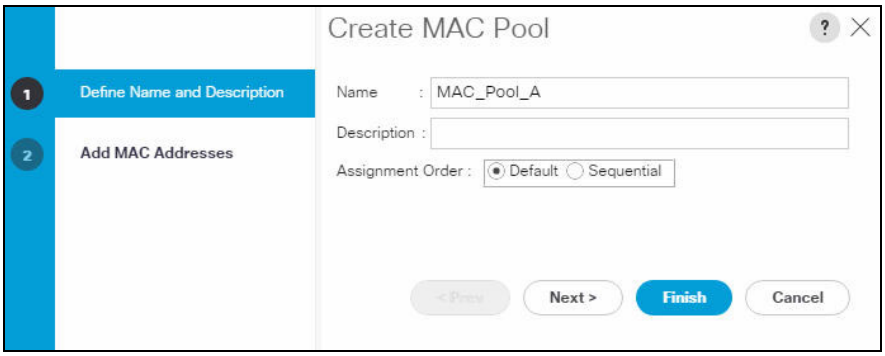


Figure 5-46 Creating a new MAC pool

5. Click **Add**. Specify a starting MAC address, as shown in Figure 5-47. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources. Then, click **OK**.

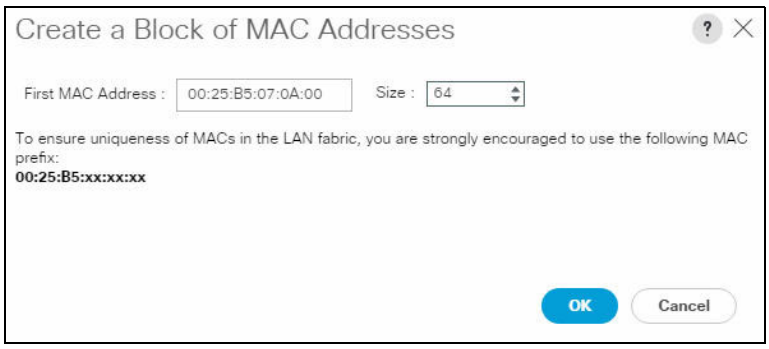


Figure 5-47 Specifying the MAC address size pool

Recommendation: For the VersaStack solution, place 0A in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as Fabric A addresses.

6. Click **Finish**.
7. In response to the confirmation message, click **OK**.

To create a second block of MAC addresses, complete the following steps:

1. Right-click **MAC Pools** under the root organization, and select **Create MAC Pool** to create the MAC address pool.
2. Enter `MAC_Pool_B` as the name of the MAC pool, and enter a description for the MAC pool (optional). Then, click **Next**.
3. Click **Add**. Specify a starting MAC address, as shown in Figure 5-48. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources. Then, click **OK**.

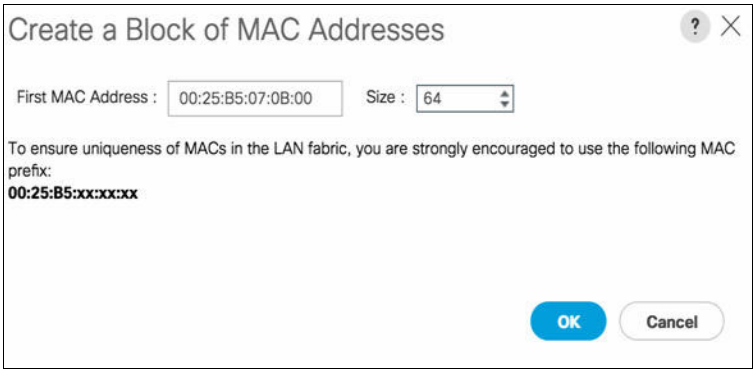


Figure 5-48 Adding a MAC address size pool (2)

Recommendation: For the VersaStack solution, place 0B in the next to last octet of the starting MAC address to identify all the MAC addresses in this pool as Fabric B addresses.

4. Click **Finish**.

5. In response to the confirmation message, click **OK**.

Figure 5-49 shows the results of creating the MAC pool.

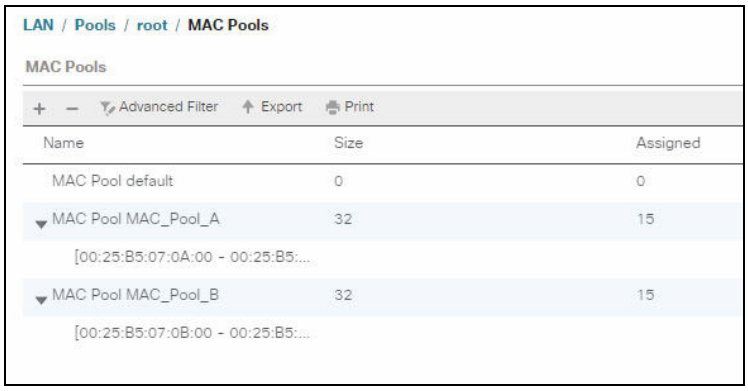


Figure 5-49 MAC pools created

5.5.3 Creating a virtual local area network

To configure the necessary virtual local area network (VLAN) for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the LAN tab in the navigation pane.

VLANs created: This procedure creates the following VLANs:

- The default VLAN ID 0 is used for Management.
- VLAN ID 3173 is used for Live Migration traffic.
- VLAN ID 3172 is for Windows Cluster traffic.
- VLAN ID 3174 is used for VM Tenant traffic.

2. Click **LAN** → **LAN Cloud**. Then, right-click **VLANs** and select **Create VLANs**.
3. Enter `IB-MGMT-VLAN` as the name of the VLAN to be used for management traffic. Keep the Common/Global option selected for the scope of the VLAN. Enter `11` as the ID of the management VLAN and the Sharing Type as None. Click **OK**. See Figure 5-50.

Figure 5-50 Creating the necessary VLANs

4. Click **OK** again.

Complete the next steps to create a cluster heartbeat VLAN:

1. Right-click **VLANs** and select **Create VLANs**.
2. Enter `MS-Cluster-VLAN` as the name of the VLAN to be used for Windows cluster heartbeat traffic. Keep the Common/Global option selected for the scope of the VLAN. Enter the `3172` for the Windows cluster VLAN and the Sharing Type as **None**.
3. Click **OK**, and then click **OK** again.

Complete the next steps to create Live Migration VLAN:

1. Right-click **VLANs** and select **Create VLANs**.
2. Enter `MS-LVMN` as the name of the VLAN to be used for Live Migration traffic. Keep the Common/Global option selected for the scope of the VLAN, and enter `3173` as the ID of the MS-LVMN VLAN. Keep the Sharing Type as **None**.
3. Click **OK**, and then click **OK** again.

Complete the next steps to create Tenant VLAN:

1. Right-click **VLANs** and select **Create VLANs**.
2. Enter `MS-Tenant-VLAN` as the name of the VLAN to be used for the Tenant traffic. Keep the Common/Global option selected for the scope of the VLAN. Enter `3174` for the Tenant VLAN. Keep the Sharing Type as **None**.
3. Click **OK**, and then click **OK** again.

After you complete the setup of VLANs, expand the list of VLANs in the navigation pane, right-click the newly created IB-MGMT-VLAN, and select **Set as Native VLAN**. Click **Yes** to confirm the changes, and then click **OK**.

5.5.4 Setting jumbo frames in Cisco UCS Fabric

To configure jumbo frames and enable quality of service (QoS) in the Cisco UCS Mini fabric, complete the following steps:

1. In Cisco UCS Manager, go to the LAN tab in the navigation pane.
2. Click **LAN** → **LAN Cloud** → **QoS System Class**.

3. Go to the General tab. On the Best Effort row, enter 9216 in the box under the MTU column as shown in Figure 5-51.

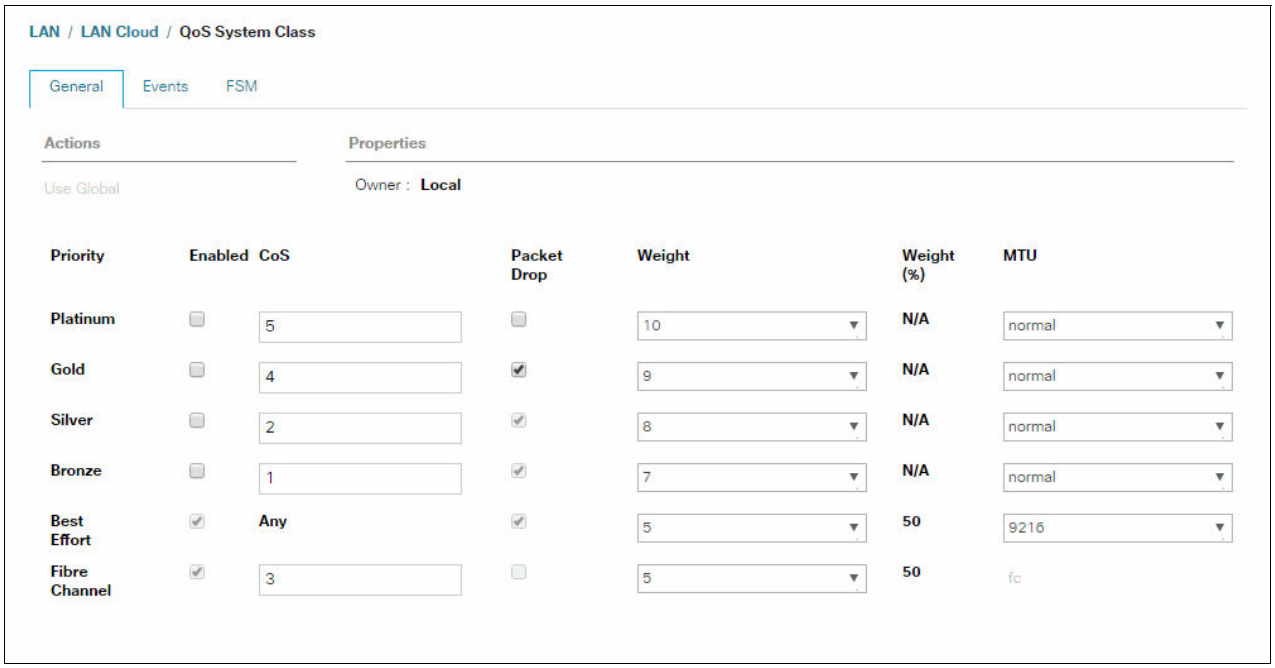


Figure 5-51 QoS System Class

4. Click **Save Changes**, and then click **OK** to complete the changes.

5.5.5 Creating a network control policy for Cisco discovery protocol

To create a network control policy that enables Cisco Discovery Protocol (CDP) on virtual network ports, complete the following steps:

1. In Cisco UCS Manager, go to the LAN tab in the navigation pane.
2. Click **Policies** → **root**.
3. Right-click **Network Control Policies** and select **Create Network Control Policy**.

4. Complete the following information, as shown in Figure 5-52:
   a. Enter `Enable_CDP` as the policy name.
   b. For CDP, select the **Enabled** option.
   c. Click **OK** to create the network control policy.

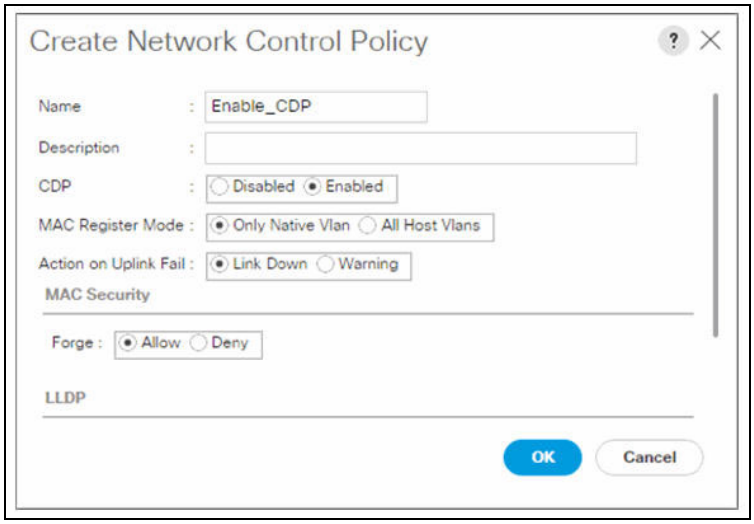


Figure 5-52 Creating the network control policy

5. Click **OK** again.

5.5.6 Creating virtual network interface card templates

This example creates two vNIC templates.

Recommendation: Do not select the Enable Failover option if your network adapters will be teamed later in the OS or hypervisor. The example described in this section teams the vNICs in this VersaStack environment; thus, the Enable Failover option is not selected.

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS Mini environment, complete the following steps:

1. In Cisco UCS Manager, go to the LAN tab in the navigation pane.
2. Click **Policies** → **root**.
3. Right-click **vNIC Templates** and select **Create vNIC Template**.

4. Complete the following information, as shown in Figure 5-53:
   a. Enter `vNIC_HOST-A` as the vNIC template name, and keep Fabric A selected.
   b. Do not select the **Enable Failover** option.
   c. Select **Primary Template** for the Redundancy Type.
   d. Leave Peer Redundancy Template as <not set>.
   e. Under Target, ensure that the VM option is not selected.
   f. Select **Updating Template** as the Template Type.

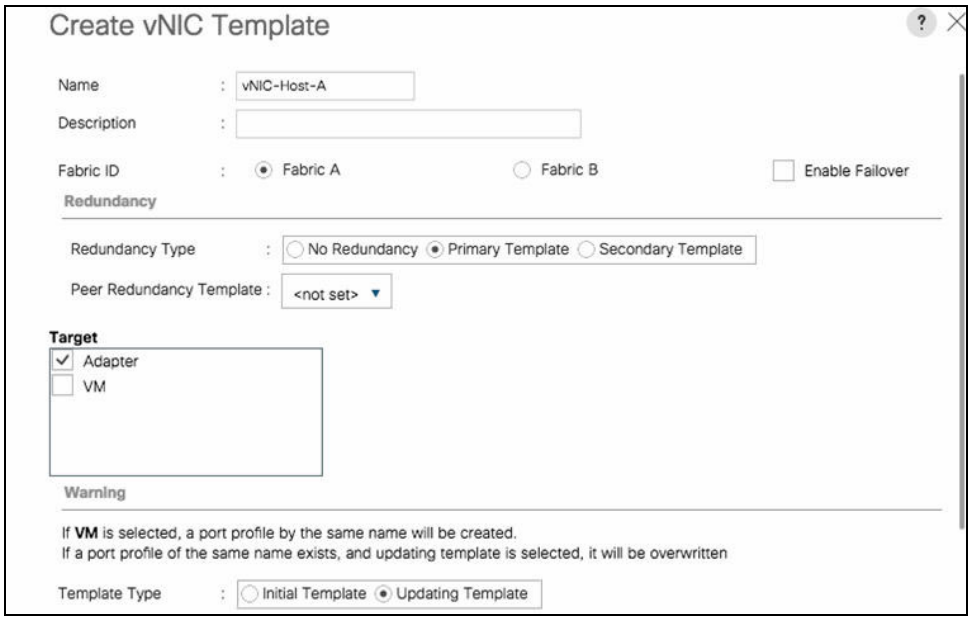


Figure 5-53 Creating the vNIC template

5. Under VLANs, select the **IB-MGMT-VLAN, MS-Cluster-VLAN, MS-Tenant-VLAN** and **MS-LVMN-VLAN** options.
6. Set IB-MGMT as the native VLAN, and leave the vNIC name selected for CDN Source, as shown in Figure 5-54.

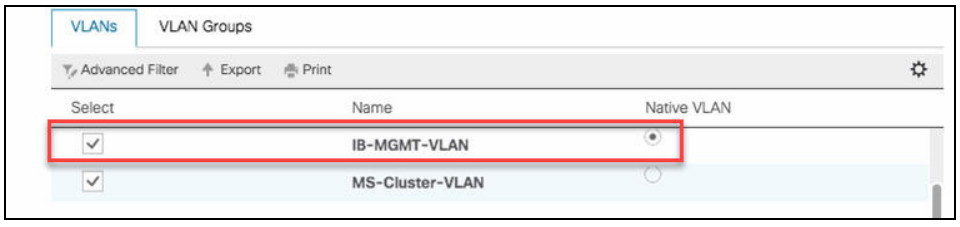


Figure 5-54 Setting IB-MGMT-VLAN as the native VLAN

7. For MTU, enter `9000`. In the MAC Pool list, select **MAC_Pool_A**.
8. In the Network Control Policy list, select **Enable_CDP**.
9. Click **OK** to create the vNIC template, and click **OK a**gain.

Follow these similar steps for the secondary redundancy vNIC-B Template:

1. In the navigation pane, go to the LAN tab.
2. Click **Policies** → **root**.
3. Right-click **vNIC Templates** and select **Create vNIC Template**.

4. Complete the following information, as shown in Figure 5-55:
   a. Enter `vNIC_Template_B` as the vNIC template name, and in Fabric ID, select **Fabric B**.
   b. Do *not* select the **Enable Failover** option.
   c. Select **Secondary Template** for the Redundancy Type.
   d. For the Peer Redundancy Template pull-down menu, select **vNIC-HOST-A**.
   e. In the MAC Pool list, select **MAC_Pool_B**. The MAC Pool is all that you need to select for the Secondary Template.
   f. Click **OK** to create the vNIC template.

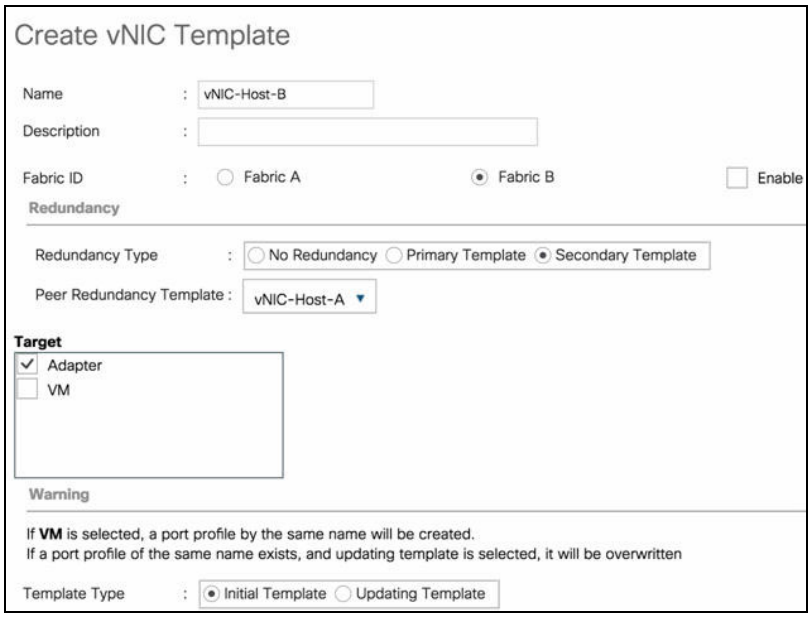


Figure 5-55 Create vNIC Template

5. Click **OK** again.

5.5.7 Creating LAN connectivity policy

To configure the required Infrastructure LAN connectivity policy, complete the following steps:

1. In Cisco UCS Manager, go to the LAN tab in the navigation pane.
2. Select **LAN** → **Policies** → **root**. Then, right-click **LAN Connectivity Policy**.
3. Select **Create LAN Connectivity Policy**.
4. Enter `HyperV-LAN-CP` as the name of the policy.
5. Click **Add** to add a vNIC.

6. Then, complete the following information, as shown in Figure 5-56:
   a. Enter `00-Host-A` as the name of the vNIC.
   b. Select the **Use of vNic Template** option.
   c. In the vNIC Template list, select **vNIC-Host-A**.
   d. In the Adapter Policy list, select **Windows**.

Figure 5-56 Creating a LAN connectivity policy for vNIC A

7. Click **OK** to add this vNIC to the policy.
8. Click **Add** to add another vNIC to the policy. Complete the following information, as shown in Figure 5-57:
   a. In the Create vNIC box, enter `01-Host-B` as the name of the vNIC.
   b. Select the **Use vNIC Template** option.
   c. In the vNIC Template list, select `vNIC-Host-B`.
   d. In the Adapter Policy list, select **Windows**.

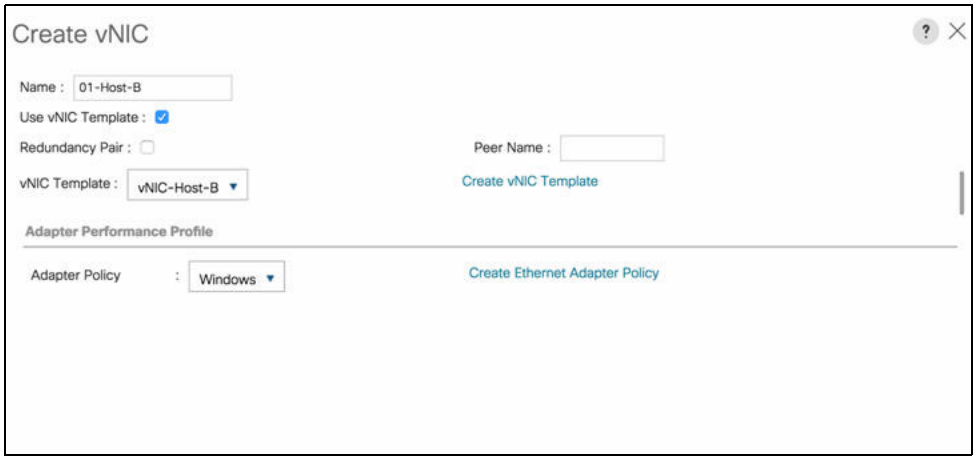


Figure 5-57 Creating a LAN connectivity policy for vNIC B

9. Click **OK** to add the vNIC to the policy.

Figure 5-58 shows an example of a connectivity policy named *HyperV-LAN-CP*.

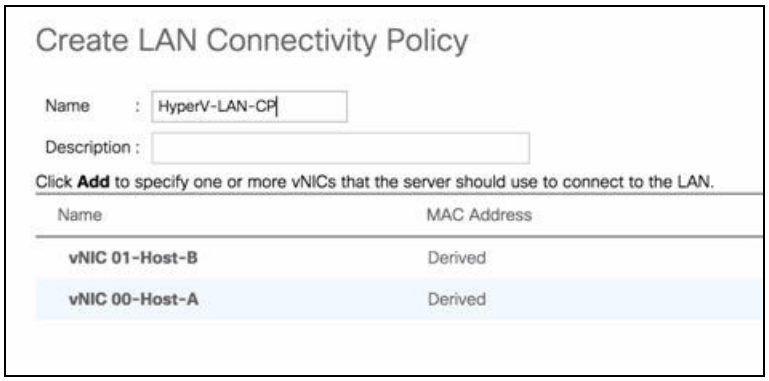


Figure 5-58 An example LAN connectivity policy

5.5.8 Creating service profile templates

To create a service profile template to use Fabric A as primary boot path:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Service Profile Templates** → **root**.
3. Right-click **root** and select **Create Service Profile Template** to open the wizard. Complete the following information, as shown in Figure 5-59:
   a. Enter `Hyper-V-Host-Infra` as the name of the service profile template. This service profile template is configured to boot from IBM FlashSystem 5030, Node 1 on Fabric A.
   b. Select the **Updating Template** option.
   c. Under UUID, select the UUID_Pool as the UUID pool.

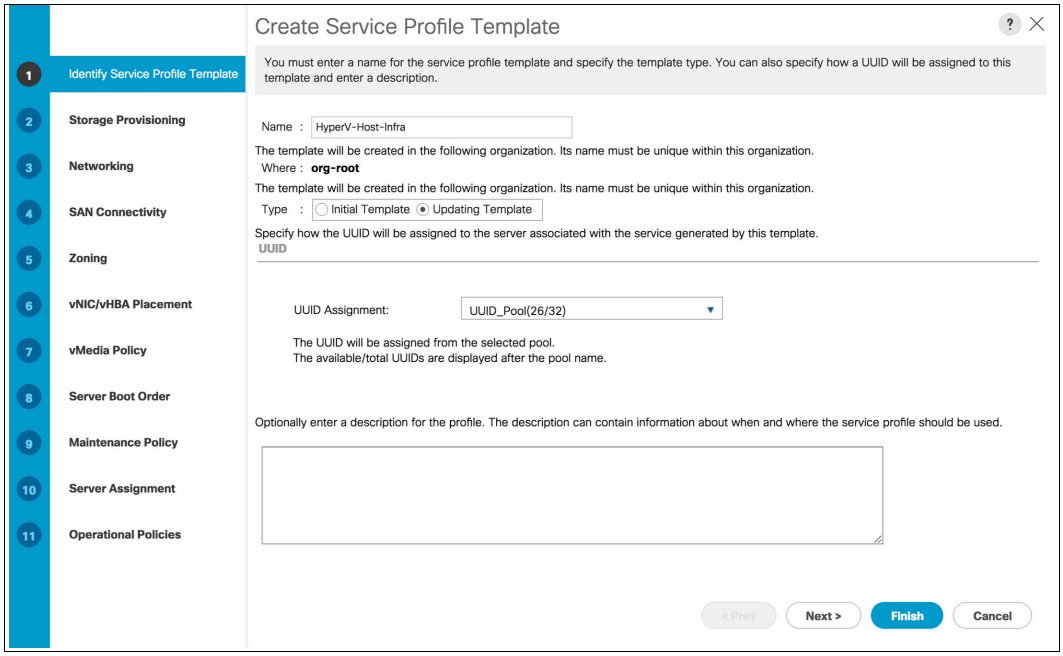


Figure 5-59 Identify the service profile template

4. Click **Next** to move to Storage Provisioning tab.

5. If you have servers with no physical disks, go to the Local Disk Configuration Policy tab, and select the **SAN-Boot Local Policy**. Otherwise, select the default **Local Storage Policy**. See Figure 5-60.

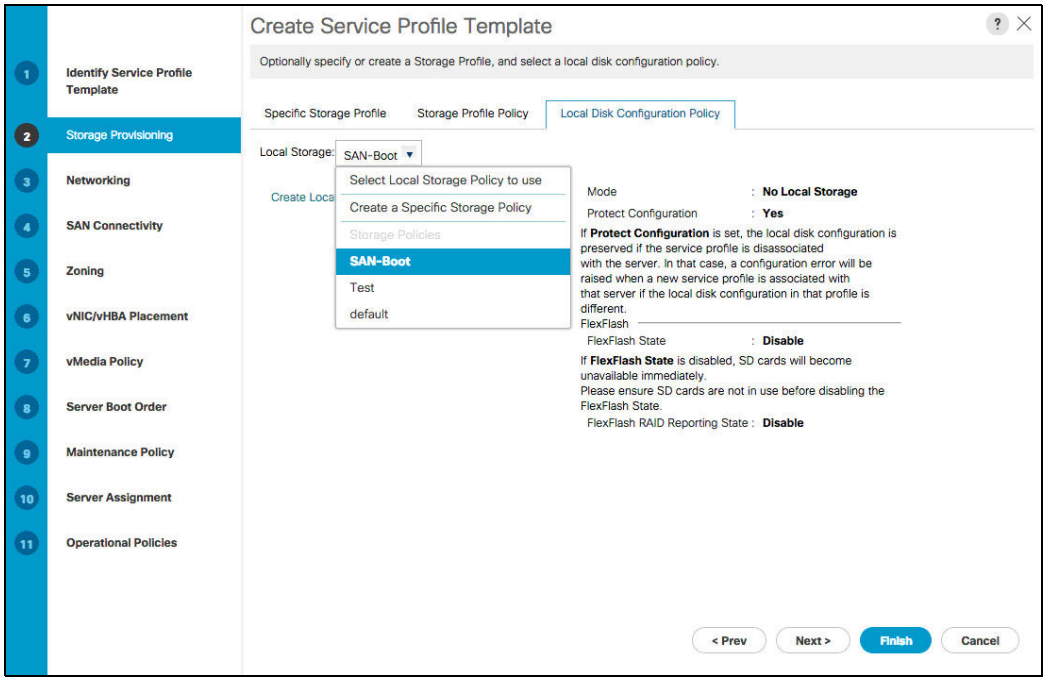


Figure 5-60 Storage Provisioning settings for Service Profile

6. Click **Next** to change to the Networking tab. Complete the following information, as shown in Figure 5-61:

   a. Keep the default settings for Dynamic vNIC Connectivity Policy.
   b. Select the **Use Connectivity Policy** option to configure the LAN connectivity.
   c. Select the **HyperV-LAN-CP** for the LAN Connectivity Policy pull-down menu.

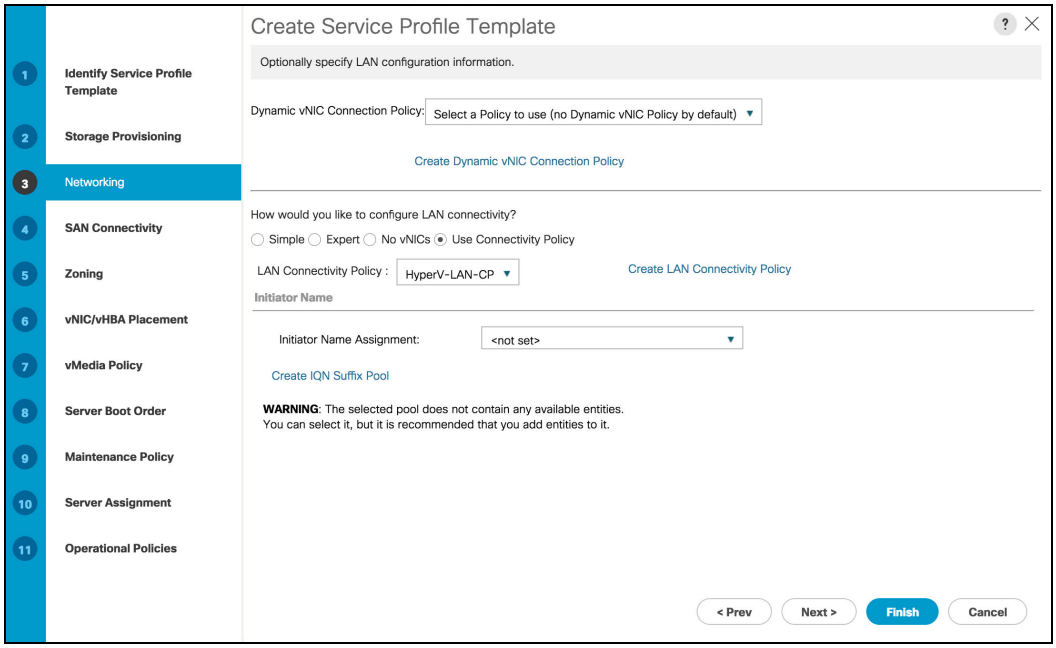


Figure 5-61 Create the service profile template

7. Click **Next** to move to SAN Connectivity tab. Complete the following information, as shown in Figure 5-62:
   a. Select the **Expert** option to configure the SAN connectivity.
   b. In the WWNN Assignment list, choose **WWNN Pool**.

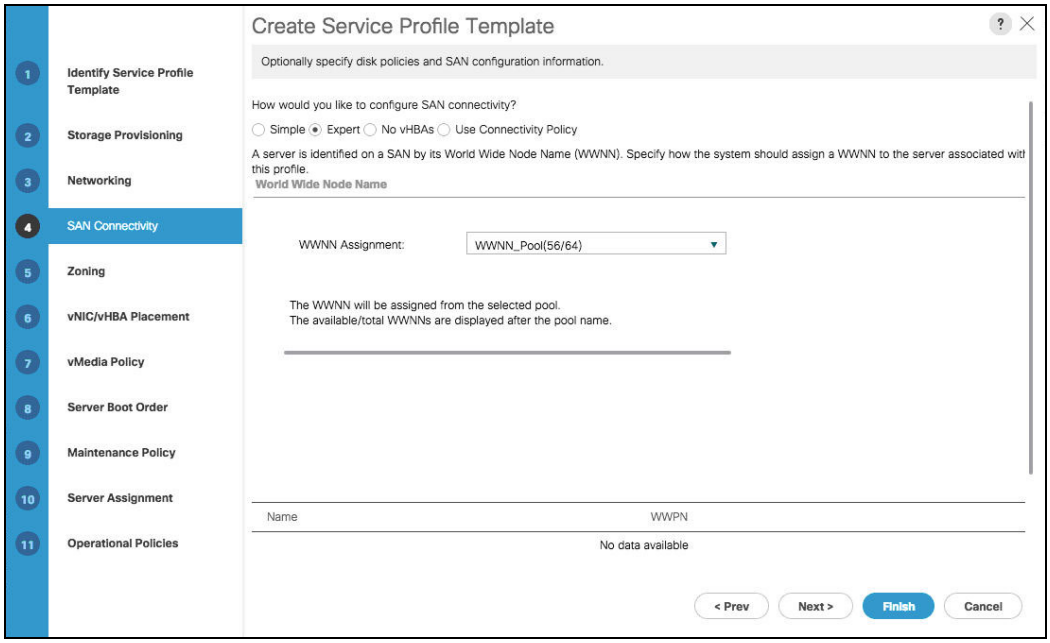


Figure 5-62 SAN Connectivity for Service Profile

8. Click **Add** to add a virtual HBA to the template. Complete the following information, as shown in Figure 5-63:
   a. In the Create vHBA dialog box, enter `Fabric-A` as the name of the vHBA.
   b. Select the **Use vHBA Template** option.
   c. In the vHBA Template list, choose **vHBA_Template_A**.
   d. In the Adapter Policy list, choose Windows.

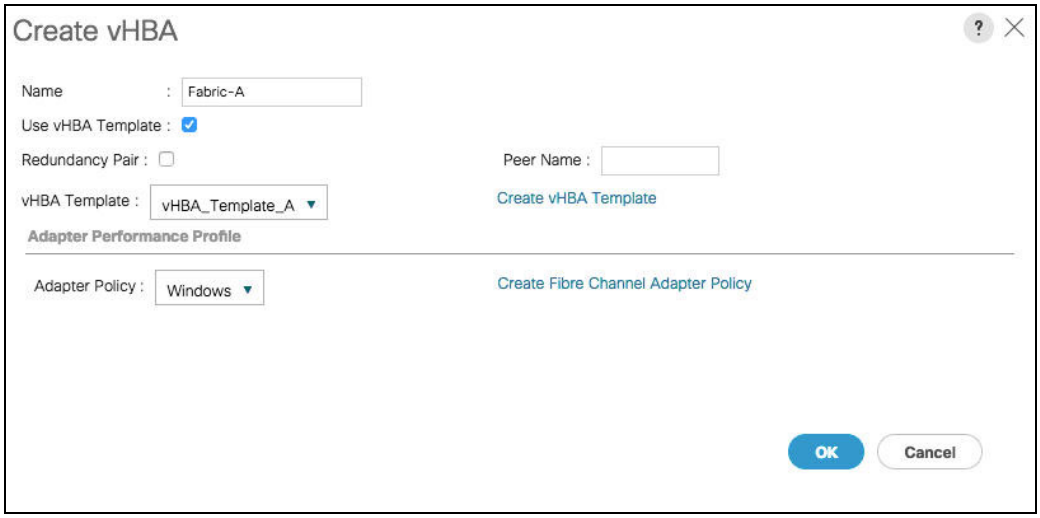


Figure 5-63 Creating a virtual HBA

9. Click **OK** to add this virtual HBA to the template.

10. On the SAN connectivity page, click **Add** to add another virtual HBA to the template. Then, complete the following information:

    a. Enter `Fabric-B` as the name of the virtual HBA.
    b. Select the **Use HBA Template** option.
    c. In the vHBA Template list, choose **vHBA_Template_B**.
    d. In the adapter Policy list, choose **Windows**.
    e. Click **OK** to add the virtual HBA to the template.

    Review the table in the SAN Connectivity page to verify that both the A and B virtual HBAs were created successfully, as shown in Figure 5-64.

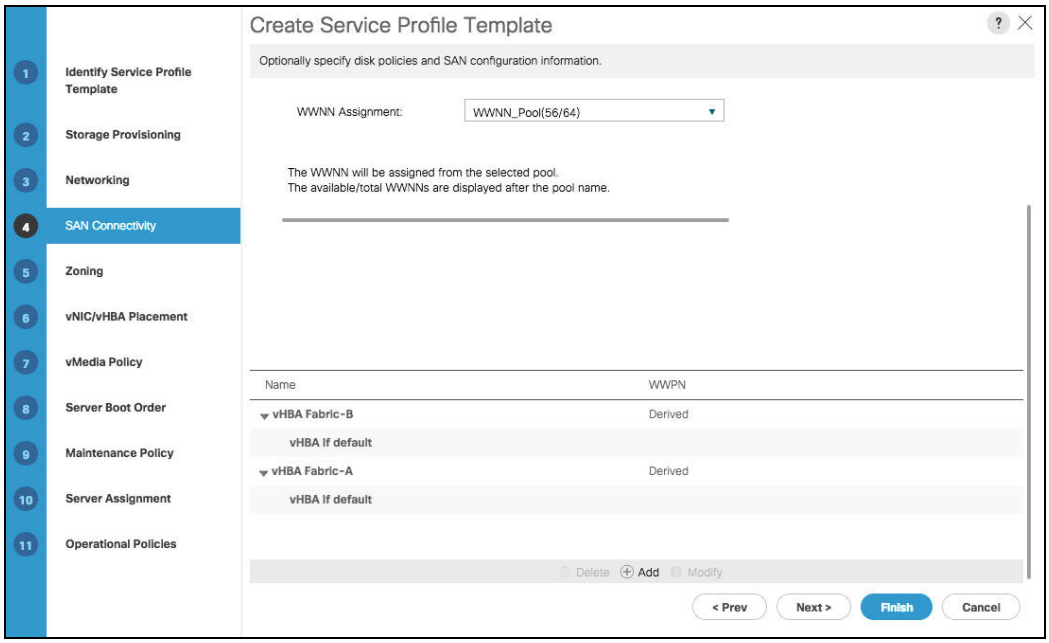


Figure 5-64 Summary of SAN Connectivity for Service Profile

11. Click **Nex**t to proceed with Zoning.
12. On the Zoning tab, select the vHBA initiators that require zoning, and click **Add To** to include them into Initiator Groups. See Figure 5-65 on page 89. Click **Next** for vNIC/vHBA Placement.

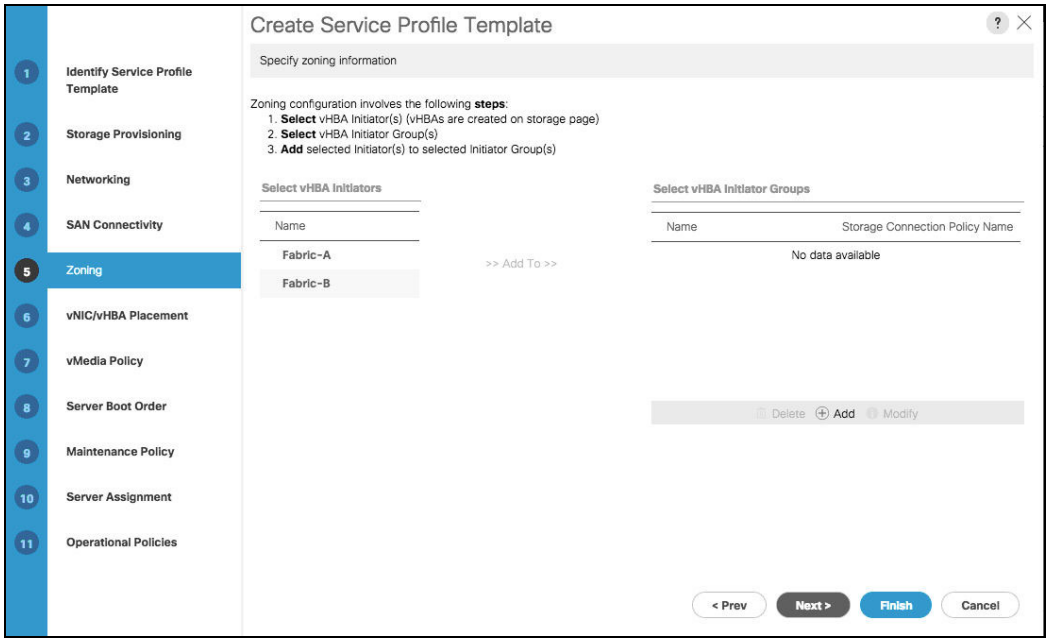


Figure 5-65 Zoning tab

13. In the vNIC/vHBA Placement, leave the placement policy as **Let System Perform Placement** and click **Next**.
14. Do not configure vMedia Policy. Click **Next**.
15. In the Configure Server Boot Order tab, select **Boot-Fabric-A** for Boot Policy as shown in Figure 5-66. Click **Next** to continue to the next section.

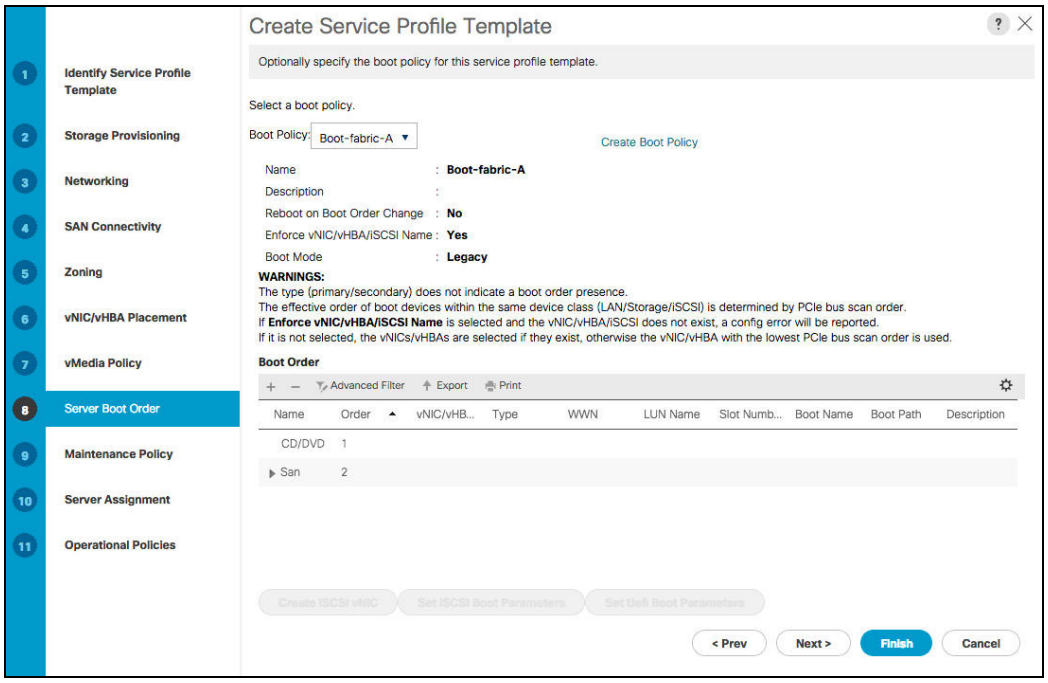


Figure 5-66 Server Boot Order

16. In the Maintenance Policy tab, change to default as shown in Figure 5-67.

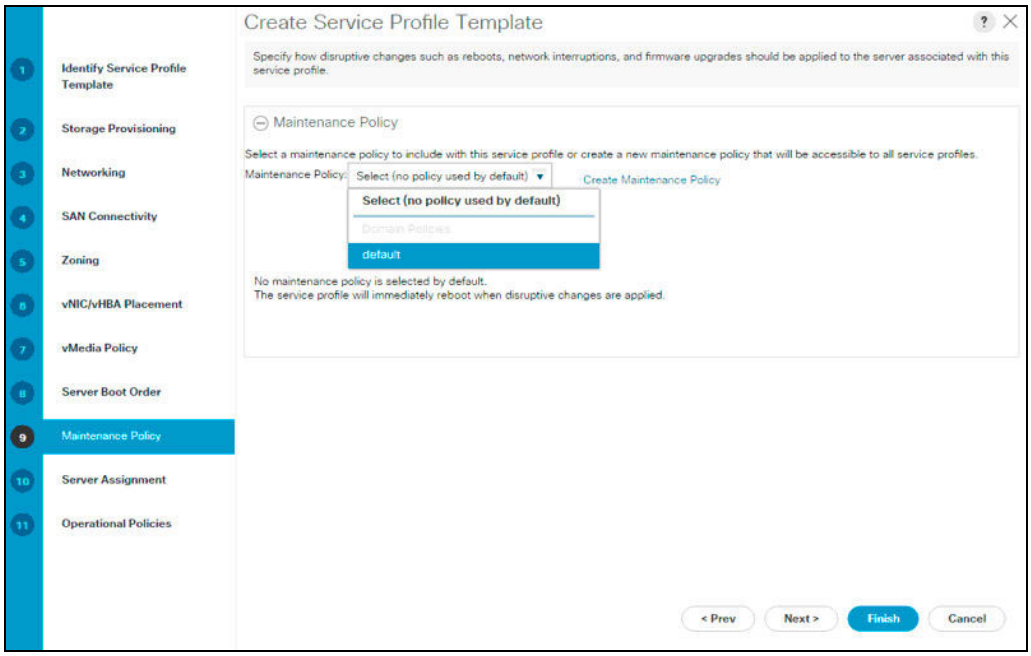


Figure 5-67 Maintenance policy for Service Profile

17. Click **Next** to move to Server Assignment tab. Complete the following information, as shown in Figure 5-68 on page 91:
    a. In the Pool Assignment list, select **Infra_Pool** and select a **Server Pool Qualification policy** (optional).
    b. Select **Down** as the power state to be applied when the profile is associated with the server.
    c. Select **UCSB-B200-M5** for the Server Pool Qualification.
    d. Firmware Management at the bottom of the page can be left alone as it will use the default from the Host Firmware list.

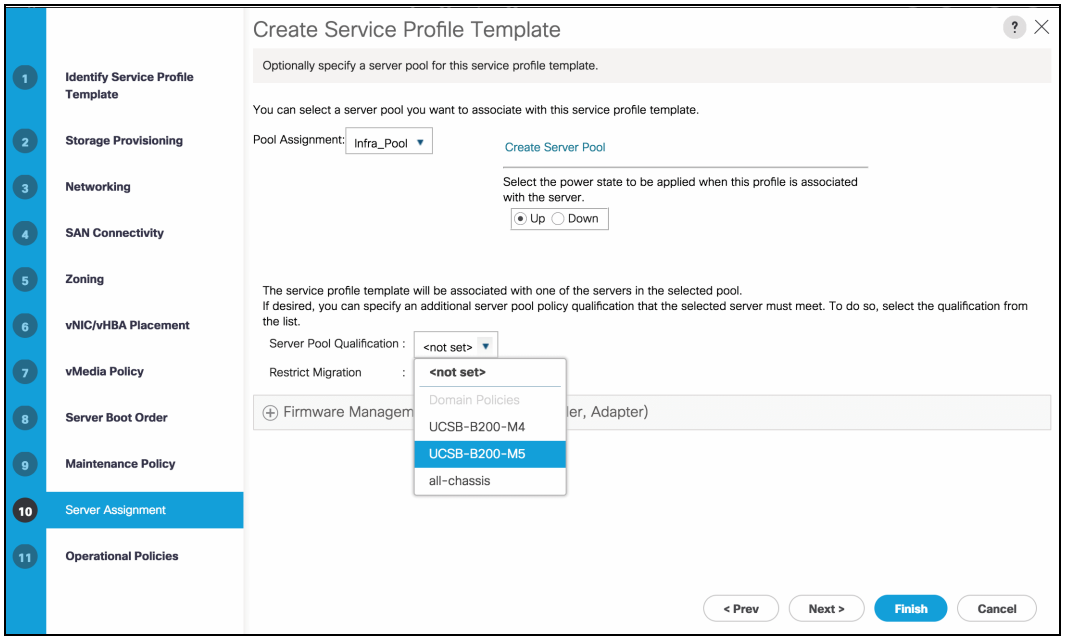


Figure 5-68 Server assignment for the service profile

18. Click **Next** to move to the Operational Policies tab. Select **HyperV-Hosts.** Expand **Power Control Policy Configuration**, and select **No-Power-Cap** in the Power Control Policy list. See Figure 5-69.

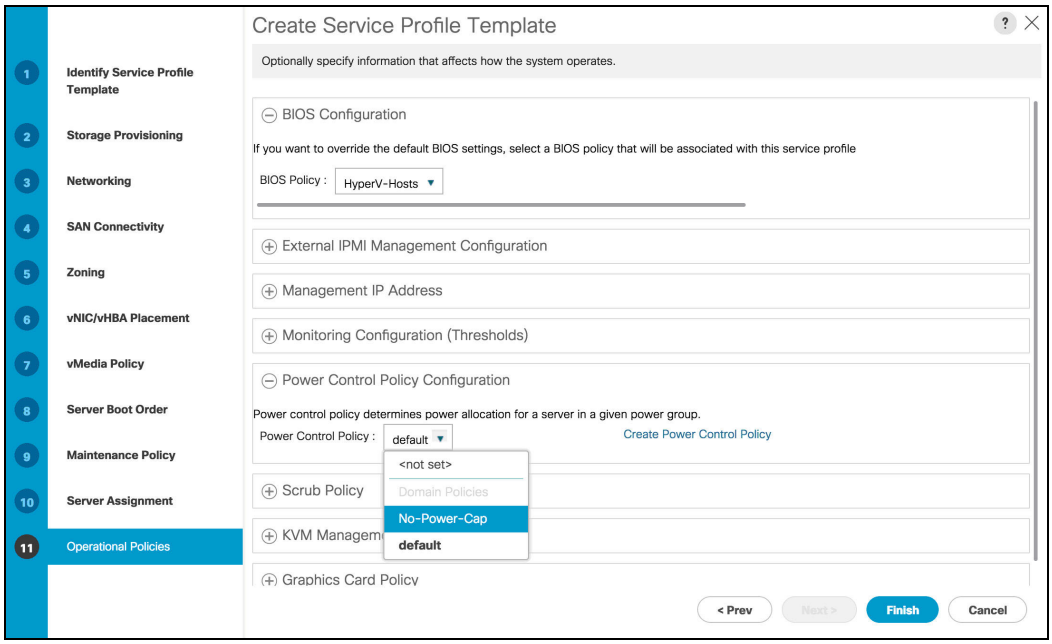


Figure 5-69 Operational policies for the service profile template

19. Click **Finish** to create the service profile template, and click **OK** for the confirmation message that display.

5.5.9 Creating service profiles

To create service profiles from the service profile template, complete the following steps:

1. In Cisco UCS Manager, go to the Servers tab in the navigation pane.
2. Click **Service Profile Templates** → **root** → **Service Template HyperV-Host-Infra**.
3. Right-click **HyperV-Host-Infra** and select **Create Service Profiles from Template**, as shown in Figure 5-70.

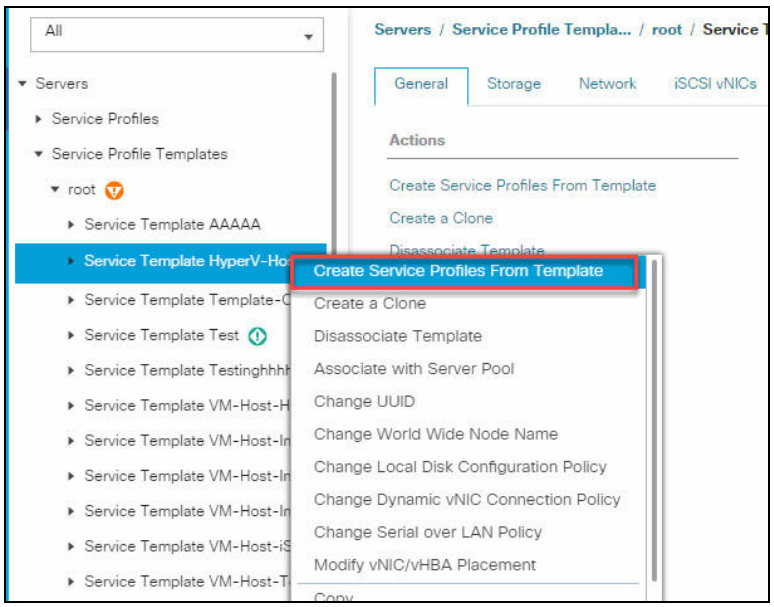


Figure 5-70 Create Service Profiles from Template

4. Complete the following information, as shown in Figure 5-71:
   a. Enter `HyperV-Host-Infra-0` as the Naming Prefix.
   b. Enter `1` as the Name Suffix Starting Number.
   c. Enter `2` as the Number of Instances.
   d. Click **OK** to create the service profile.

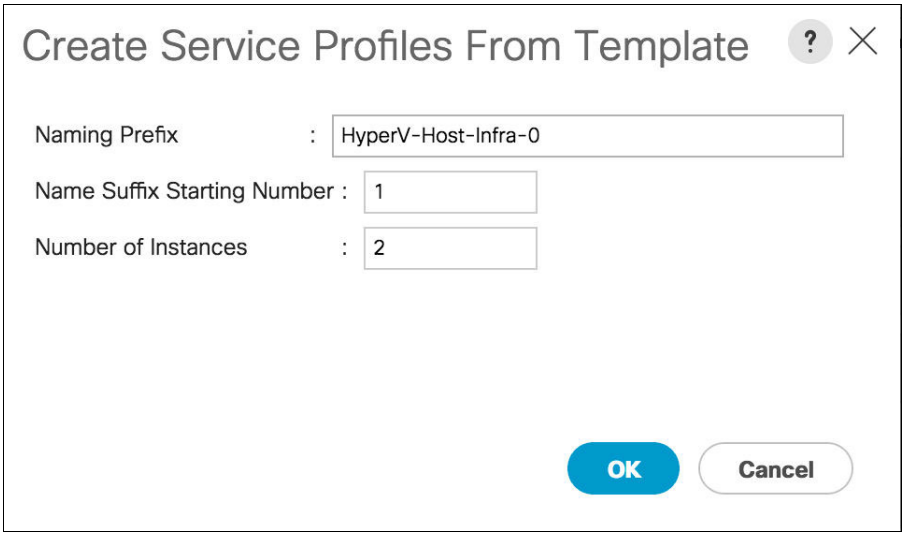


Figure 5-71 Creating service profiles from a template

5. Click **OK** in the confirmation message to provision two VersaStack service profiles.

5.6 Back up the Cisco UCS Manager configuration

Back up your Cisco UCS Mini configuration. By running the backup using the Cisco UCS Manager, you take a snapshot of all or part of the system configuration and export the file to a location on your network. You cannot use Cisco UCS Manager to back up data on the servers.

You can take a backup while the system is running. The backup operation saves only information from the management plane. It does not have any impact on the server or network traffic.

You can find more information about backup and restore procedures online.

6

SAN Boot in a Cisco UCS Mini environment

This chapter describes the steps to set up the Cisco UCS Mini environment to allow SAN Boot implementation. The Cisco UCS Mini chassis allows system administrators to opt for SAN Boot implementation scenarios to increase storage and systems efficiency by using a centralized management and operational systems image.

The SAN Boot technique allows servers to use an operating system image that is installed an on external component, such as an high-available storage array, that contains storage capacity with several layers of disk protection and optimal cache structure.

This chapter includes the following topics:

6.1 Overview of a SAN Boot using Cisco UCS Mini

A SAN Boot can be categorized as modern technique to provision new servers. Because the IBM FlashSystem 5030 is a high-available storage array, organizations can use SAN Boot techniques for a number of reasons. For example, when a server is booting from SAN and the server hardware fails, the operation system image can be easily assigned to an alternate hardware to reduce the downtime and to increase availability.

The next sections describe the steps that are required to set up a Microsoft Windows Server 2016 to have its operational system volume and data stored in the IBM FlashSystem 5030. To configure a server running Windows Server 2016 to boot from SAN, it is assumed that the service profile for SAN boot was configured previously, as described in 5.4.8, “Creating boot policies” on page 72.

6.2 Preparing the SAN Boot for Windows Server 2016

This section describes the guidelines to enable servers in the Cisco UCS Mini environment to be configured as SAN Boot.

6.2.1 Boot policy

The Cisco UCS Manager boot policy overrides the boot order in the BIOS setup menu, and determines the following information:

- Selection of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You can either create a named boot policy that can be associated with one or more service profiles or create a boot policy for a specific service profile. A boot policy must be included in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, Cisco UCS Manager applies the default boot policy.

Boot policy changes: Changes to a boot policy might be propagated to all servers created with an updating service profile template that includes that boot policy. Re-association of the service profile with the server to rewrite the boot order information in the BIOS is triggered automatically.

6.2.2 Unified Extensible Firmware Interface boot mode

Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. Cisco UCS Manager uses UEFI to replace the BIOS firmware interfaces. This method allows the BIOS to run in UEFI mode while still providing existing support.

You can choose either legacy mode or UEFI boot mode when you create a boot policy. Legacy boot mode is supported for all Cisco UCS servers. UEFI boot mode is supported only on M3 servers and allows you to enable UEFI secure boot mode.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is supported only on Cisco UCS B-Series M3 Blade Servers and Cisco UCS C-Series M3 Rack Servers.
- UEFI boot mode is not supported with the following combinations:
  - Gen-3 Emulex and QLogic adapters on Cisco UCS blade and rack servers that are integrated with Cisco UCS Manager.
  - PXE boot for all adapters on Cisco UCS rack servers that are integrated with Cisco UCS Manager.
  - iSCSI boot for all adapters on Cisco UCS rack servers that are integrated with Cisco UCS Manager.
- If you want to use UEFI boot mode with two iSCSI LUNs, you must manually specify a common iSCSI initiator name in the service profile that is applied to both underlying iSCSI eNICs, rather than allowing Cisco UCS Manager to select the name from an IQN suffix pool. If you do not supply a common name, Cisco UCS Manager cannot detect the second iSCSI LUN.
- You cannot mix UEFI and existing boot mode on the same server.
- The server boots correctly in UEFI mode only if the boot devices that are configured in the boot policy have UEFI-aware operating systems installed. If a compatible OS is not present, the boot device is not displayed on the Actual Boot Order tab in the Boot Order Details area.
- In some corner cases, the UEFI boot might not succeed because the UEFI boot manager entry was not saved correctly in the BIOS NVRAM. You can use the UEFI shell to enter the UEFI boot manager entry manually. This situation might occur in the following situations:
  - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and the blade is powered on manually using the Equipment tab or the front panel.
  - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and a direct VIC firmware upgrade is attempted.
  - If a blade or rack server with UEFI boot mode enabled is booted off SAN LUN, and the service profile is migrated.

6.2.3 UEFI secure boot

Cisco UCS Manager supports UEFI secure boot on Cisco UCS B-Series M3 Blade servers. When UEFI secure boot is enabled, all executables, such as boot loaders and adapter drivers, are authenticated by the BIOS before they can be loaded. To be authenticated, the images must be signed by either the Cisco Certificate Authority (CA) or a Microsoft CA.

The following limitations apply to UEFI secure boot:

- UEFI boot mode must be enabled in the boot policy.
- The Cisco UCS Manager software and the BIOS firmware must be at Release 2.2 or greater.
- User-generated encryption keys are not supported.
- UEFI secure boot can only be controlled by Cisco UCS Manager.
- If you want to downgrade to an earlier version of Cisco UCS Manager and if you have a server in secure boot mode, you must disassociate, and then re-associate, the server before downgrading. Otherwise, server discovery is not successful.

6.3 Preparing and performing SAN Boot

In this section, we assume that the UCS Server Profile SAN Boot policy are previously configured. SAN booting does not require support for special SCSI operations; it is not different from any other SCSI disk operation. The vHBA uses code and specific drivers to enable the host to discover and to boot from a LUN on the storage system.

To define the HBA initiation in the IBM FlashSystem 5030, you must add hosts and map the boot volumes on the IBM FlashSystem 5030:

1. Open the IBM FlashSystem 5030 management GUI log in with your superuser or admin account.
2. In the left pane, click the **Host** icon, which is the fourth icon down, and click **Hosts**.
3. Click **Create Host** (in the upper, left menu and the fourth icon down in Figure 6-1) to start the wizard.

   Figure 6-1 shows the Add Host window, which shows options for host name, host connection type (FC or iSCSI) hosts.

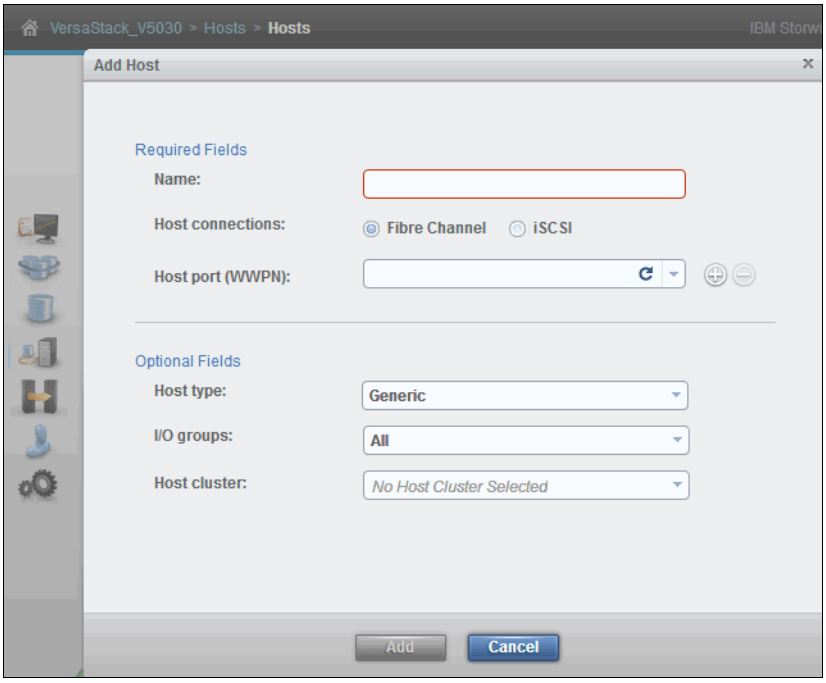


Figure 6-1 Add Host window

4. Enter the host name, and select the **Fibre Channel** option.
5. Enter the World Wide Port Name (WWPN) of the host that is to configure as SAN Boot.
6. In the Optional Fields section, select **Generic**, as this is the suitable host type for Microsoft Windows Server.
7. Select the I/O group to which the host should have access.
8. Because this host requires SAN Boot Volume and the volume must not be shared, the Host Cluster option should not contain any host cluster entity.
9. Click **Close** to complete the creation of host object in IBM FlashSystem 5030.

Next, you need to create an IBM LUN to be used as a boot device and then map it to a host as `LUN ID 0`.

6.4 Provisioning IBM LUN as a SAN Boot volume

For the purpose of this example, we provision a 128 Gb size volume to be used as a boot volume. Complete the following steps to create and assign a SAN Boot volume to a host using the IBM FlashSystem 5030:

1. Log on to IBM FlashSystem 5030, click **Volumes** (from the left side menu), and then select **Volumes** as shown in Figure 6-2.

Figure 6-2 Assigning a new volume

2. The wizard starts as shown in Figure 6-3, and guides you through the process using the **Quick Volume Creation** menu to create Basic and Mirrored volumes. Select **Basic**. In the Pool click in the drop-down menu to select the storage pool, set the quantity equals to `1` and volume capacity to `128 GB`. In the “Capacity savings” field, select **None** to provision a fully allocated volume. Enter the volume name and the I/O group the volume should be created.
3. Click **Create and Map** to create the volume and assign the volume to a host.

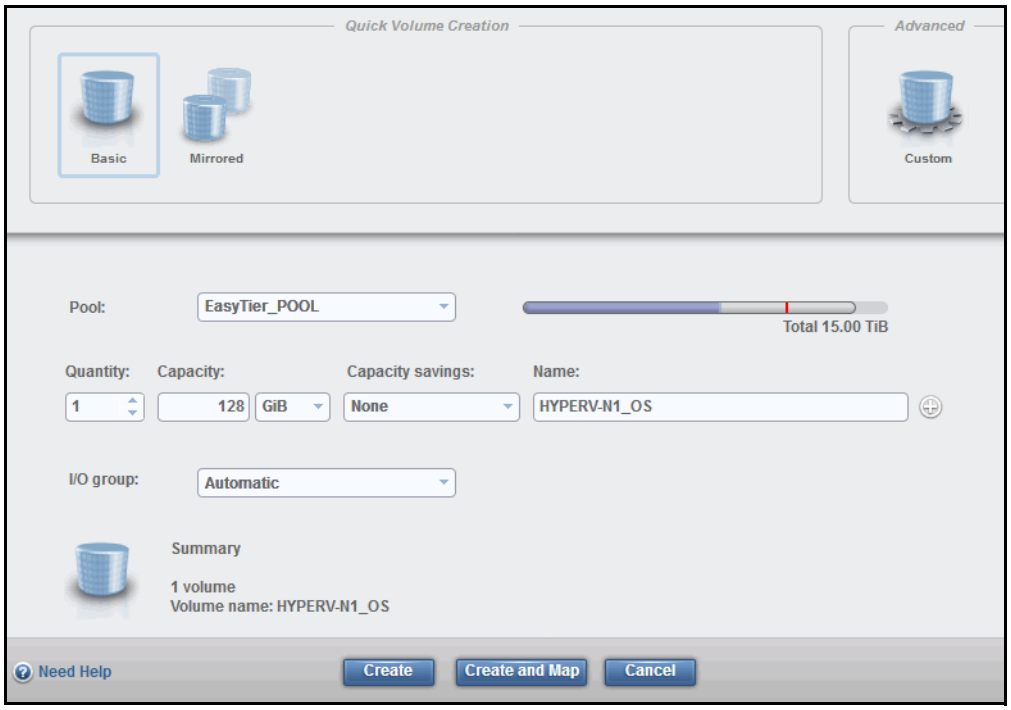


Figure 6-3 Provisioning a new volume using IBM FlashSystem 5030 GUI

4. After the wizard completes, a new wizard opens to guide you through the process to select the host to which the volume must be mapped. Select the host as shown in Figure 6-4.

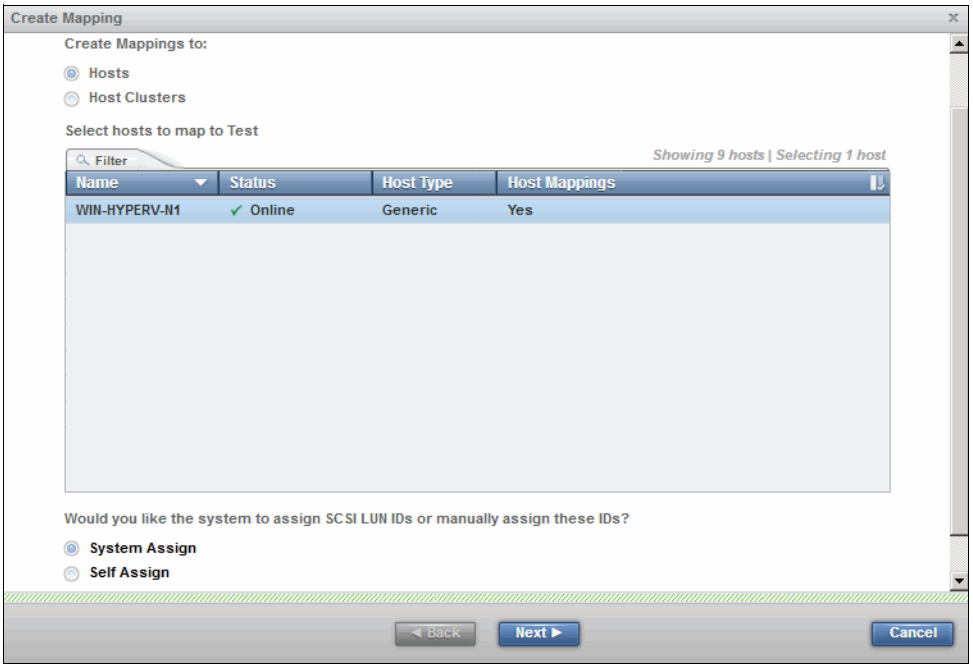


Figure 6-4 Creating a host cluster mapping

5. Scroll down to select the SCSI ID assignment. When selecting **System Assign**, the IBM FlashSystem 5030 assigns the next available SCSI ID incrementally. By choosing **Self Assign**, the system allows you to enter the SCSI ID before the mappings are created. Select **System Assign** and click **Next**.
6. Review the summary of volume mapping. Ensure the SAN Boot volume gets SCSI ID 0, and click **Map Volumes** to complete.

> **Note:** For most of the Operational System vendors, use the SAN boot volume as *LUN ID 0*.

6.5 Setting up Microsoft Windows Server 2016

This section provides detailed instructions for installing Microsoft Windows Server 2016 in an environment. After the procedures are complete, two booted Windows Server 2016 hosts will be provisioned.

For this section, it is assumed that the boot policy was properly configured and that a single initiator was set to discover the IBM LUN device through a single path.

To start the Cisco UCS Mini to discover the SAN Boot volume to install the OS:

1. Using a web browser, log on to the Cisco UCS Mini, and select **Servers**. Then, select the server that is associated with the service profile.
2. You can verify the actual boot order in the Boot Order details area on the General tab for the server, or you can change to the Boot Order tab to ensure that the boot policy instance is applied, as shown in Figure 6-5 on page 102.

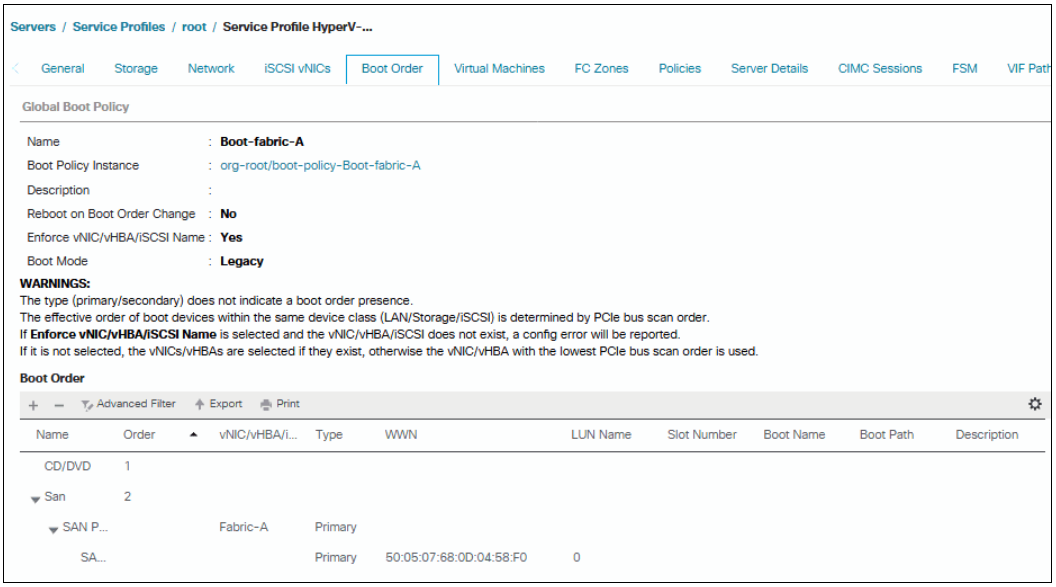


Figure 6-5 Boot Order details

3. To proceed with the Windows OS installation, return to the main menu, and click **Servers**.
4. Select **Servers** → **Service Profiles** → **root** → **HyperV-Host-Infra-01**. Right-click **HyperV-Host-Infra-01** and select **KVM Console**. Then, follow the prompts to launch the Java-based KVM console.
5. Select **Servers** → **Service Profiles** → **root** → **HyperV-Host-Infra-02**. Right-click **HyperV-Host-Infra-02** and select **KVM Console**. Then, follow the prompts to launch the Java-based KVM console.
6. From the virtual KVM Console, go to the Virtual Media tab, and select **Add Image** in the right pane.
7. Browse to the Windows Server 2016 installation ISO image file, and click **Open**.
8. Map the image that you just added by selecting **Mapped**.
9. To boot the server, go to the KVM tab, and select **Power On Server** in the KVM interface Summary tab. Then click **OK**.

   On boot, the machine detects the presence of the Windows installation media.
10. After the installer loads, enter the relevant region information, and click **Next**.
11. Click **Install now**, enter the Product Key, and then click **Next**.
12. Select **Windows Server 2016 Standard** (Server with a GUI), and click **Next**.

> **Option:** You can remove the GUI after the Hyper-V cluster is operational.

13. After reviewing the license agreement, accept the terms, and click **Next**.
14. Select **Custom (advanced) installation**.
15. In the Virtual Media Session manager, clear the mapped option for the Windows ISO, and select **yes** to confirm. Then click **Add Image**.

16. Click **Open**, as shown in Figure 6-6.

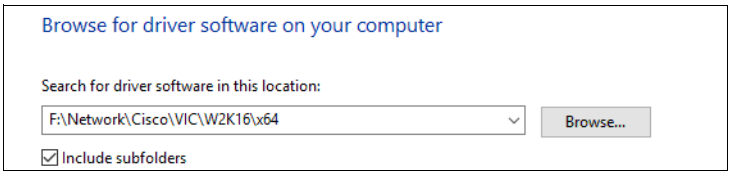


Figure 6-6 Browsing for the Cisco fNIC driver ISO

17. Back in the KVM Console, click **Load Driver**, and then, click **OK**. The Cisco VIC FCoE Storport Miniport driver is detected automatically, as shown in Figure 6-7.

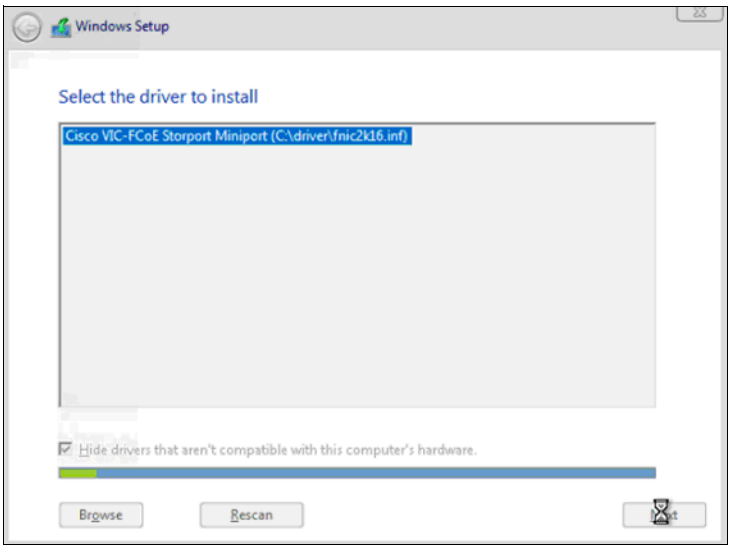


Figure 6-7 Selecting the Cisco VIC FCoE Storport Miniport driver

18. Click **Next** to load the driver to the installation process.
19. When prompted regarding where you want to install, only a single LUN instance should display. Multiple instances of the same LUN indicate that there are multiple paths to the installation LUN. Verify that the SAN zoning is correct, and then restart the installation.

    The following message displays because the Windows installation ISO image is not mapped at this time:

    ```
    Windows can't be installed on this drive
    ```

20. You can load the Cisco eNIC driver at this point in the same way as the fNIC driver. Loading the eNIC driver at this time bypasses the need to load the eNIC driver, as described in 6.5.1, “Installing Intel chipset and Cisco eNIC drivers for Microsoft Windows” on page 104.

21. As shown in Figure 6-8, select the **LUN,** and click **Next** to continue with the installation. When the installation completes, enter an administrator password on the settings page, and click **Finish**.

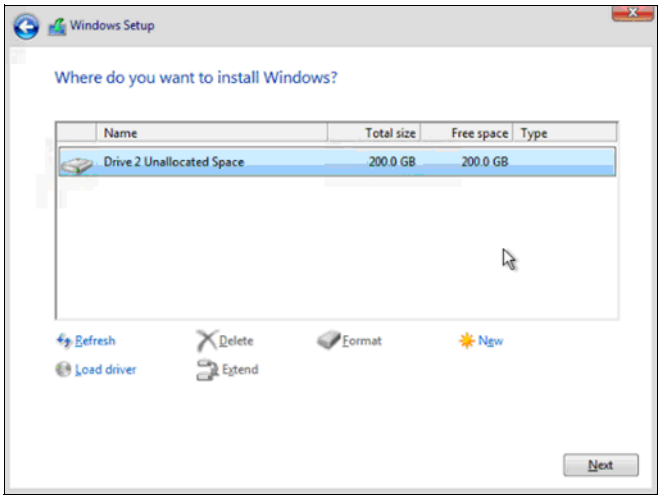


Figure 6-8 Selecting the LUN to install Windows

Important: At this point, the Windows OS is installed in the IBM LUN. Then, you must enable the Multipath I/O feature and install the IBM Subsystem Device Driver Device Specific Module (SDDDSM) multipathing software. Be sure to change the policy in the Service Profile to enable dual fabric connectivity.

6.5.1 Installing Intel chipset and Cisco eNIC drivers for Microsoft Windows

To install the Intel chipset and Cisco eNIC drivers, complete the following steps:

1. In the Virtual Media Session manager, clear the Mapped option for the Windows ISO.
2. Click **Add Image**, browse to the Cisco UCS driver ISO, and click **Open**.
3. Select the Mapped option for the Cisco UCS driver ISO. Browse to **CD ROM** → **Chipset** → **"Intel > <*Server Model*> W2K16 > x64"**.
4. Double-click **Setup Chipset** to install the chipset driver and then reboot the system.
5. In the KVM console, open the Server Manager, and select **Tools** → **Computer Management**. In the Computer Manager, select **System Tools** → **Device Manager** → **Other devices**.

6. As shown in Figure 6-9, right-click the Ethernet Controller, and select **Update Driver Software**.

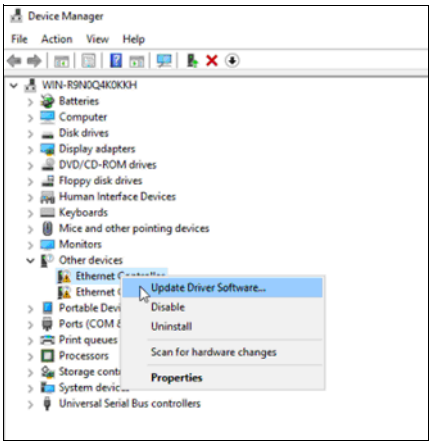


Figure 6-9 Updating driver software

7. Click **Browse**, and select CDROM drive, click **OK**.
8. Next install the driver. After Windows completes the installation, click **Close** as shown in Figure 6-10.

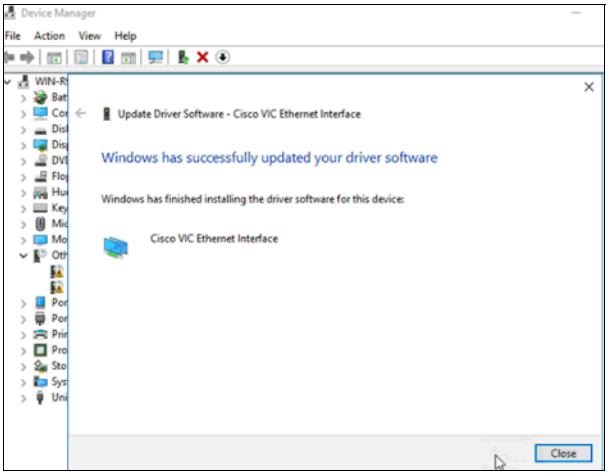


Figure 6-10 Windows completes the driver installation

9. Right-click the next Ethernet Controller and select **Update Driver Software**.
10. Click **Search automatically for update driver software**. When completed, click **Close**.
11. Repeat these steps for the remaining Ethernet Controllers. All Cisco VIC Ethernet devices display under Network Adapters.

6.5.2 Cloning an OS volume

By using cloning techniques, you can copy the entire contents of one SAN boot volume to another. After Windows OS is installed in the IBM LUN, dual fabric connectivity is enabled via a Service Profile, and the multipath is installed, you can use IBM FlashSystem 5030 Flash Copy techniques to maximize your deployment of servers.

FlashCopy creates a point-in-time copy of a source volume on the target volume. When you initiate a FlashCopy (type Clone) operation, a FlashCopy relationship is created between a source volume and target volume. This relationship allows a point-in-time copy of that source volume to be copied to the associated target volume. This relationship exists until the storage units are copied from the source to the target volume. After this relationship is completed and the target volume becomes an independent volume, this volume can be assigned to another Service Profile (hardware). Then the system administrator should be able to start the computer using this duplicated volume.

To prepare this new computer to run with a cloned volume, you must run the **Sysprep** tool to complete the Windows deduplication.

The System Preparation (**Sysprep**) tool prepares an installation of Windows for duplication, which is also called *imaging*. The **Sysprep** tool enables you to capture a customized Windows image to re-use throughout your organization.

You can find more information about the **Sysprep** tool online.

7

Failover cluster and Hyper-V configuration

This chapter provides instructions for installing and configuring the Microsoft Hyper-V feature using the Failover Clustering feature for high availability virtual servers using the Cisco UCS Mini environment.

For the purposes of this book, the Failover Clustering feature is installed on Microsoft Windows Server 2016. Because several methods exists to install and configuring the Windows servers for clustered services, this procedure focuses on how to use the built-in keyboard, video, mouse (KVM) console, and virtual media features in Cisco UCS Manager to map the remote installation media to each individual server and to connect to the boot logical unit numbers (LUNs) provisioned by IBM FlashSystem 5030.

This chapter has the following sections:

7.1 Introduction to Hyper-V Cluster for high availability

Hyper-V was first introduced in Microsoft Windows 2008, and many improvements, enhancements, and features have been included since its first release. Hyper-V can provide high-availability and disaster-recovery solutions, and when combined with proper hardware architecture, Hyper-V can maximize high availability and offsite recovery with minimal effort.

By using Microsoft Failover Clustering combined with Cisco UCS Mini solution, you can protect your virtualized computer environment against physical system outages that can affects multiples machines.

7.2 Physical topology for Hyper-V

The physical topology consist of two chassis of Cisco VersaStack, two Nexus 9000 series, and IBM FlashSystem 5030 direct-attached through redundant Fabric Interconnects. The IBM FlashSystem 5030 provides a high redundancy, high-performance storage solution for the deployment of Hyper-V.

This solution design uses direct-attached Fibre Channel (FC) storage connectivity for compute, enabling a simple, flexible and cost-effective solution.

This VersaStack design utilizes Cisco UCS Mini platform with Cisco M5 half-width blades and Cisco UCS C220 M5 rack mount servers connected and managed through Cisco UCS 6324 Fabric Interconnects and the integrated UCS manager. These high performance servers are configured as stateless compute nodes where using FC SAN boot.

The Cisco Unified Computing System and Cisco Nexus 9000 platforms support active port channeling using 802.3ad standard Link Aggregation Control Protocol (LACP). Port channeling is a link aggregation technique offering link fault tolerance and traffic distribution (load balancing) for improved aggregate bandwidth across member ports.

Each Cisco UCS Fabric Interconnect is connected to both the Cisco Nexus 9372 switches using Virtual PortChannel (vPC) enabled 10GbE uplinks for a total aggregate bandwidth of 20 Gbps. The Cisco UCS Mini can be extended by connecting a second Cisco UCS Chassis with eight blades and with two Cisco UCS rack-mount servers by using the 40GbE Enhanced Quad SFP (QSFP+) ports that are available on the Cisco UCS 6324 Fabric Interconnects.

Figure 7-1 shows the physical topology used in this deployment.

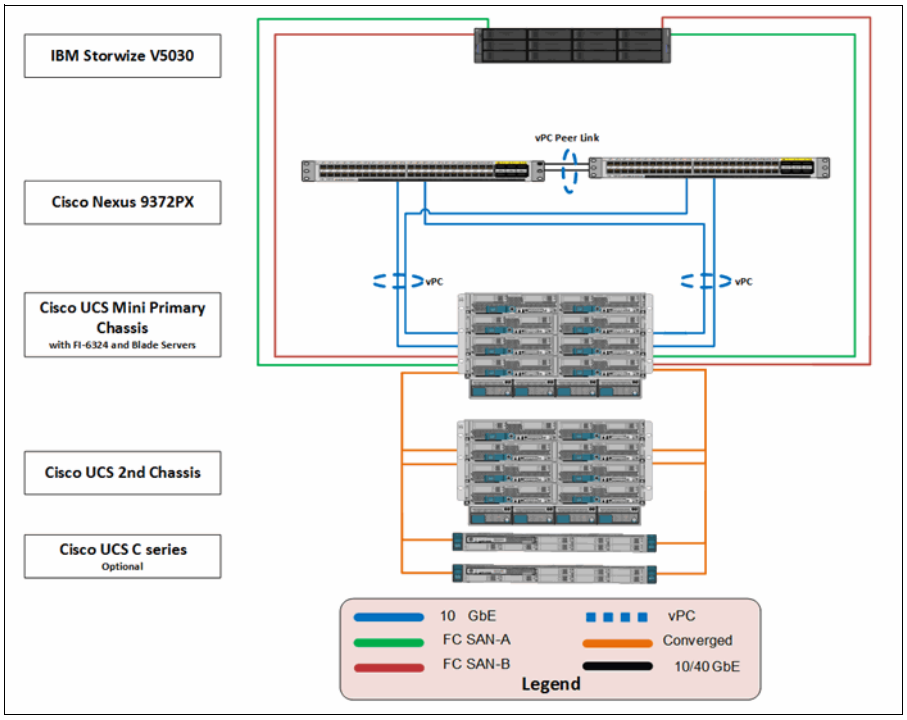


Figure 7-1 VersaStack physical topology

7.3 Microsoft Windows 2016 Failover Clustering feature requirements

This section describes the system requirements to install the Microsoft Failover Clustering feature. The Failover Clustering consists in several components, and it's important to meet all the software requirements to provide optimal stable solution.

The following instructions are required to provision a minimum of two nodes running Microsoft Windows Server 2016 Datacenter edition running Failover Clustering feature.

- Cluster nodes use the same hardware and operation system configuration.
- Cluster nodes must belong to the same Active Directory Domain.
- Proper administrative rights are set up in each node of the cluster.
- Each node of the cluster has the proper number of NIC cards and TCP/IP configurations. If iSCSI is employed, dedicated network adapters are set up.
- At least one shared logical drive device is used for cluster services.
- The Failover Clustering feature is installed on all cluster nodes running Microsoft Windows.

7.4 Configuring features and tools for failover cluster nodes

We assume that the operating system is already installed on the nodes. This section provides the instructions to install the required features and tools to support the Failover Clustering feature running on Microsoft Windows Server 2016 Datacenter edition.

7.4.1 Installing Data Center Bridging and multipath I/O

Data Center Bridging (DCB) is a set of standards that enables the operating system to allocate proper bandwidth and enhancements whereas data storage, IP networking and cluster interprocess communication (IPC) and management traffic share the same network component or infrastructure.

For systems running Microsoft Windows 2016, the DCB provides interoperability layer between DCB-capable network adapters and DCB-capable switches. DCB allows system administrators to allocate bandwidth to class of traffic or priority-based on specific protocols or TPC/UDP ports.

The multipath I/O feature allows the system to use multiple paths components by creating multiple logical paths between the server and the storage array. In the event of ore or more of these logical paths fails, the multipath uses alternate path for I/O so the application can continue to access the data without interruption.

To install the DCB and multipath I/O to all of your Hyper-V nodes:

1. From the dashboard in the Server Manager panel of your Windows Server 2016, select **Manage** → **Add Roles and Features**, as shown in Figure 7-2.

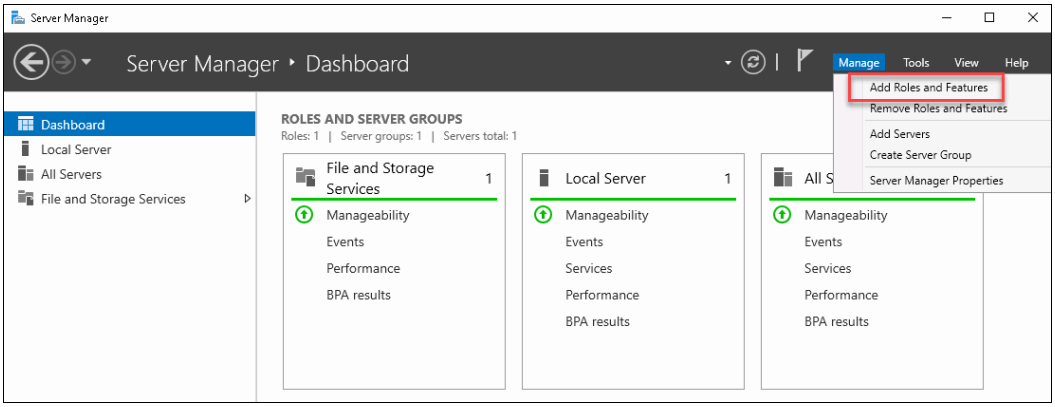


Figure 7-2 Add Roles and Features

2. The wizard initiates to assist system administrators in installing the roles, roles services, and features. Click **Next** to choose the installation type, and then click **Next** again to select a server from a server pool. If you need to configure multiple servers to the server pool, ensure that you select the correct server, and click **Next**.

3. If a server pool is not configured, follow the wizard by selecting the server to install the DCB and multipath I/O, as shown in Figure 7-3.

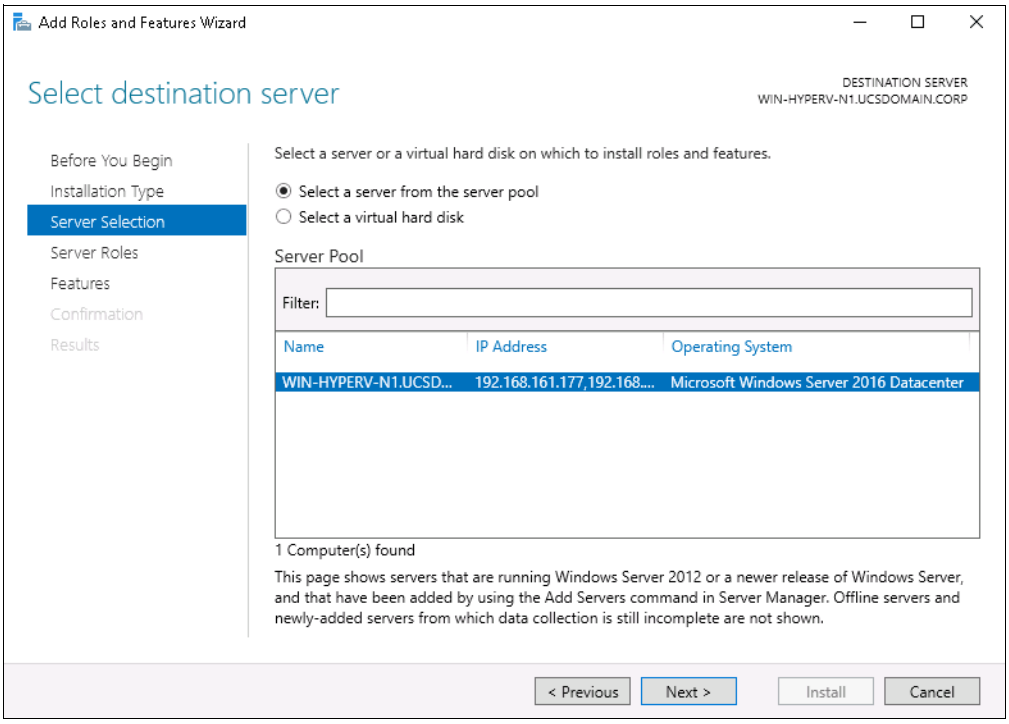


Figure 7-3 Selecting the destination server to install roles and features

4. Click the **Features** menu, and then select the **Data Center Bridging** and **Multipath I/O** options, as shown in Figure 7-4. Click **Next**.

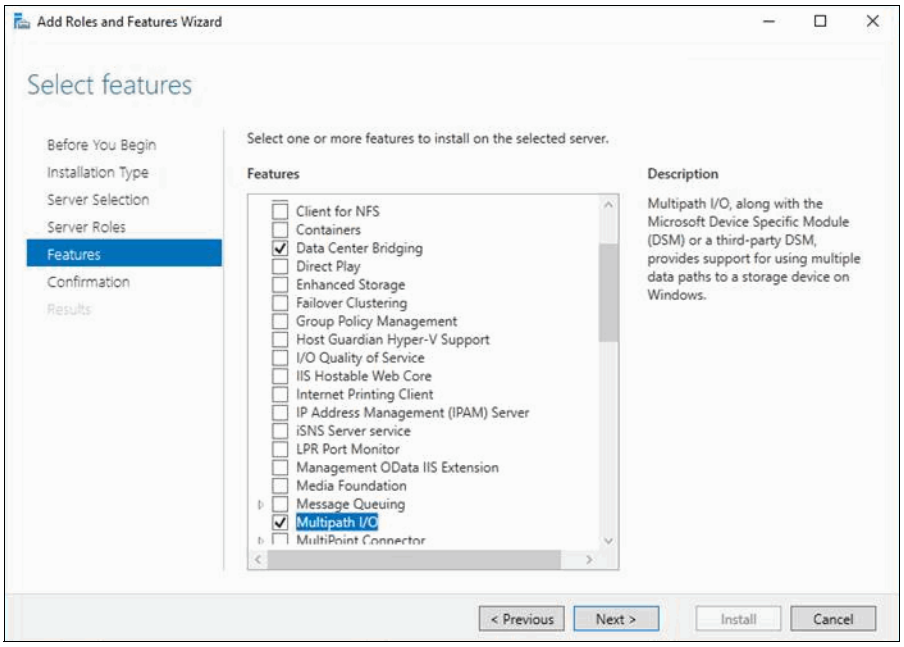


Figure 7-4 Installing DCB and Multipath I/O

5. Select the option to restart the server automatically after the installation or clear the option to restart the server at later time. Click **Install** to complete the installation.

7.4.2 Installing the IBM SDDDSM multipathing software

The IBM Subsystem Device Driver Device Specific Module (SDDDSM) is an IBM multipath software solution. The SDDDSM is a drive-specific module designed to support IBM storage arrays on a range of various operation systems platforms. The IBM SDDDSM provides software capabilities that allows the operational system to support multiple and redundant configuration environment for IBM Storage systems. For example, the IBM SDDDSM can provide load-balancing and also can protect a host from link failures, including a port failure on IBM FlashSystem 5030.

Important: Be sure to install the same version of the IBM SDDDSM on all cluster nodes.

Always verify the compatibility matrix to determine the correct and most suitable version of the IBM SDDDSM. Use the most recent version of the IBM SDDSDM. You can find the most recent version online.

Complete the following steps to download and install the IBM SDDDSM:

1. The examples in this book use the IBM SDDSDM package for IBM FlashSystem 5030, for OS platform Microsoft Windows 2016. You can download the software package from the IBM Support website.
2. Copy the software package to your Microsoft Windows server. With proper rights, run the `setup.exe` file to install the IBM SDDDSM. A command prompt window opens. Choose **Yes** to confirm the installation Figure 7-5.

Figure 7-5 Installing the IBM SDDDSM on Windows Server 2016

3. When the installation is completed, enter **Yes** to restart the system as shown in Figure 7-6.

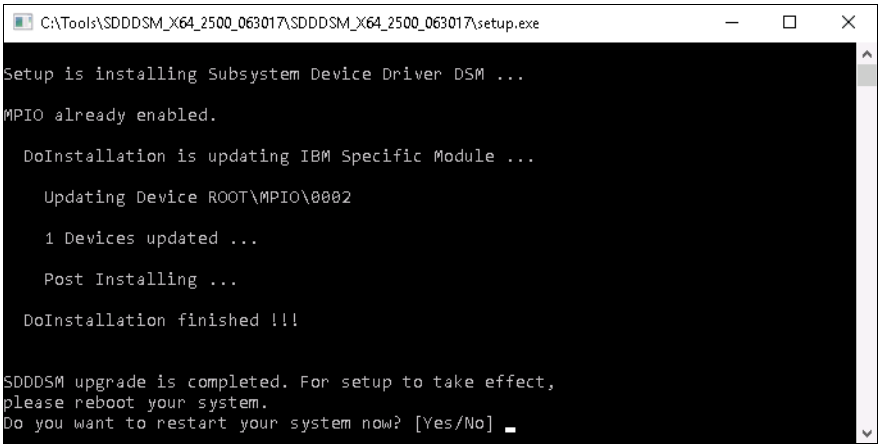


Figure 7-6 Completion of the IBM SDDDSM installation

4. FlashSystem 5030After the installation is complete and the server is back online, you can verify the IBM SDDDSM version by opening a command prompt window (or Windows PowerShell) and by running the **datapath query version** command, as shown in Example 7-1.

Example 7-1 Output of the datapath query wwpn command

```
C:\Program Files\IBM\SDDDSM>datapath query version
IBM SDDDSM Version 2.5.0.0
Microsoft MPIO Version 6.2.14393.82
```

5. The IBM SDDDSM is also useful to determine the host world wide port name (WWPN) that is assigned by Cisco UCS Mini. The WWPNs are required to perform SAN zoning for the host FC ports and to create host objects in the IBM FlashSystem 5030. To determine the host WWPN using SDDDSM, run the **datapath query wwpn** command, as shown in Example 7-2.

Example 7-2 Output of the datapath query wwpn command

```
C:\Program Files\IBM\SDDDSM>datapath query wwpn

        Adapter Name    PortWWN
        Scsi Port0:     20000025B5010A2E
        Scsi Port1:     20000025B5010B2E

C:\Program Files\IBM\SDDDSM>
```

7.5 Creating a host attachment in IBM FlashSystem 5030

This section guides you through the host configuration procedures that are required to attach supported hosts to the IBM FlashSystem 5030 attached to the Cisco UCS Mini environment. The IBM FlashSystem 5030 supports a wide range of host platforms, which makes it possible to consolidate storage in an open system environment into a common pool of storage. Hosts that are attached to IBM FlashSystem 5030 system by using FC protocol must be zoned appropriately, as described in 5.4, “Configuring UCS SAN connectivity” on page 62.

To create a host in the IBM FlashSystem 5030:

1. Log in to IBM FlashSystem 5030 and open the host configuration panel, as shown in Figure 7-7.

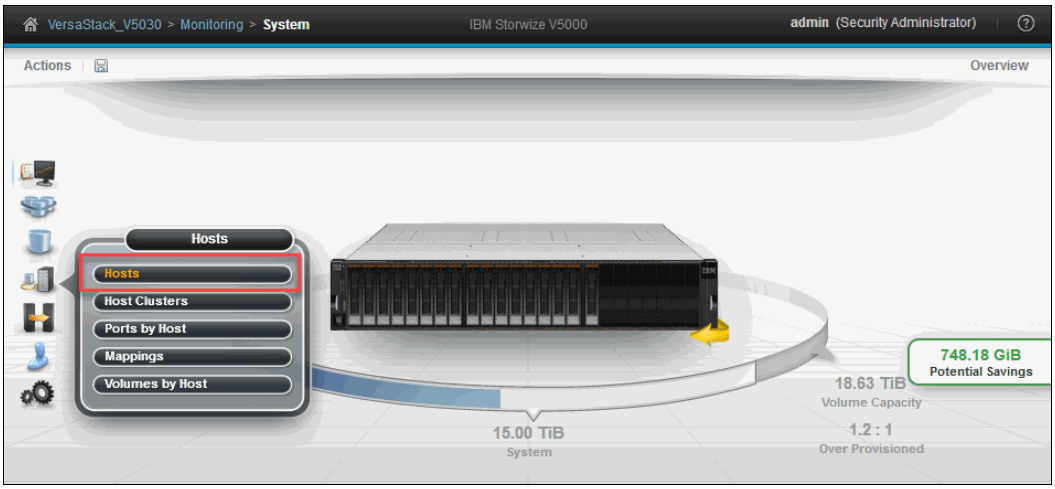


Figure 7-7 Creating a host in IBM FlashSystem 5030

2. Select **Add Host** to start the wizard, as shown in Figure 7-8.

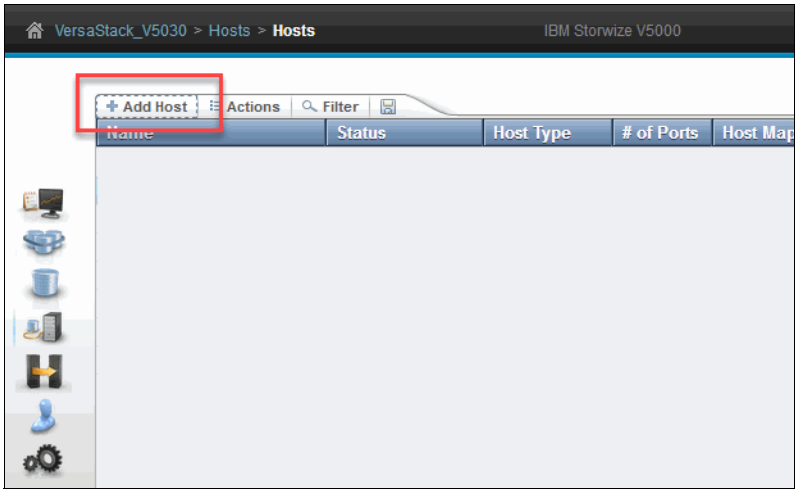


Figure 7-8 Adding new host to IBM FlashSystem 5030

3. To create a FC host, you need to enter a name and you must select the Fibre Channel host connection option, as shown in Figure 7-9. To add a Host Port (WWPN), click the down arrow to display a list of all WWPNs that are available to associate to that particular host.

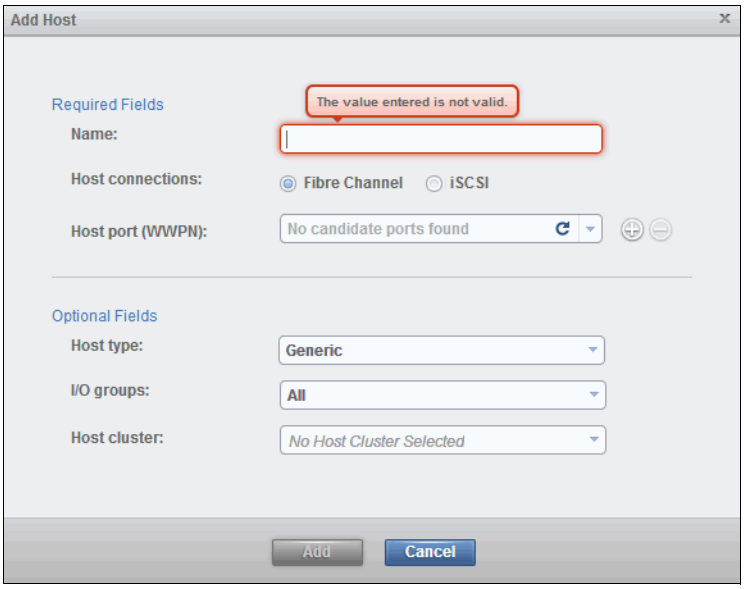


Figure 7-9 Creating a FC host

In the Optional Fields pane, specify the Host type and I/O group. Leave the Host cluster field as default, because you will create the host cluster in 7.6, “Creating a host cluster in the IBM FlashSystem 5030” on page 115 (the next section).

If you are creating a HP-UX host, select **HP-UX** as the Host type. For the I/O group, select the number of I/O groups that the host can have access from.

*For hosts running Microsoft Windows, choose **Generic** as the Host type.*

4. Click **Add** to create a host object in the IBM FlashSystem 5030.

7.6 Creating a host cluster in the IBM FlashSystem 5030

A host cluster allows a user to create a group of hosts to form a cluster, which is treated as one entity instead of dealing with all of the hosts individually in the cluster. The host cluster is useful for hosts that are participating in a cluster at host operating system levels. By defining a host cluster, the user can map one or more volumes to the host cluster object. As a result, the volume or set of volumes gets assigned to each individual host object that is part of the host cluster. In addition, each of the volumes gets mapped with the same SCSI ID to all the hosts that are part of the host cluster with just one command.

To create the Hyper-V hosts in the IBM FlashSystem 5030:

1. Log on to IBM FlashSystem 5030 and select **Host Clusters** from the **Host** menu, as shown in Figure 7-10.

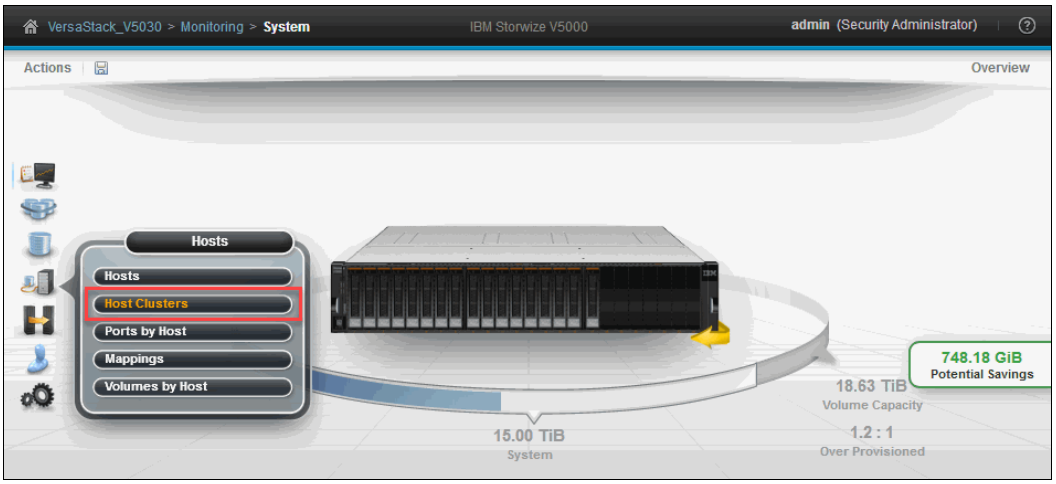


Figure 7-10 Creating a host cluster

2. Click **Create Host Cluster** to start the wizard, as shown in Figure 7-11.

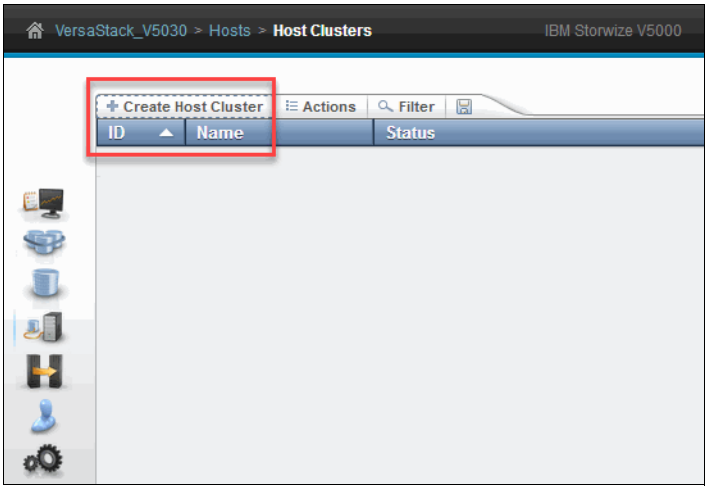


Figure 7-11 Starting the wizard

3. To create a host cluster, you need to specify a *name* for the host cluster and select the *hosts objects* to assign to the new host cluster, as shown in Figure 7-12. Any current volume mappings become the shared mappings for all the hosts on the host cluster. You can always add, remove, and modify the host clusters objects. Click **Next** to complete the host cluster creation.

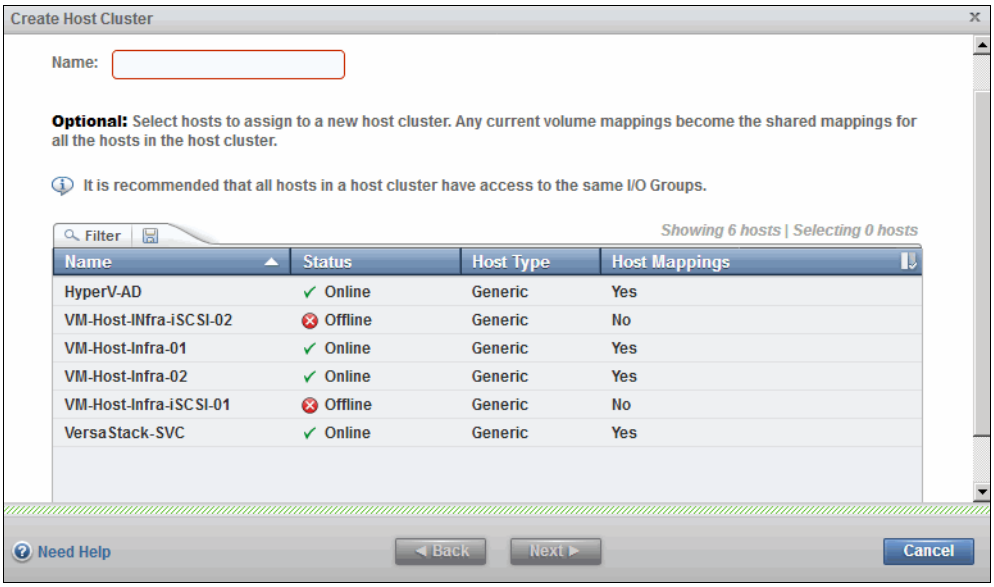


Figure 7-12 Creating a host cluster

This example creates a host cluster that contains two members of host objects, as shown in Figure 7-13.

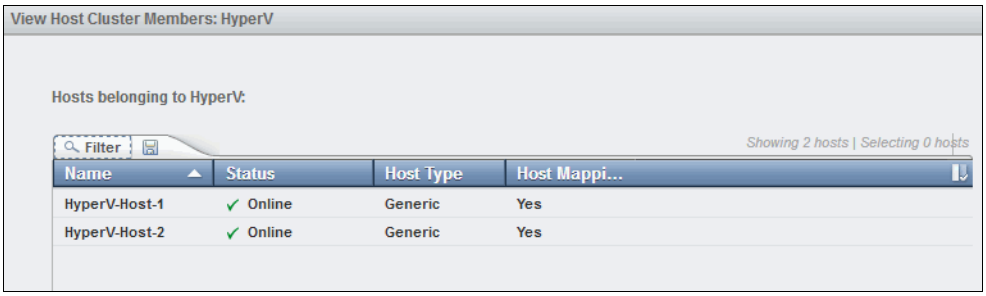


Figure 7-13 Viewing cluster members

7.7 Provisioning IBM Storwize Volume for Cluster Shared Volumes

Cluster Shared Volumes (CSV) allows multiple cluster nodes in a failover cluster to simultaneously have read-write access to the same logical unit number (LUN) presented by the IBM FlashSystem 5030 in a general-purpose, clustered file system, which is layered above NTFS.

Using CSV, clustered nodes can fail over the cluster resources quickly from one node to another node without requiring a change in drive ownership or dismounting and remounting a volume. CSV also help simplify the management of multiple LUNs that are assigned to failover clusters.

For the purposes of this implementation, the CSV is an important component and is used mainly to support the clustered virtual hard disk (VHD) files for the virtual machines running on top of Hyper-V cluster.

The examples that follow assume that host cluster object is already created in the IBM FlashSystem 5030 and that a number of volumes need to be provisioned for all nodes of the cluster that will be part of Failover Clustering feature.

Also for the purposes of this example, a 1 Gb size volume is provisioned, and a similar procedure must be followed to assign additional volumes that will be used as clustered shared volumes.

To assign volumes to the host cluster using the IBM FlashSystem 5030:

1. Log on to IBM FlashSystem 5030, click the **Volumes** icon and select the **Volumes** menu, as shown in Figure 7-14.

Figure 7-14 Assigning new volume

2. The wizard starts, as shown in Figure 7-15 on page 119, and guides you through the Quick Volume Creation menu to create Basic and Mirrored volumes in a system with this topology. Also, you can use the Advanced option to provision volumes with a number of presets available in the IBM FlashSystem 5030 GUI.

> **Capacity Savings parameter:** The Quick Volume Creation wizard provides the Capacity Savings parameter, which is the ability to change the default provisioning of a Basic or Mirrored Volume to Thin-provisioned or Compressed. For more information, see Chapter 9, “The IBM FlashSystem 5030 advanced functions” on page 205.

When using the Quick Volume Creation, the IBM FlashSystem 5030 allows you to create basic type of volume, which is fully provisioned, with the entire size dedicated to the defined volume. The host or the cluster object defined in the system see the fully allocated space.

To create a Basic volume, click the **Basic** icon, shown in Figure 7-15. This action opens an additional input window where you must define the following information:

- *Pool*: The pool in which the volume is created (drop-down)
- *Quantity*: The number of volumes to be created (numeric up/down)
- *Capacity*: Size of the volume in units (drop-down)
- *Capacity Savings*:
  - None
  - Thin-provisioned
  - Compressed
- *Name*: Name of the volume (cannot start with a numeric)
- *I/O group*

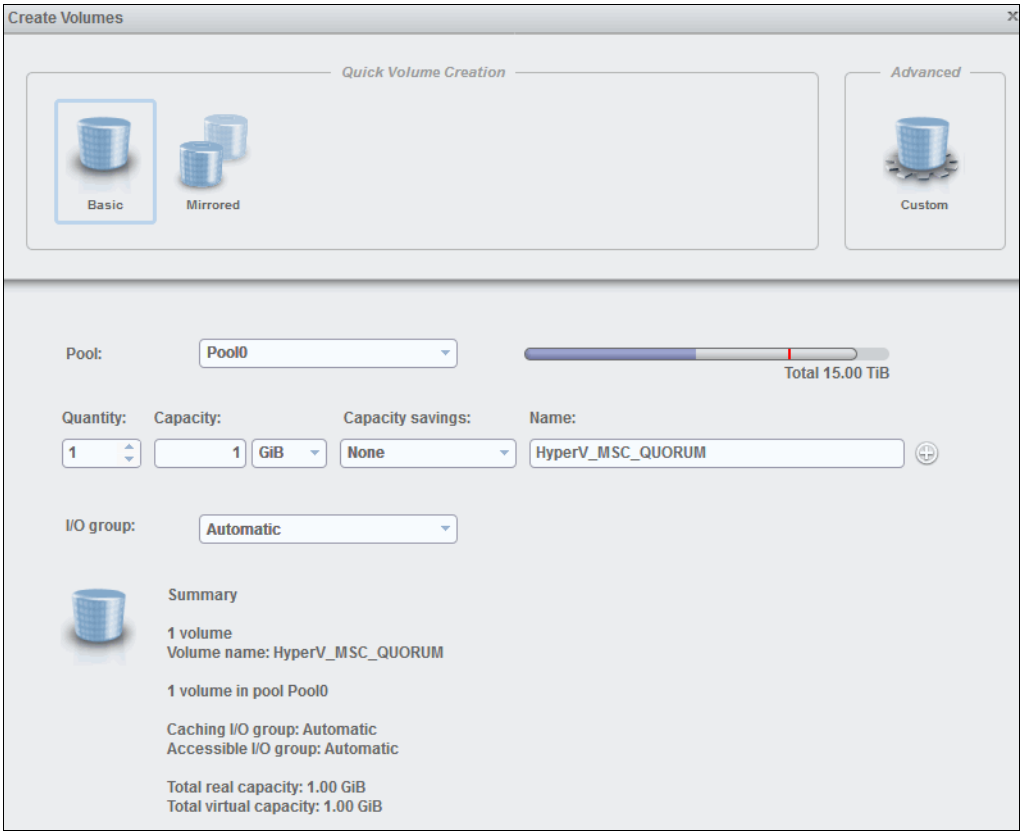


Figure 7-15 Provisioning a new volume using IBM FlashSystem 5030 GUI

3. Click **Create and Map** to create the volume and assign to a host or cluster.

   When the wizard completes the volume creation, a new wizard opens and allows you to select the host or the host clusters that is to have the volume mapped.

4. Select **Host Clusters** and **Hyper-V host cluster** object as shown in Figure 7-16.

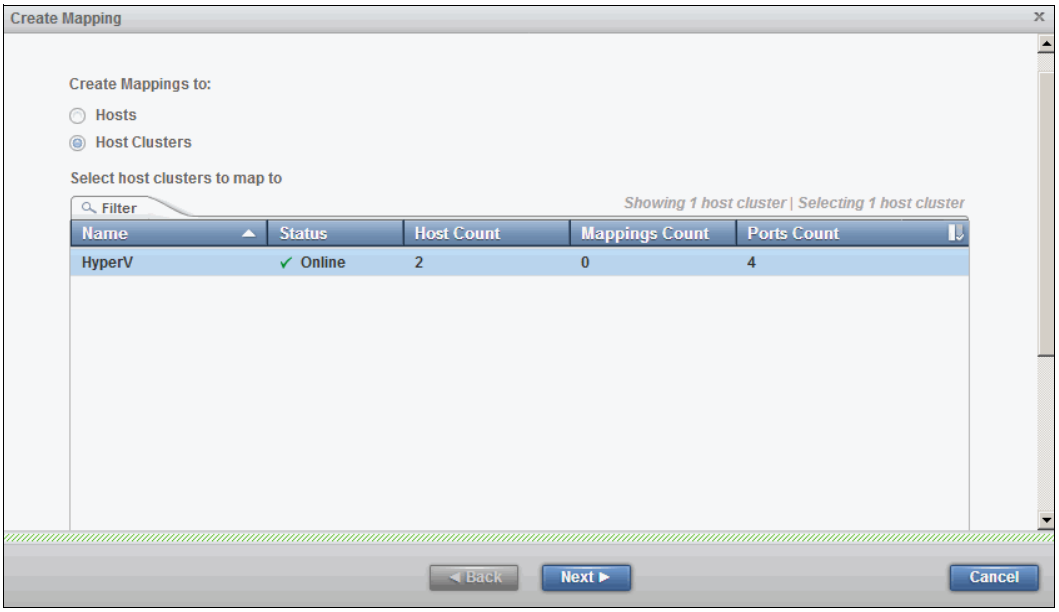


Figure 7-16 Creating a host cluster mapping

5. Scroll down to select the SCSI ID assignment. When selecting **System Assign**, the IBM FlashSystem 5030 assigns the next available SCSI ID incrementally. By choosing **Self Assign**, the system allows you to enter the SCSI ID before the mappings are created. In this option, you always must select an ID that is not in use; otherwise, the volume cannot be assigned to a host or host cluster. Select **System Assign** and click **Next** to continue.
6. The *HyperV_MSC_QUORUM* volume is mapped to host cluster object Hyper-V, and the SCSI ID is assigned automatically, as shown in Figure 7-17 on page 120. Click **Map Volumes** to map the volume. Wait for the wizard to complete the disk assignment, and then close the wizard.

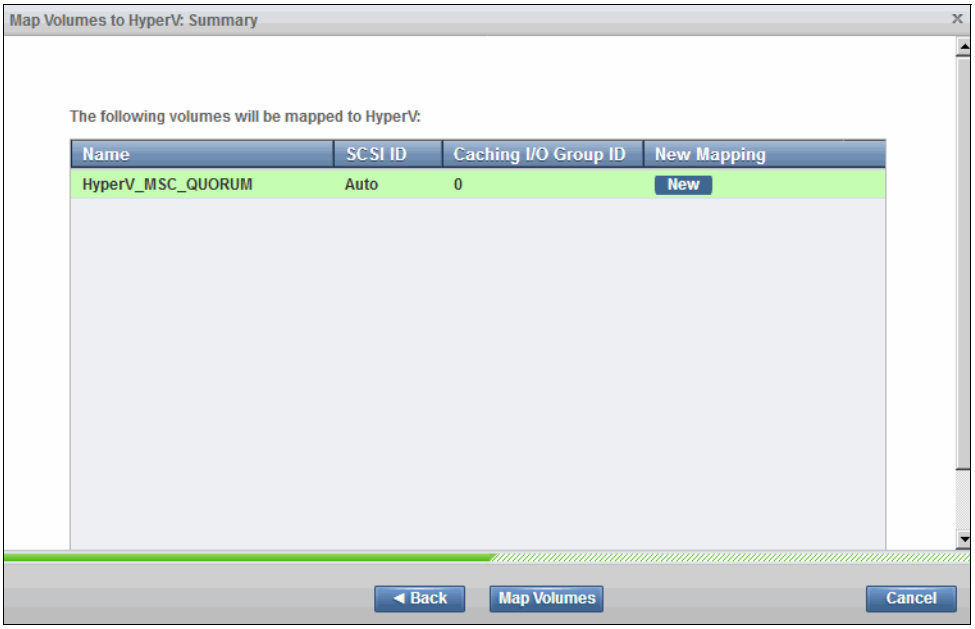


Figure 7-17 Mapping a volume to Host Cluster

7.8 Rescanning and assigning the cluster shared volumes

You can use one of the following methods to rescan the new disks presented to Windows Servers:

- `diskpart.exe`
- PowerShell
- The Disk Management utility (GUI)

For each node of the cluster, complete the following steps to rescan and assign the IBM LUNs as a cluster shared volume:

1. Log on to each node of the Windows Failover Cluster.
2. In the Server Manager panel, go to **Tools** → **Computer Management**.
3. Switch to **Disk Management** as shown in Figure 7-18 on page 121.

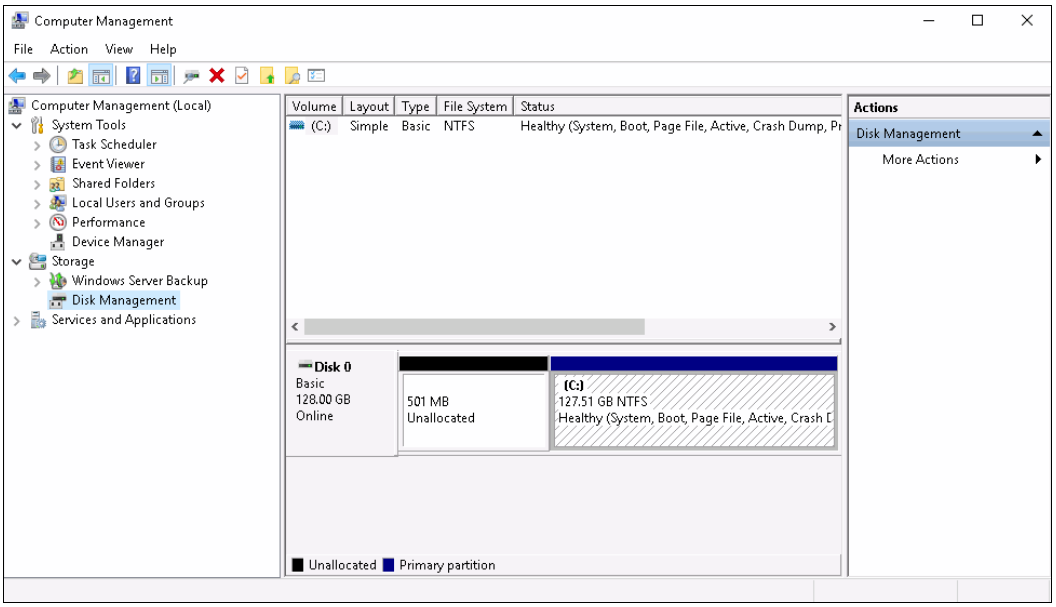


Figure 7-18 Windows Disk Management utility

4. Select **Action** → **Rescan Disks**, as shown in Figure 7-19, to rescan all disk devices and the operation system displays the new volumes that are connected to the Windows host.

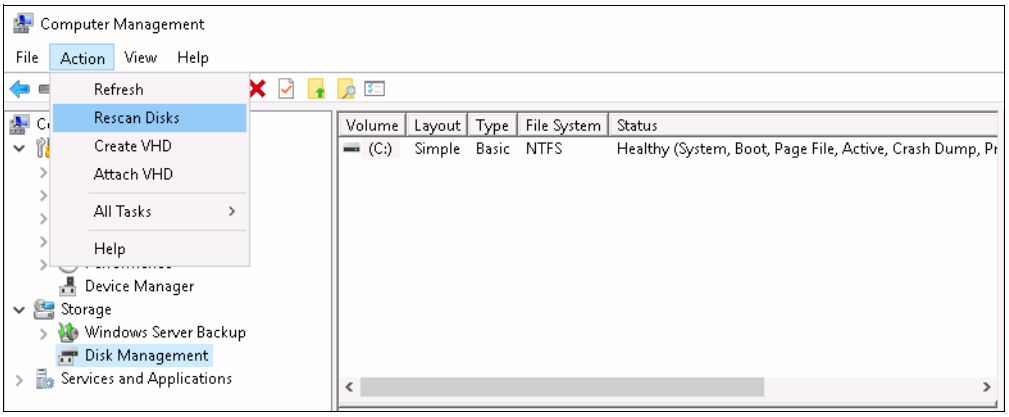


Figure 7-19 Rescan Disks

The new disk volumes are listed as offline.

Tip: If the status of the volume shows *online*, the volume was initialized before. In this case, you can skip this step.

5. Right-click the volume, and select **Initialize Disk** to initialize the volume. The volume comes online and is unallocated, as shown in Figure 7-20 on page 122.

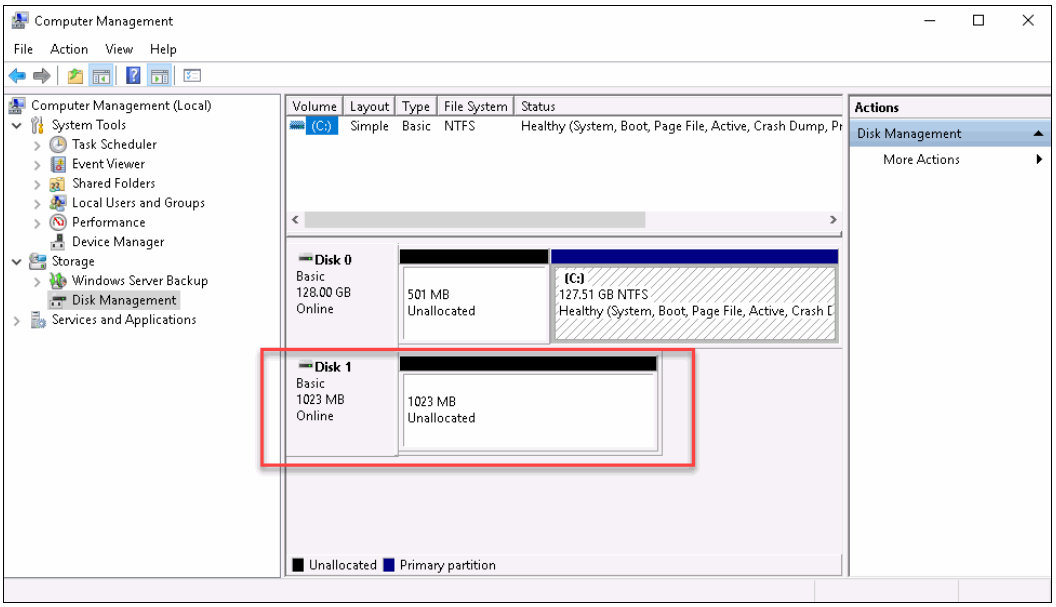


Figure 7-20 Disk rescanning operation

6. If the volume is online and unallocated, you must right-click the volume and select **New Simple Volume**. The wizard then guides you through the process to create a new simple volume. When complete, click **Finish**, as shown in Figure 7-21.

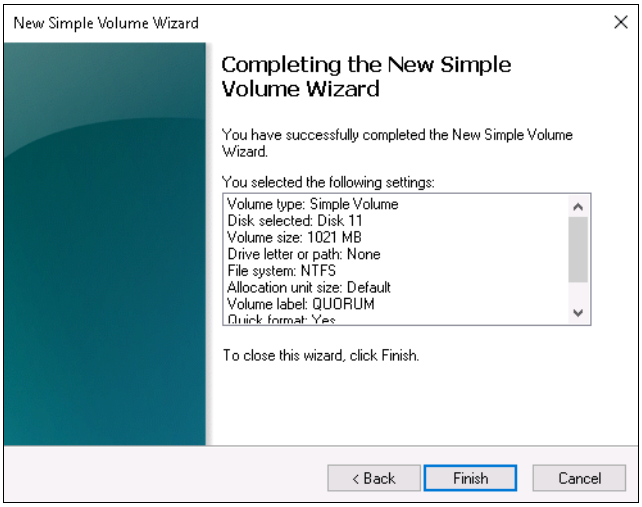


Figure 7-21 Creating a new simple volume

7. Repeat the previous step for other nodes of the cluster, because this step is a prerequisite to configure the failover cluster.

7.9 Configuring the Failover Clustering feature

This section describes the steps to configure the Failover Clustering feature. The Failover Clustering feature can be installed with using Server Manager, PowerShell, or Microsoft System Center.

To add the Failover Clustering feature into both nodes of the cluster:

1. In the Server Manager panel, select **Manage** → **Add Roles and Features** to start the wizard as shown in Figure 7-22.

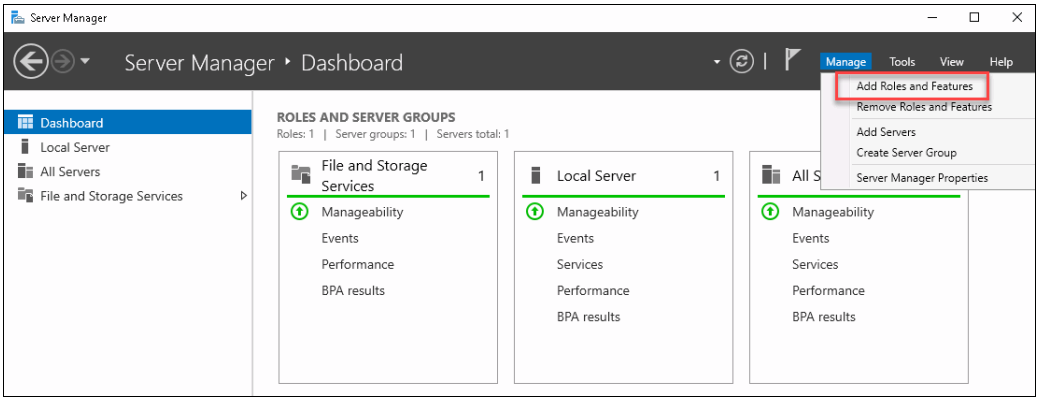


Figure 7-22 Starting the wizard

2. This wizard guides you through the process to validate each node for potential failover clusters and to configure changes to the failover clusters. Select **Validate the Configuration**, as shown in Figure 7-23, to initiate the validation tests in order to determine whether this configuration of two nodes of servers and attached storage is set up correctly to support the Failover Cluster capabilities.

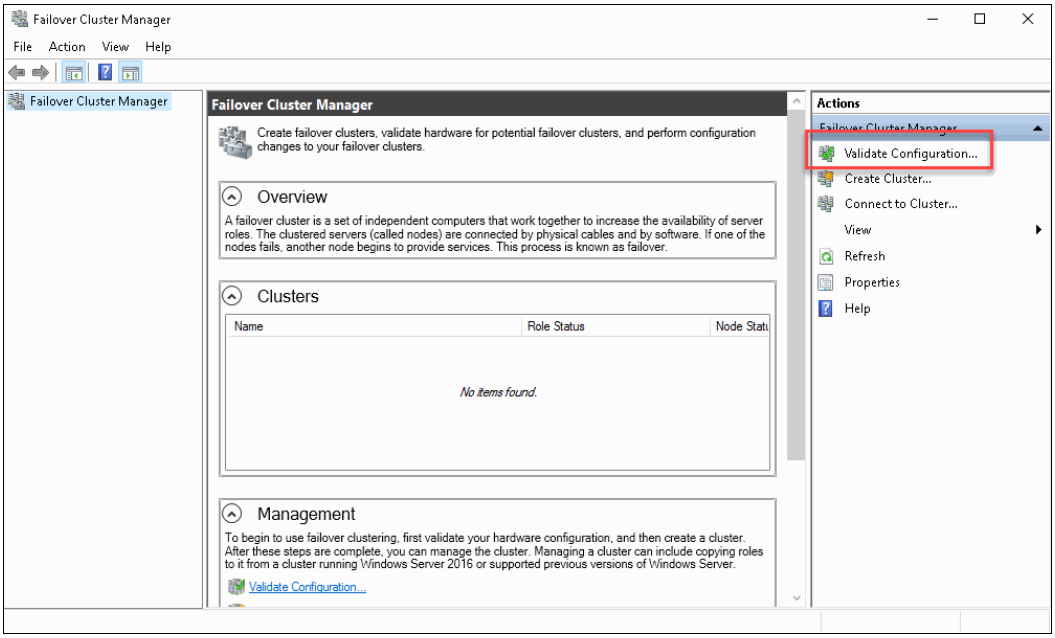


Figure 7-23 Validating the cluster configuration

3. Enter the host name or the IP addresses of the nodes of the failover cluster, as shown in Figure 7-24 on page 124. Click **Next** to move to the next step.

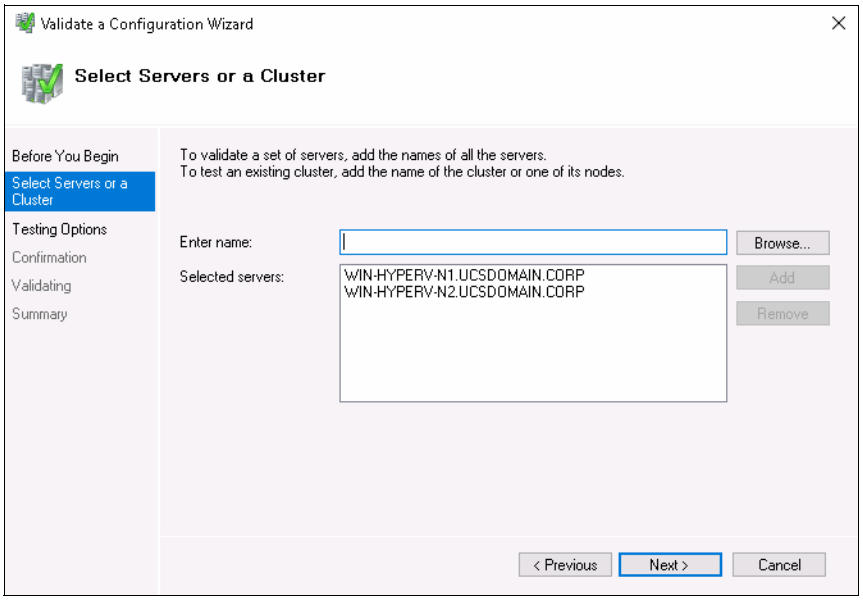


Figure 7-24 Entering the name or IP address of the nodes

4. The wizard recommends to run all the tests that include overall systems that are necessary for cluster configuration, Hyper-V configuration, inventory, network and shared storage, as shown in Figure 7-25. Click **Next** to run all tests.

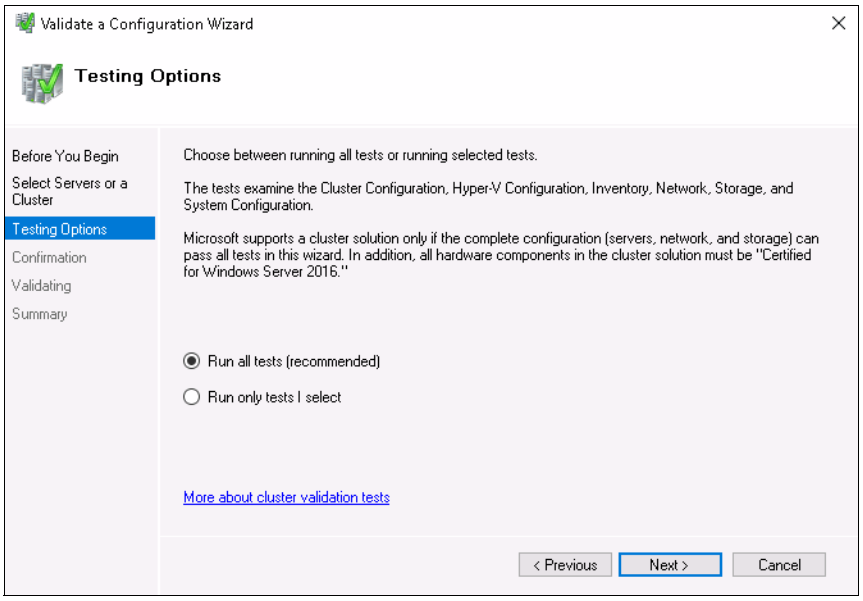


Figure 7-25 Cluster test for pre-configuration cluster

5. In the next panel, select **Next** to examine all components listed by the wizard.
6. Ensure that the test completes successfully and that there are no pending actions. You can always go back to make further system-wide adjustments. Click **Finish** when the wizard completes the verification.

7. In the main wizard, select **Create Cluster**, as shown in Figure 7-26.

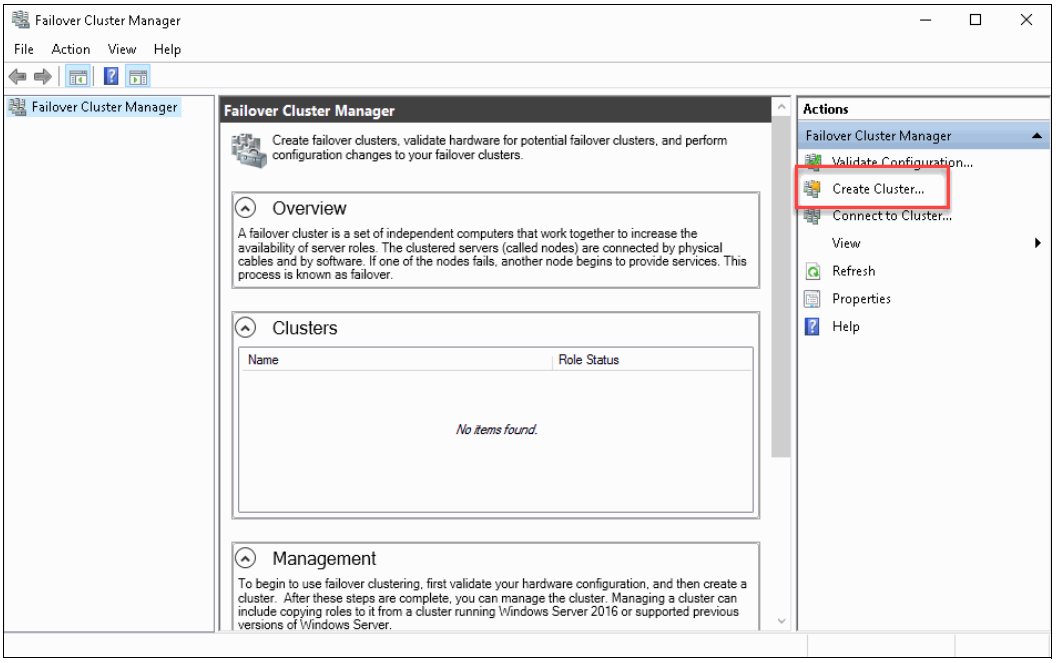


Figure 7-26 Creating a failover cluster

8. In the “Before You Begin” panel, click **Next** and the wizard allows you to enter the cluster nodes, as shown in Figure 7-27.

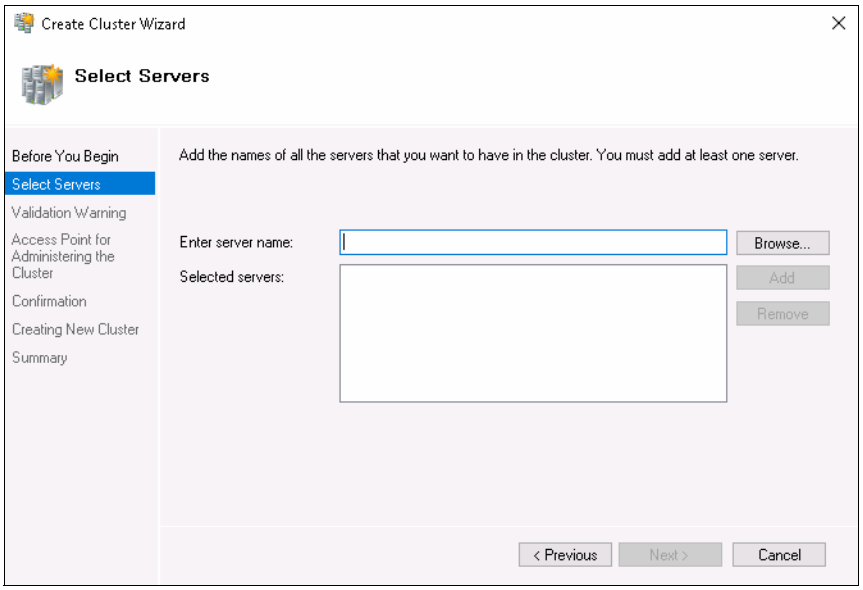


Figure 7-27 Create a cluster node

9. Enter the FQDN or IP address of each member of the cluster and click **Next** to continue.

10. Next enter the cluster name (Figure 7-28). The cluster name is generally used when administering the cluster using Windows tools, such as Failover Cluster Manager. Click **Next** to move to the next step.

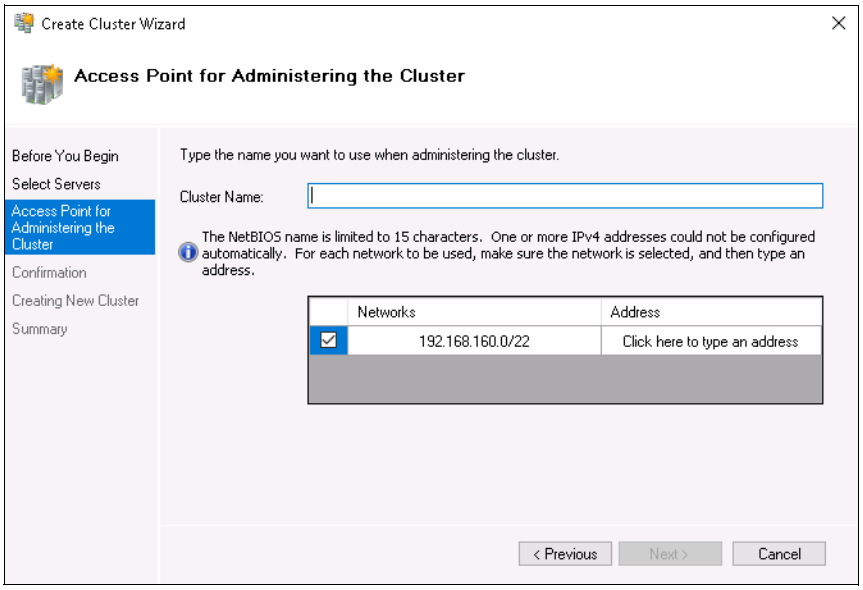


Figure 7-28 Enter a cluster name

11. After entering the cluster name and the cluster IP address, you can review the cluster configuration as shown in Figure 7-29. Click **Next** and **Finish** to confirm and complete the failover cluster configuration.

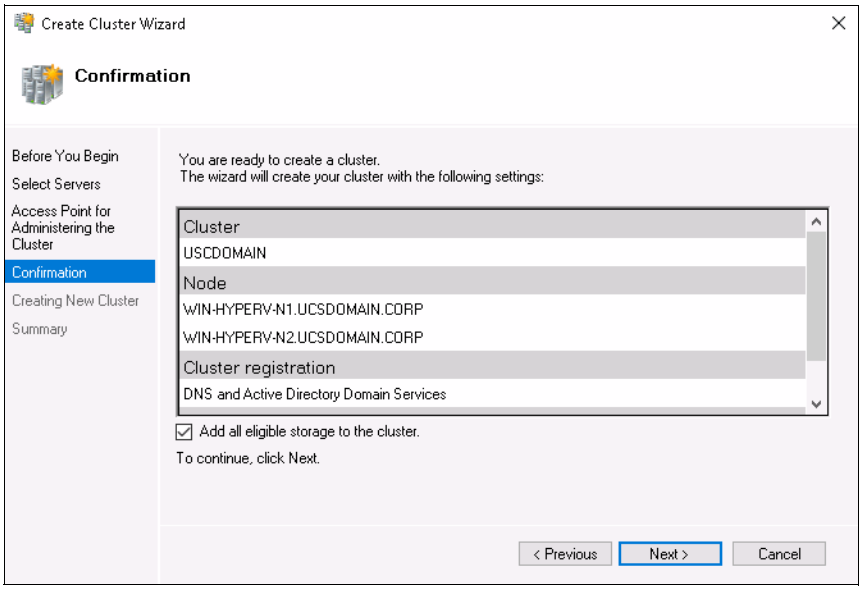


Figure 7-29 Confirmation to create the cluster

12. As shown in Figure 7-30, the cluster configuration was successful. The wizard automatically opens the Failover Cluster Manager GUI.

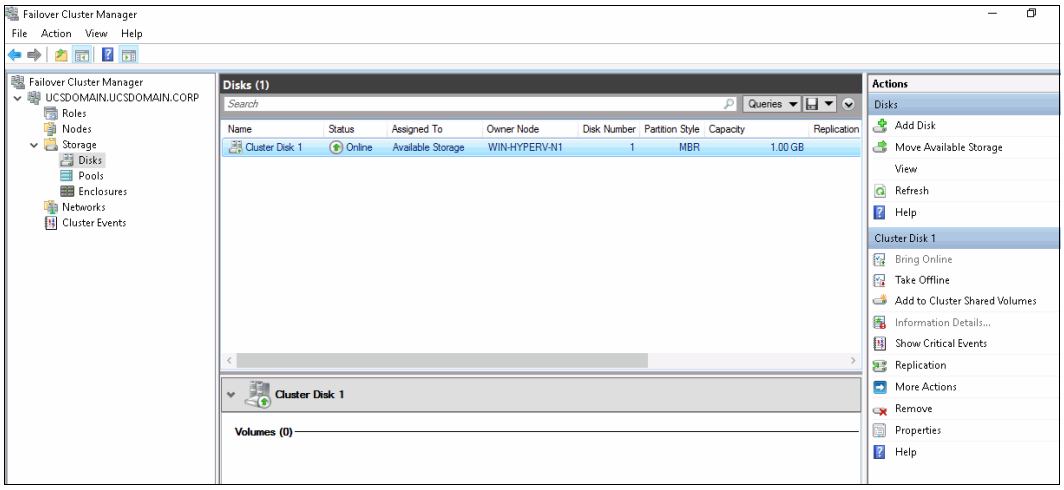


Figure 7-30 Failover Cluster Manager GUI

7.10 Adding the Hyper-V feature

To add the Hyper-V feature to both nodes of the cluster previously set up:

1. By using the dashboard in the Server Manager panel, navigate to **Manage** → **Add Role and Features**, as shown in Figure 7-31.

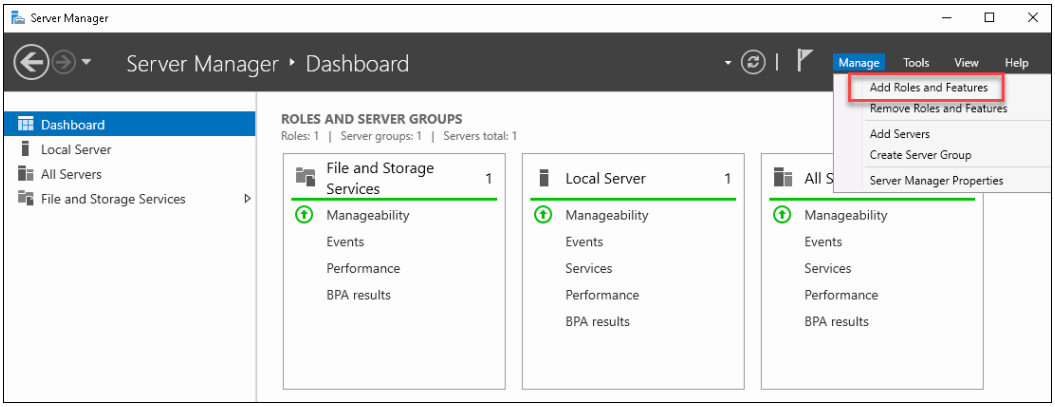


Figure 7-31 Adding the Hyper-V feature

2. Click **Next** when the wizard opens. Be sure to select the **Robe-base feature installation** option, and then click **Next** again to select the required feature to add.

3. Click **Next** after selecting the server from Server Pool list, as shown in Figure 7-32.

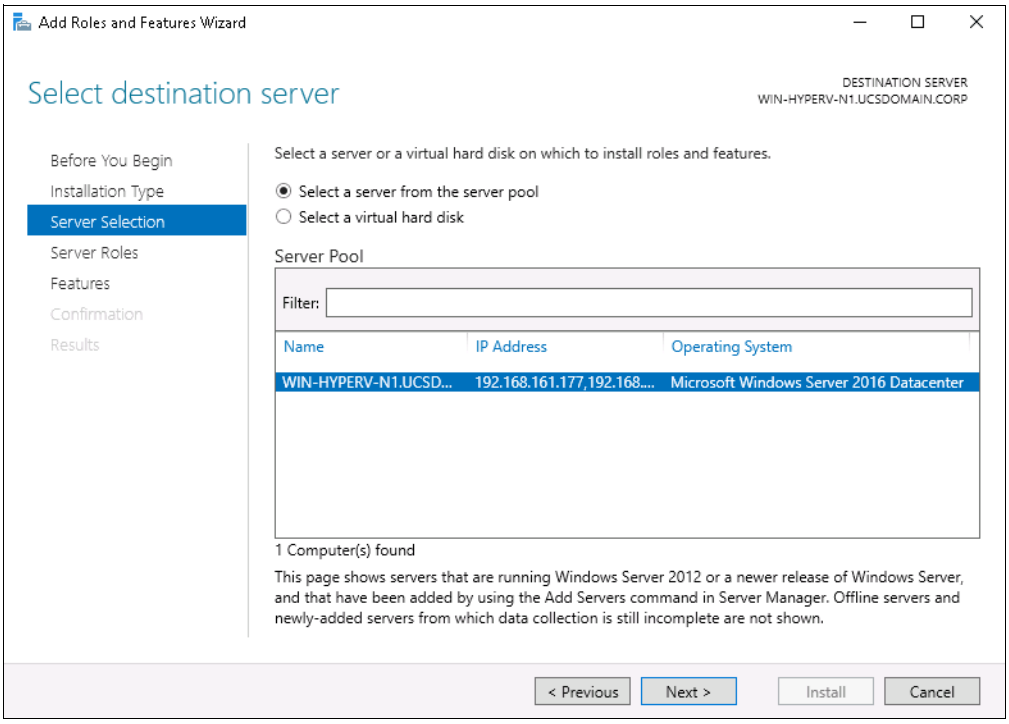


Figure 7-32 Selecting the Server to add the Hyper-V feature

4. Select the Hyper-V feature and select the check box to include all management tools, as shown in Figure 7-33. Click **Add Features** and then click **Next** again.

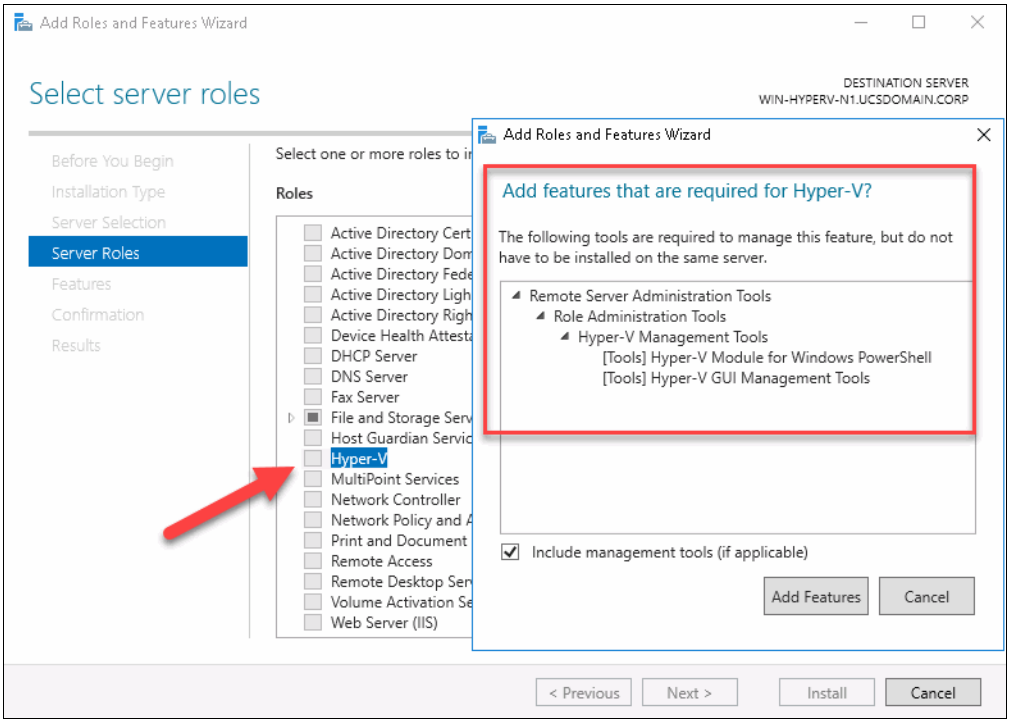


Figure 7-33 Adding the Hyper-V feature tools

5. Next, you can choose the number of virtual switches to be created to communicate with other computers in the same environment. In this example, one virtual switch is created for each network adapter, as shown in Figure 7-34. Click **Next** to continue with the installation.

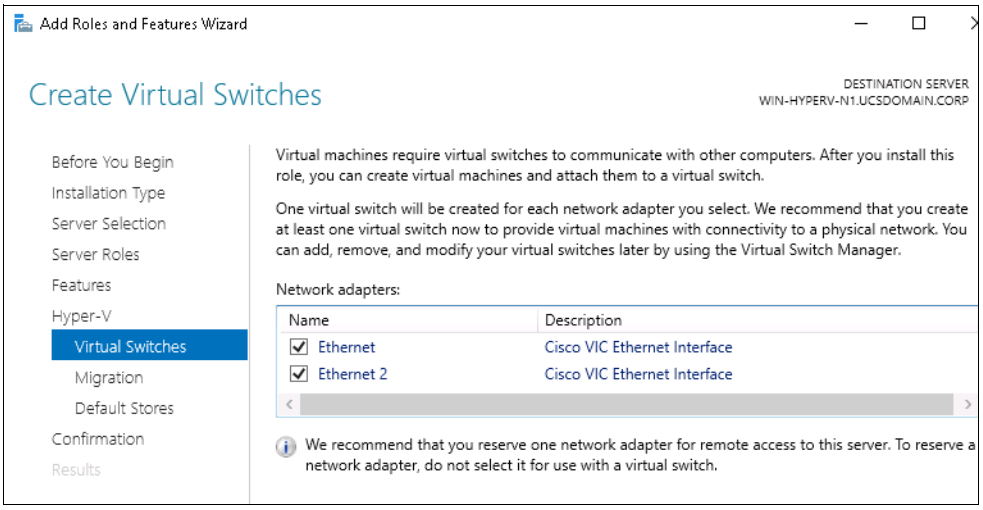


Figure 7-34 Create virtual switches

6. Next, you can set the rights to send and receive live migrations of virtual machines in the Hyper-V servers. This example selects the **Allow this server to send and receive live migrations of virtual machines** options, as shown Figure 7-35. Click **Next**.

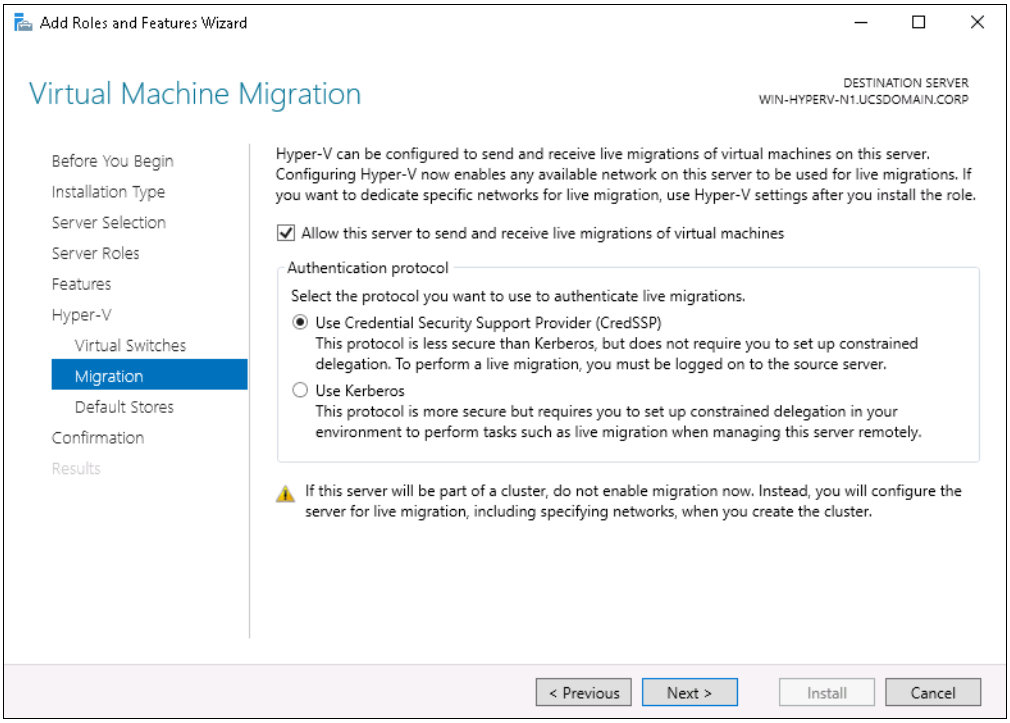


Figure 7-35 Hyper-V for live migration setup

7. Now, you can set default locations for virtual hard disks. For the purposes of this installation, the default locations are set. You can change these settings later by using the Hyper-V settings. Click **Next** to proceed with the Hyper-V feature installation, as shown in Figure 7-36.

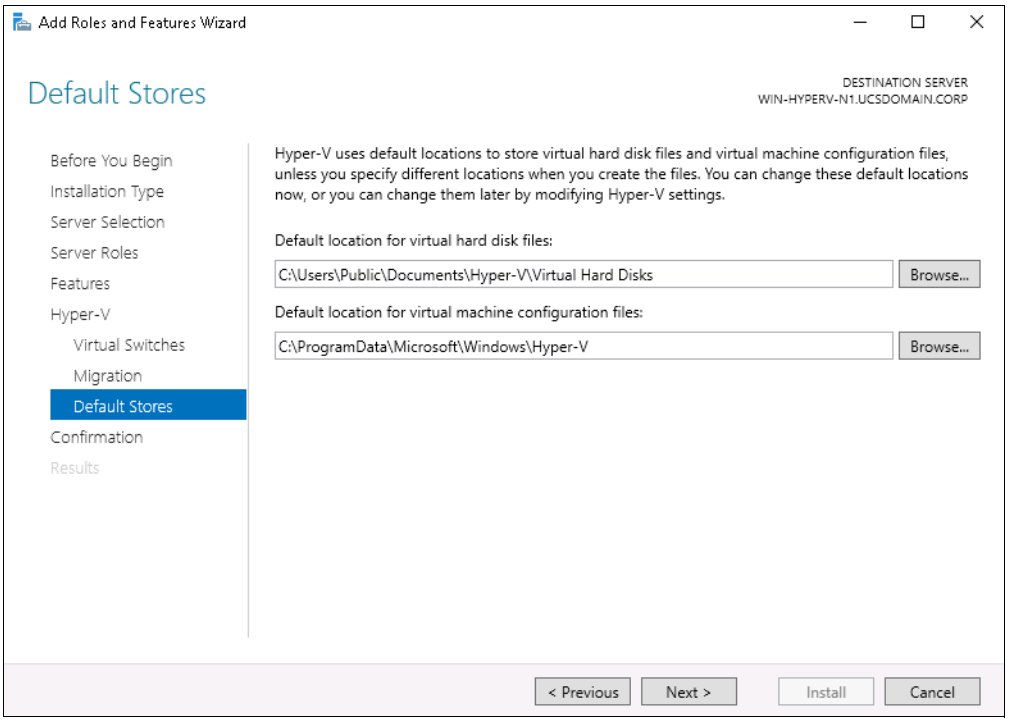


Figure 7-36 Hyper-V settings for virtual disk files

8. Confirm the installation selections for the Hyper-V feature, and click **Install**. You can select the **Restart the destination server automatically if required** option to allow the system to restart the server and to commit the few feature. Click **Install** (as shown in Figure 7-37 on page 131) to allow the wizard to complete the installation of the Hyper-V feature.

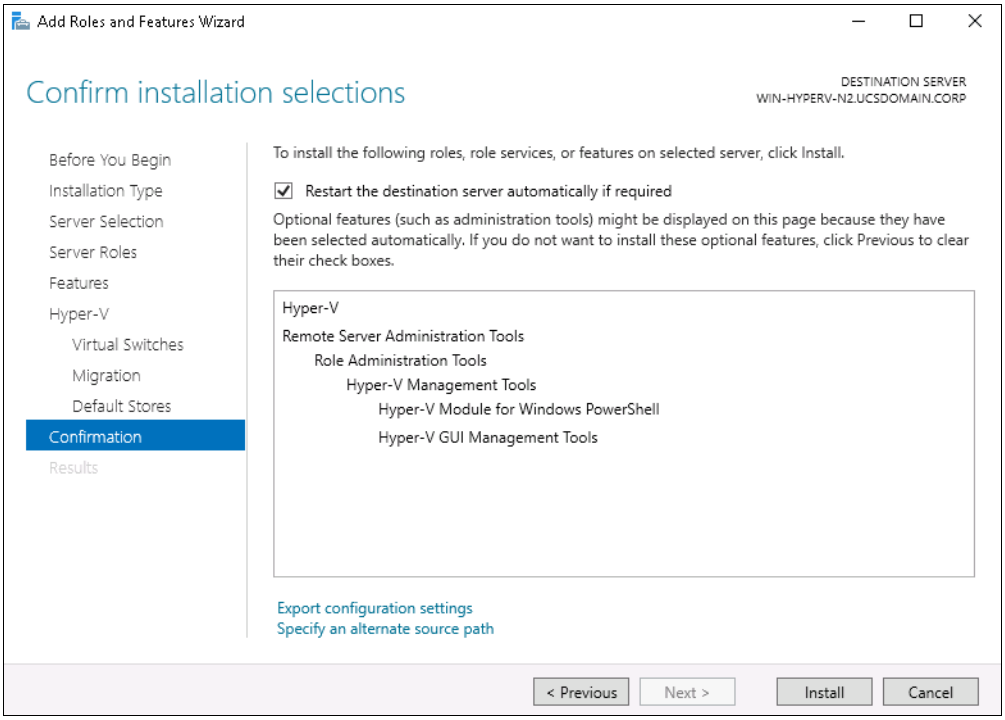


Figure 7-37 Installing the Hyper-V feature and tools

7.11 Microsoft Virtual Machine Manager

Microsoft Virtual Machine Manager (VMM) provides a unified user interface across on-premises, service provider, and the Azure cloud. By using VMM, you can configure and manage your data center components, such as physical and virtual components, as a single fabric. VMM provisions and manages the resources needed to create and deploy virtual machines and services to private clouds.

This document uses the VMM release 2016.

7.12 Configuring the Hyper-V virtual network using Microsoft Virtual Machine Manager

This section describes the steps to configure optimal network settings in your Hyper-V environment using Cisco UCS Mini. The steps described in this section assume that the Microsoft System Center VMM is installed and running.

Microsoft System Center provides a set of tools for datacenter virtualization tools that enables you to configure and manage your virtual hosts, network aspects and storage resources. Throughout this section, examples use the VMM, which is essentially a component of the entire System Center solution.

This section focuses on configuring the network, storage, and servers in VMM to deploy and manage the entirely Hyper-V environment and virtual servers, in various aspects.

7.12.1 Network settings

Figure 7-38 provides a high-level view of the steps that this section discusses.

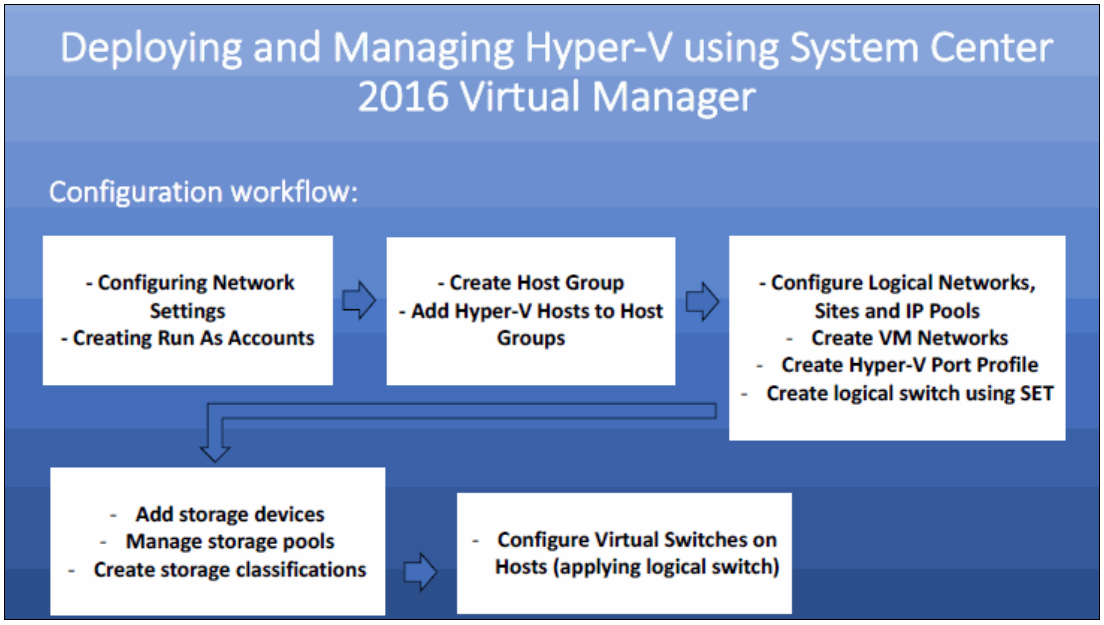


Figure 7-38 Deploying a virtual environment using System Center 2016

By default, VMM creates logical networks automatically. When you provision a host in the VMM fabric and there is no VMM logical network associated with a physical network adapter on that host, VMM automatically creates a logical network and associates it with an adapter.

To disable automatic logical network creation:

1. Open Microsoft System Center VMM, and then open the Settings workspace.
2. Select the **General** navigation node.
3. Double-click **Network Settings** in the details pane.

4. In the Network Settings dialog box, clear the **Create Logical Networks Automatically** option (Figure 7-39), and click **OK**.

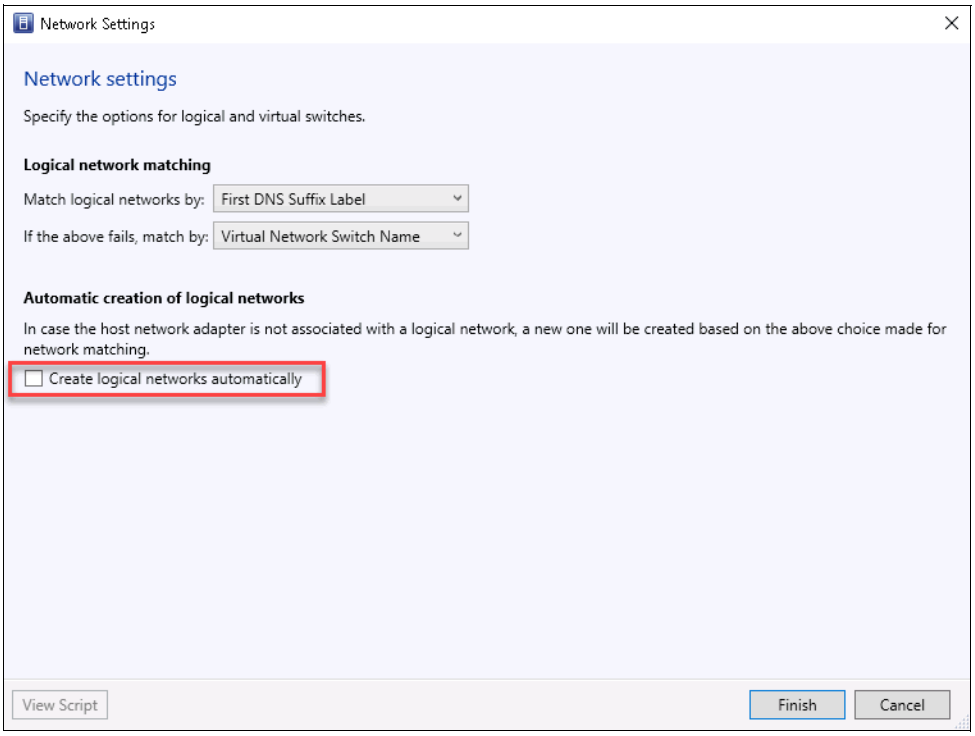


Figure 7-39 Network settings using VMM

5. Click **Finish**.

7.12.2 Configuring Run As account

A *Run As account* is a container for a set of stored credentials. In VMM a Run As account can be provided for any process that requires credentials. Administrators and delegated administrators can create Run As account.

For this deployment, create a Run As account to add the Hyper-V hosts, the IBM FlashSystem 5030 and many other tasks. To create a Run As account:

1. Click **Settings**, and in the Create menu, click **Create Run As account**.
2. In the Create Run As account field, specify a name and an optional description to identify the credentials in VMM.
3. In the User name and Password fields, specify the credentials. The credentials can be a valid Active Directory user or group account, or local credentials.
4. Clear the **Validate domain credentials** option if you don't need it, and click **OK** to create the Run As account. Figure 7-40 on page 134 shows an example of this dialog box.

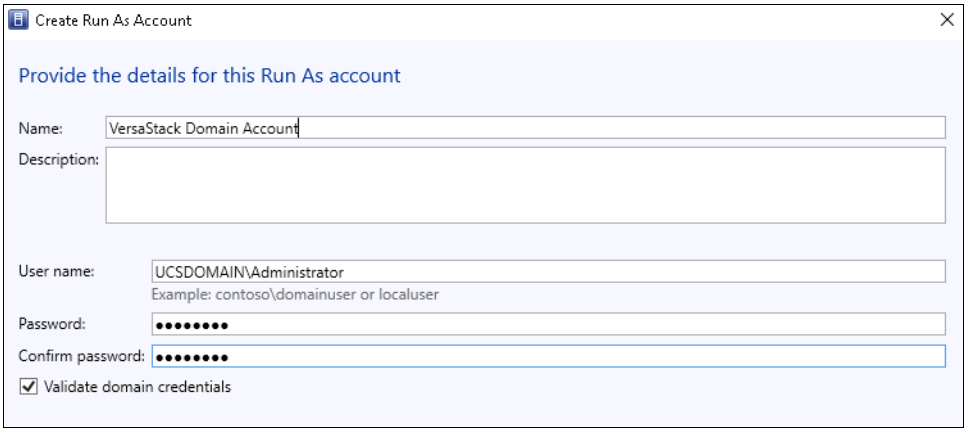


Figure 7-40 Creating a Run As account in VMM

You can follow these same steps to create an additional Run As account to add the IBM FlashSystem 5030 in VMM. If the storage array is not configured to use the Active Directory as authentication services, ensure that you enter the correct user name and password and then clear the **Validate domain credentials** option.

7.12.3 Host group containers

This section covers the creation of host groups and how to add Windows Server machines to the host groups. You can use host groups to group hosts in meaningful ways, often based on the physical site location, private cloud or resource allocation.

To create a host group structure in VMM that aligns with your organizational needs:

1. Open the Fabric workspace.
2. In the Fabric pane, expand **Servers**, and then do either of the following actions:
   a. Right-click **All Hosts** and then click **Create Host Group** as shown in Figure 7-41.
   a. Click **All Hosts**. In the Folder tab, in the Create group, click **Create Host Group**. VMM creates a new host group that is named as `New host group`, with the host group name highlighted. Just enter the new name of the host group.

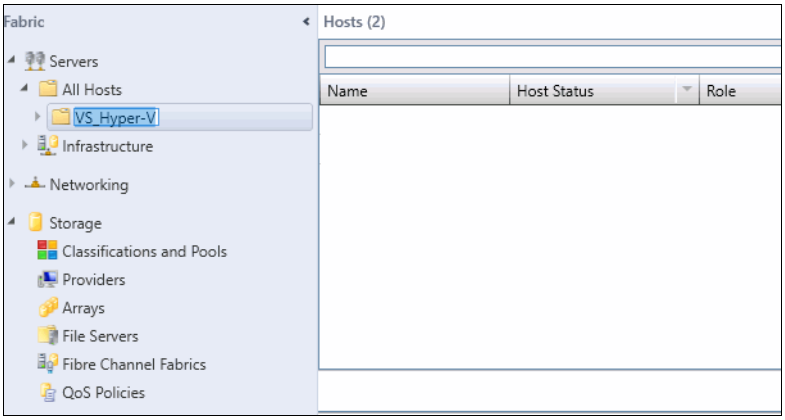


Figure 7-41 Creating a host group

3. Repeat the steps in this section to create the additional host group structure.

7.12.4 Adding the Hyper-V Cluster to host groups

The steps in this section assume that you have completed the steps in 7.9, “Configuring the Failover Clustering feature” on page 123 and 7.10, “Adding the Hyper-V feature” on page 127. Later in this chapter, sections cover steps and requirements to add a stand-alone Windows Server to VMM.

After the host group is created, you can add the Hyper-V hosts to VMM host group. To add a Hyper-V host to host group:

1. Open the Fabric workspace.
2. Select a host group, using the top menu, click **Add Resources**, and then click add **Hyper-V Hosts and Clusters**. The Add Resource wizard starts.
3. On the Resource location page, click **Windows Server computers in a trusted Active Directory domain**, and then click **Next**.
4. On Credentials page, select **Use an Run As account**. Then, click **Browse** and add the Run as account that you created earlier and click **Next**.
5. On Discovery scope, select specify Hyper-V Servers computers by names and enter the Computer names as shown in Figure 7-42 and click **Next**.

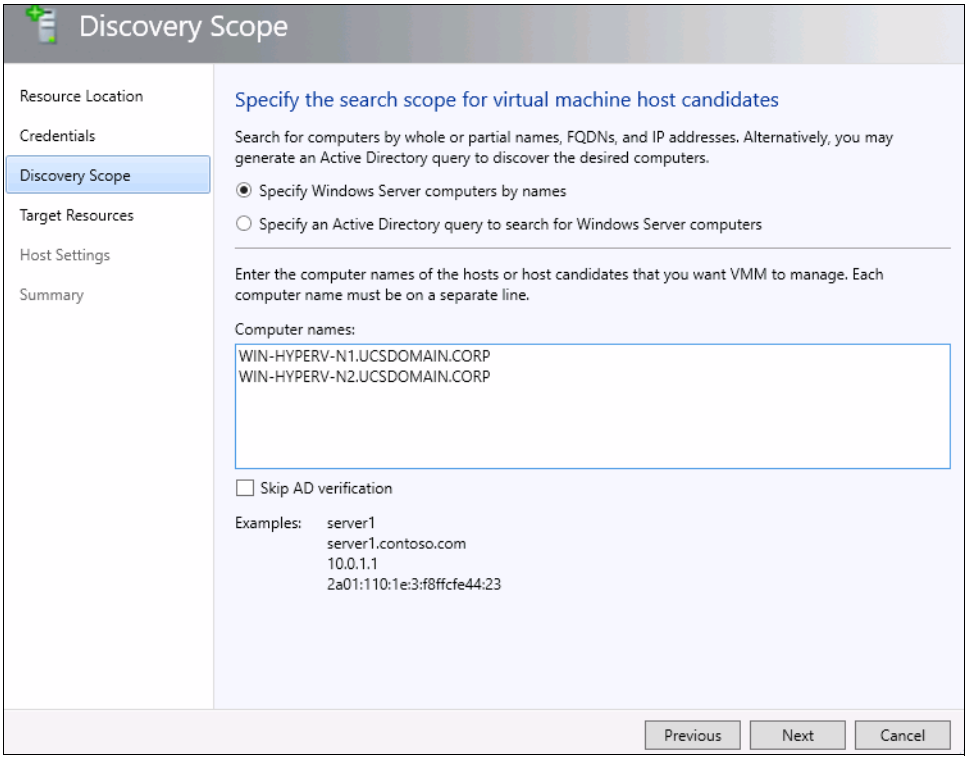


Figure 7-42 Adding Hyper-V servers to VMM host group

6. Under Target Resources, select the check box next to the computer names that need to be the part of the Hyper-V host group. Because the failover cluster was previously configured in 7.9, “Configuring the Failover Clustering feature” on page 123, you might see the cluster name as shown in Figure 7-43 on page 136.

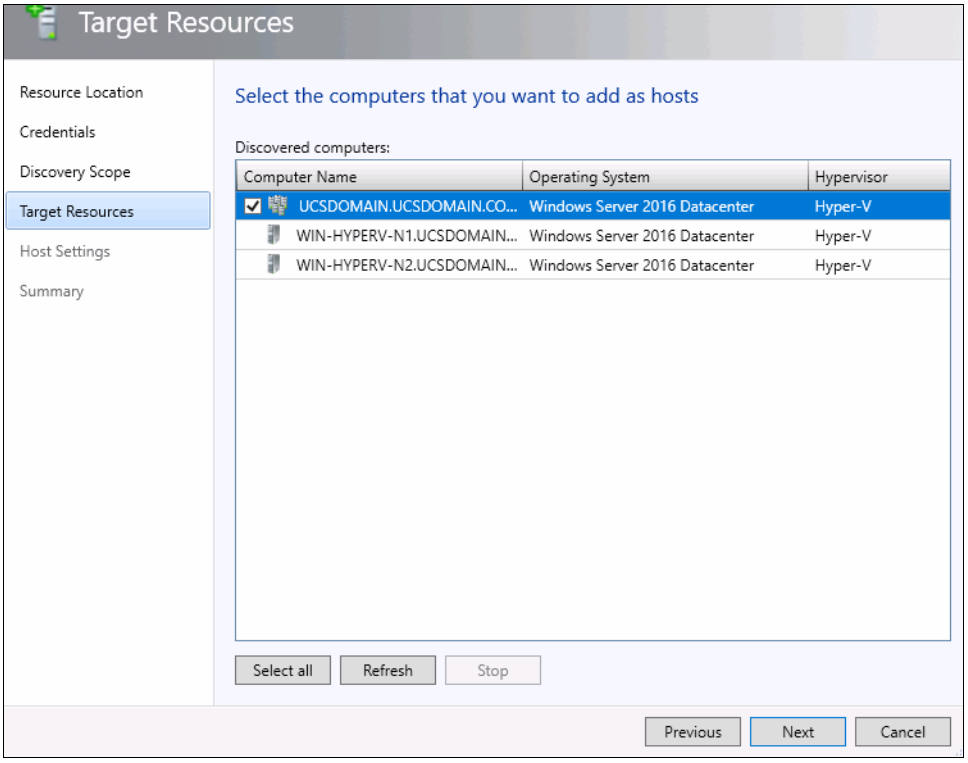


Figure 7-43 Selecting the Hyper-V hosts to add to host group

7. On the Host settings page, select the host group to which you want to assign the cluster, as shown in Figure 7-44.

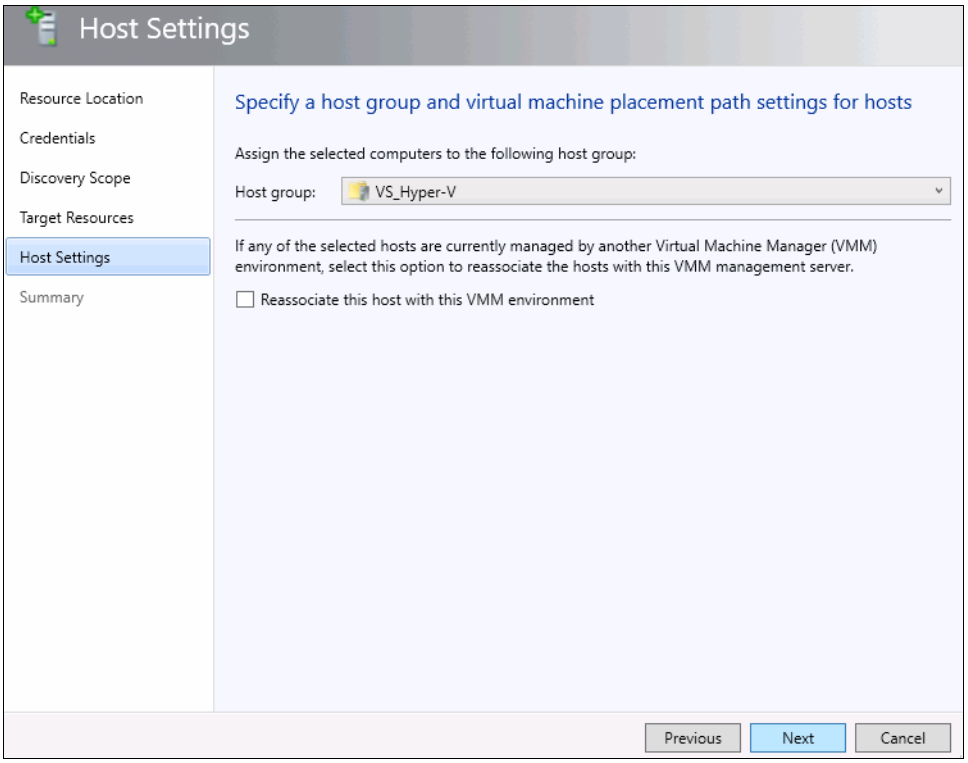


Figure 7-44 Adding Hyper-V hosts to custom host group

8. On the Summary page, confirm the settings, and then click **Finish**.

7.12.5 Hyper-V networking

Figure 7-45 shows the logical representation of the network that is configured in the example in this section using the Microsoft System Center VMM. This scenario uses and deploys *Switch Embedded Teaming (SET)*, a new feature released in Windows server 2016. SET is a teaming solution that is integrated with the Hyper-V switch.

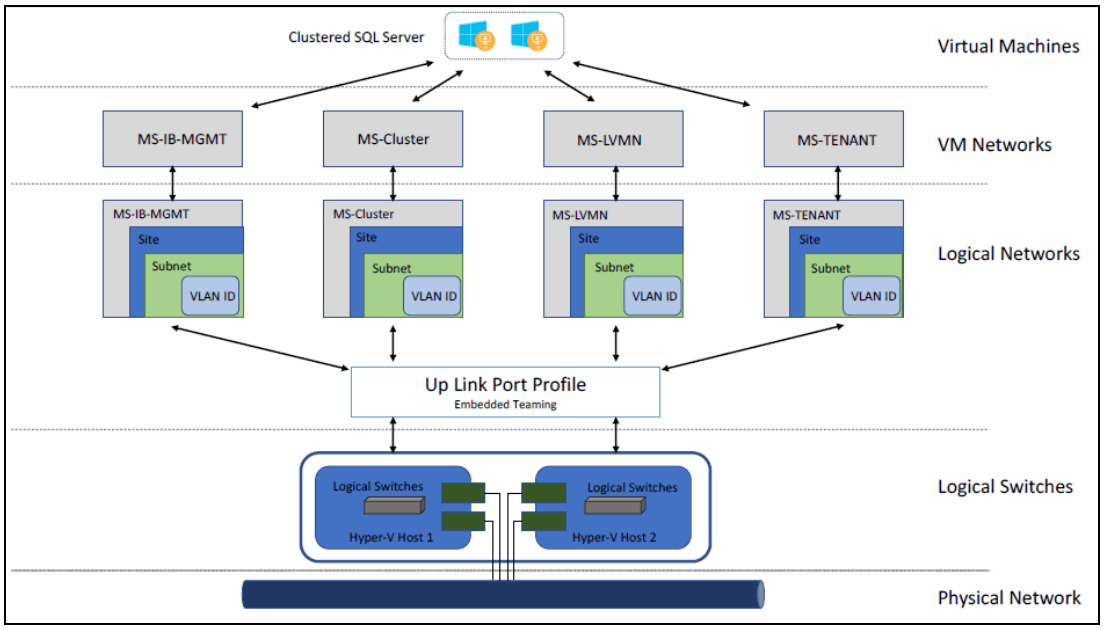


Figure 7-45 Hyper-V logical representation

This section includes the following topics:

- Configuring logical networks, sites, and IP pools
- Creating a static IP address pool for a logical network
- Creating VM networks
- Customizing the Hyper-V port profile
- Configuring Hyper-V logical switch using SET

Configuring logical networks, sites, and IP pools

In this particular environment, four virtual networks model as logical networks. However, they are all separate virtual local area networks (VLANs) on the same physical network that are controlled by setting the VLAN ID on the virtual network adapter. The physical ports on the switch are configured to allow all of the various VLANs that can be configured (similar to a trunk port).

The configuration includes the following logical networks:

- *MS-IB-MGMT*: This logical network is used for management traffic and has its own IP subnet.
- *MS-Cluster*: This network is used for Microsoft Hyper-V cluster communication and has its own IP subnet and VLAN.

- *MS-LVMN*: This network is used for Live Migration traffic and has its own IP subnet and VLAN.
- *MS-Tenant-VM*: This network is used for all the VM traffic and has its own IP, subnet, and VLAN.

Complete the following steps to create logical networks and sites:

1. Open Microsoft System Center VMM console, and open the Fabric workspace.
2. Select the **Networking Logical Networks** navigation node.
3. Click **Create Logical Network**, which launches the Create Logical Network wizard.
4. Enter a name and description for the logical network and click **Next**.
5. In the Settings tab, select the option to which best describes the logical network. Because there are four logical networks, when you create logical networks specify whether networks are isolated physically or virtually, using network virtualization and VLANs. Because there are network isolation using VLAN at the Cisco UCS physical network, select VLAN-based independent network as shown in Figure 7-46 and click **Next**.

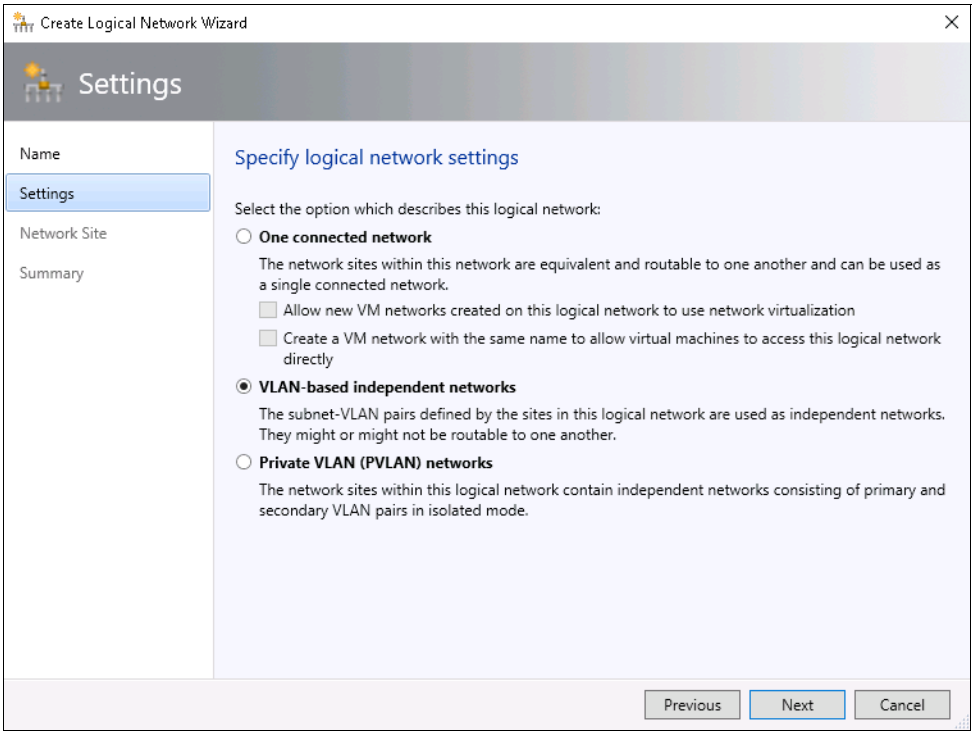


Figure 7-46 Settings for logical networks

6. In the Network Site panel, the click **Add** to create a new network site. A name must provided for network site, VLAN and the IP subnet range. Also, the new network site has to be assigned to one or more host groups. Repeat this step for each logical network listed in "Configuring logical networks, sites, and IP pools" on page 137. See the complete list of all logical networks created in Figure 7-47 on page 139.

IP subnet note: If IP addresses are to be managed by corporate DHCP servers, leave the IP subnet blank. If the network does not use VLANs, set the VLAN ID to *0*, which tells System Center VMM that VLANs are not to be configured. By default, sites are given the name `<Logical Network>_<number>`, but you can rename the default name to something more useful.

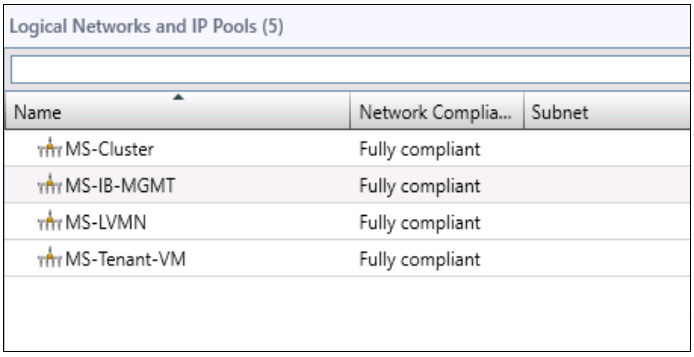


Figure 7-47 Logical networks

Creating a static IP address pool for a logical network

To create a static IP address pool for each logical network that you created in “Configuring logical networks, sites, and IP pools” on page 137, complete these steps:

1. Log on to VMM and change to **Fabric workspace**.
2. Click **Create IP Pool**, or right-click the logical network. Then, select the **Create IP Pool** context menu action.
3. Enter a name and description. From the drop-down list, select the logical network for the IP pool, as shown in Figure 7-48. Click **Next** to proceed.

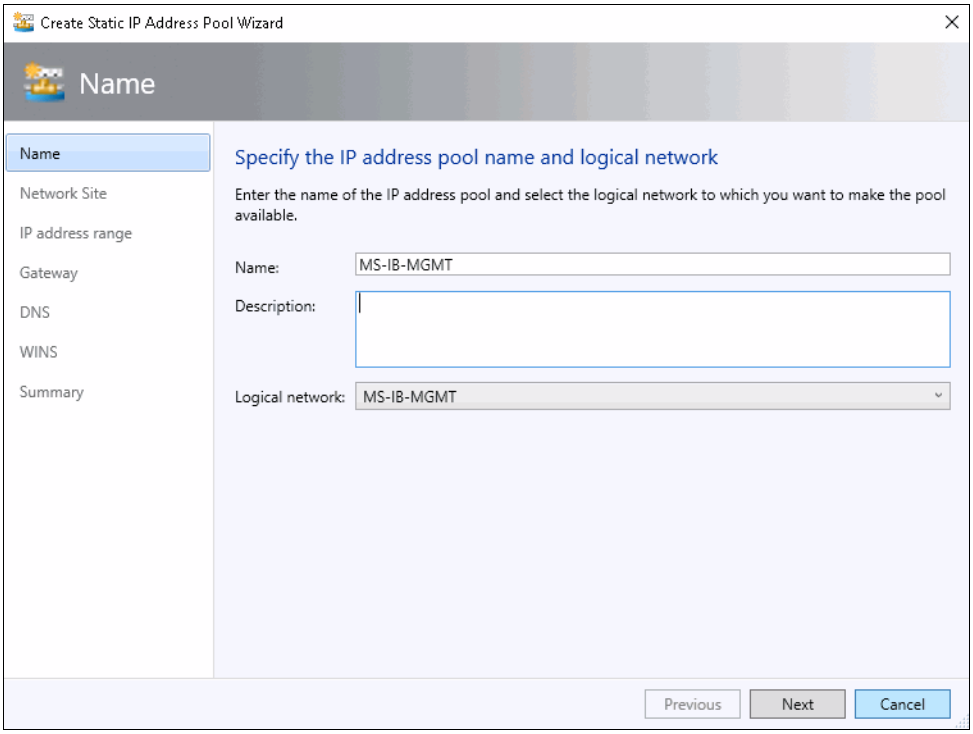


Figure 7-48 Creating an IP pool

4. The next dialog box allows you to use an existing network site or create a new one. Choose to use an existing one, as shown in Figure 7-49, and then click **Next**.

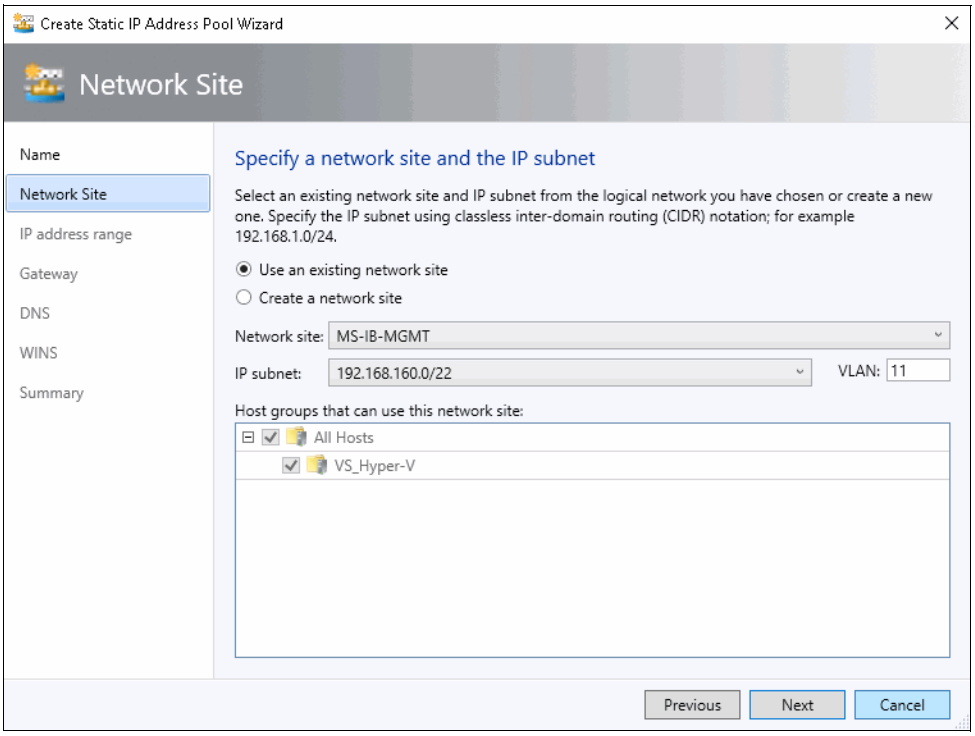


Figure 7-49 Creating IP Pool for existing logical network

5. The next dialog box (Figure 7-50 on page 141) allows you to set an IP address range and reservations. The IP address range allows configuration of the IP addresses that System Center VMM will manage and allocate to the resources such as virtual machines and load balancers. Within the range, you can configure specific addresses to be reserved for other purposes or for use by load-balancer virtual IPs (VIPs) that System Center VMM can allocate. Click **Next**.

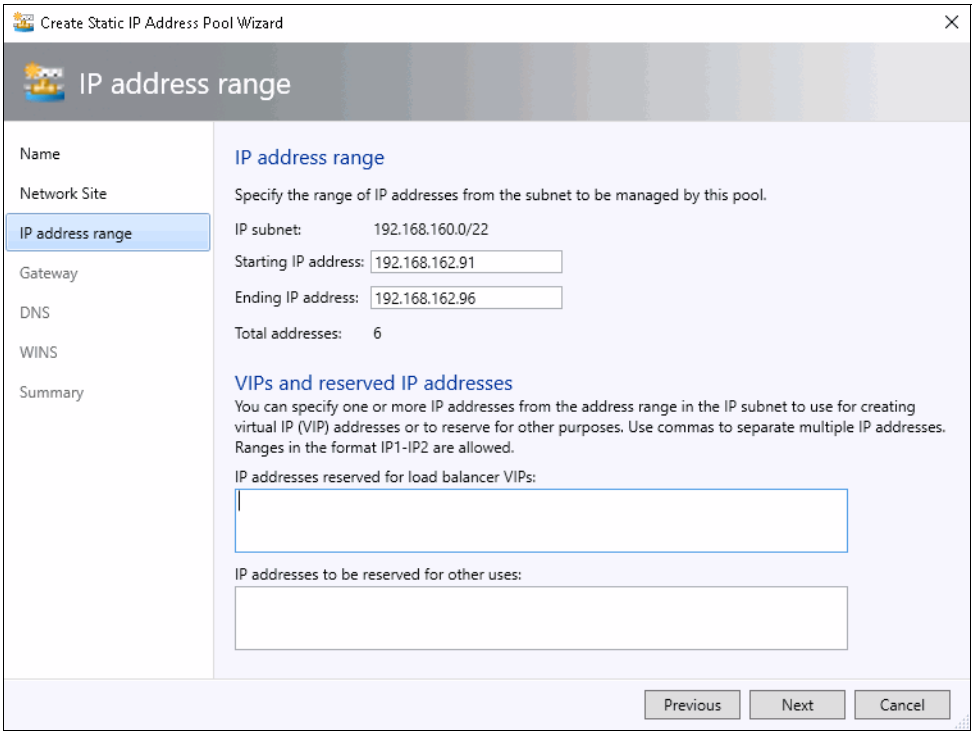


Figure 7-50 IP address range for logical networks

6. The dialog box shown in Figure 7-51 allows to enter the gateway IP address and network routes. If applicable, enter the default gateway and routes and click **Next**.

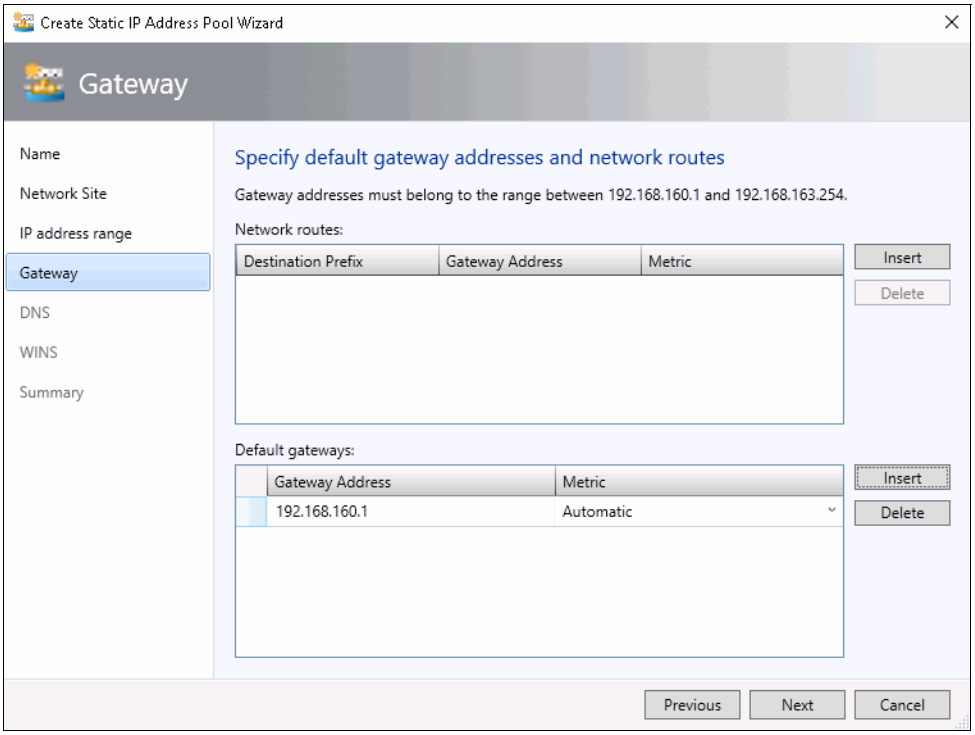


Figure 7-51 Entering the default gateway and routes

7. The next dialog box (Figure 7-52) allows you to configure the DNS servers, DNS suffix, and additional DNS suffixes to append. Enter the required values, and then click **Next**.

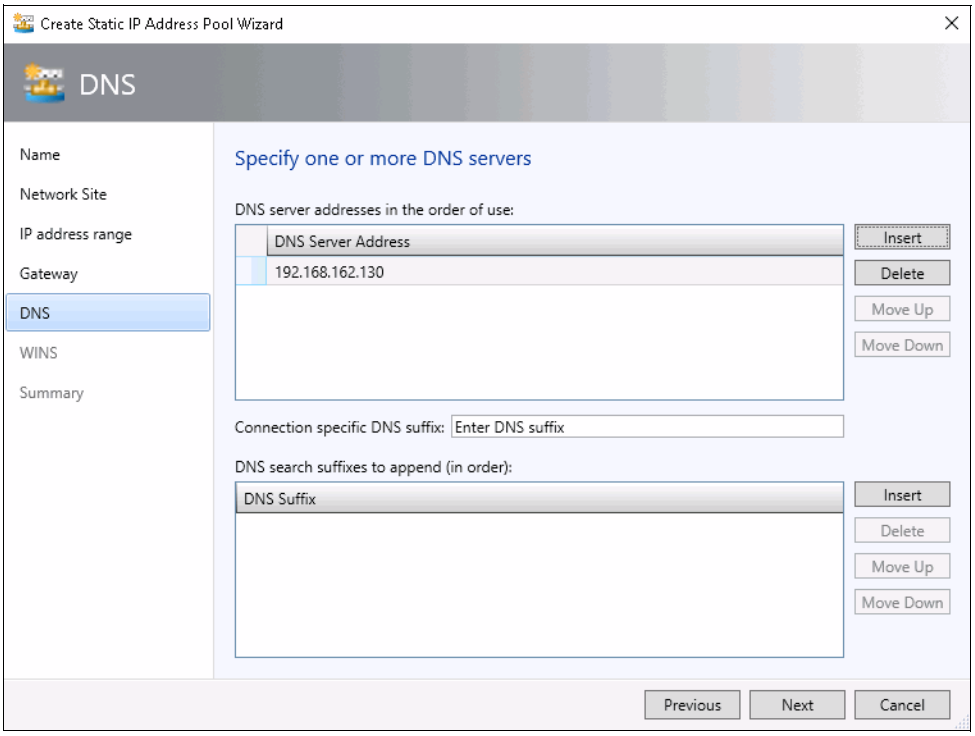


Figure 7-52 Entering the DNS for logical network

8. In the next window you enter the WINS server details, if used, and click **Next**.
9. On the Summary window, confirm the configuration, click **View Script** to see the PowerShell that will be used, and then click **Finish** to create the IP pool as shown Figure 7-53 on page 143.

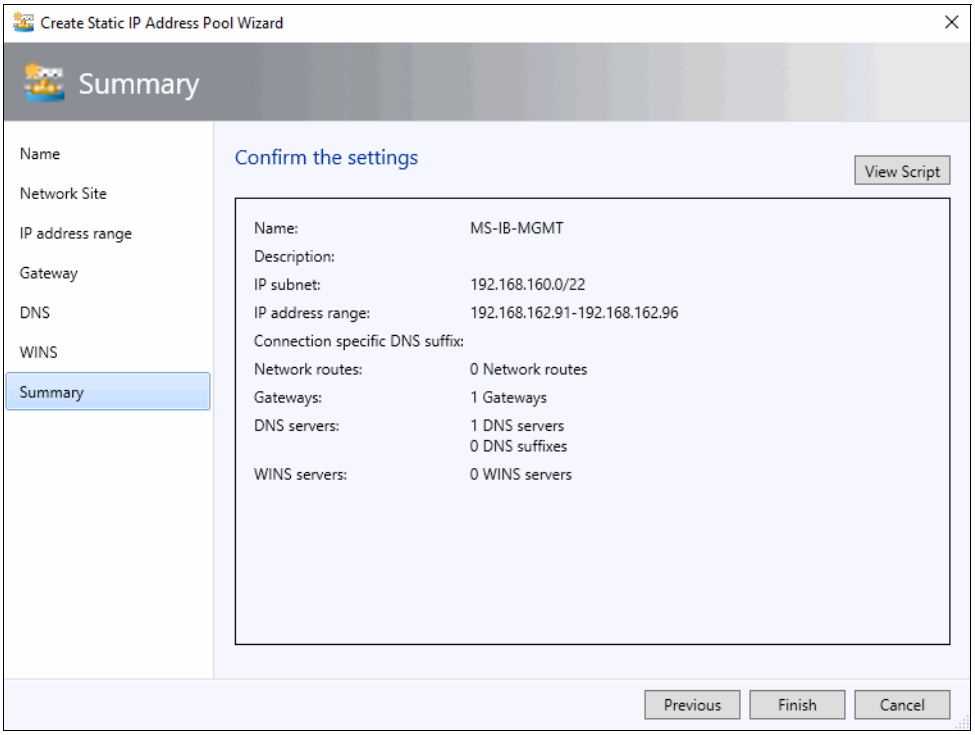


Figure 7-53 IP pool summary

Creating VM networks

After the logical networks are created, the next step is to create the VM networks. VM networks allows you to abstract virtual machine network from the underlying logical network. VM networks can be considered as an abstract layer that act as an interface to logical networks.

To create four VM Networks (one VM Network for each logical network created in “Configuring logical networks, sites, and IP pools” on page 137).

1. Log on to Microsoft System Center VMM and open the VMs and Services workspace.
2. Select the **VM Networks** navigation node and click the **Create VM Network** button.
3. In the General tab enter a name for the new VM Network and click **Next**.
4. In the Isolation options, you must specify a VLAN and an existing network site. Select the network site that corresponds to the VM Network and click **Next**.

   This example create one Virtual Machine Network for each network site and logical network, as shown in Figure 7-54.

Figure 7-54 VM networks

5. For each VM network, an IP pool must be created. Select the **VM Network** and click **Create IP Pool** to create a range of IP addressed. Repeat this step for each VM network. See an example for VM network `MS-Cluster` shown in Figure 7-55.

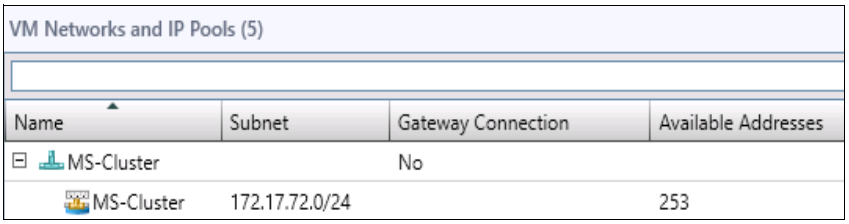


Figure 7-55 VM Network IP Pool

6. Click **Next t**o review the summary page and **Finish** to complete the changes.

Customizing the Hyper-V port profile

This section shows how to create a Hyper-V port profile and to define the load balancing algorithm for an adapter. It also explains how to specify team multiple network adapters on a host that use the same Hyper-V port profile. This profile is used in conjunction with the logical network that you associated with the adapter.

To create an Hyper-V port profile for each logical network:

1. Log on to Microsoft System Center VMM and open the Fabric workspace.
2. Select **Networking** → **Port Profiles**.
3. Click the **Create** button drop-down and select **Hyper-V Port Profile.**
4. Enter the name and description for the new port profile, as shown in Figure 7-56 on page 145. Select the **Uplink Port Profile** radio button. Leave the **Load balancing algorithm** option at the default (to Host) and set the Teaming Mode option to **Switch Independent**. Then, click **Next**.

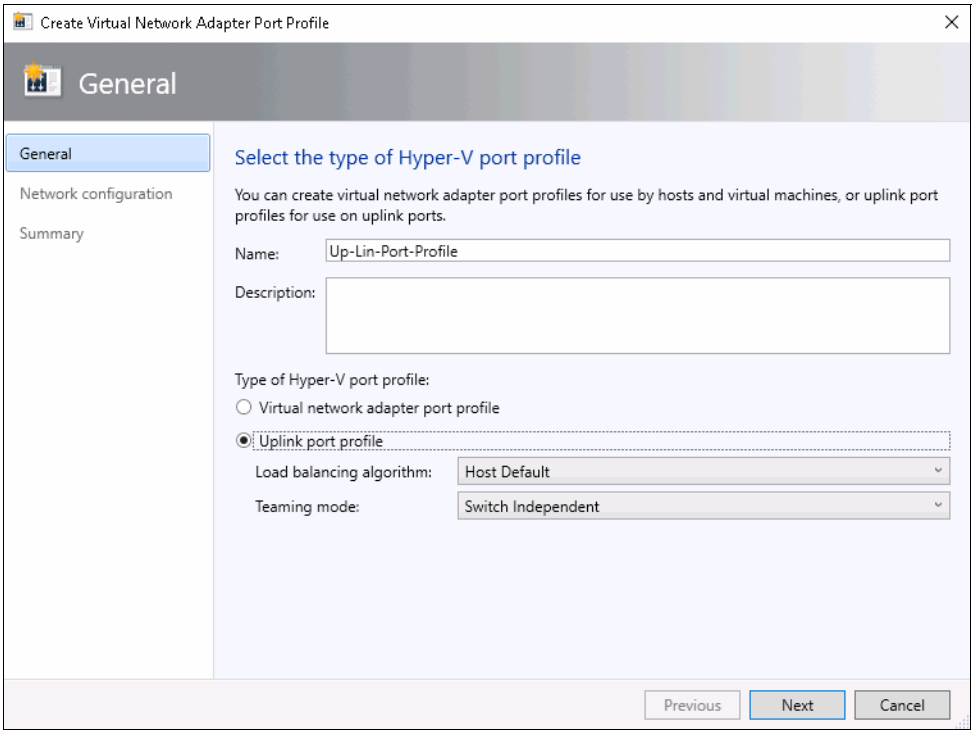


Figure 7-56 Creating up-link port profile

5. Select the network sites that are part of your logical networks and that can be connected to via this Hyper-V port profile, as shown in Figure 7-57, and click **Next**.

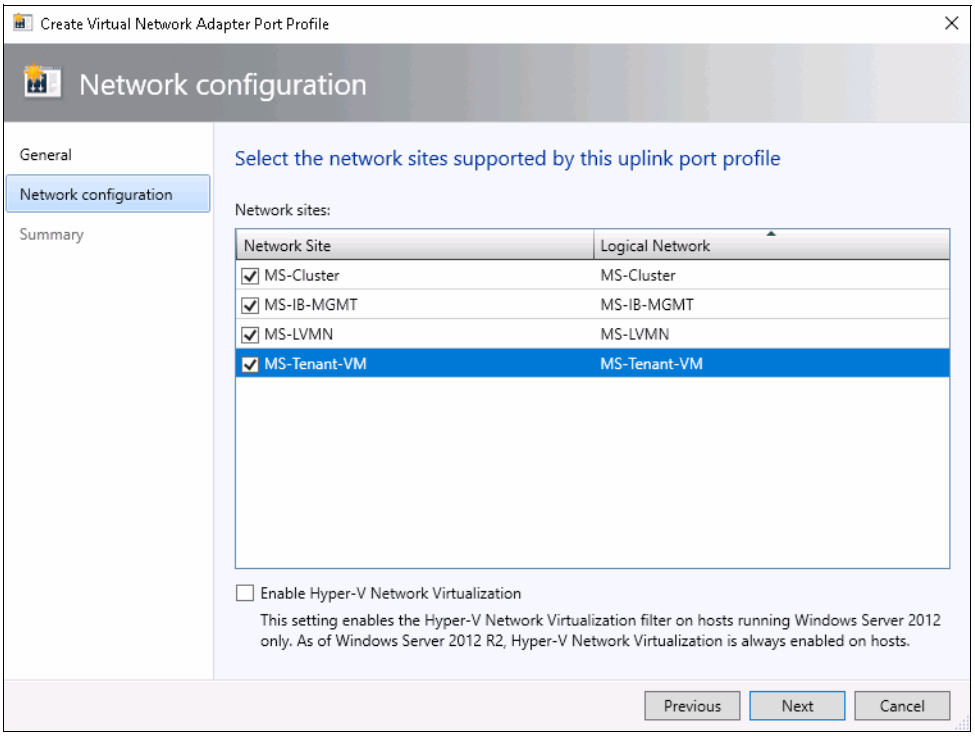


Figure 7-57 Selecting the sites to associate to Uplink Port

6. Review the summary page and click **Finish** to complete the settings.

Configuring Hyper-V logical switch using SET

A logical switch brings virtual switch extensions, Hyper-V port profiles, and port classifications together so that you can configure each network adapter with the settings you need, and have consistent settings on network adapters across multiple hosts.

This section covers the steps to create a logical switch using embedded team as the uplink mode. Windows Server 2016 introduces Switch Embedded Teaming (SET) which, as the name suggests, teams multiple adapters directly in the VM Switch instead of creating a separate NIC team by using the Load Balancing and Failover (LBFO) functionality. SET has the benefit of enabling mixed use of adapters with the VM switch and utilizing remote direct memory access (RDMA).

The logical switch will bring all of the components together. To create a logical switch:

1. Open Microsoft System Center VMM, and click **Fabric** → **Networking** → **Logical Switches** → **Create Logical Switch**. From the Getting Start information, click **Next**.
2. Enter a name and description for the new logical switch, and select **Embedded Team** as the Uplink mode to deploy the switch with SET-based teaming, as shown in Figure 7-58. Then, click **Next**.

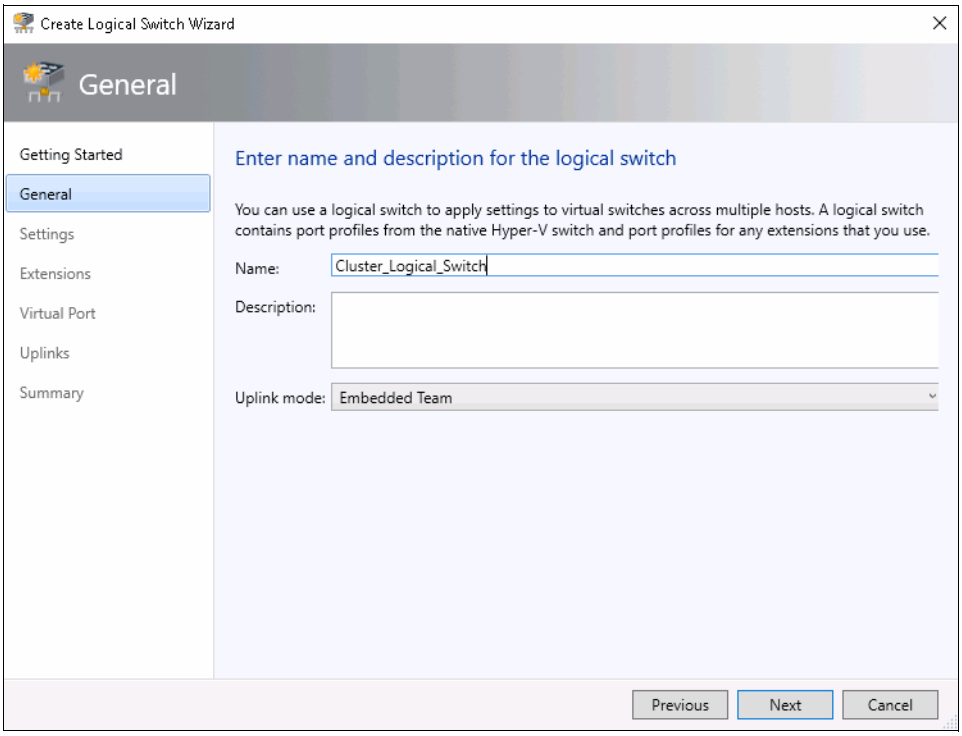


Figure 7-58 Creating a logical switch

3. Select the minimum bandwidth mode as **Weight**, which quantifies minimum bandwidth for workloads, and click **Next**.
4. In Extensions selection window, leave the default, and click **Next**.
5. In Virtual Port window, click **Add**. Next, click **Browse** to select the port classification. Then select **Include a virtual network adapter port profile in this virtual port** option and select the virtual port profile that corresponds. For example, if you select the high-bandwidth port classification, most likely you would select the High Bandwidth Adapter virtual port profile object. Click **OK**. Repeat this process to add classifications.

Select the classification that you want as the default, and click **Set Default**. See the example in Figure 7-59. Click **Next**.

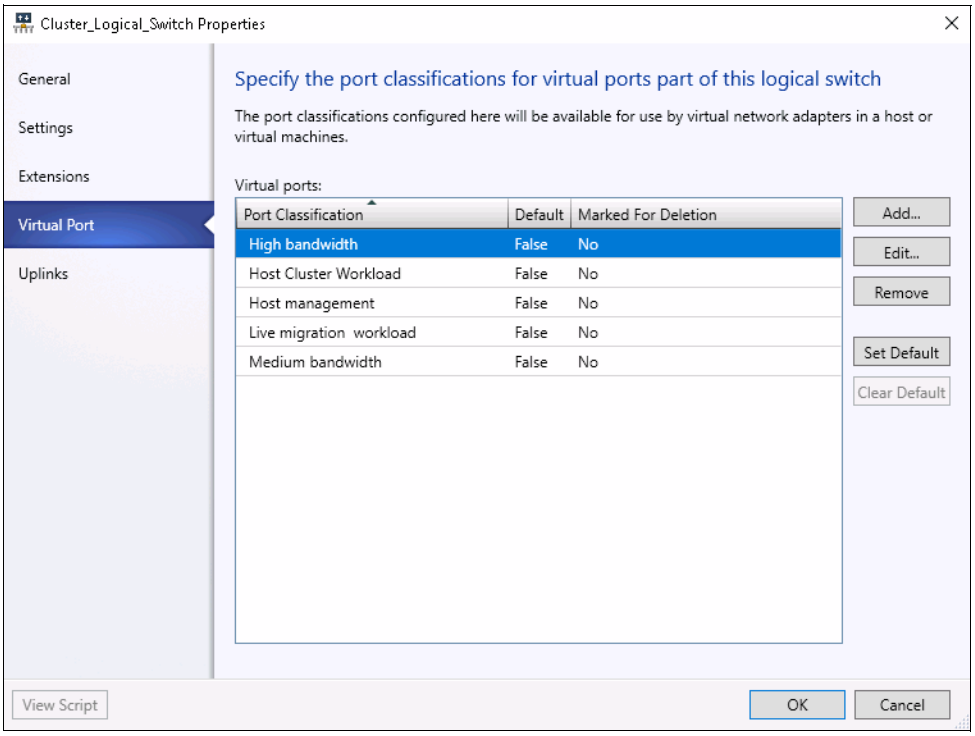


Figure 7-59 Port classification

6. In the Uplinks window, click the **Add** button and then select **Existing Uplink Port Profile**. A new dialog box opens and allows you to select a Hyper-V Port profile using a drop-down menu. Select the existing port profile, as shown in Figure 7-60, and click **OK**.

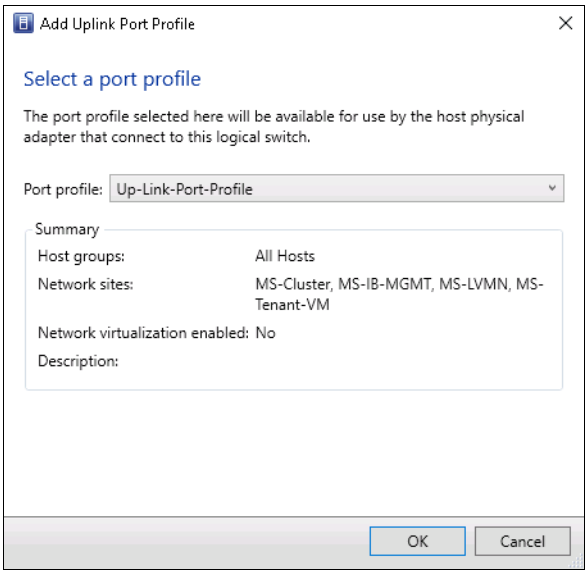


Figure 7-60 Selecting existing Hyper-V port profile

7. Next, you must select Up-Link-Port-Profile, and click **New virtual network adapter** to add a virtual network adapter, click Browse to add the VM Networks and enter the name to match the VM Network. Under IP address configuration, select Static option and choose the IP Pool. See Figure 7-61 as an example for MS-Cluster virtual adapter.

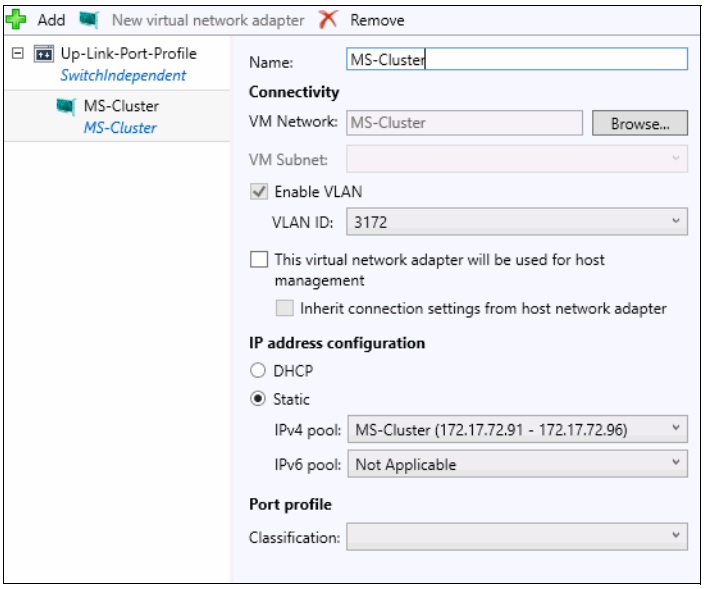


Figure 7-61 Virtual adapter in Up Link port profile

8. Repeat the previous step to add all the virtual network adapters needed for your infrastructure as shown Figure 7-62.

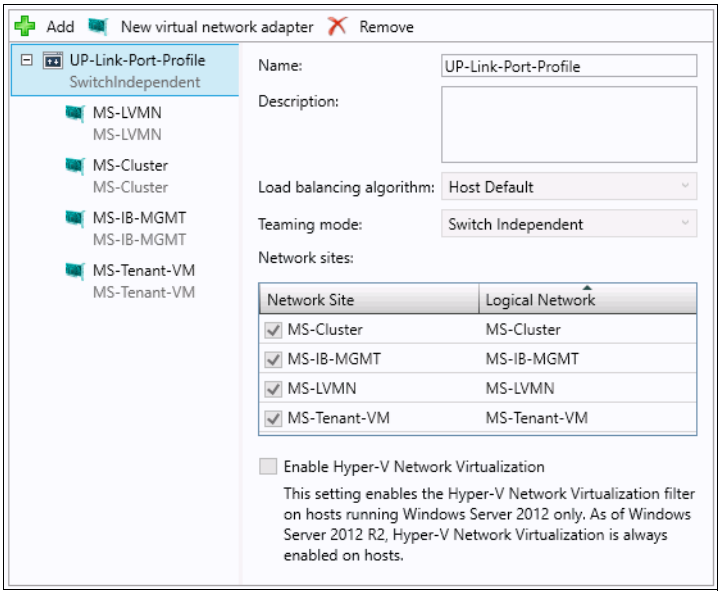


Figure 7-62 UP Link port profile

Figure 7-63 shows our example for MS-LVMN virtual network adapter.

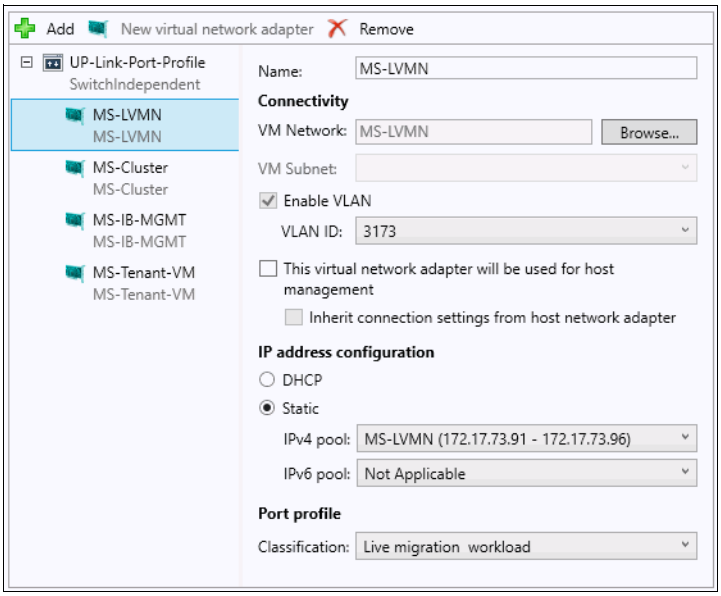


Figure 7-63 UP Link port profile for LVMN Network

Figure 7-64 shows our example for MS-Cluster virtual network adapter.

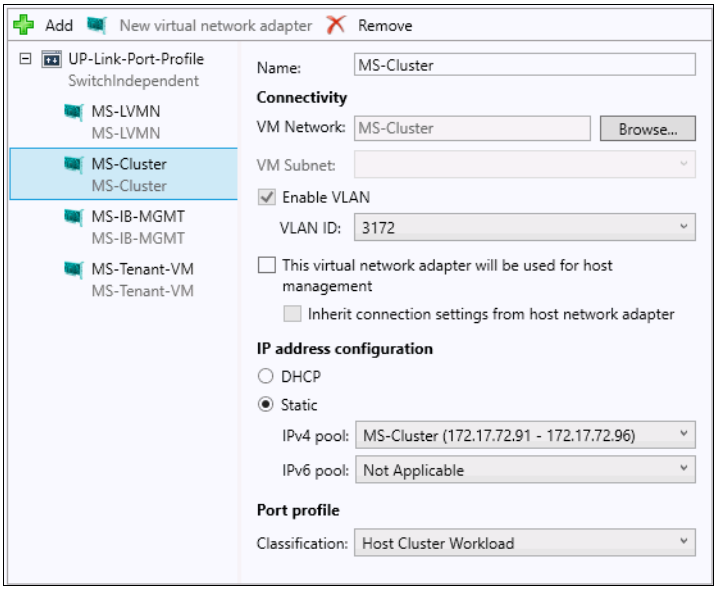


Figure 7-64 UP Link port profile for MS Cluster

Figure 7-65 shows our example for MS-IB-MGMT network site. You might noticed virtual network adapter will have check box enabled for **This virtual network adapter will be used for host management** and **Inherit connection settings from host network adapter.** This option ensures continued connectivity for the host.

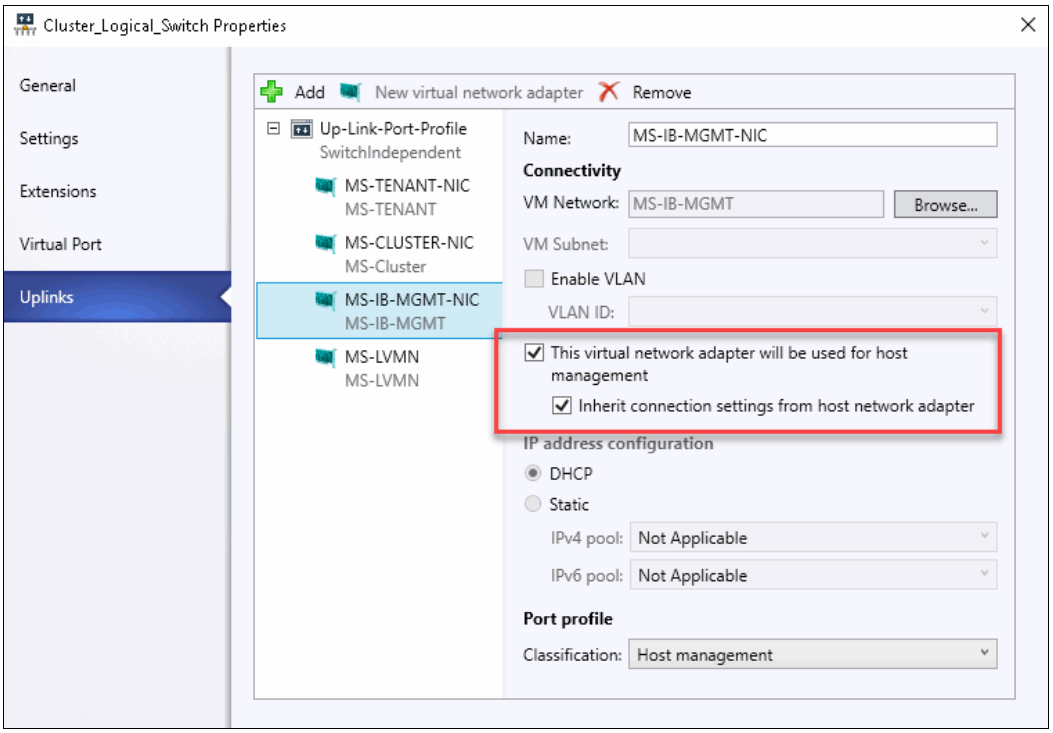


Figure 7-65 UP Link port profile for MS-IB-MGMT

And Figure 7-66 shows our example for MS-Tenant virtual network adapter.

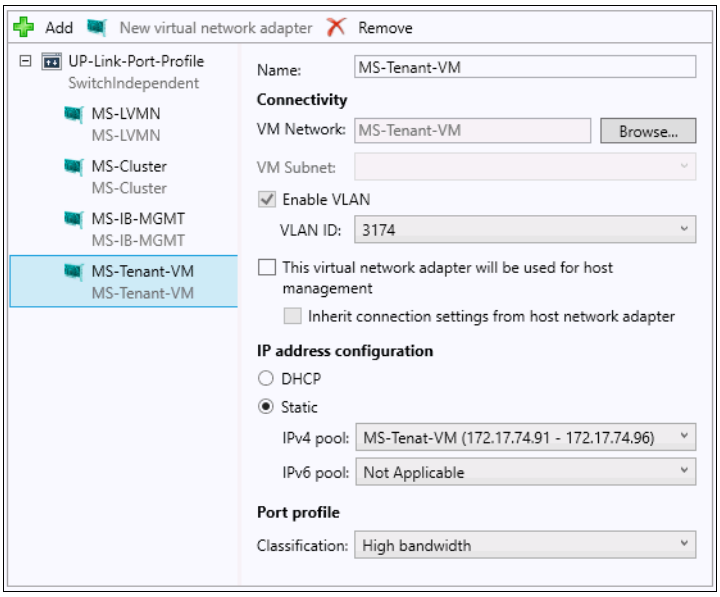


Figure 7-66 UP Link port profile for MS-Tenant-VM

9. Click **Finish** to commit and changes and completing the Logical Switch Embedded Teaming configuration.

7.12.6 Adding the IBM FlashSystem 5030 to VMM

By using Microsoft System Center VMM, you can manage storage that you can assign to virtual hosts and clusters, and virtual machines. You can manage the underlying storage presented as part of your virtual infrastructure using either local or remote storage.

Local storage is storage is that is directly attached to the VMM server, which is commonly a disk drive on the server. This type of managed storage is not shared and does not provide resilience or high availability.

Remote storage is the block and file-based storage that is specific storage arrays that are supported in VMM 2016. VMM uses State Model API (SMAPI) and the Storage Management service, which functions as an SMI-S client, to manage the Storage Management Initiative Specification (SMI-S) storage devices.

To set up the IBM FlashSystem 5030 storage array in VMM, see Chapter 4, “VersaStack Cisco Nexus 9000 network configuration” on page 31.

7.12.7 Storage classifications

In the VMM, *storage classifications* provide a layer of abstraction over specific storage devices. You can group storage devices together based on their characteristics. For example, you can classify a storage array that contains a storage pool with a full set of solid-state drives (SSDs) or flash drives as *IBM FlashSystem 5030 Gold* or a system that does not hold SSDs but HDDs only as *IBM FlashSystem 5030 Silver*.

Before creating or renaming the storage classifications, we assume the IBM FlashSystem 5030 is properly configured in the VMM.

To create or rename a storage classification:

1. Log on to Microsoft System Center VMM, and go to the Fabric workspace.
2. Go to **Storage** and select **Storage Classification and Pools.**
3. In the main panel, IBM FlashSystem 5030 is listed.

4. Rename the classification that is related to IBM FlashSystem 5030 by clicking in **Properties**, as shown in Figure 7-67.

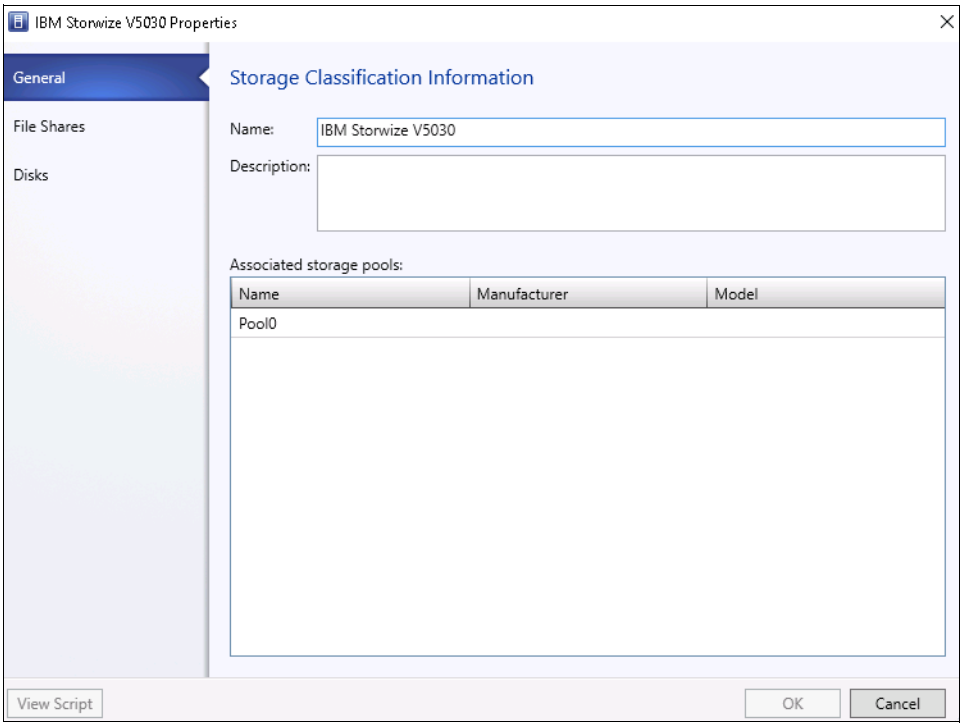


Figure 7-67 Storage classification

5. Rename accordingly and click **OK**.
6. To create a new storage classification, click **Create Storage Classification** from the top menu and enter the name and description, as shown in Figure 7-68.

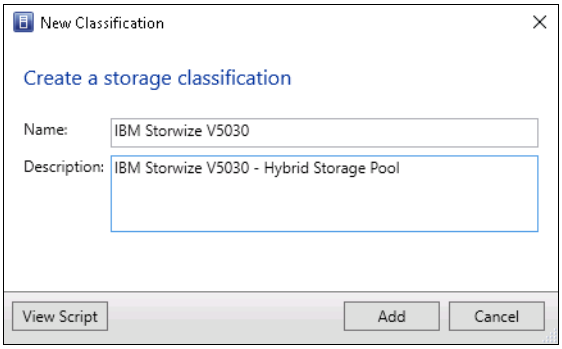


Figure 7-68 New storage classification

7. Click **Add** to complete the changes.

7.12.8 Configuring virtual switches on Hyper-V hosts

After the logical networks, sites, IP Pools, VM networks, UP-links and logical switches are configured, the next step is applying these settings to each Hyper-V host defined in VMM. To apply the network settings to Hyper-V hosts:

1. Log on to VMM and select the **Fabric** workspace.
2. Under Servers, navigate to the host group where the Hyper-V nodes are defined.
3. Select the Hyper-V Host and choose **Properties** from the top menu.
4. Click **Virtual Switches** from the menu, and then select **New Virtual Switch** → **New Logical Switch**.
5. Select the Virtual Switch that you created in “Configuring Hyper-V logical switch using SET” on page 146. Under Adapter, select the Hyper-V physical adapters by clicking the **Add** button those to the logical switch, as shown in Figure 7-69.

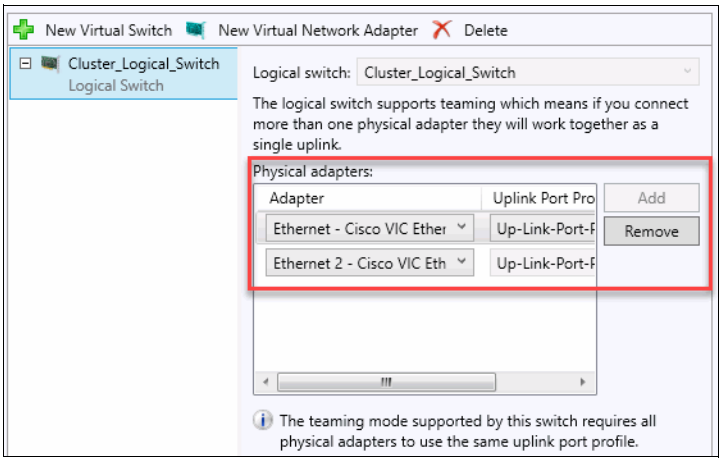


Figure 7-69 Selecting the physical adapters

6. Select the logical switch created previously, and click **New Virtual Network Adapter**, as shown in Figure 7-70.

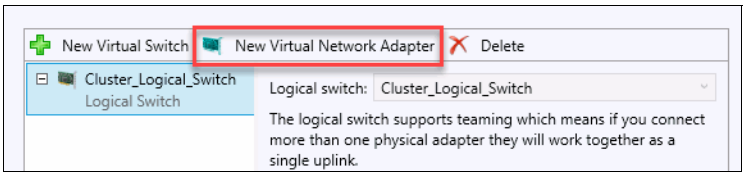


Figure 7-70 Adding a virtual network adapter to the logical switch

7. Enter a name for the new virtual network adapter and under Connectivity, select the **VM Network and subnet**. Configure it to start with MS-IB-MGMT VM network.

8. For MS-IB-MGMT virtual network adapter, in the “IP address configuration” select **Static**; this setting assures the management IP address of the Hyper-N nodes will not change. See Figure 7-71 as example and click **OK**.

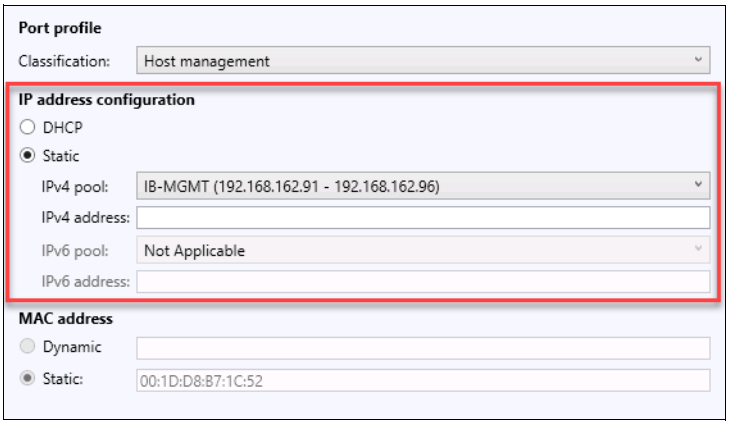


Figure 7-71 Port profile

9. Repeat steps 6-8 to create a virtual network adapter for all VM networks and VM subnets.
10. For VM network adapters that are created in the Hyper-V hosts, select the IPv4 pool and enter the IP address that should be assigned to the virtual network adapter. See an example for MS-Cluster virtual interface in Figure 7-72.

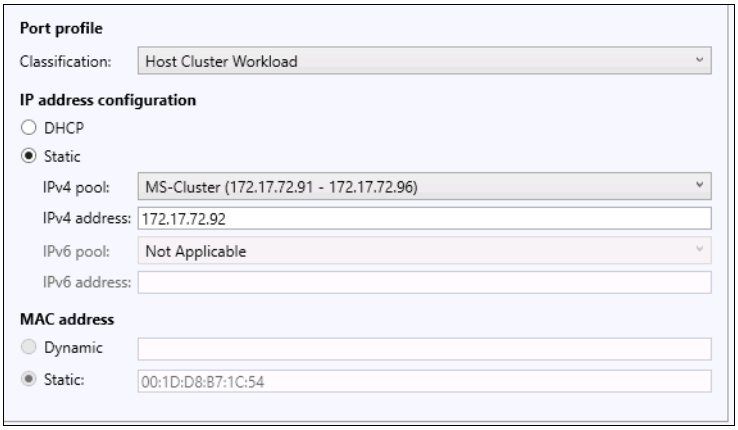


Figure 7-72 IP settings for virtual network interface

11. Repeat the previous step for MS-LVMN and MS-Tenant VM networks. Figure 7-73 shows an example of logical switch and the network virtual adapters that are to be configured for each Hyper-V node.

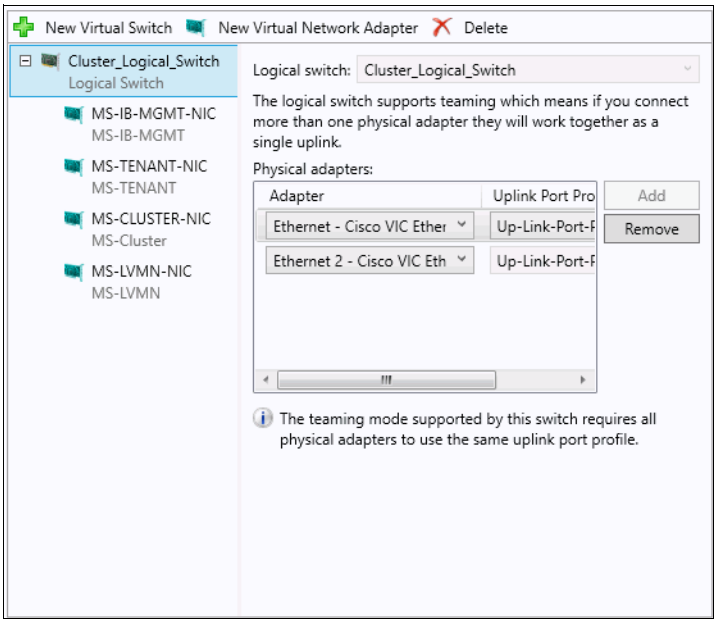


Figure 7-73 Logical switch and virtual adapters

7.13 Hardware profiles

In VMM, a hardware profile enables you to specify the hardware configuration for various virtual hardware components for virtual machines. You can use a hardware profile to customize new virtual machines as you create them or to customize one or more templates that you use to create new virtual machines. By creating and reusing hardware profiles, you can ensure consistent hardware settings in each set of virtual machines created by using that hardware profile.

A stand-alone hardware profile is a collection of hardware settings that you can import into a new virtual machine or into a new template. You can also specify hardware profile settings for a virtual machine or template directly while running the New Virtual Machine Wizard or the New Template Wizard.

VMM stores hardware profiles in the library catalog in the VMM database. Hardware profiles are database objects that are not represented by a physical configuration file and thus are not associated with any library share.

To create a hardware profile:

1. Log on to Microsoft System Center VMM, and select the Library workspace.
2. From the Library panel, select **Hardware Profile** under **Profiles.**
3. Right-click over **Hardware Profile** and select Create Hardware Profile (optionally, you can use the top menu by selecting **Create** → **Hardware Profile**) to initiate the wizard.

4. Enter a name for the Hardware Profile and, using the drop-down menu, choose between Generation 1 or 2, as shown in Figure 7-74.

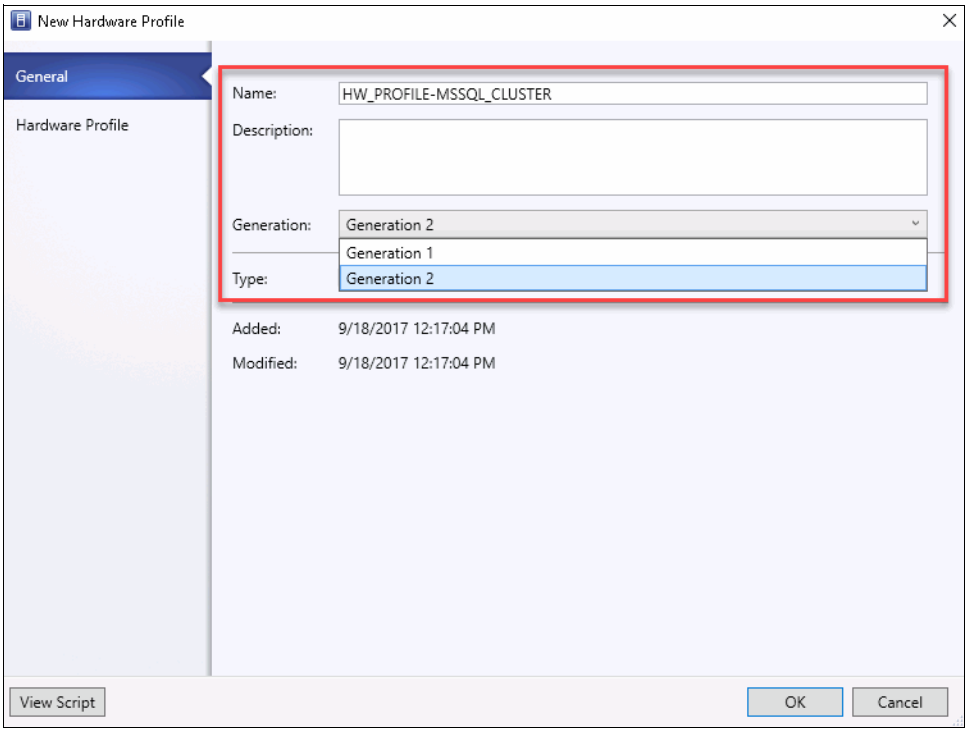


Figure 7-74 Hardware Profile wizard

5. Go to **Hardware Profile** tab to customize the settings for this hardware profile. In the Hardware Profile panel, you can select from the following options:
   - *Cloud Capability (optional)*: Allows the VMM to provide a validation state.
   - *Processor*: Sets the required number of processors. If you require improved capability between different processors versions, select the **Allow migration to a virtual machine host with different processor version** option, as shown in Figure 7-75.

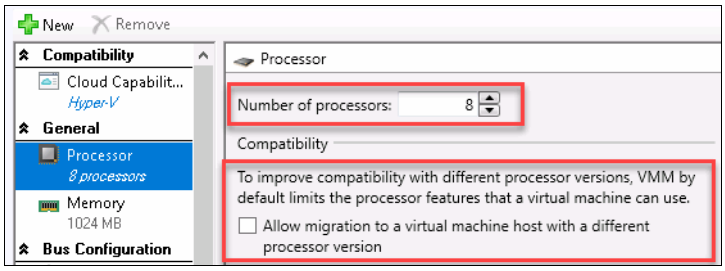


Figure 7-75 Processor options

   - *Memory*: Sets the amount of memory to allocate for this hardware profile or specifies a range that allows the VMM to allocate memory dynamically. Dynamic memory allocation requires you to enter the following information:
     - Startup memory
     - Minimum memory
     - Maximum memory
     - Memory buffer percentage

For the purpose of this scenario, the virtual SQL Servers require *static memory allocation* as shown in Figure 7-76.

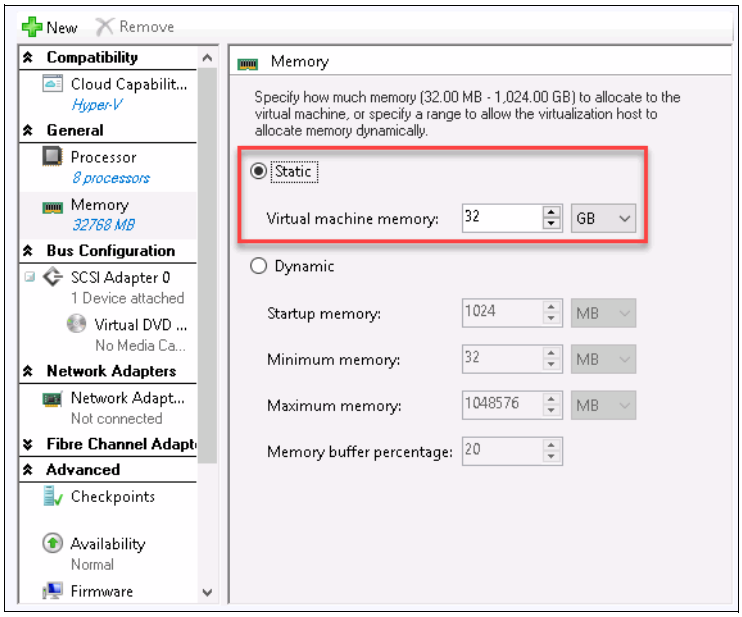


Figure 7-76 Memory allocation settings

– *Bus Configuration (optional)*: Sets the bus configuration options. You must select the **SCSI ID channel** and the **Media** options. The Media options allows you to pre-select an existing ISO image to be mounted in the virtual server. See Figure 7-77 on page 158.

ISO images note: ISO images must be previously imported to the VMM Library. To import an ISO image, first create a shared folder in Windows that is running the VMM server. In this folder, store the ISO images that you intend to use with VMM. Then, import the folder to the VMM Library by using **Library Servers** → **Select the Library Server FQDN** → **Add to Library Server**.

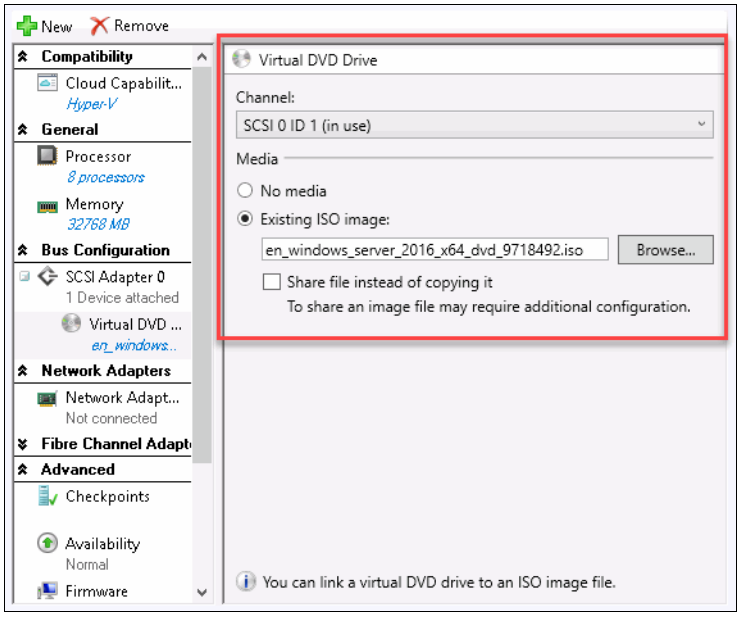


Figure 7-77 Bus configuration

– *Network Adapters (optional)*: Allows one or more optional virtual network adapters to be added. By default, a virtual network adapter that you add is not connected to a virtual network. Optionally, you can specify that a virtual machine created from this hardware profile is connected to an internal network or to an external network after the virtual machine is deployed on a host.

Figure 7-78 shows three network adapters that are connected to MS-Cluster, MS-IB-MGMT, and MS-LVMN VM Networks.

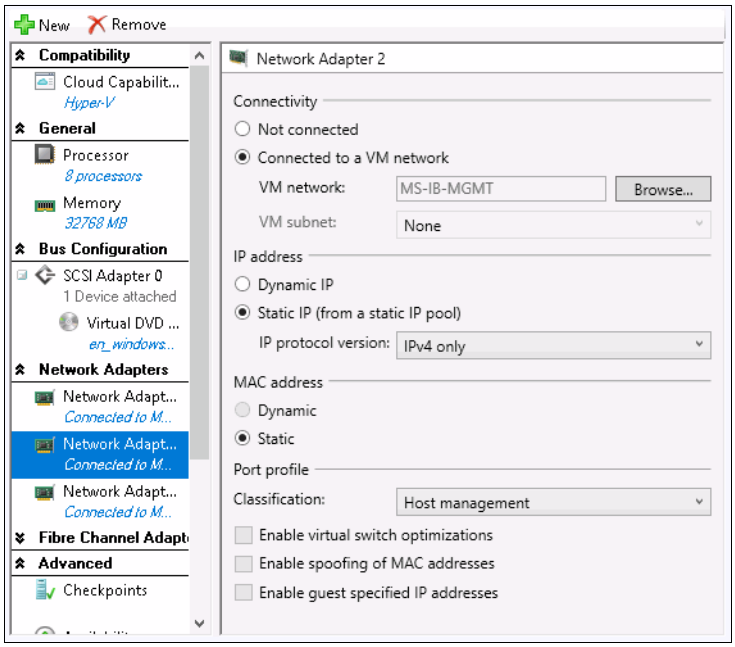


Figure 7-78 Hardware profile network adapters

– Advanced options: The following advanced options are also available:

  - *Checkpoints*: Allows the Hyper-V virtual environment to use backup technologies to create data-consistency checkpoints for the virtual machine. When enabling checkpoints, you must to select between production and standard checkpoints. See Figure 7-79.

> **Checkpoints for a clustered guest:** Always check the Microsoft official repository when using checkpoints for a clustered guest.

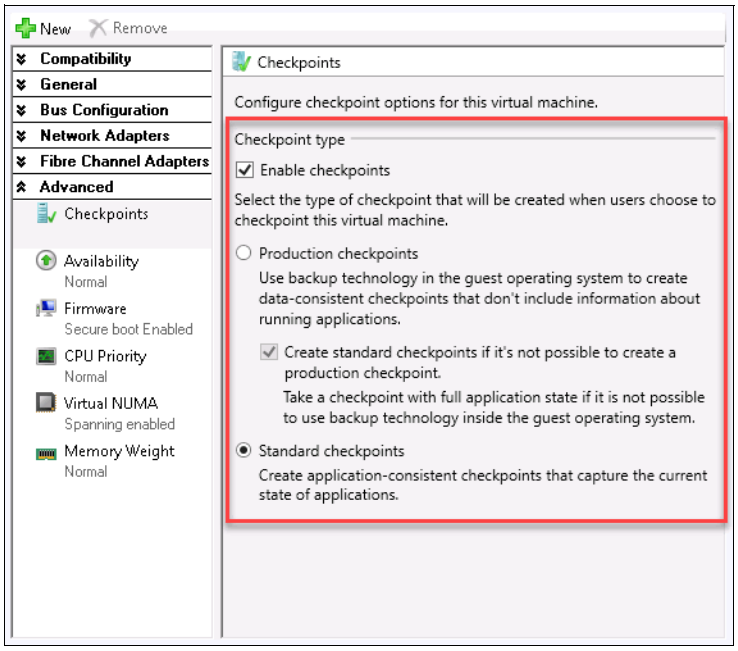


Figure 7-79 Hardware profile checkpoint

  - *Availability*: Allows placement of the virtual machine on a virtualization platform that is part of a host cluster. Select the **Make this virtual machine highly available** option. In the Virtual Machine priority section, select the **High** option to assign a high level of priority when the virtual machine is started and placed on a node. See Figure 7-80 on page 160.

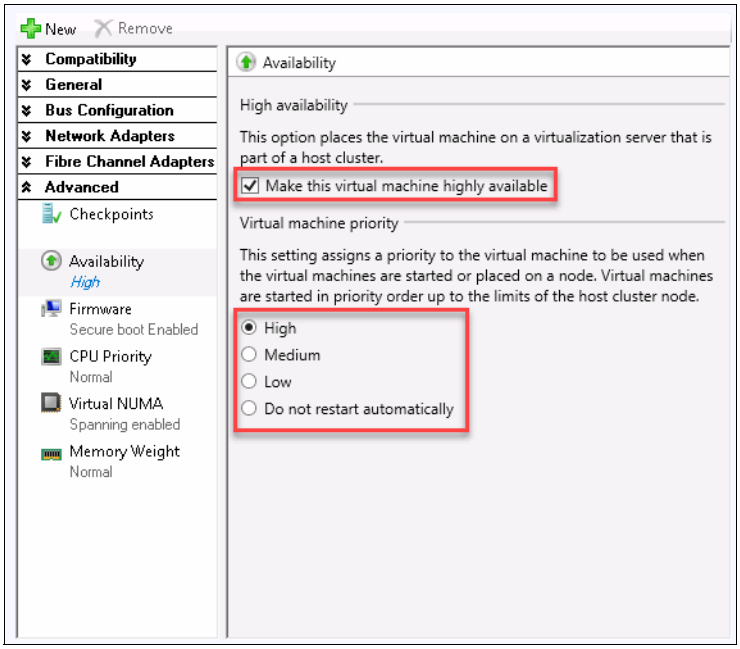


Figure 7-80 Hardware profile high availability sets

- *Firmware*: Allows you to employ secure boot for the virtual machine.
- *CPU Priority*: Allows you assign a priority for a virtual machine when allocating CPU resources to the host. In this scenario, the default options are selected.
- *Virtual NUMA*: Can help to improve the performance on virtual machines that are configured with large amounts of memory. When a virtual machine is started, the Hyper-V attempts to allocate all memory across hardware NUMA nodes. Select the option to allow the virtual machine to span hardware NUMA nodes.
- *Memory Weight*: Allows you to set the priority level to allocate memory resources. When a virtual machine is high, it gets allocated memory space before virtual machines with lower priority.

6. Click **OK** to complete the hardware profile.

   You can always view, modify, and copy the hardware profile. Deletion of a hardware profile is allowed only when there are no dependencies associated. To view the dependencies, select the hardware profile and use the Properties options.

7.14 Creating virtual machines using hardware profiles

Hardware profiles enable you to specify the hardware configuration for various virtual hardware components for virtual machines. Hardware profiles are used to provision new virtual machines as you create them or to customize one or more templates that you use to create new virtual machines.

When using VMM, virtual machines can be provisioned using a number of methods. For purposes of this book, we are provisioning virtual machines from a template, which allows us to create virtual machines with consistent settings configured in a hardware profile.

To create a new virtual machine using a hardware profile:

1. Log on to VMM and select **VMs and Services** → **Create Virtual Machine** → **Create Virtual Machine**. The wizard opens.
2. In Select Source section, click the **Create the new virtual machine with a blank virtual hard disk** option, and click **Next**.
3. In Identity, specify the VM name and an optional description. In the Generation box, select **Generation 2** and then click **Next**.
4. In the Configure Hardware page, either select the profile that you want to use from the Hardware profile list or configure the hardware settings manually. Select the Hardware profile created in 7.13, “Hardware profiles” on page 155, and click **Next** (Figure 7-81).

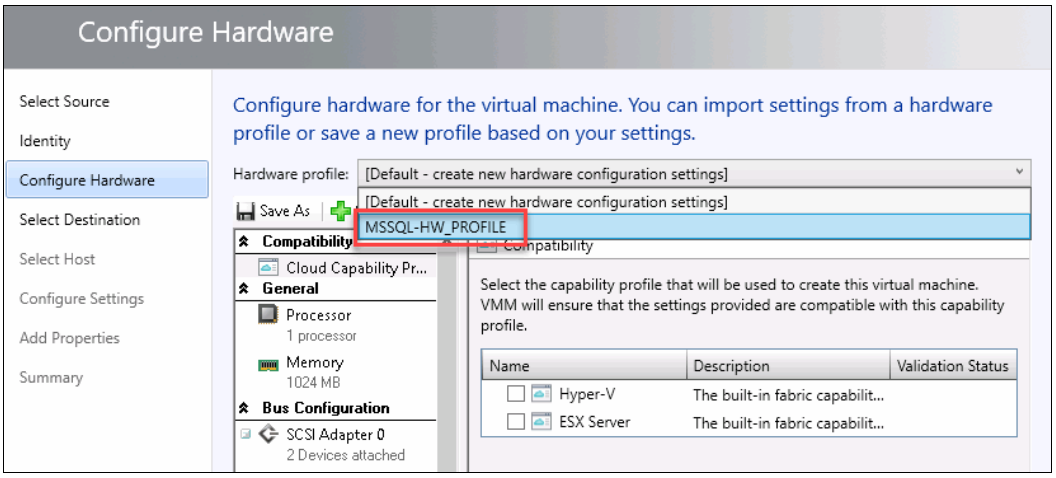


Figure 7-81 Selecting existing hardware profile

Ensure the following Hardware settings:

- *Compatibility:* Select **Hyper-V**, as you want to deploy the virtual machine to a private cloud environment using Cisco UCS.
- *Bus Configuration*: Select the ISO image that is available. The ISO image file must be present in the VMM library.
- *Network Configuration*: Ensure to select the required virtual network interfaces.
- *Advanced*: As covered in 7.13, “Hardware profiles” on page 155, there are number of advanced presets available. Ensure to set the appropriate settings.

5. In Select Destination, there are three options. You can either select the host group that you want to associate this virtual machine to, or select whether you want to store the virtual machine in the VMM library before you deploy it to a host. See Figure 7-82 on page 162 as example.

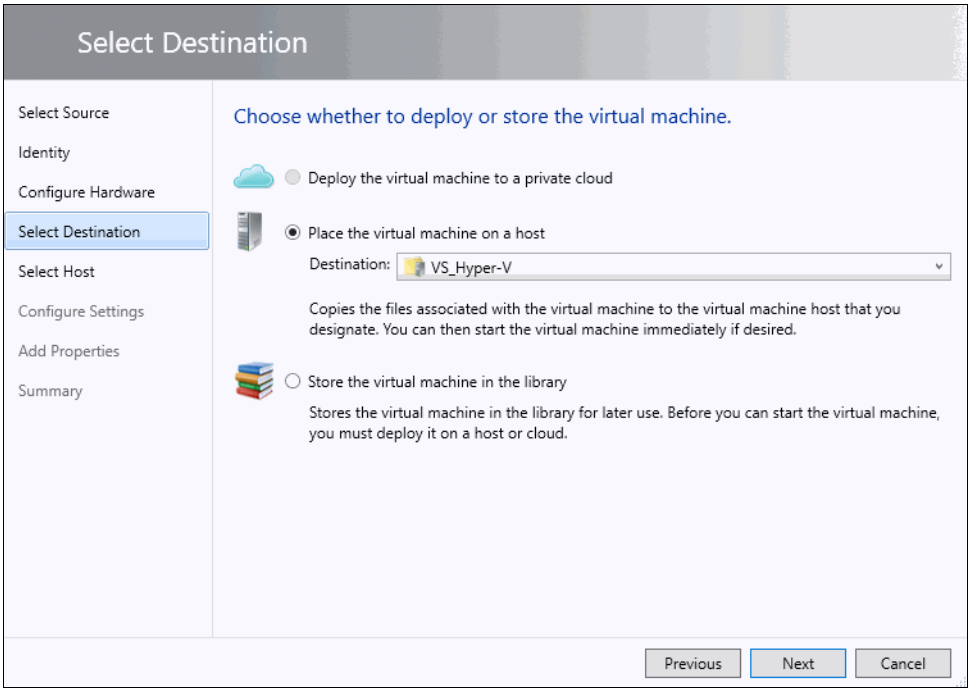


Figure 7-82 Destination of virtual machine

6. In Select Host, the VMM rates the available Hyper-V hosts based on expected utilization. Select one Hyper-V host from the list, as shown in Figure 7-83.

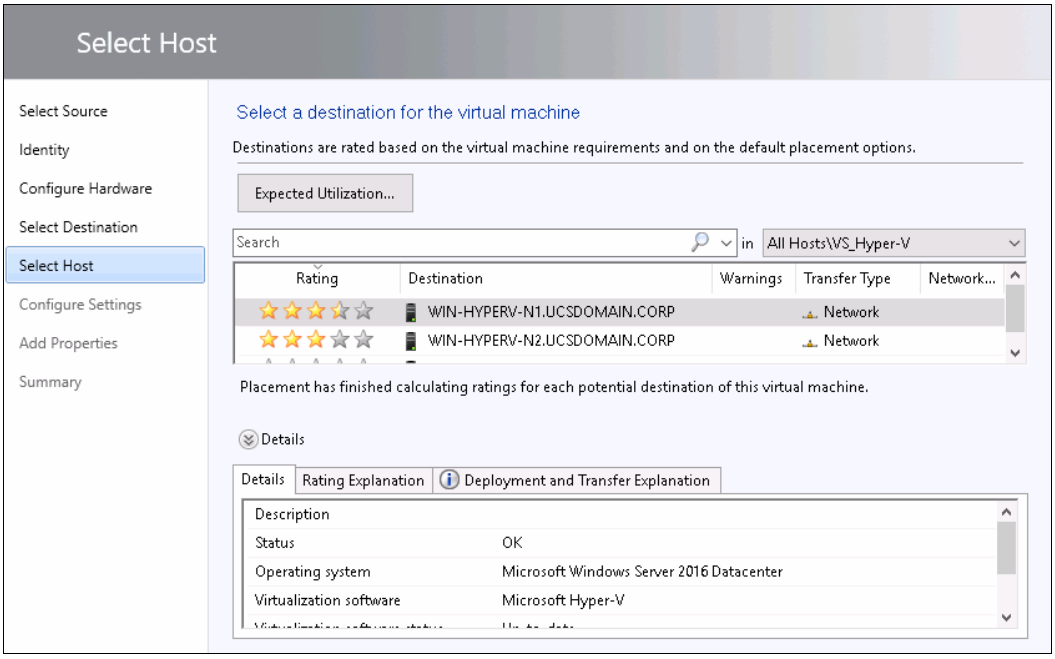


Figure 7-83 Selecting the Hyper-V host

7. In Configure Settings, you can review the virtual machine settings, such as the virtual machine path, networking, and the virtual machine disk drive deployment details, as shown in Figure 7-84 on page 163.

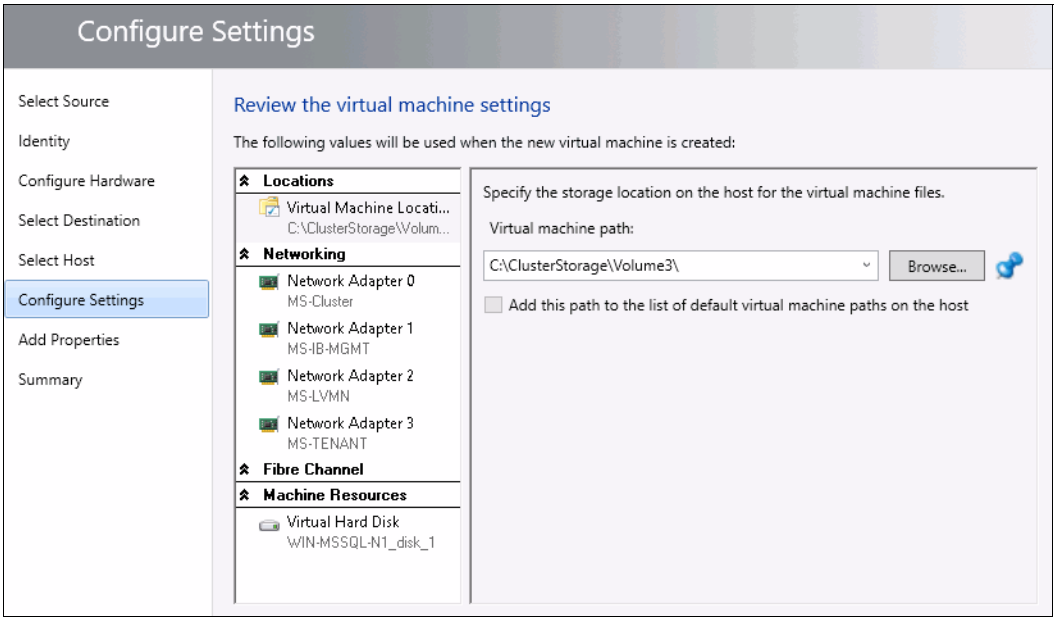


Figure 7-84 Configuring settings for the new virtual machine

8. In Add Properties, configure the action to take when the host starts or stops and the operating system that you will install on the VM, as shown in Figure 7-85.

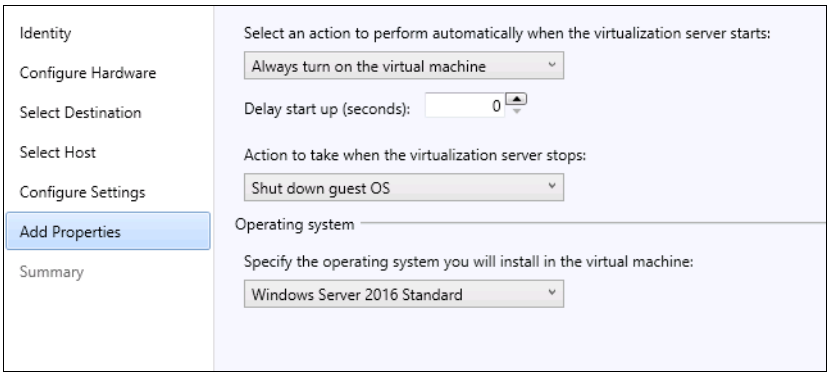


Figure 7-85 Virtual Machine virtualization properties

9. Confirm the settings on the Summary page. Select the **Start the virtual machine after deploying it** option if you want the VMM to start the virtual machine immediately after the build. Alternatively, leave the option clear to start the virtual machine at later time.

8

Microsoft SQL Server setup and failover cluster implementation

This chapter provides detailed instructions about how to set up Microsoft SQL Server and how to implement the Failover Clustering feature. It includes the following topics:

8.1 Before you begin

You need to have the following configuration information available before you begin the setup:

- Host names of both Hyper-V cluster hosts
- Host names of both SQL Server virtual machines (VMs)
- Virtual Machine Manager (VMM) client access
- Administrator login credentials for all VMs (domain account)
- V5030 GUI and CLI access
- A new host name for the Windows Failover cluster (and an unused IP address)
- A new host name for the SQL Server cluster (and an unused IP address)
- A new SQL server service account (domain account)

8.1.1 Review the virtual machine configuration

Two virtual machines (VMs) are required to configure SQL Server in a failover clustering configuration. The VMs can be deployed quickly using the `MSSQL-HW-PROFILE` hardware template discussed in 7.13, “Hardware profiles” on page 155. Using a template ensures that you create an identical configuration for both VMs. The VMs deployed using the template will have the characteristics listed in Table 8-1.

Table 8-1 Virtual machine configuration

VM name	Hyper-V cluster node hosting Hyper-V cluster host VM	vCPU	Memory	Boot disk size	Operating system
`WIN-MSSQL-N1`	`WIN-HYPERV-N1`	8	32 GB	100 GB	Windows Server 2016 STD
`WIN-MSSQL-N2`	`WIN-HYPERV-N2`	8	32 GB	100 GB	

8.1.2 Review the OS configuration

Install Microsoft Windows Server 2016 on both the VMs after they are powered up by the Virtual Machine Manager (VMM). A standard version with a GUI is recommended for both VMs.

Install an OS with the default and identical setup parameters to ease configuration. Also, both VMs need to join a single Active Directory (AD) server.

Complete the network adapter configuration on each VM before you begin the installation.

8.2 Provisioning storage volumes for Hyper-V cluster nodes

In this section, you use two Hyper-V VMs to set up Microsoft SQL Server database in failover configuration. Both VMs need access to shared storage via the underlying failover cluster that is running on the parent Hyper-V cluster hosts.

Provisioning storage volumes is a multi-step process, as follows:

1. Create volumes on V5030 storage and assign those volumes to Hyper-V cluster.
2. Configure the Cluster Shared Volumes (CSV) on the Hyper-V cluster.

3. Create a shared Hyper-V virtual hard disk (VHD) using the CSV assigned in the previous step and allocate this VHD to the Microsoft SQL virtual machines.
4. Configure the CSV on the Microsoft SQL VMs.
5. Configure Microsoft SQL Server to use the assigned CSV.

Create the set of volumes listed in Table 8-2 on the V5030 for installation of Microsoft SQL Server. See 5.1, “Completing the initial setup of the Cisco UCS 6324 Fabric Interconnects” on page 44 for information about creating the volumes using V5030 GUI.

Table 8-2 Volumes to be created on V5030

Volume Name	Capacity	Easy Tier	MDisk Tier	Purpose
HyperV-MSSQL-Quorum	1.2 GB	OFF	SAS	Cluster quorum
HyperV-MSSQL-System	103 GB	ON	SSD + SAS	System files
HyperV-MSSQL-TempDB	103 GB	OFF	SSD	Temp databases
HyperV-MSSQL-UserData-0	203 GB	ON	SSD + SAS	Database data files (striped)
HyperV-MSSQL-UserData-1	203 GB	ON	SSD + SAS	Database data files (striped)
HyperV-MSSQL-UserData-2	203 GB	ON	SSD + SAS	Database data files (striped)
HyperV-MSSQL-UserData-3	203 GB	OFF	SSD + SAS	Database data files (striped)
HyperV-MSSQL-UserLog	103 GB	OFF	SSD	Database log files

Tip: Each volume loses a few GBs to NTFS structures that are created at the Hyper-V level, and effective capacity that is available to the Microsoft SQL Server database can be less than expected by the database administrator.

8.2.1 Creating easy-tiered volumes on the IBM Storwize V5000 for data files, quorum, and system files

You can create the volumes that are required for the Microsoft SQL Server’s data files, quorum, and system files via the V5030 GUI by completing the following steps:

1. Enter the IP address of the management GUI into a browser and start the Management GUI.
2. Navigate to **Volumes**, and then select **Create Volumes**.
3. Use *None* for **Capacity Savings** to create *thick* volumes.
4. Select **EasyTier_POOL** pool.
5. Provide volume names and capacities to create the volumes.

8.2.2 Creating volumes on the V5030 for the tempdb and log files

For better performance, keep the `tempdb` and `log` file volumes on solid-state drive (SSD) managed disks (MDisks). If a separate pool is not available, keep these volumes in a shared easy tier pool but confined only within SSD MDisks.

By default, a volume created in easy tier pool spans across serial-attached SCSI (SAS) disks in the pool only. After easy tier identifies hot extents, these SAS disks get moved to SSD disks. To allocate extents directly from SSD disks, you can create the volumes manually by using the CLI. Turn off easy tier on the volumes to prevent the extents from migrating to SAS disks.

To create volumes on the V5030 for the `tempdb` and `log` files:

1. Open a Secure Shell (SSH) connection the V5030 CLI using the V5030 management IP address, and then log in using your GUI user credentials.
2. Run the **`mkvdisk`** command to create the volumes.

> **Specifying all the MDisks:** You must specify a list of all the SSD MDisks in the pool. You can determine this list by using the **`lsmdisk`** command.

Example 8-1 shows the **`mkvdisk`** command. Replace <*`volume_name`*> and <*`size`*> with the appropriate values for your system.

Example 8-1 The mkvdisk command

```
mkvdisk -cache readwrite -nofmtdisk -mdiskgrp EasyTier_POOL -mdisk SSD_MDisk -name
<volume_name> -size <size> -unit gb -easytier off
```

8.2.3 Mapping volumes to Hyper-V cluster nodes

Use the GUI to map the newly created volumes to Hyper-V cluster nodes. Use the host cluster object that you created in the GUI earlier to map the volumes. This process ensures that the same SCSI ID is assigned to volumes on both Hyper-V cluster nodes, as shown in Figure 8-1 on page 169.

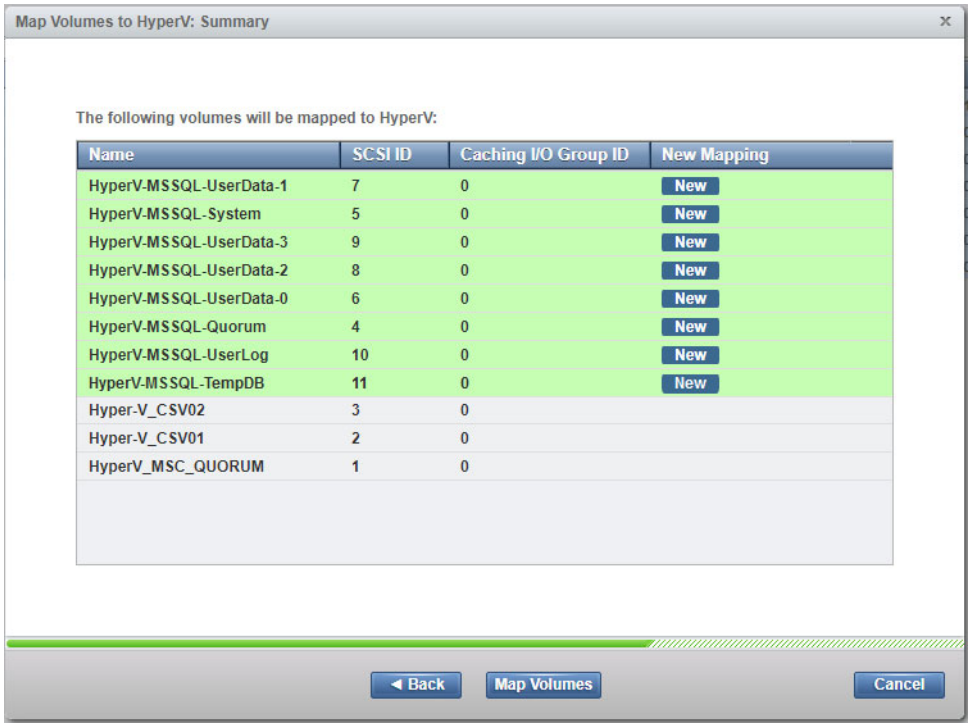


Figure 8-1 Map volumes to Hyper-V cluster

8.3 Creating CSV on a Hyper-V cluster

This section describes how to configure CSV using the newly provisioned volumes.

8.3.1 Initializing disks using the Disk Management facility

To initialize disks using the Disk Management facility:

1. Connect to the first Hyper-V cluster host by using Remote Desktop Protocol (RDP).
2. Start the Disk Management facility, and then select **Actions** → **Rescan Disks**. The new disks show as *offline* disks.
3. Right-click each disk, and select **Online**.
4. Right-click one new disk, and select **Initialize Disks**.
5. Select all the new disks, and then select **MBR (Master Boot Record)** as the partition style.
6. Click **OK** to complete the disk initialization.

8.3.2 Create a file system volume on the disks

To create a file system volume on the disks:

1. Right-click shaded/unallocated area of the disk, and select **New Simple Volume** to start the wizard. Click **Next**.
2. Specify volume size.
3. Select the **Do not assign drive letter or drive path** option.

4. Provide a volume label that matches the volume name of corresponding V5030 volume.
5. Select **NTFS** as the file system for the volume.
6. Select **64K** for the allocation unit size.
7. Click **Next** and **Finish** to complete the process.
8. Repeat this process for all new volumes.

After all the disks are ready, log on to the second Hyper-V cluster host, and bring the disks online using the Disk Management facility. You do not need to re-create file systems on the second node.

8.3.3 Adding disks into the Hyper-V cluster

To add the disks into the Hyper-V cluster:

1. Click **Server Manager** → **Tools** and select **Failover Cluster Manager**.
2. Click **Connect to Cluster**, and select **Cluster on this server**. Then click **OK**.
3. Navigate to **Storage** → **Disks**. Then, click **Actions** → **Add Disk**.
4. Select all the required disks from Available Storage, and click **OK**. The disks are added to the cluster as a potential resource.
5. Right-click each disk, and select **Properties**.
6. Rename the disk by typing the corresponding V5030 volume name in the **Name** text box, and click **OK** to save, as shown as shown in Figure 8-2.

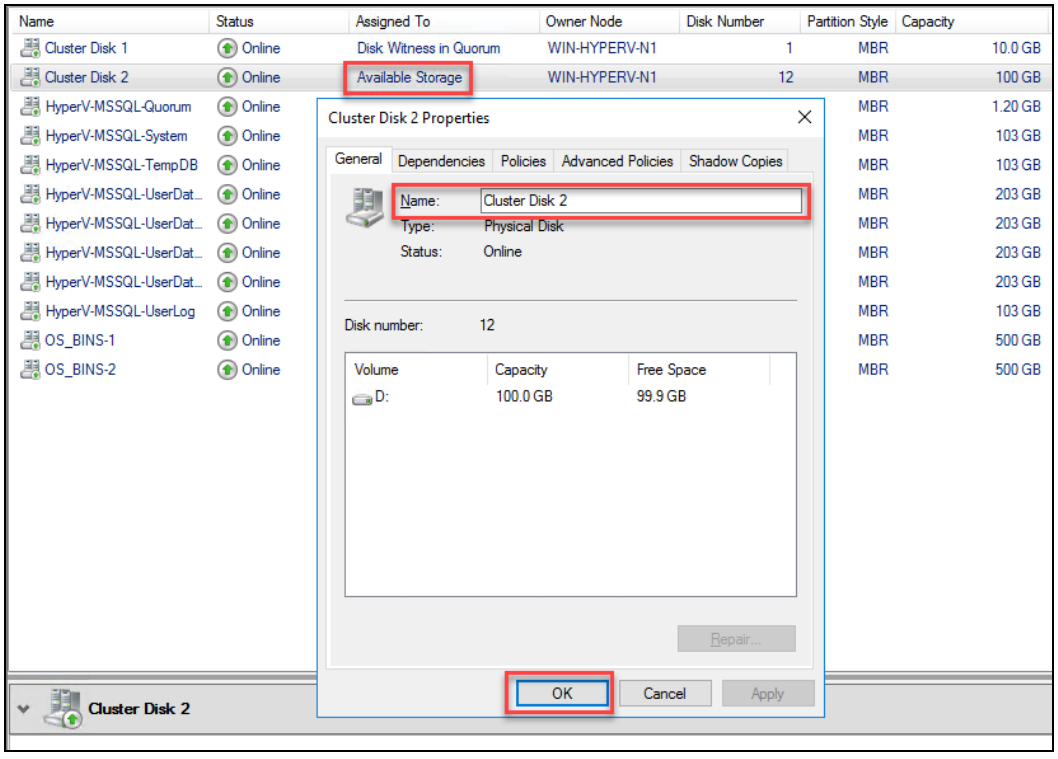
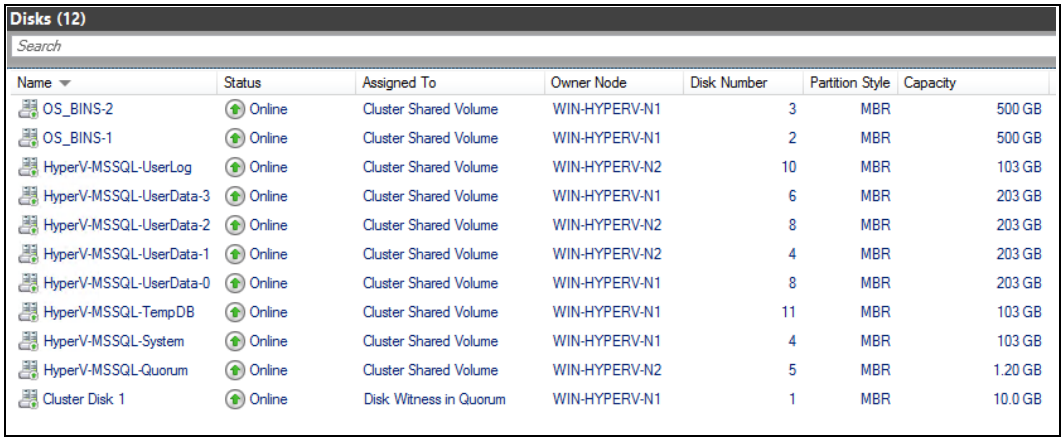


Figure 8-2 Rename the cluster disk resource

7. Right-click all the disks, and select **Add to Cluster Shared Volumes.** This option adds the disks as shared cluster volumes (CSVs) that can be accessed simultaneously by all the nodes in the cluster, as shown in Figure 8-3.



Disks (12)

Search

Name	Status	Assigned To	Owner Node	Disk Number	Partition Style	Capacity
OS_BINS-2	Online	Cluster Shared Volume	WIN-HYPERV-N1	3	MBR	500 GB
OS_BINS-1	Online	Cluster Shared Volume	WIN-HYPERV-N1	2	MBR	500 GB
HyperV-MSSQL-UserLog	Online	Cluster Shared Volume	WIN-HYPERV-N2	10	MBR	103 GB
HyperV-MSSQL-UserData-3	Online	Cluster Shared Volume	WIN-HYPERV-N1	6	MBR	203 GB
HyperV-MSSQL-UserData-2	Online	Cluster Shared Volume	WIN-HYPERV-N2	8	MBR	203 GB
HyperV-MSSQL-UserData-1	Online	Cluster Shared Volume	WIN-HYPERV-N2	4	MBR	203 GB
HyperV-MSSQL-UserData-0	Online	Cluster Shared Volume	WIN-HYPERV-N1	8	MBR	203 GB
HyperV-MSSQL-TempDB	Online	Cluster Shared Volume	WIN-HYPERV-N1	11	MBR	103 GB
HyperV-MSSQL-System	Online	Cluster Shared Volume	WIN-HYPERV-N1	4	MBR	103 GB
HyperV-MSSQL-Quorum	Online	Cluster Shared Volume	WIN-HYPERV-N2	5	MBR	1.20 GB
Cluster Disk 1	Online	Disk Witness in Quorum	WIN-HYPERV-N1	1	MBR	10.0 GB

Figure 8-3 Disks added as CSV

All of these shared volumes are mounted by Windows as New Technology File System (NTFS) mount points inside `C:\ClusterStorage` on both nodes. These mount points are given default junction points as `C:\ClusterStorage\Volume`*nn* by Windows, and it is highly recommended that you rename these mount points to match the V5030 volume names.

8. Rename the mount points online using the **`REN`** command on the command prompt or using the Windows Explorer Rename option. Rename the mount point only on one Hyper-V cluster host. A sample output is show in Figure 8-4.

```
C:\ClusterStorage>dir
 Volume in drive C has no label.
 Volume Serial Number is 5A69-FAA0

 Directory of C:\ClusterStorage

09/19/2017  05:51 AM    <DIR>          .
09/19/2017  05:51 AM    <DIR>          ..
09/19/2017  05:21 AM    <JUNCTION>     Volume3 [\??\Volume{839699f1-f684-4396-8bf5-96dd7d6973a7}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume4 [\??\Volume{0b9c7ef1-708a-46a4-96cc-704371c810e0}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume5 [\??\Volume{ca1f7f04-d0b2-41a7-870b-92f4cc1ae3cd}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume6 [\??\Volume{a5d5fb18-9c86-47e9-9f72-6fac24e4aacd}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume7 [\??\Volume{5bca7221-d3d1-479a-8f65-6a4cb94831f0}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume8 [\??\Volume{83a9fea3-dc76-4ae8-be7b-845db639b045}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume9 [\??\Volume{230c918d-5079-4e31-b31b-a77150360116}\]
               0 File(s)              0 bytes
               9 Dir(s)  91,690,311,680 bytes free

C:\ClusterStorage>ren Volume3 HyperV-MSSQL-System

C:\ClusterStorage>ren Volume4 HyperV-MSSQL-TempDB

C:\ClusterStorage>ren Volume5 HyperV-MSSQL-UserData-0

C:\ClusterStorage>ren Volume6 HyperV-MSSQL-UserData-1

C:\ClusterStorage>ren Volume7 HyperV-MSSQL-UserData-2

C:\ClusterStorage>ren Volume8 HyperV-MSSQL-UserData-3

C:\ClusterStorage>ren Volume9 HyperV-MSSQL-UserLog
```

Figure 8-4 Rename the CSV mount points

8.4 Assigning the V5030 volumes as shared drives to SQL VMs

This section describes how to assign CSV volumes to SQL VMs as SCSI LUNs. You need to create Hyper-V virtual hard disk (VHD) files on CSV volumes and assign them to SQL VMs. Hyper-V presents VHD files to VMs as SCSI LUNs.

8.4.1 Creating shared drives and assigning them to first SQL VM

Complete the following steps to create shared drives in the Hyper-V cluster for the first node:

1. Log on to the Hyper-V server (`WIN-HYPERV-N1`) using RDP.
2. Click **Server Manager** → **Tools** and select **Failover Cluster Manager**.
3. Select **Roles** from the navigation pane on the left.

   In the right pane, a role displays for each child VM in the cluster, and the Owner column indicates whether that role is currently owned by this Hyper-V server as shown in Figure 8-5.

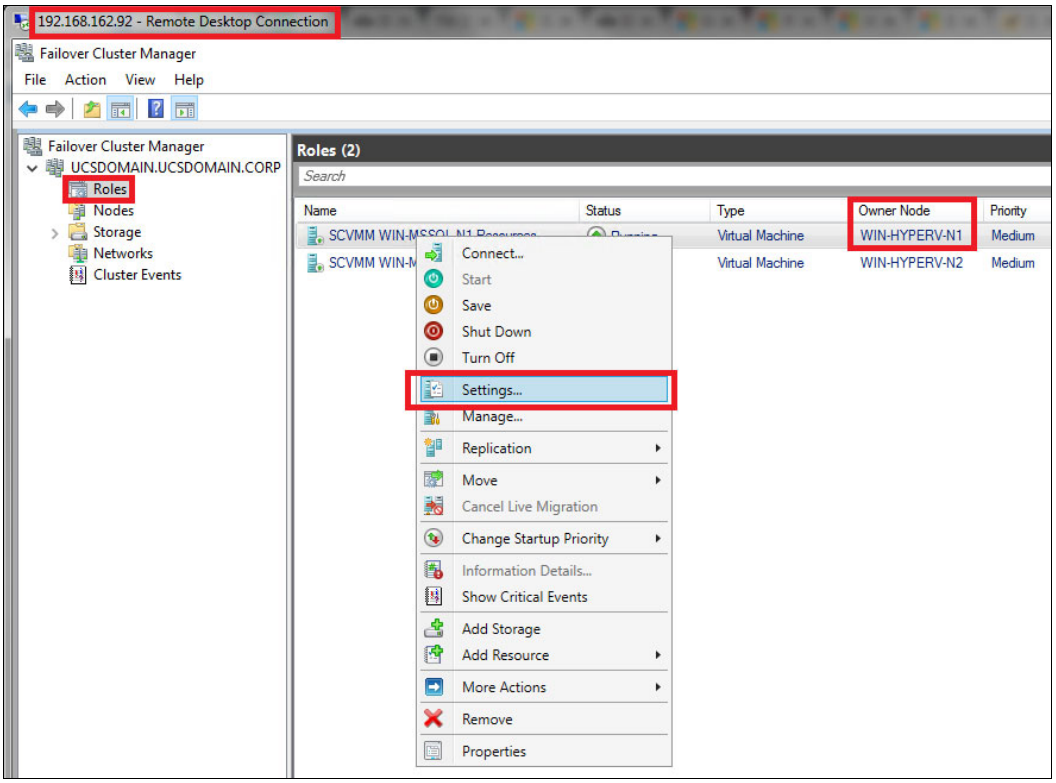


Figure 8-5 Change VM role settings

4. Right-click the role that is owned by this Hyper-V server, and select **Settings**.

5. Navigate to **SCSI Controller**, select **Shared Drive** from the selection, and click **Add**, as shown in Figure 8-6.

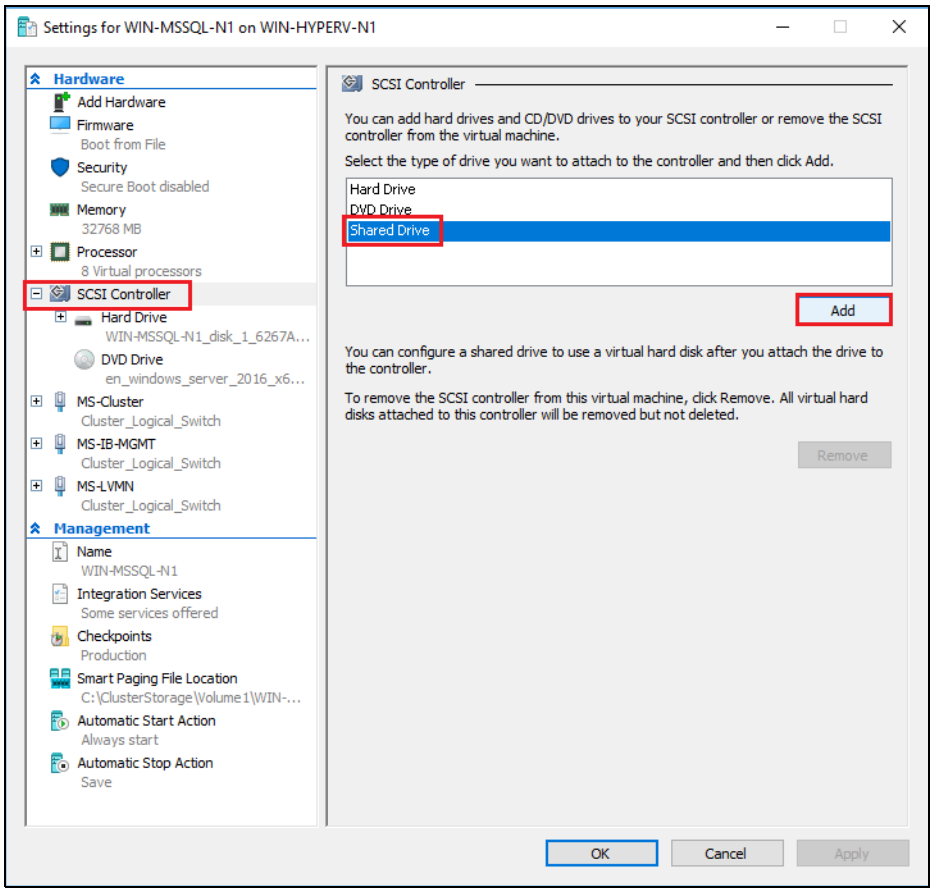


Figure 8-6 Add shared drives to the VM

6. Click **New** as indicated in Figure 8-7 to start the wizard. Click **Next** if you are prompted with an introduction.

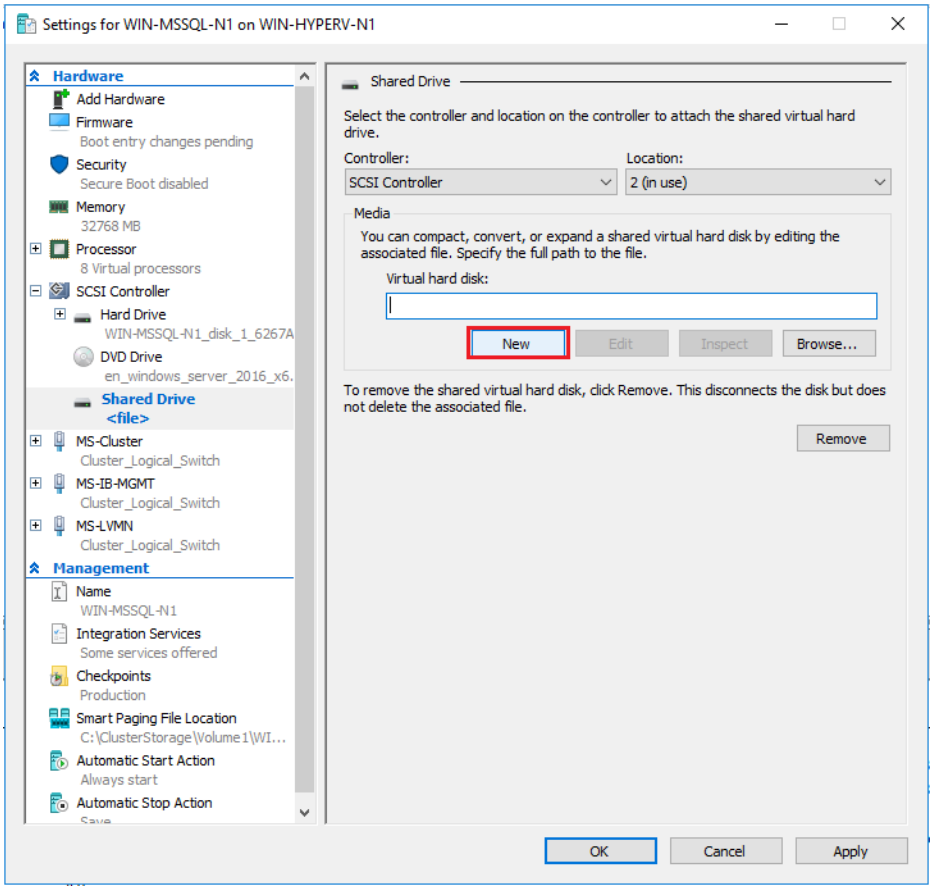


Figure 8-7 Create a new VHD file

7. Click **VHDX** to choose the VHDX format for the virtual hard disk, as shown in Figure 8-8.

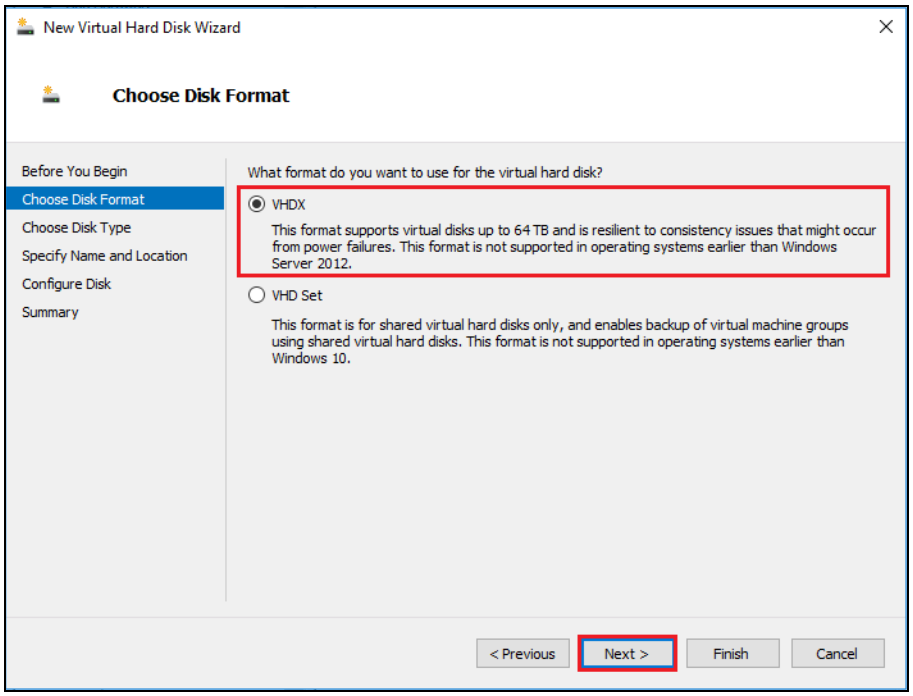


Figure 8-8 Select the VHDX format

8. Select **Fixed size** as the disk type for the VHDX file, and click **Next**, as shown in Figure 8-9.

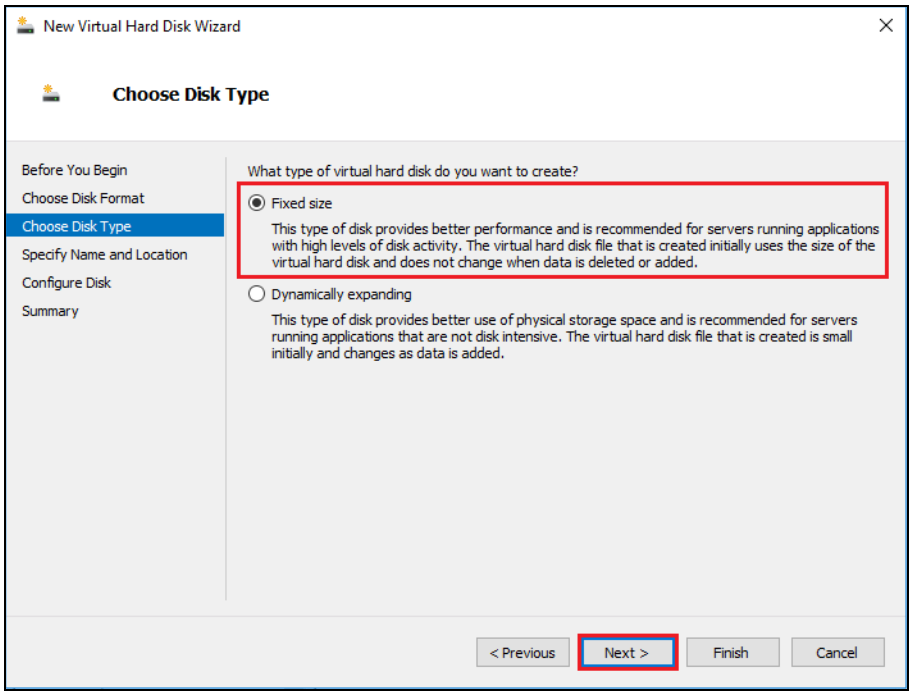


Figure 8-9 Select a fixed size to allocate all capacity

9. Select the location to create the VHDX file. This location is the shared NTFS mount point that is created by cluster earlier, as shown in Figure 8-10. Provide a name for the VHDX file that corresponds to each mount point to enable easy identification.

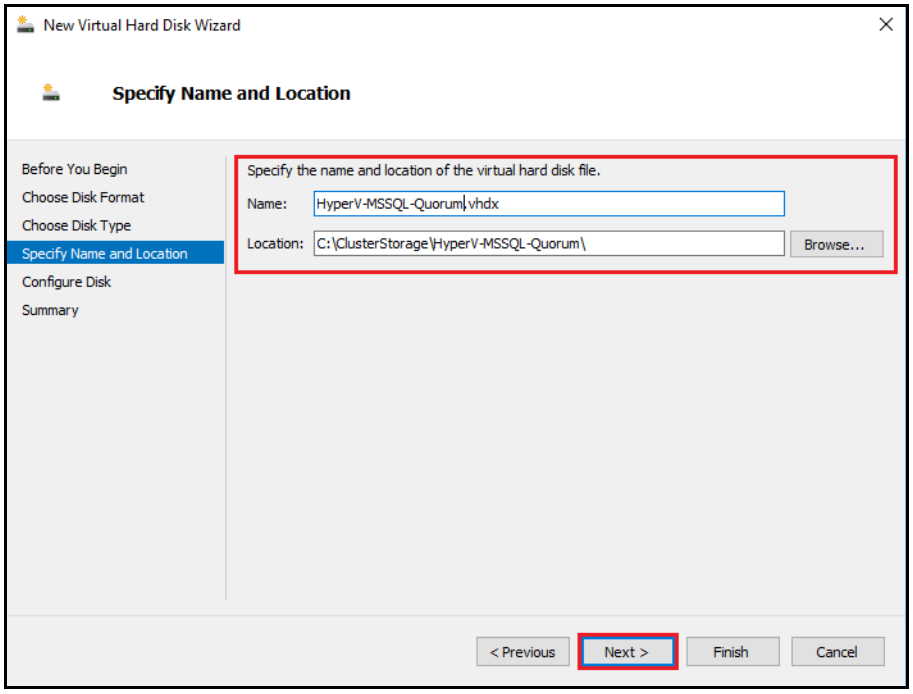


Figure 8-10 Specify VHDX name and location

10. Select the **Create a new blank virtual hard disk** option, provide a size (in GB), and click **Next** to continue, as shown in Figure 8-11. Check the free capacity that is available on the mount point, and enter the same value here to span the VHDX file across the entire disk. The creation of the VHDX file fails if enough capacity is not available on the CSV mount point.

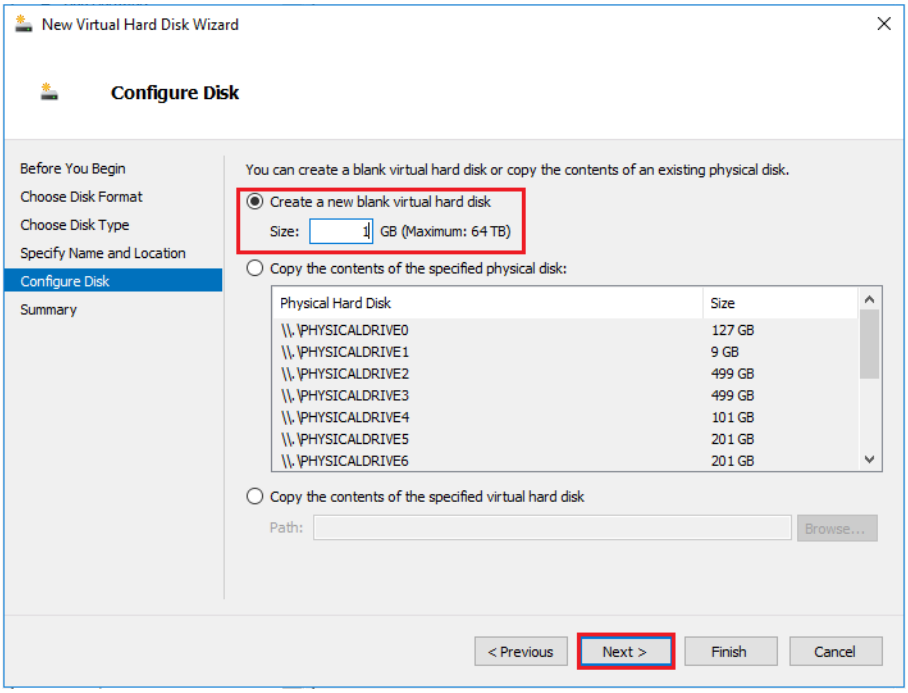


Figure 8-11 Provide the VHDX file size

11. Review the summary, and click **Finish** to complete the creation of the VHDX file as shown in Figure 8-12.

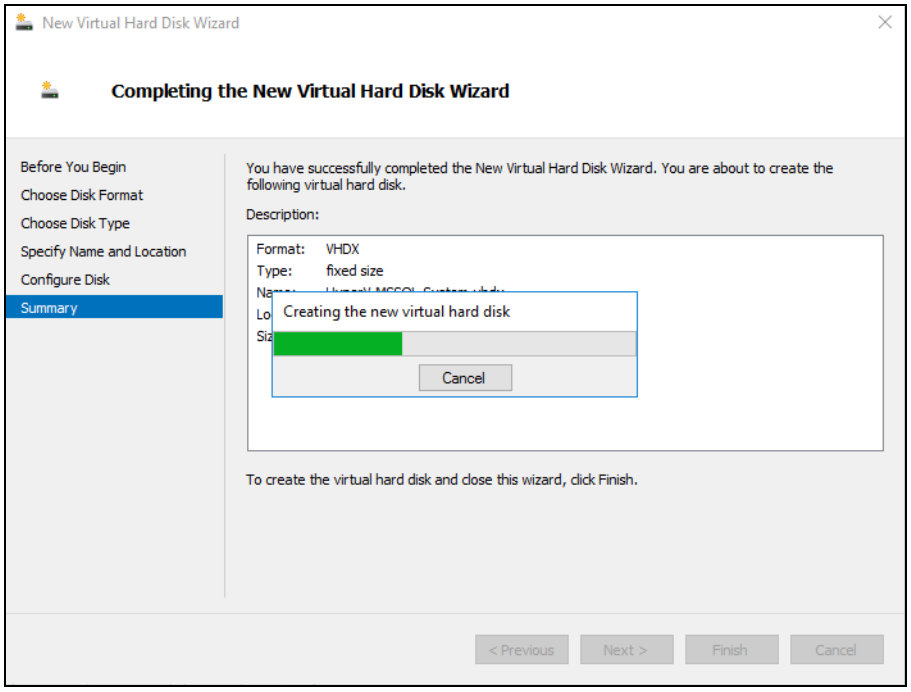


Figure 8-12 New VHDX creation progress

12. Repeat steps 5-11 to create shared drives using all the remaining mount points, and click **OK** to update the VM settings.

8.4.2 Assigning shared drives to a second SQL VM

You need to assign the shared drives that you created in the previous section to a second VM without creating new ones. The drives are marked as *shared drives*, thus Hyper-V allows simultaneous access to both VMs, such as storage LUNs shared via SAN.

Complete the following steps to assign the drives to a second SQL VM:

1. Log on to the second Hyper-V server (`WIN-HYPERV-N2`) using RDP.
2. Click **Server Manager** → **Tools** and select **Failover Cluster Manager**.
3. Select **Roles** from the navigation pane on the left.

   In the right pane, a role for each child VM in the cluster displays, and the Owner column indicates whether that role is currently owned by this Hyper-V server.
4. Right-click the role that is owned by this Hyper-V server, and select **Settings**, as shown in Figure 8-13.

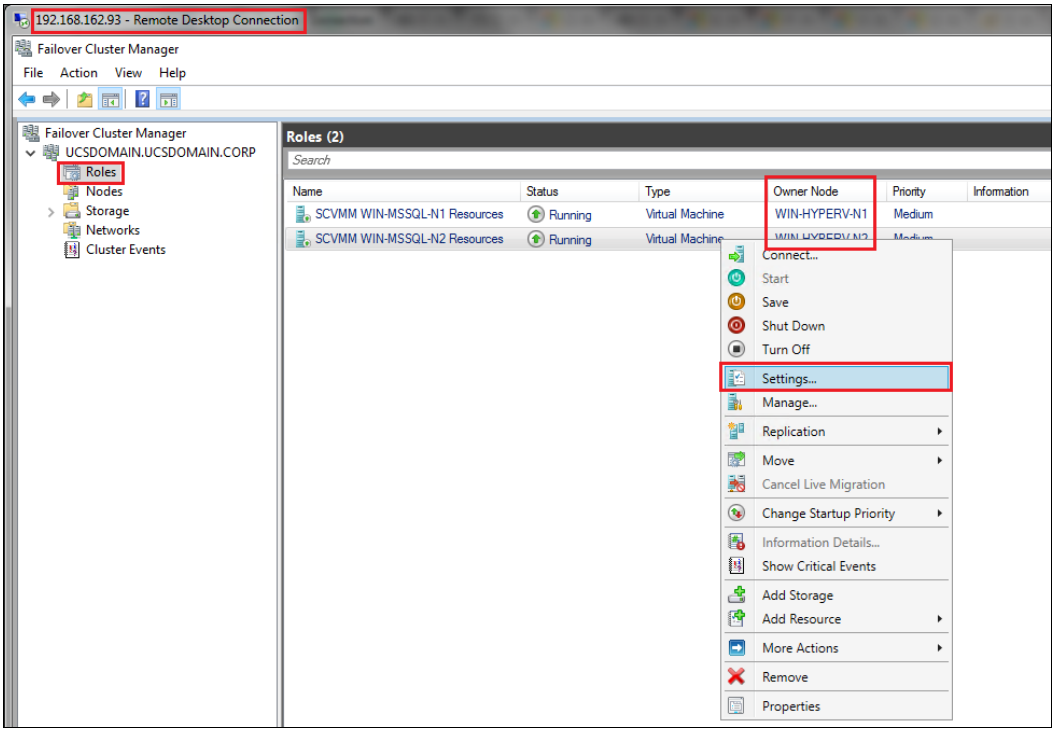


Figure 8-13 Change the VM role settings

5. Navigate to **SCSI Controller**, select **Shared Drive** from the selection, and click **Add**, as shown in Figure 8-14.

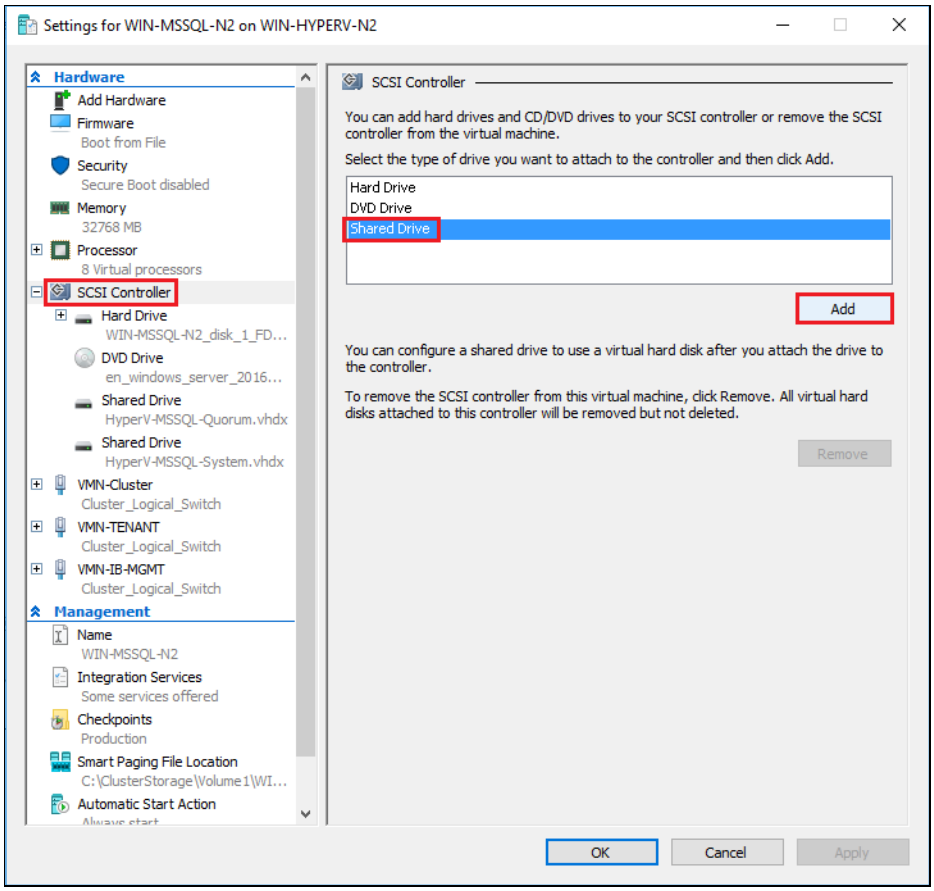


Figure 8-14 Add shared drives to the VM

6. Click **Browse**, and select the location of shared drive (VHDX file), as shown in Figure 8-15.

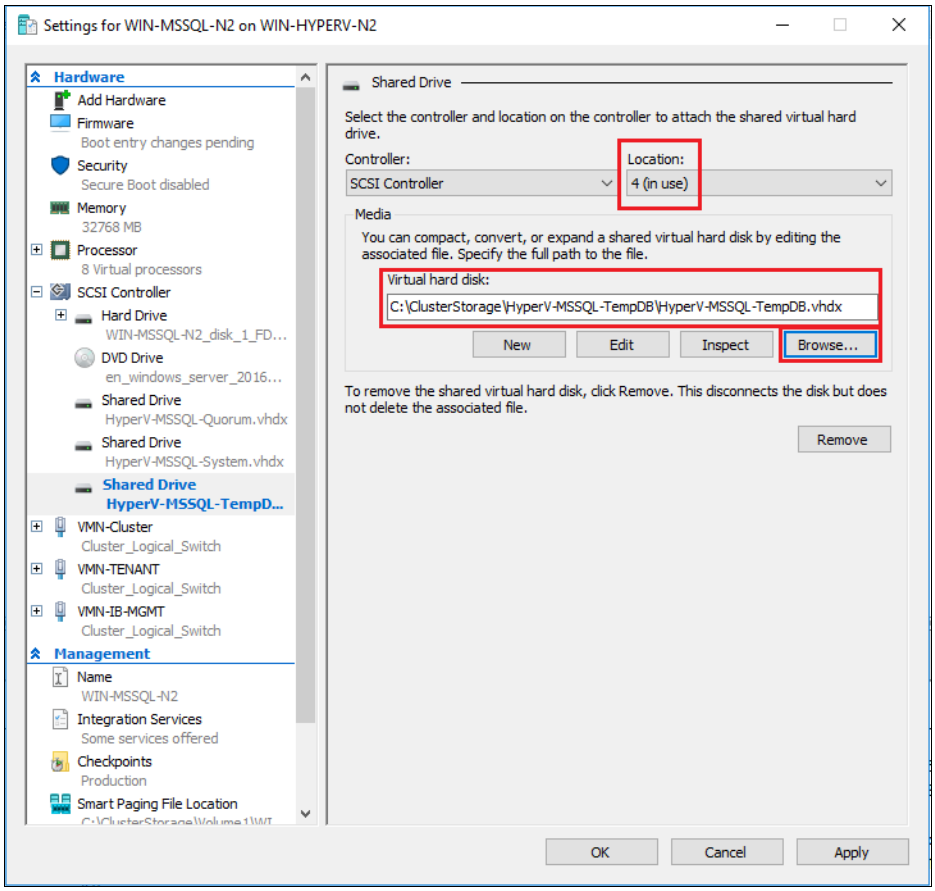


Figure 8-15 Provide VHDX location

LUN location note: For each VHDX file, use the same LUN location that is assigned on node 1. Both the nodes should see each VHDX at same SCSI LUN ID.

7. Repeat steps 5 and 6 for all the VHDX files, and click **OK** to save the changes.

8.5 Preparing the Cluster Shared Volumes on SQL VMs for Windows Failover Cluster

After the shared drives are presented to SQL VMs, you need to prepare them for setting up the Windows Server Failover Clustering feature. This process is similar to that described in 8.3.1, “Initializing disks using the Disk Management facility” on page 169. This section describes this process.

8.5.1 Initializing disks using the Disk Management facility

To configure Cluster Shared Volumes (CSV) using the newly provisioned volumes:

1. Connect to the first SQL VM (`WIN-MSSQL-N1`) using RDP.
2. Start **Disk Management**. Then, select **Actions** → **Rescan Disks**. New disks should be visible as offline disks.
3. Right-click each disk, and select **Online**.
4. Right-click one new disk, and select **Initialize Disks**.
5. Select all the new disks, and then select **MBR (Master Boot Record)** as the partition style.
6. Click **OK** to complete disk initialization.

8.5.2 Creating a file system volume on the disks

To create a file system volume on the disks:

1. Right-click the shaded/unallocated area of the disk, and select **New Simple Volume** to start the wizard. Then, click **Next**.
2. Specify the volume size.
3. Select the **Do not assign drive letter or drive path** option.
4. Provide a volume label that matches the volume name of the corresponding V5030 volume.
5. Select **NTFS** as the file system for the volume.
6. Select **64K** for the allocation unit size.
7. Click **Next** and **Finish** to complete the process.
8. Repeat this process for all new volumes.

After all the disks are ready, log on the second Hyper-V cluster host, and bring the disks online using the Disk Management facility. You do not need to re-create the file systems on the second node.

8.6 Installing the Windows Failover Clustering feature on SQL virtual machines

This section provides detailed instructions about how to set up a two-node Windows server failover cluster on the VMs. This section focuses on validating and setting up failover cluster on VMs. After the completion of this task, a Microsoft SQL Server 2016 failover cluster instance can be installed.

Complete the following steps:

1. Connect first to SQL VM (`WIN-MSSQL-N1`) via RDP.
2. Click **Server Manager** → **Tools** and select **Failover Cluster Manager**.

3. In the Failover Cluster Manager window, click **Validate Configuration** under the Management section, as shown in Figure 8-16.

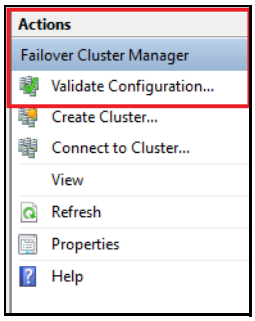


Figure 8-16 Start the cluster validation wizard

4. Enter the host names of the nodes, or browse and select them. Then, click **Next**, as shown in Figure 8-17.

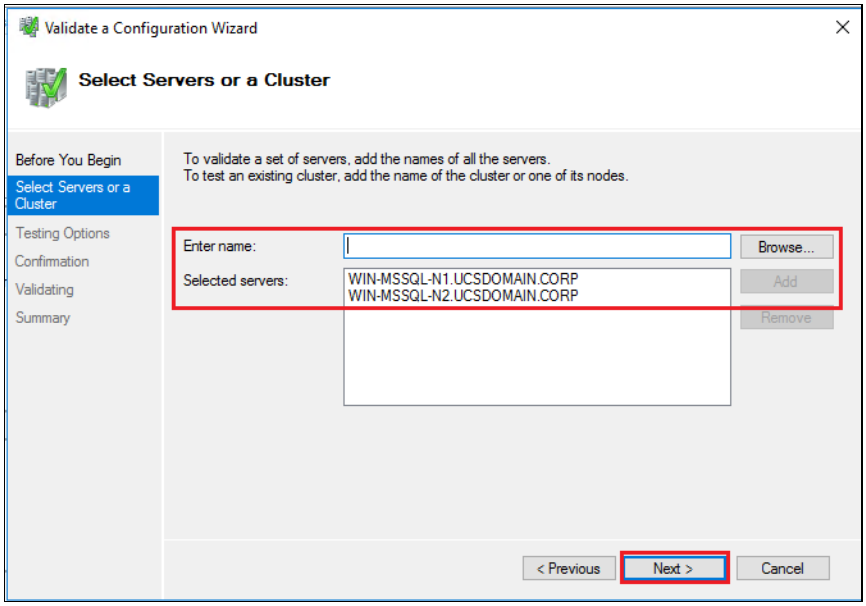


Figure 8-17 Enter host names

5. Select the **Run all tests (recommended)** option, and click **Next** as shown in Figure 8-18.

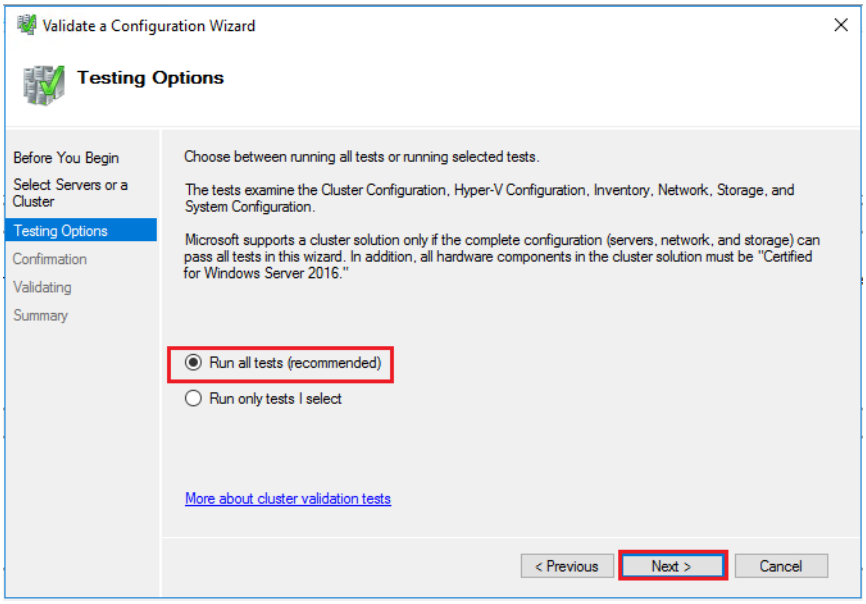


Figure 8-18 Choose testing options for validation

6. After the validation process is complete, review the report and fix any errors, as shown in Figure 8-19.

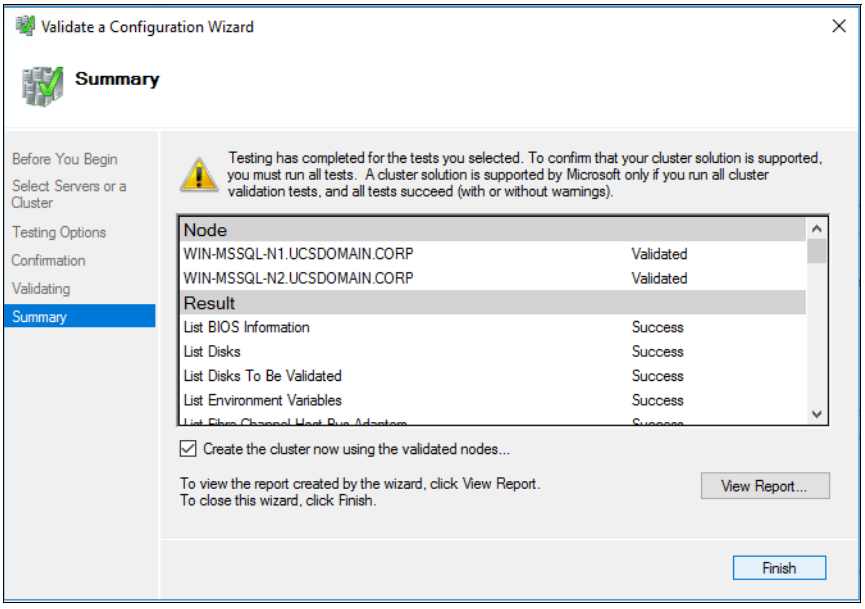


Figure 8-19 Validation summary

7. If the validation is successful without any issues, select the **Create the cluster using the validated nodes** option and click **Finish**.

8. Enter a cluster name and IP address for the cluster and click **Next**, as shown in Figure 8-20. The name and IP address should not be used on a network by other hosts and devices.

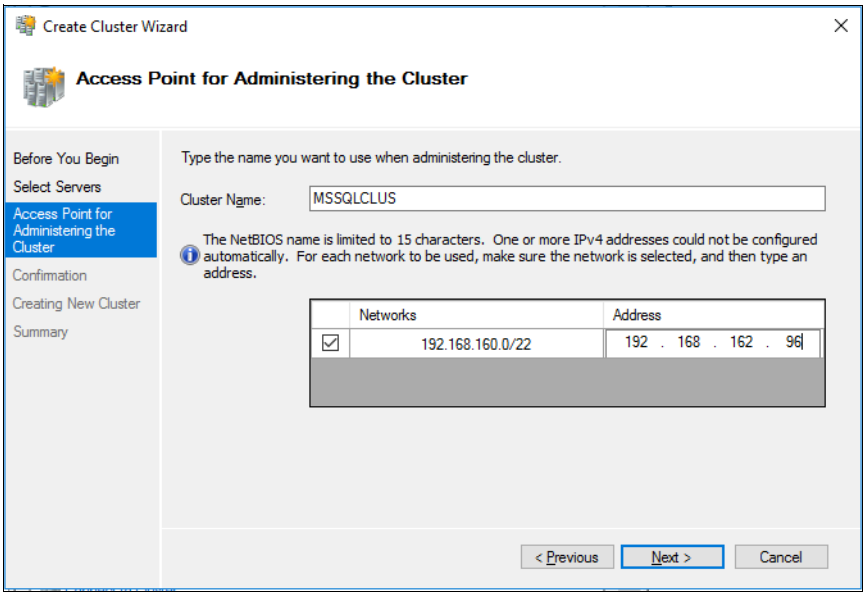


Figure 8-20 Provide cluster name and IP address

9. Review the settings in the Confirmation window, select the **Add all eligible storage to the cluster** option, and click **Next**, as shown in Figure 8-21.

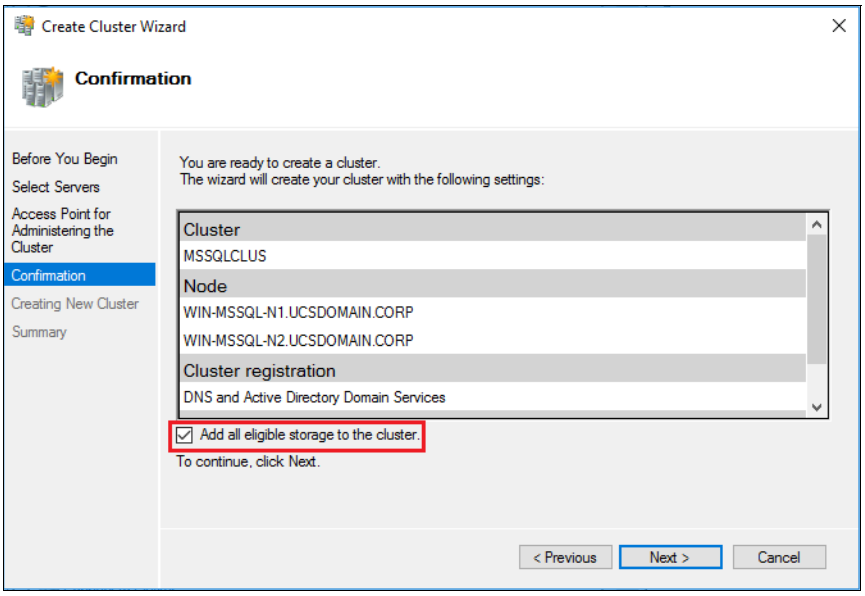


Figure 8-21 Complete the cluster creation

This process executes the cluster creation wizard and adds all the available volumes to the cluster resources.

10. In the Failover Cluster Manager window, verify that the statuses of the Cluster Core Resources, Network, and Storage are all online, as shown in Figure 8-22.

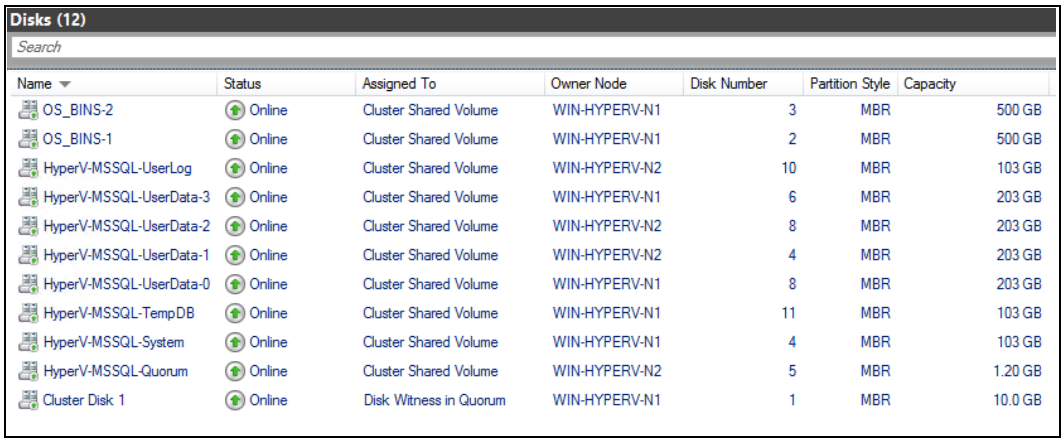


Figure 8-22 Verify the status of the cluster resources

11. Right-click the cluster name in the Failover Cluster Manager window, and select **More Actions** → **Configure Cluster Quorum Settings**, as shown in Figure 8-23.

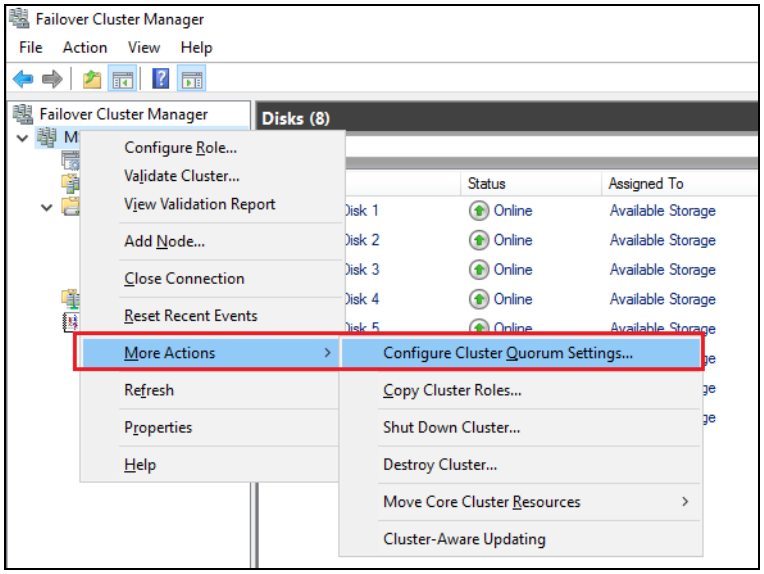


Figure 8-23 Configure Cluster Quorum Settings

12. Next, click the **Select the quorum witness** option, and click **Next**, as shown in Figure 8-24.

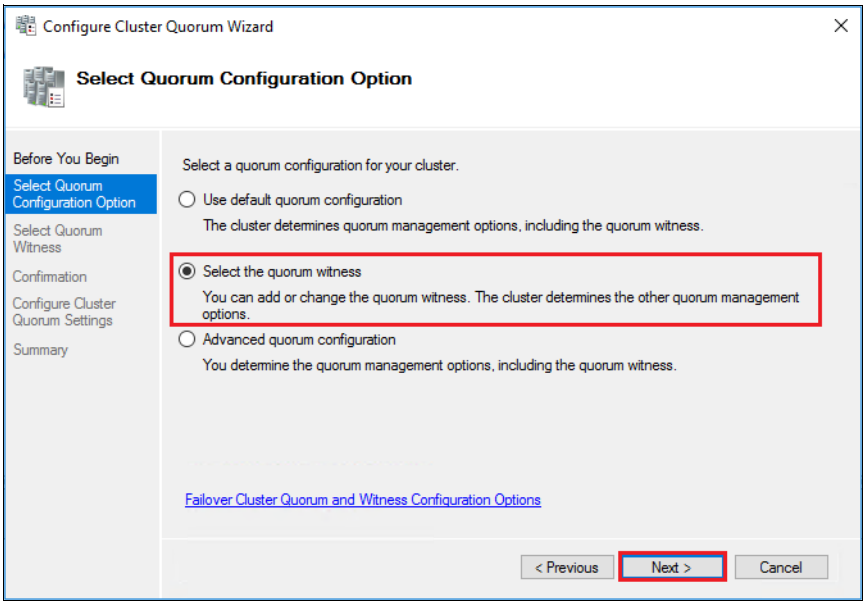


Figure 8-24 Select the quorum witness option

13. Click the **Configure a disk witness** option, and click **Next** to continue, as shown in Figure 8-25.

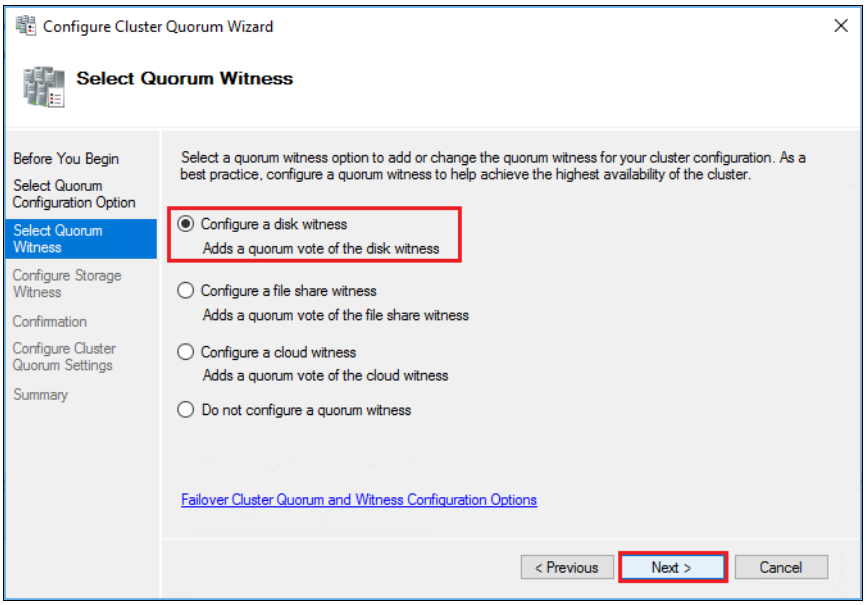


Figure 8-25 Configure a disk witness

14. Select the 1 GB volume that was assigned to the host for qourum, and click **Next** as shown in Figure 8-26.

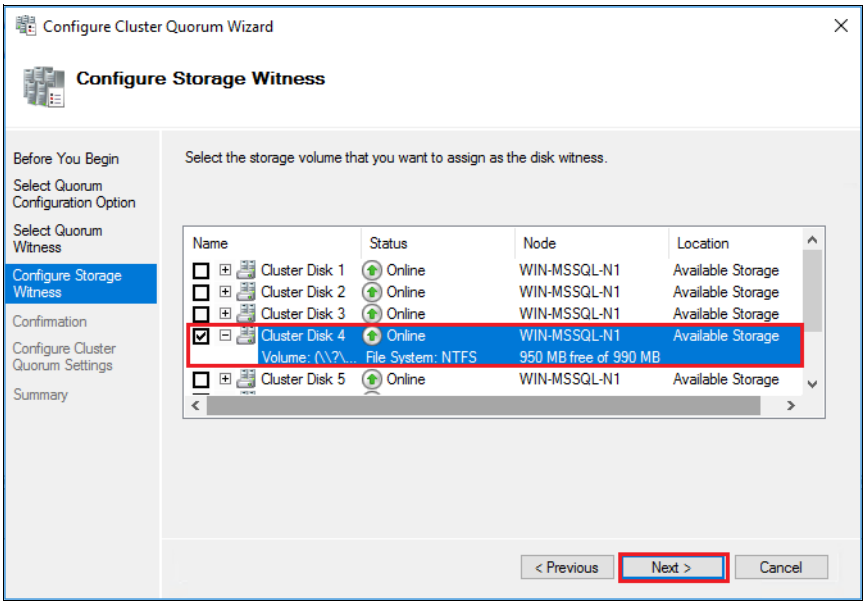


Figure 8-26 Select the cluster quorum disk

15. Click **Next** and **Finish** to complete the wizard as shown in Figure 8-27. This disk displays as **Disk Witness Quorum** in the **Assigned To** column in the Failover Cluster Manager.

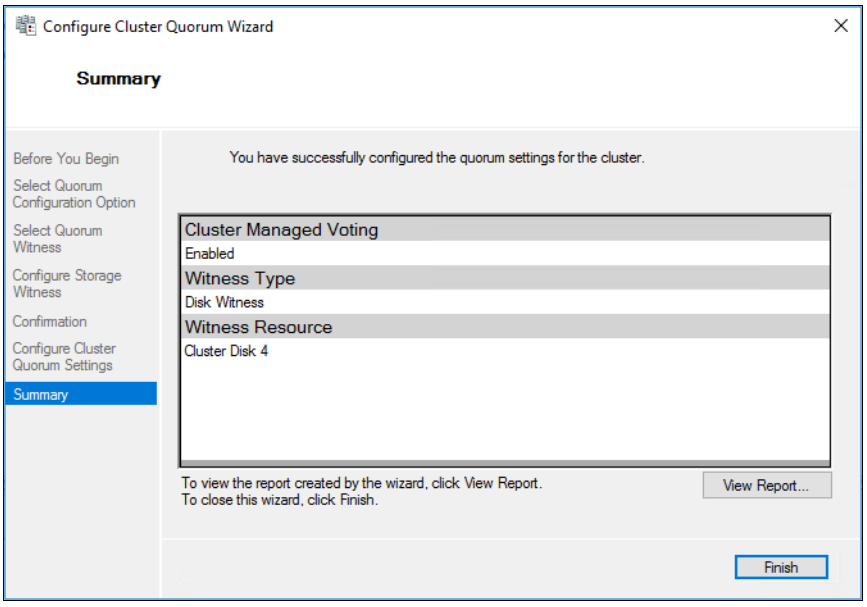


Figure 8-27 Complete the quorum setting changes

16. Verify that the CSV status is online. Right-click only those cluster disks that will be used by Microsoft SQL Server, and select **Add to Cluster Shared Volumes**, as shown in Figure 8-28.

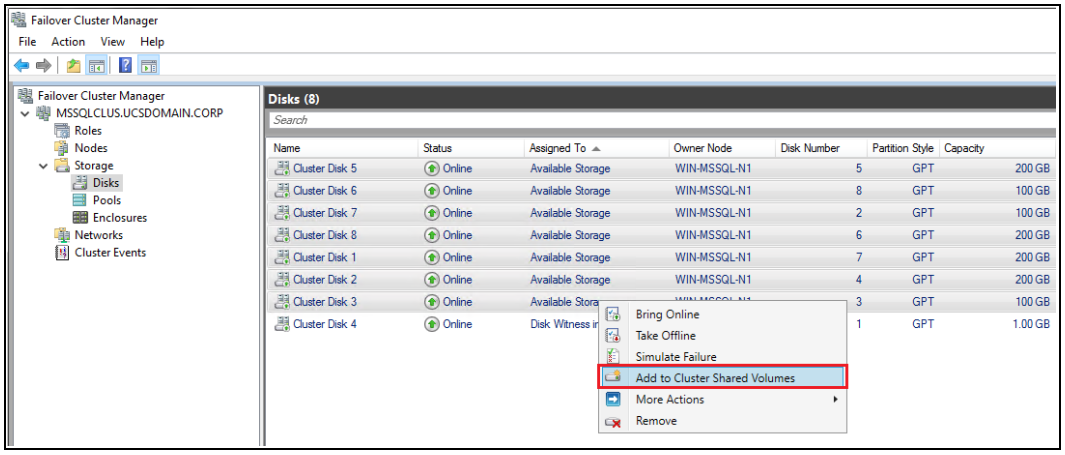


Figure 8-28 Add disks to CSV

All these shared volumes are mounted by Windows as NTFS mount points inside `C:\ClusterStorage` on both nodes. These mount points are given default junction points as `C:\ClusterStorage\Volume`*nn* by Windows, and it is highly recommended that you rename these mount points to match the V5030 volume names.

17. Rename the mount points online using the **`REN`** command on the command prompt (Figure 8-29) or by using the Windows Explorer Rename option. You only need to rename the mount points on one Hyper-V cluster host.

```
C:\ClusterStorage>dir
 Volume in drive C has no label.
 Volume Serial Number is 5A69-FAA0

 Directory of C:\ClusterStorage

09/19/2017  05:51 AM    <DIR>          .
09/19/2017  05:51 AM    <DIR>          ..
09/19/2017  05:21 AM    <JUNCTION>     Volume3 [\??\Volume{839699f1-f684-4396-8bf5-96dd7d6973a7}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume4 [\??\Volume{0b9c7ef1-708a-46a4-96cc-704371c810e0}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume5 [\??\Volume{ca1f7f04-d0b2-41a7-870b-92f4cc1ae3cd}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume6 [\??\Volume{a5d5fb18-9c86-47e9-9f72-6fac24e4aacd}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume7 [\??\Volume{5bca7221-d3d1-479a-8f65-6a4cb94831f0}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume8 [\??\Volume{83a9fea3-dc76-4ae8-be7b-845db639b045}\]
09/19/2017  05:21 AM    <JUNCTION>     Volume9 [\??\Volume{230c918d-5079-4e31-b31b-a77150360116}\]
               0 File(s)              0 bytes
               9 Dir(s)  91,690,311,680 bytes free

C:\ClusterStorage>ren Volume3 HyperV-MSSQL-System

C:\ClusterStorage>ren Volume4 HyperV-MSSQL-TempDB

C:\ClusterStorage>ren Volume5 HyperV-MSSQL-UserData-0

C:\ClusterStorage>ren Volume6 HyperV-MSSQL-UserData-1

C:\ClusterStorage>ren Volume7 HyperV-MSSQL-UserData-2

C:\ClusterStorage>ren Volume8 HyperV-MSSQL-UserData-3

C:\ClusterStorage>ren Volume9 HyperV-MSSQL-UserLog
```

Figure 8-29 Using the REN command to rename the mount points

8.7 Installing a Microsoft SQL Server failover cluster

This section provides instructions about how to install the Microsoft SQL Server 2016 failover cluster instance. Before carrying out the installation of SQL Server FCI, gather the required information, such as the SQL Server cluster name and cluster IP address. To start the installation of SQL Server FCI, complete the following steps:

1. Install Microsoft SQL Server FCI on the first node.
2. Add the second node to the SQL Server FCI.

8.7.1 Installing the Microsoft SQL Server on the first SQL VM

Complete the following steps:

1. See 7.13, “Hardware profiles” on page 155 and attach Microsoft SQL Server installation ISO to DVD drive on first SQL VM.
2. Log in to the VM by using the appropriate domain credentials, and browse to the DVD drive to start the SQL Server installation wizard.

3. In the Installation window, click **New SQL Server failover cluster installation**, as shown in Figure 8-30.

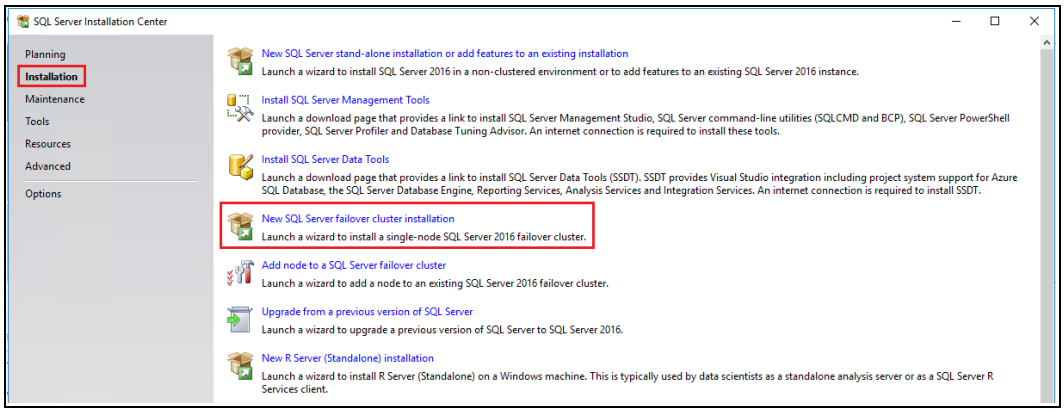


Figure 8-30 Start a new SQL server failover cluster installation

4. In the Product Key window, enter the product key and click **Next**. For this example, we used the Evaluation edition.
5. In the License Terms window, read and accept the license terms to install the Microsoft SQL Server installation, and click **Next**.
6. If the Microsoft Update option in Control Panel\All Control Panel Items\Windows Update\Change settings is not selected, the Microsoft Update window opens next. Selecting the Microsoft Update page changes the computer settings to include the latest updates when you scan for a Windows Update.
7. The Install Failover Cluster Rules window runs the rules that are essential for a successful Microsoft SQL Server cluster creation. Confirm that this step displays no errors and verify the warnings. Click **Next**.
8. In the Feature Selection window, choose the Database Engine services, and click **Next**, as shown in Figure 8-31.

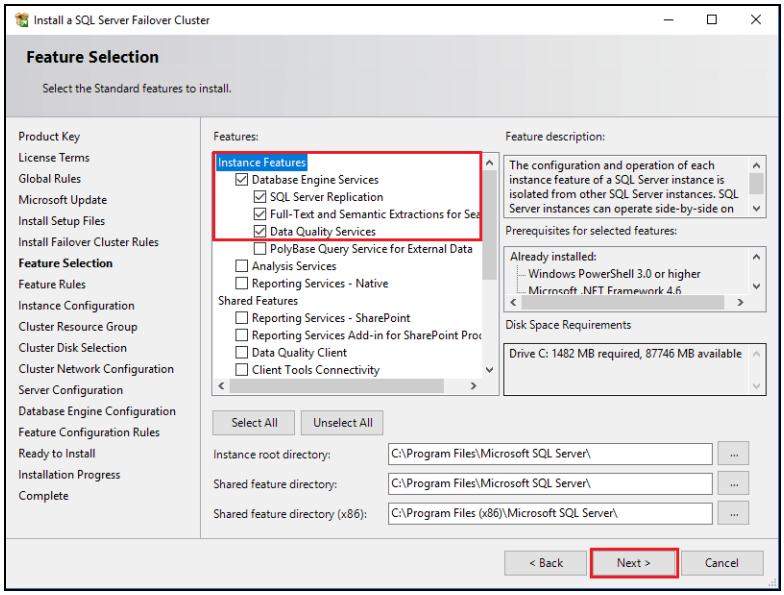


Figure 8-31 Select Microsoft SQL features to be installed

9. In the Instance Configuration window, specify the SQL Server Network Name and the Instance ID and click **Next**, as shown in Figure 8-32.

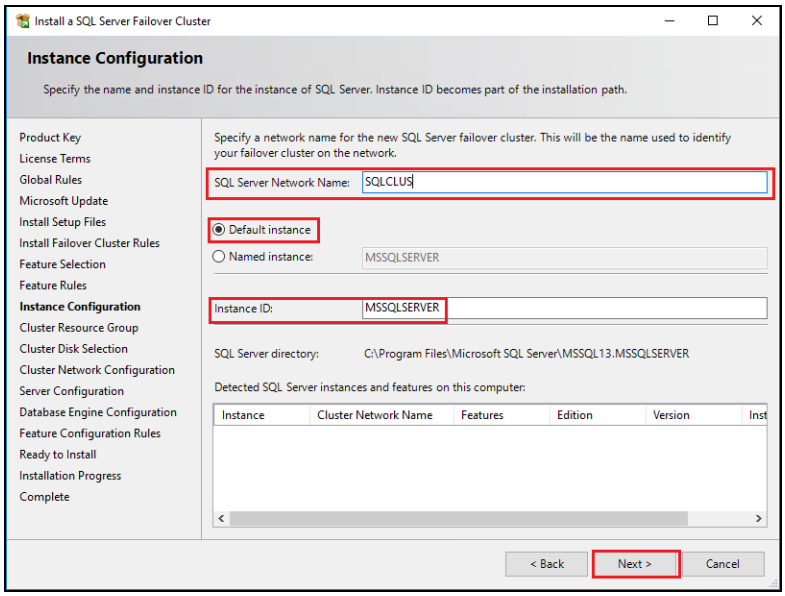


Figure 8-32 Instance configuration

10. In the Cluster Resource Group window, select the SQL Server cluster resource group name from the list or create a resource group and click **Next**, as shown in Figure 8-33.

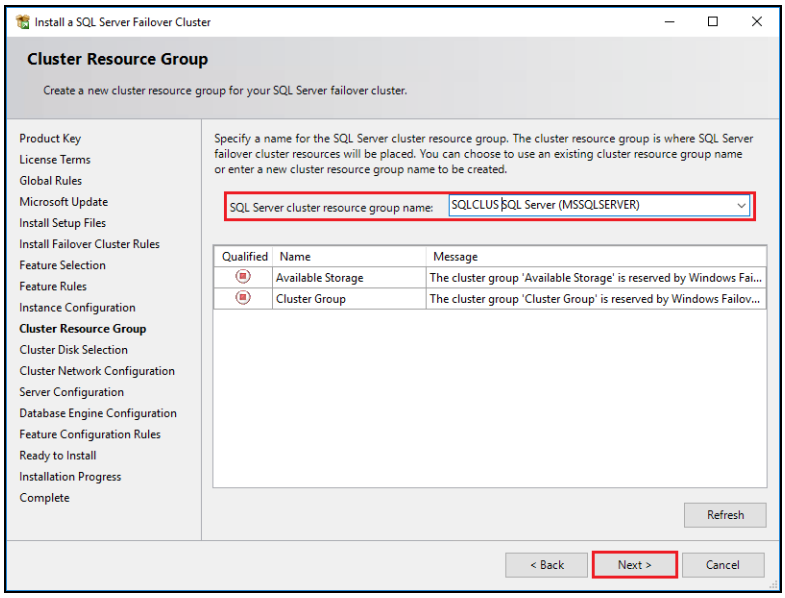


Figure 8-33 Create cluster resource group

11. In the Cluster Disk Selection window, select the shared cluster disks from the list, as shown in Figure 8-34. These disks were added to be part of the Guest cluster. Click **Next**.

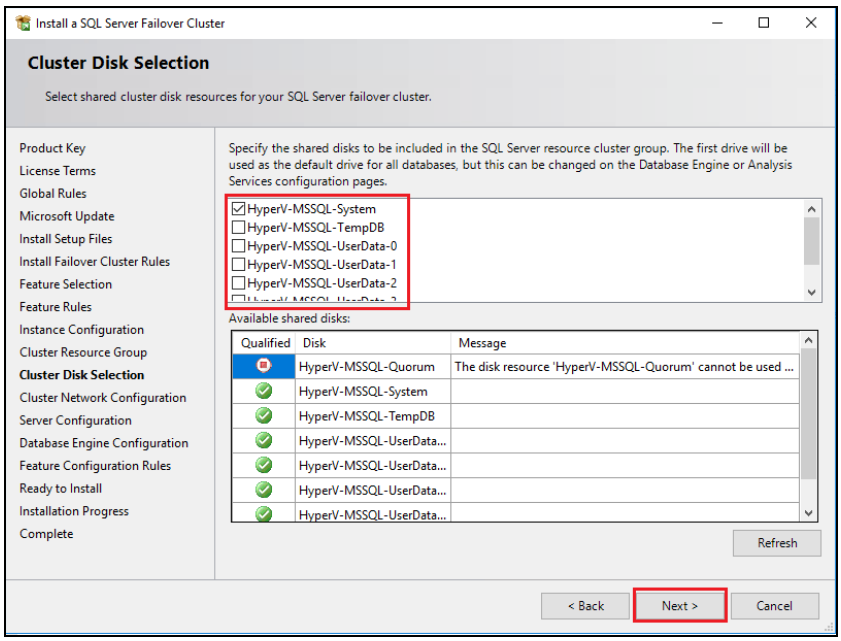


Figure 8-34 Select cluster disk resources

12. In the Cluster Network Configuration window, provide the cluster IP address that will be used by SQL Server for public connectivity. The SQL server daemon listens for connections on this IP address. Click **Next** to continue when complete, as shown in Figure 8-35.

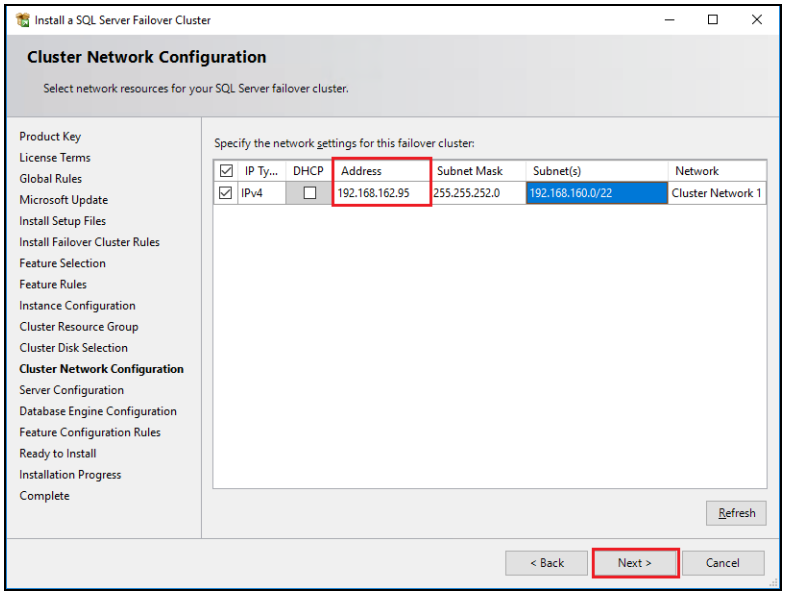


Figure 8-35 Provide cluster IP address for SQL Server

13. In the Server Configuration window, specify the service accounts and collation configuration details and click **Next**, as shown in Figure 8-36.

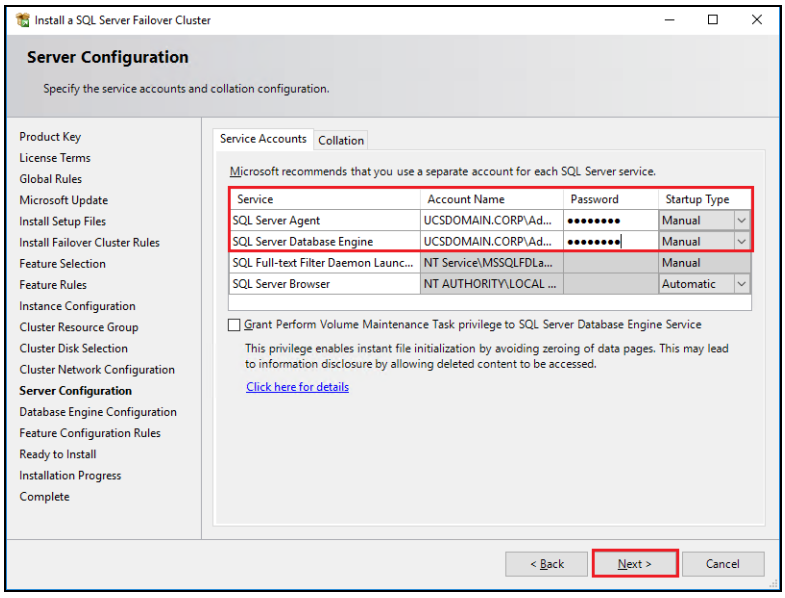


Figure 8-36 Server Configuration

14. In the Database Engine Configuration window, specify the database engine authentication mode and administrators, as shown in Figure 8-37.

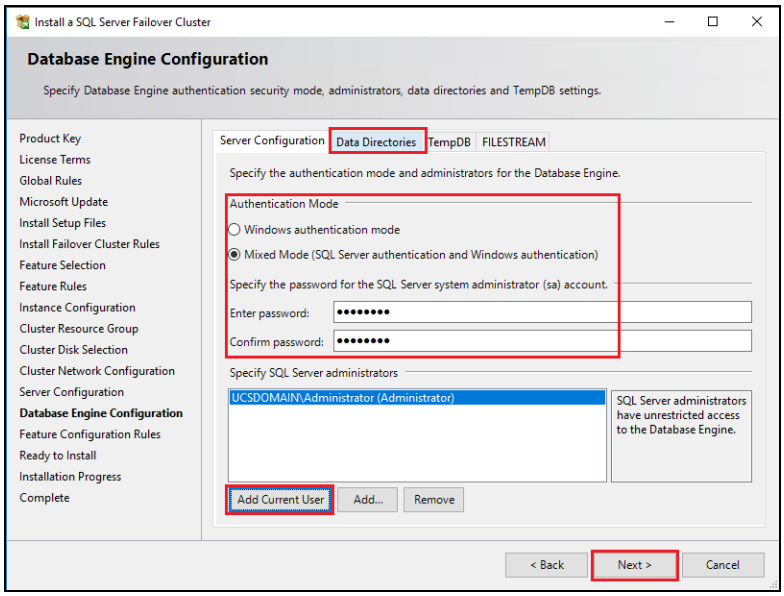


Figure 8-37 Specify the authentication mode and administrators

15. In the Data Directories tab, specify `C:\ClusterStorage\HyperV-MSSQL-System` as the mount point for the system database directory, as shown in Figure 8-38.

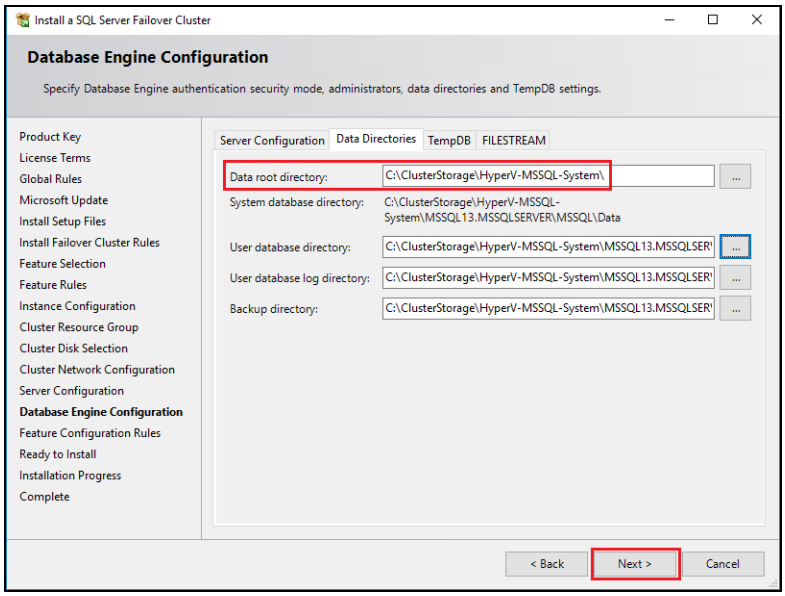


Figure 8-38 Specify the data root directory and the system database directory

16. In the TempDB tab, specify `C:\ClusterStorage\HyperV-MSSQL-TempDB` as the mount point for the TempDB directories, as shown in Figure 8-39. Click **Next** to continue.

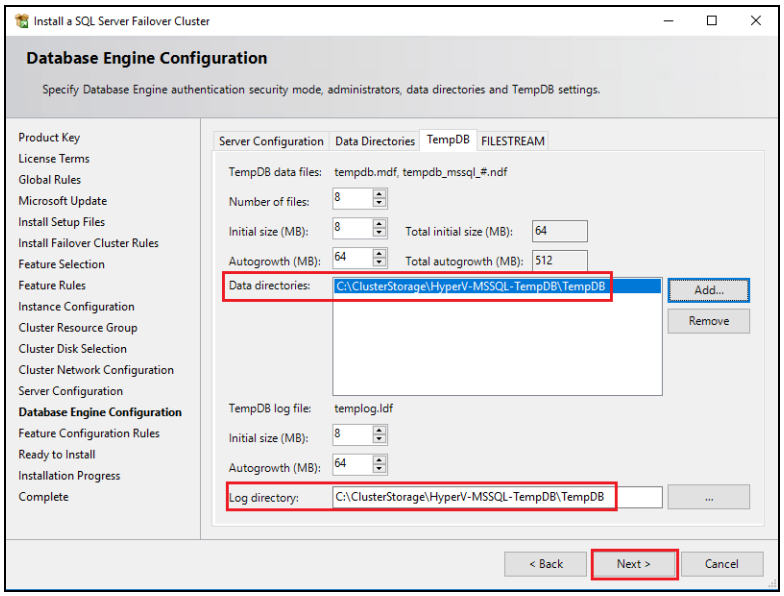


Figure 8-39 Specify TempDB directories

17. The feature runs the configuration rules automatically. Verify the output and click **Next**.

18. In the Ready to Install window, verify the installation options, and click **Install** to start the SQL Server Failover Cluster installation, as shown in Figure 8-40.

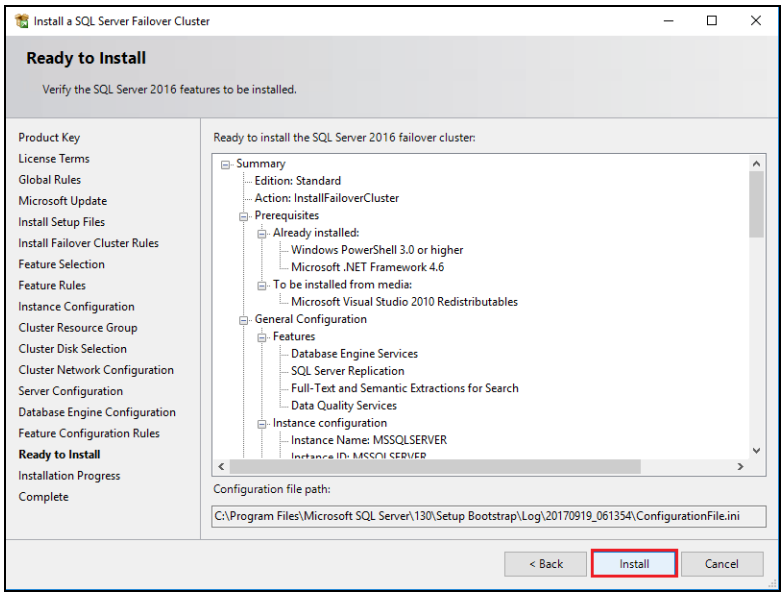


Figure 8-40 Review installation summary

19. After the installation completes, verify the installation summary, and click **Close**, as shown in Figure 8-41.

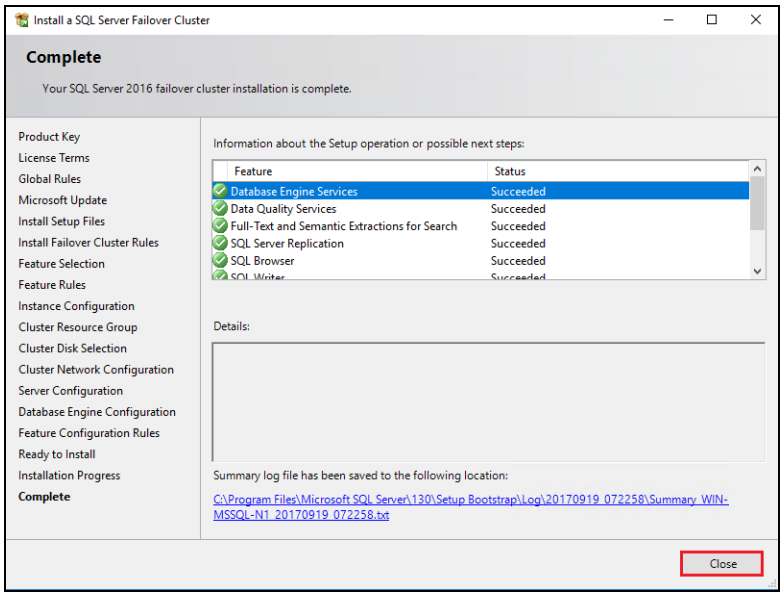


Figure 8-41 Complete installation

8.7.2 Adding a second node to the SQL Server Failover Cluster instance

To add the second VM node to the SQL Server Failover Cluster instance that was created in 8.7.1, “Installing the Microsoft SQL Server on the first SQL VM” on page 189, complete the following steps:

1. Start the SQL Server installation wizard from the mounted SQL Server DVD drive.
2. In the Installation window, click **Add node to a SQL Server Failover Cluster**, as shown in Figure 8-42.

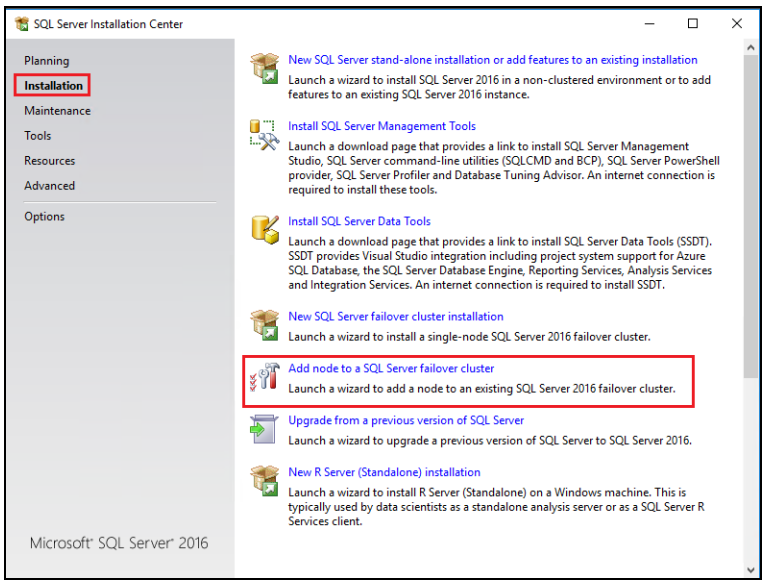


Figure 8-42 Add a node to SQL Server failover cluster

3. In the Product Key window, enter the product key details, and click **Next**.
4. In the License Terms window, read and accept the license terms to install the SQL Server installation, and click **Next**.
5. If the Microsoft Update option in Control Panel\All Control Panel Items\Windows Update\Change settings is not selected, the Microsoft Update window opens next. Selecting the Microsoft Update page changes the computer settings to include the latest updates when you scan for a Windows Update.
6. The Install Failover Cluster Rules window runs the rules that are essential for a successful SQL Server cluster creation. Confirm that this step displays no errors, and verify the warnings. Click **Next**.
7. The Add Node Rules window runs the rules that are essential for adding the node to the SQL Server cluster. Confirm that this step shows no errors, and verify the warnings. Click **Next**.

   If there is a failure, you must correct the error before running the setup.

8. In the Cluster Node Configuration window, verify the existing SQL Server Failover Cluster details, and click **Next**, as shown in Figure 8-43.

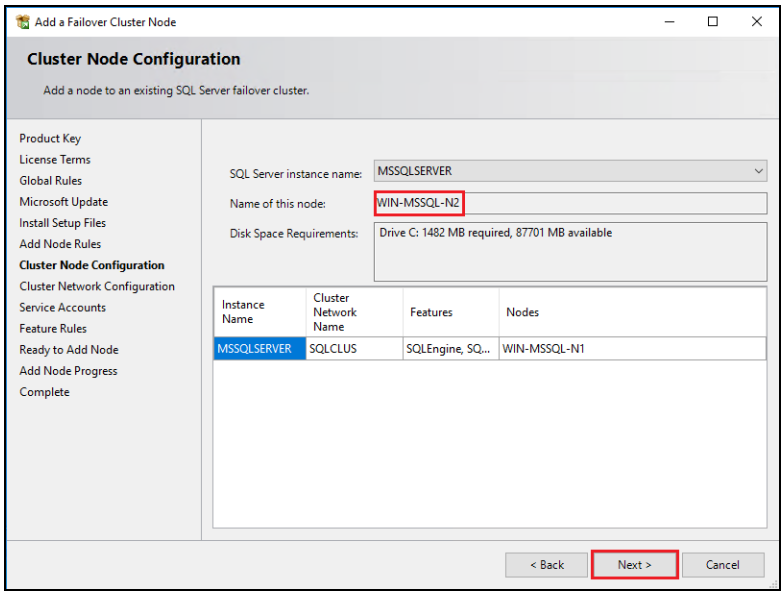


Figure 8-43 Verify the node configuration

9. In the Cluster Network Configuration window, select the public connectivity network settings for the failover cluster, as shown in Figure 8-44. The shared network address is taken from configuration of first node. Verify and click **Next**.

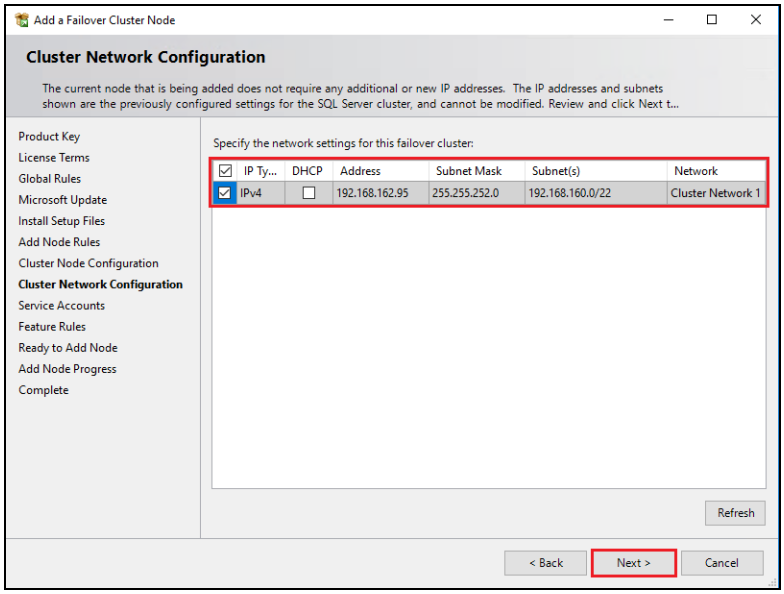


Figure 8-44 Cluster network selection for the second node

10. In the Service Accounts window, specify the passwords for the service accounts that are configured for the first node of the cluster, and click **Next**.
11. The Feature Rule window shows the rule executions and automatically advances if all the rules pass.
12. In the Ready to Add Node window, verify the summary of the settings, and click **Install**, as shown in Figure 8-45.

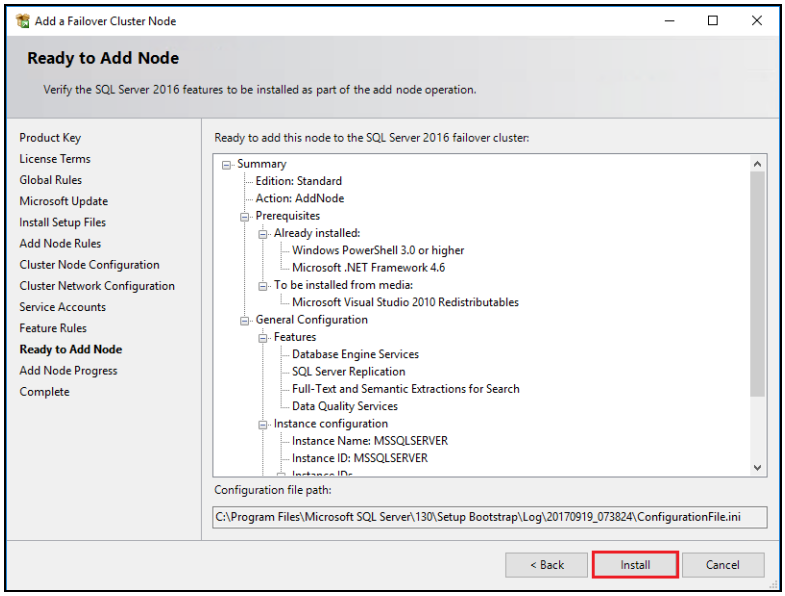


Figure 8-45 Ready to add the node

13. After the installation is complete, verify the installation summary, and click **Close**, as shown in Figure 8-46.

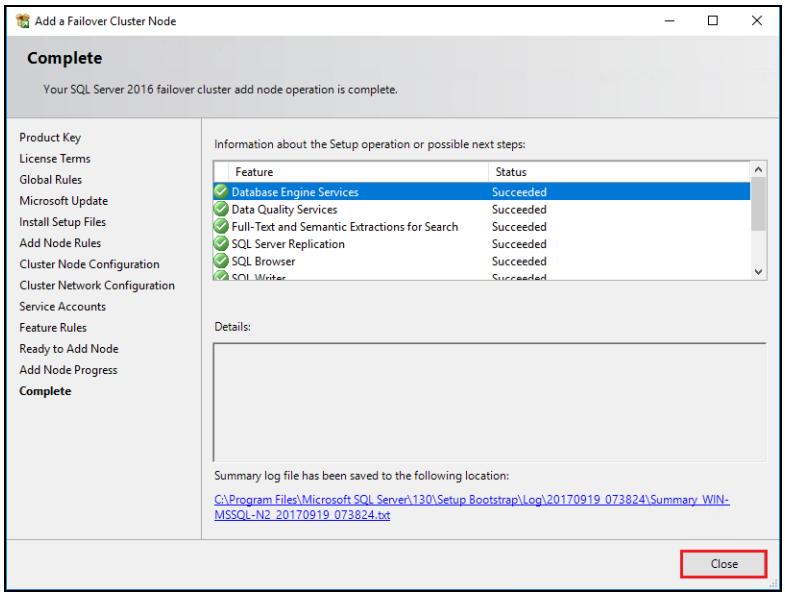


Figure 8-46 Installation on the second node complete

The setup is now complete.

8.7.3 Installing SQL Server Management Studio

SQL Server Management Studio (SSMS) is graphical client that is provided by Microsoft to manage SQL Server instance and associated databases. You need to download SSMS separately for SQL Server 2016.

The most current download link for SSMS is provided in the SQL Server Installation Center main window, as indicated in Figure 8-47.

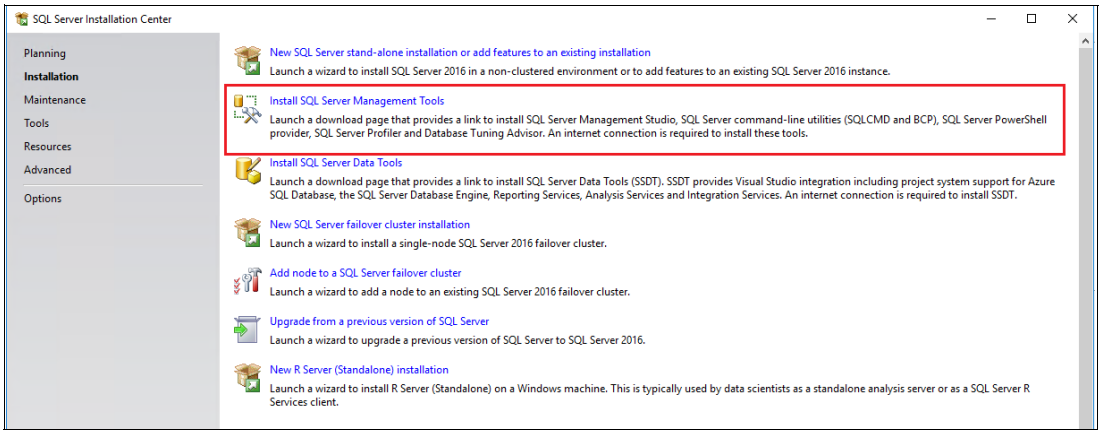


Figure 8-47 Download link for SSMS

You need Internet access to download the installation binaries, or you can download them on a different machine. Run the installation, and then follow the prompts to install Microsoft SQL Server Management Studio, as shown in Figure 8-48.

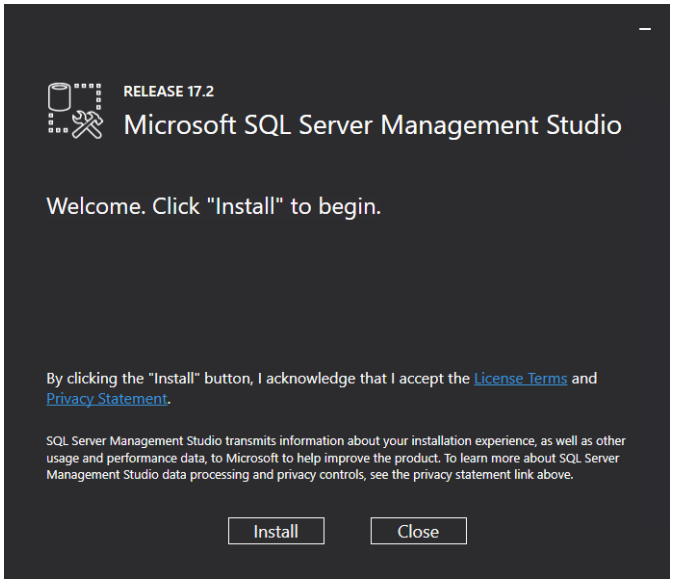


Figure 8-48 Install Microsoft SQL Server Management Studio

8.7.4 Connecting to SQL Server using SSMS

You launch SSMS from the Windows Start Menu by clicking the newly added icon, as indicated in Figure 8-49.

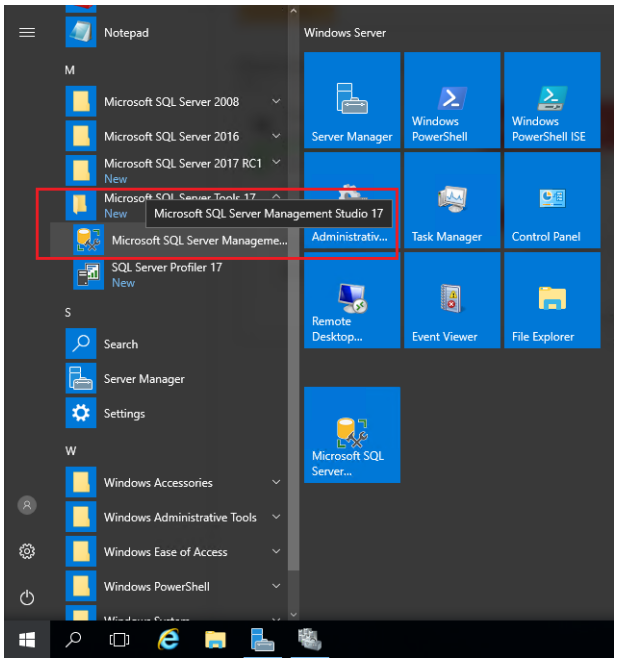


Figure 8-49 Launching SQL Server Management Studio

At the login prompt, provide the SQL Server network name or cluster IP and login credentials to log in, as shown in Figure 8-50. This network name and IP was provided during installation as described in 8.7.1, “Installing the Microsoft SQL Server on the first SQL VM” on page 189.

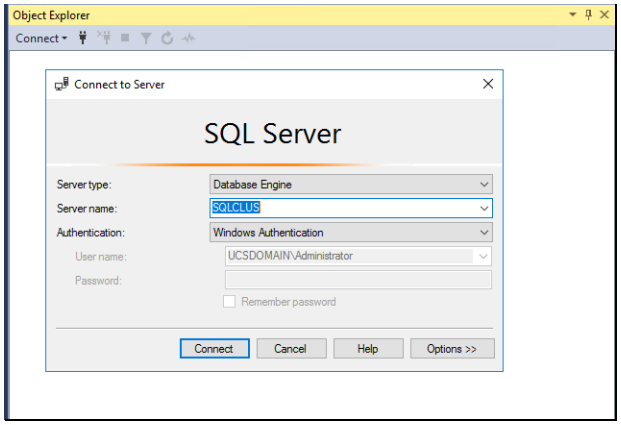


Figure 8-50 Connect to SQL Server using SSMS

8.8 Creating a sample database

After you connect to SQL Server using SSMS, you can create a new sample database by using the following steps:

1. Confirm that the SQL Server instance is operational. If the instance is operational, the root object in the explorer tree has a green arrow next to it.
2. Expand the root object, right-click **Databases** and then select **New Database**.
3. In the New Database window, use the **Add** button to create one file on each data mount point. This example allocates four different V5030 volumes for storing data (for example, `C:\ClusterStorage\UserData-0...3`). SQL Server spreads I/O on all the data files to provide better performance.

   Provide a separate mount point for storing transaction log files for the corresponding database. This example assigns the `C:\ClusterStorage\UserLog` mount point that is on SSD MDisks on the V5030.

   Specify Autogrowth as *None* and specify an Initial Size of a data file size to match all the available capacity on the underlying mount point.

After you enter the details, click **OK** to continue, as shown in Figure 8-51.

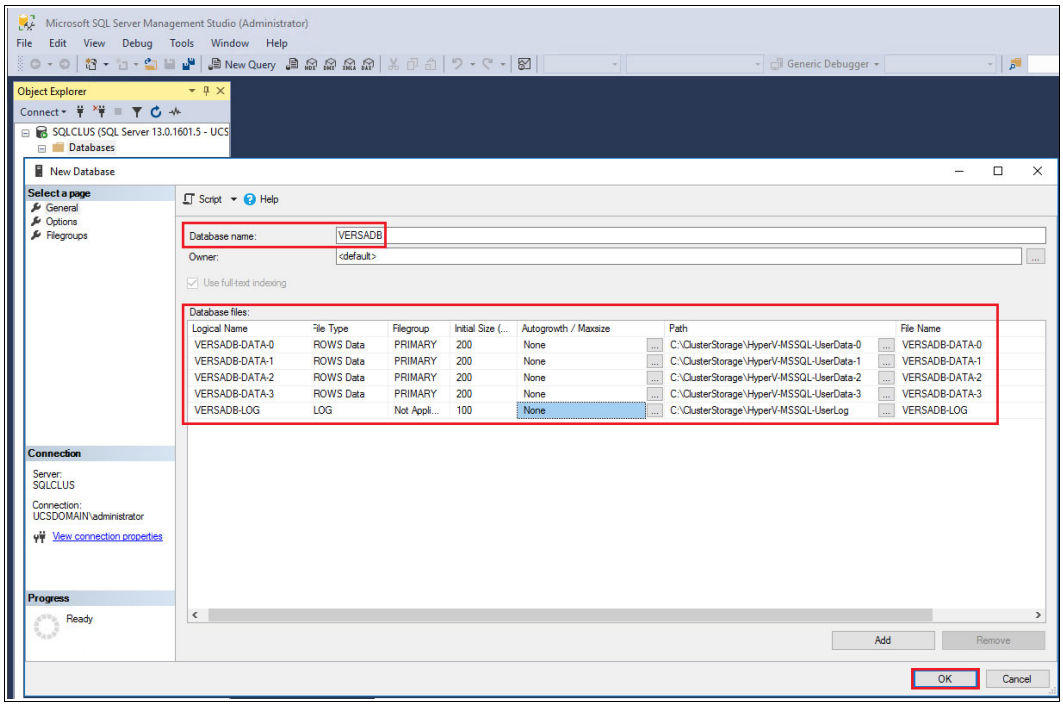


Figure 8-51 Specify the data and log files for the new database

8.9 Configure Hyper-V level redundancy for SQL VMs

A Hyper-V solution that is paired with two Cisco UCS chassis supports additional features to minimize any single point of failure (SPOF) on the hosted VMs. Using the feature, you can run each VM in a separate chassis during normal operation by setting the following properties for VMs:

- *Possible Owner* is a list of Hyper-V cluster hosts that can host each VM. Each available Hyper-V cluster host can be selected or de-selected to host the VM by using the check boxes.
- *Preferred Owner* is a list of Hyper-V cluster hosts out of possible owners that can host each VM. Multiple owners can be specified and also their preference order can be specified.

8.9.1 Setting Preferred Owner and Possible Owner for VMs

You can use these properties to distribute both SQL VMs over two different chassis in a Cisco UCS Mini system as follows:

1. Log on to the VMM, and navigate to **VMs and Services**. Then, select the first SQL VM.
2. Right-click the VM and select **Properties**.

3. In the **Settings** options, clear the second Hyper-V cluster host from the list of **Preferred Owners**, and click OK to complete the change as shown in Figure 8-52.

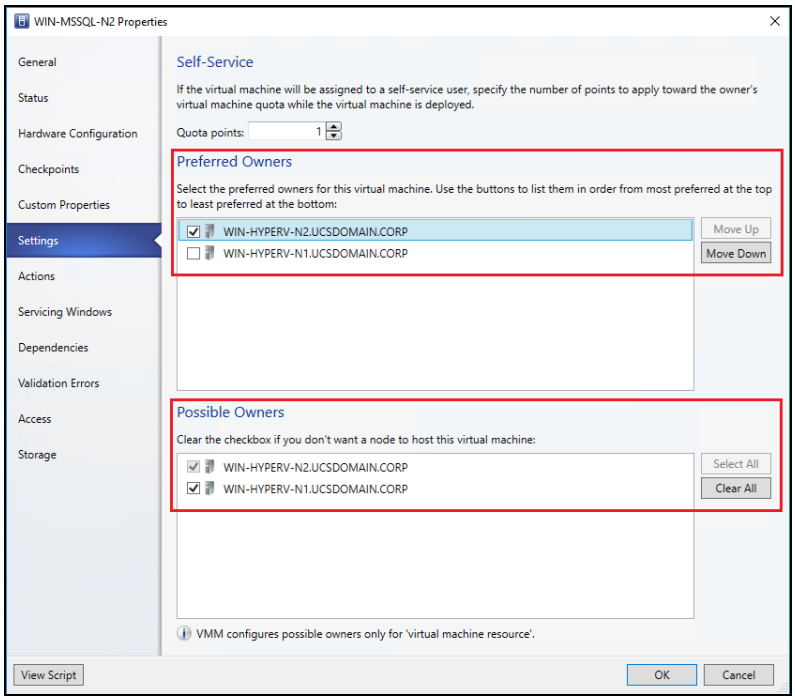


Figure 8-52 Setting the Preferred Owners and Possible Owners for a VM

4. Repeat these steps for the second SQL VM, and remove the first Hyper-V cluster host from the list of **Preferred Owners**.

Notes:

In this example, both VMs can still run from single Hyper-V cluster host, if either of the following conditions is true:

- The VM is migrated manually to same Hyper-V cluster host.
- One of the Hyper-V cluster host is not running or is shutdown manually.

You can use the Possible Owners property to restrict VMs within specific chassis or to set up Hyper-V VMs by de-selecting servers outside the chassis. If a Hyper-V cluster host fails, the VM can still be contained within a chassis to achieve chassis-level redundancy.

8.10 Database tuning

Microsoft SQL Server installation provides a fair response to a wide variety of user workloads by default. However, every database instance might need further, specific tuning for optimal performance. Microsoft provides various tools to measure SQL Server performance and to tune it. You can apply these changes at the database level, to database services, or even to the underlying OS.

You need to make any such workload specific performance measurement and tuning changes now. For more information, see the Microsoft SQL Server documentation.

9

The IBM FlashSystem 5030 advanced functions

This chapter describes the following advanced functions that are provided by the IBM FlashSystem 5030:

The chapter takes each of these items, describes the function, and provides an example of how it might benefit the VersaStack solution that is described in this book.

9.1 IBM Easy Tier

The IBM Storwize V5000 includes IBM Easy Tier, a function that responds to the presence of drives in a storage pool that contains a mixed set of flash and hard disk drive (HDD) drive types. The system automatically and nondisruptively moves frequently accessed data from HDD managed disks (MDisks) to flash drive MDisks. This process puts the more frequently accessed data on a faster tier of storage.

9.1.1 IBM Easy Tier overview

IBM Easy Tier automatically moves highly active data to faster responding tiers of storage without manual intervention. The movement of data between tiers is called *automatic data replacement* and is seamless to the application on the host. Manual controls might change the default Easy Tier behavior to write to a specific tier or to pause automatic data replacement.

Easy Tier supports the following disk types:

- Tier 0 flash

  Tier 0 flash is the fastest tier available. Use this tier only for high performance class solid-state drives (SSDs), or externally virtualized flash systems, such as the IBM FlashSystem 900.

- Tier 1 flash

  Tier 1 flash is reserved for the Read Intensive SSDs. This tier is considered to be in between Enterprise and Tier 0 flash. Tier 1 flash drives are lower-cost flash drives, typically with larger capacities but with slightly lower performance and write endurance characteristics. This tier was first introduced in IBM Spectrum Virtualize V7.8. Prior to V7.8 the Read Intensive SSD was treated as enterprise-class drives. If you want to use a Read Intensive SSD in an multi-tier pool, upgrade to V7.8 or higher.

- Enterprise

  The enterprise tier exists when enterprise-class MDisks containing serial-attached SCSI (SAS) drives are in the pool. Both 10,000 RPM and 15,000 RPM drives are considered to be enterprise tier. These two different speeds of drives cannot be mixed in the same pool while being configured as the same tier.

- Nearline

  The nearline tier exists when 7,200 RPM or slower nearline-class SAS MDisks are in the pool.

All MDisks on the V5000 belong to one of the tiers. All externally virtualized MDisks default to enterprise class unless manually changed by the administrator. Mixing tiers of storage in a single pool enables Easy Tier automatically and operates as shown in Figure 9-1.

Tier 0	Tier 1	Tier 2
Three tier Pools:		
SSD	Enterprise	Nearline
Two Tier Pools:		
SSD	Enterprise	
SSD	Nearline	
	Enterprise	Nearline
Single Tier Pools:		
SSD		
	Enterprise	
		Nearline

Figure 9-1 Easy Tier configurations

If a pool contains only one type of disk, Easy Tier automatically goes into *balanced mode*. In this mode, individual disks that are being accessed frequently are known as *hot* disks. Easy Tier redistributes extents from these hot disks across other disks in the same pool to balance the workload across all the disks in the pool.

9.1.2 Easy Tier limitations and requirements

Easy Tier supports the following storage configurations:

- Internal flash drives in a storage pool with internal hard disk drives (HDDs)
- Internal flash drives in a storage pool with external HDDs
- External flash drives in a storage pool with internal SAS HDDs
- External flash drives in a storage pool with external HDDs
- External flash drives and HDDs in a storage pool

All MDisks in a pool tier must have the same speed and size to ensure optimal performance from Easy Tier.

Automatic data placement is not supported on image mode or sequential volumes, such as volume copies. You need to convert these volumes to striped volumes to enable automatic data placement.

Mirrored volumes do support automatic data placement on each copy of the volume, and Easy Tier works independently on each volume. Thus, automatic data placement could be disabled on one copy but not the other.

If a volume is migrated out of a pool that Easy Tier is managing, data placement is disabled on that volume. Data placement turned off when a volume is being migrated between pools. It will be turned back on after the volume migration is complete, if the new pool has automatic data placement enabled.

For a complete list of limitations and requirements, visit IBM Knowledge Center.

9.2 IBM HyperSwap

The IBM HyperSwap® high availability (HA) function in the IBM Storwize V5000 allows business continuity in a hardware failure, power failure, connectivity failure, or disasters, such as fire or flooding. It is available on the IBM SAN Volume Controller, IBM Storwize V5000, IBM Storwize V7000 Unified (only for the Block Data protocol), and IBM Storwize V7000 products.

HyperSwap provides highly-available volumes that are accessible through two sites at up to 300 km (186.4 miles) apart. A fully-independent copy of the data is maintained at each site. When data is written by hosts at either site, both copies are synchronously updated before the write operation completes. (Round trip time should not exceed 80 ms.) The HyperSwap function automatically optimizes itself to minimize the data that is transmitted between sites and to minimize host read and write latency. If the nodes or storage at either site go offline, leaving an online and accessible up-to-date copy, the HyperSwap function automatically fails over access to the online copy. The HyperSwap function also automatically resynchronizes the two copies when possible.

The HyperSwap function builds on the following existing technologies in the product:

- The Nondisruptive Volume Move (NDVM) function that was introduced in V6.4 of the SAN Volume Controller software
- Remote Copy features that include Metro Mirror and Global Mirror with Change Volumes

Figure 9-2 depicts a high-level design for a V5030 HyperSwap configuration.

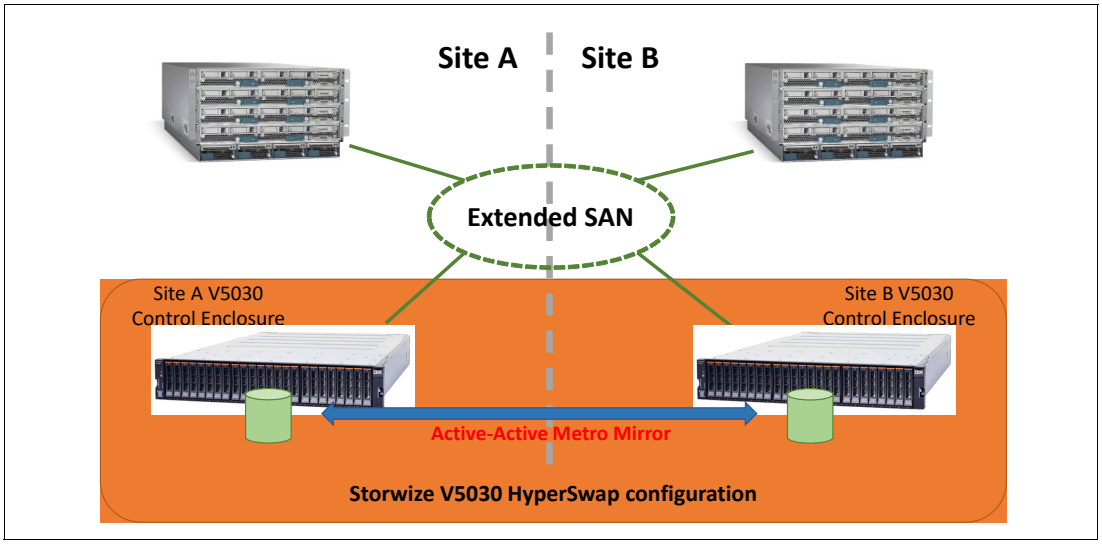


Figure 9-2 High-level overview of V5030 HyperSwap configuration

You can file more details about implementing HyperSwap in *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

9.3 Remote copy

The V5030 has several options for replicating data to another IBM Storwize or SAN Volume Controller system. The Copy Services functions can be used as part of a disaster recovery (DR) strategy or to migrate data from an existing IBM Storwize array to a replacement IBM Storwize array. This section discusses the following Copy Services functions:

- Global Mirror (GM)
- Metro Mirror (MM)
- Global Mirror with Change Volumes (GMCV)

Global Mirror, Metro Mirror, and Global Mirror with Change Volumes all require a partnership between a minimum of two and a maximum of four IBM Storwize arrays. There are several possible arrangements for the partnership, up to and including a full-mesh with all four IBM Storwize systems in a relationship with the other three. Details about the possible supported configurations of the partnerships are available in IBM Knowledge Center.

The relationship between the systems can be two-way. That is, both sites can have a mix of primary and secondary volumes. Figure 9-3 illustrates this concept.

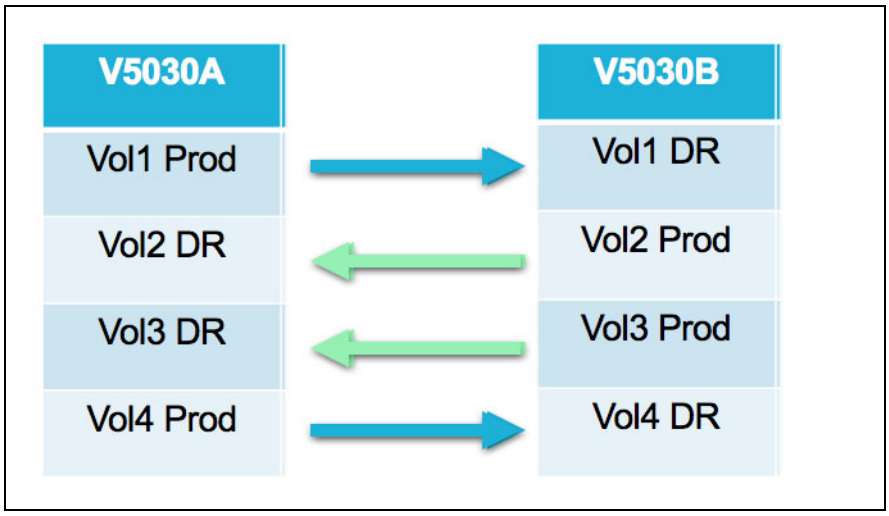


Figure 9-3 A mix of primary and secondary volumes

There is a mix of volumes on V5030A and V5030B. The direction of the arrows indicates the direction that the data is being replicated. As shown, Vol1 has its production volume on V5030A and its DR volume on V5030B. Conversely, Vol2's production volume is on V5030B and its DR volume is on V5030A.

Each volume's replication direction is governed by selecting which volume on which system will be the master and which will be the auxiliary. The master volume is always the source of the relationship. The IBM Storwize copies data from the master to the auxiliary volume until the data in the auxiliary volume is synchronized with the master. After the data is synchronized, further changes to the master volume are replicated to the auxiliary. The replication method depends on the type of remote copy selected.

The following types of relationships can be used for remote copy. Each type has its own methodology and impact on the overall system:

- Metro Mirror

  Metro Mirror (MM) provides *synchronous* writes to the primary and secondary volumes. Thus, the IBM Storwize system does not confirm write success back to the host until the write is completed on both the master and auxiliary volumes. The maximum supported distance for Metro Mirror is 180 miles (300 km). However, systems separated by long distance and using Metro Mirror will add latency to the write commands that can cause performance problems on the host.

- Global Mirror

  Global Mirror (GM) provides *asynchronous* writes to the primary and secondary volumes. Thus, the IBM Storwize system provides write status back to the host after the write is completed on the primary volume. The write is then mirrored to the secondary volume. It is possible for the secondary volume to get out of synch with the primary, but using Global Mirror instead of Metro Mirror protects the host from latency on the link between the IBM Storwize systems.

- Global Mirror With Change Volumes

  Global Mirror with Change Volumes (GMCV) is Global Mirror with a cycling mode enabled. It is intended for use in situations where there is low bandwidth between the locations where the IBM Storwize systems are located. As with Global Mirror, changes are written to the primary volume, and write success is returned to the host. However, the IBM Storwize does not immediately mirror the changes to the secondary volume. Instead, data is sent to the master change volume using a periodic FlashCopy, which then replicates changes to the auxiliary change volume. When both change volumes are synchronized, the data is committed from the auxiliary change volume to the auxiliary volume.

For more information about configuring remote copy partnerships and relationships, see *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

9.4 IBM FlashCopy

The IBM FlashCopy function creates a point-in-time copy of a source volume to a target volume, as shown in Figure 9-4.

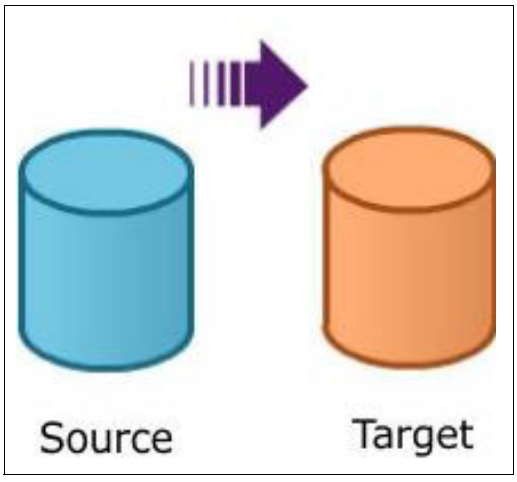


Figure 9-4 FlashCopy flow

FlashCopy creates copies of content from a source volume to a target volume. Any data that existed on the target volume is lost and is replaced by the copied data. After the copy operation completes, the target volumes contain the contents of the source volumes as they existed at a single point in time. After the copy completes, the target volume is not updated unless another FlashCopy operation is run, Although the copy operation takes some time to complete, the resulting data on the target volume is available instantly.

FlashCopy is commonly used to create copies of dynamic data for test purposes and to create copies of data for data mining or audits. FlashCopy is also used to create copies of volumes so that the target volume can then be backed up to tape without interrupting applications.

It can be difficult to make a consistent copy of a data set that is constantly updated. The techniques used by FlashCopy help solve this problem. If a copy of a data set is created using a technology that does not provide point-in-time techniques (such as tape backup) and if the data set changes during the copy operation, the backup might contain data that is not consistent. For example, if a reference to an object is copied earlier than the object itself and the object is moved before it is copied, the copy contains the referenced object at its new location, but the copied reference still points to the previous location. Having the backup run using a FlashCopy volume as the source eliminates this problem.

For more information about FlashCopy, *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

9.5 Encryption

Encryption protects against the revealing of sensitive information contained on lost or stolen storage devices. The IBM FlashSystem 5030 supports encryption of data at rest, as shown in Figure 9-5.

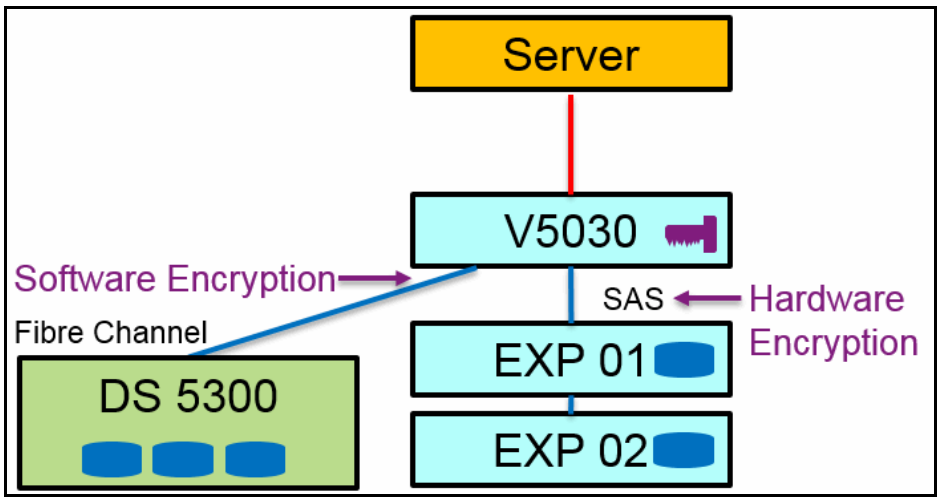


Figure 9-5 Encryption

Support note: Software encryption on external attached Storage systems is also supported.

To use this feature an encryption license is required for each enclosure. For more information about configuring encryption, see *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

9.6 Volume mirroring

Volume mirroring allows a volume to have two physical copies within the same IBM Storwize clustered storage system. This process differs from Metro Mirror and Global Mirror, which are write and replicate models. With mirrored volumes, the system writes changes to both volumes simultaneously. A volume's secondary mirror does not have to be the same type of volume as the original. It can be image, striped, sequential, and either thin-provisioned, compressed, or fully allocated. It can also be on a different type of backend drive (speed or size) than the primary mirror.

You might employ mirrored volumes for the following reasons:

- Improving availability of volumes by protecting them from a single storage system failure. One copy can be on one storage pool, and the other copy can be on a different pool. In this scenario, if a failure were to occur bringing down a single pool, the volume and its data will still be available in the other pool.
- Providing concurrent maintenance of a storage system that does not natively support concurrent maintenance. Before starting maintenance on a storage system that requires it to be taken out of service, you can mirror the existing volumes to other storage pools or then perform the maintenance and bring the storage system back into service.
- Providing an alternative method of data migration with better availability characteristics than using the data migration feature. When using the data migration feature, it is vulnerable to failures on both the source and target storage pool. Mirroring provides an alternative because you can start with a non-mirrored volume in the source storage pool and then add a copy to that volume in the destination storage pool. When the volume is synchronized, delete the original copy that is in the source storage pool. During the synchronization process, the volume remains available even if there is a problem with the destination storage pool.
- Converting between fully allocated volumes and thin-provisioned volumes.
- Mirroring between flash or SSD drives and HDDs. Setting the flash as the primary volume induces reads to be performed at the faster tier, while keeping a mirrored copy of written data on both tiers.

9.7 Thin provisioning

Volumes can be created as thin-provisioned where no physical storage is allocated to the volume until it is written to. Volumes have a *real capacity*, a *virtual capacity*, and a *used capacity*:

- Real capacity is the capacity that is physically allocated in the system.
- Virtual capacity is the capacity that is presented to the host.
- Used capacity is the space written to the volume by the host plus thin provisioning metadata.

When a thin-provisioned volume is created, the used capacity typically is near zero, the virtual capacity is the full size of the volume shown to the host, and the real capacity is pre-allocated to be 2% of the virtual capacity.

You can find more information about thin-provisioned volumes in IBM Knowledge Center.

9.8 IBM Real Time Compression

IBM Real Time Compression software compresses data as it is written in real time to selected volumes. In most cases, compression will further reduce the physical capacity a single volume consumes compared to thin provisioning, as shown in Figure 9-6.

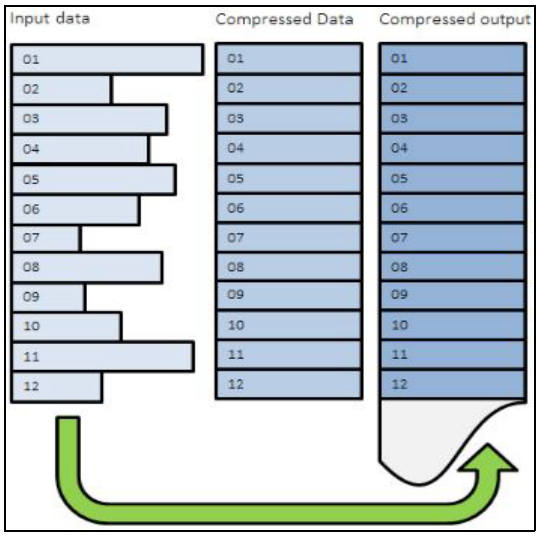


Figure 9-6 Compression operation diagram

IBM Real Time Compression must be licensed for the IBM Storwize array, and volumes must be designated as compressed when created or mirrored (you can mirror from an uncompressed volume to a compressed one, or vice versa). The software is optimized for random workloads. As such, careful planning is needed when compressing sequential workloads as well as for backup operations.

For more information about compression, see *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

9.9 Microsoft offloaded data transfer

Microsoft offloaded data transfer (ODX) is a feature that allows copy operations to take place on compatible storage controllers without going through the host operating system, as shown in Figure 9-7.

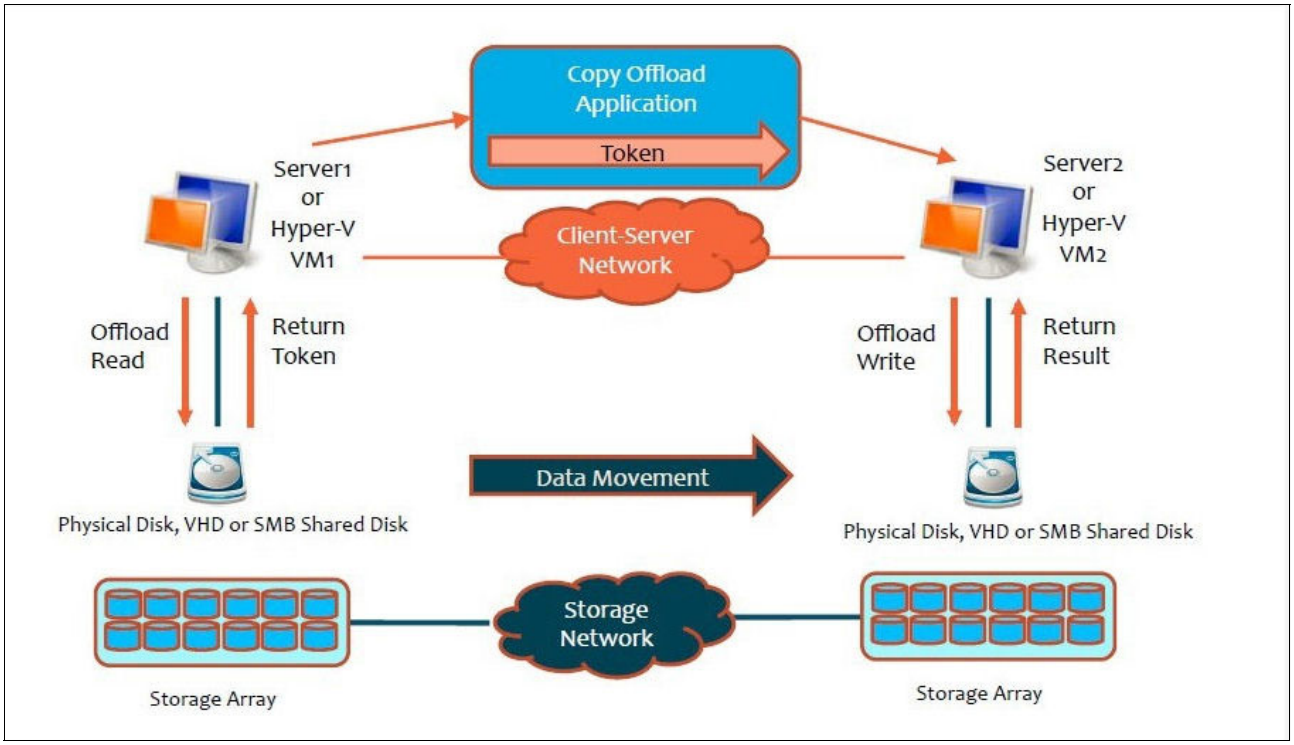


Figure 9-7 ODX operation

This function is helpful for virtual machine (VM) operations and large data transfers. Microsoft ODX offloads the heavy lifting of data movement to the host storage array instead of doing normal read and write operations. Examples of this type of copy operations include:

- VM creation
- VM migration
- VM cloning
- Microsoft Windows Virtual Hard Disk (VHD) creation
- VHD conversion
- VM backup and recovery
- File copy

ODX is most relevant in a Microsoft Hyper-V environment for VM heavy lifting operations. Standard buffered copy is run by reading the data from the storage controller into the host, buffering it, and then writing it to another volume. The ODX function frees up hosts and speeds the copy process by offloading the entire orchestration to a storage array. This offloading is done by using tokenization for read operations and write operations, and it avoids buffering, which can ultimately cut down on processor cycles.

To enable the copy offload function, you must have IBM subsystem device driver device-specific module (SDDDSM) version 2450 or later installed. ODX is disabled by default so that you can install the correct version of SDDDSM. After the correct SDDDSM version is installed, you enable ODX by entering the **`chsystem -odx on`** CLI command on the host.

10

Managing the VersaStack solution

This chapter describes the following methods to manage the VersaStack solution that is described in this book:

- 10.1, “Management application integration” on page 216
- 10.2, “The IBM FlashSystem 5030 Manager” on page 219
- 10.3, “The Cisco UCS GUI manager” on page 227
- 10.4, “Microsoft System Center Virtual Machine Manager” on page 231

The chapter describes each of these items and provides examples about how to configure each component of the configuration in this book.

10.1 Management application integration

The management applications for the IBM FlashSystem 5030, the Cisco UCS, and Microsoft Windows and Hyper-V can be integrated under the Microsoft Management Console (MMC) that is part of Windows server. This section gives an overview of the management integration options. You can find more information about the integration options and details about implementation at the links provided in the next section.

10.1.1 Microsoft System Center Virtual Machine Manager

Microsoft System Center Virtual Machine Manager (SCVMM) is a management tool that is a plug-in to the Microsoft Management Console (MMC) on the Windows Domain Controller that is configured for the solution in this book. This section focuses on integrating the V5030 and UCS components into SCVMM.

V5030 integration: The version of SCVMM used in this book is SCVMM 2016. This version does not support integration of V5030 management. Earlier versions of SCVMM do. While integration of the V5030 is possible using the steps described here, it is not supported in SCVMM 2016 at the time of publication of this book. You can find a list of currently supported storage arrays online.

The IBM Storwize products are not supported, because by default SCVMM 2016 does not support the TLS1.1 or TLS1.2 protocols. You can perform the following steps as a workaround for this issue and integrate IBM Storwize Products into SCVMM. The following listing assumes that you are working with the V5030 from this solution, but the procedure is the same for other IBM Storwize products.

Complete these steps to integrate IBM Storwize Products into SCVMM:

1. Open a VMM PowerShell console and issue the following command to enable TLS1.1/TLS1.2:

   Important: *This step is a key step.*

   ```
   [System.Net.ServicePointManager]::SecurityProtocol=[System.Net.SecurityProtocol
   Type]::Tls12,[System.Net.SecurityProtocolType]::Tls11
   ```

2. In VMM PowerShell, use the following commands to define the user credentials for the V5030 user account:

   ```
   $userName="superuser"#user name to manage the storage
   $password="passw0rd"#password to manage the storage
   $pswSecStr=ConvertTo-SecureString -String $password -AsPlainText -Force
   $cred=New-Object pscredential ($userName,$pswSecStr)
   ```

3. In VMM PowerShell, use the following command to create the account in SCVMM used to connect to the V5030:

   ```
   runas=New-SCRunAsAccount -Name svc.superuser -Credential $cred -Description
   "passw0rd"#
   ```

4. In VM PowerShell use the following command to verify that the `$runas` variable is correct and not empty:

   ```
   $runas
   ```

Example 10-1 lists the expected output.

Example 10-1 Output of the $runas command

```
Name                  : svc.superuser
UserName              : superuser
Domain                :
Enabled               : True
IsBuiltIn             : False
GrantedToList         : {}
UserRoleID            : 7570Ocd5-893e-4f68-ada7-50ef4668acc6
UserRole              : Administrator
Owner                 : CSS\Administrator
ObjectType            : RunAsAccount
Accessibility         : Public
IsViewOnly            : False
Description           : passwOrd
AddedTime             : 9/14/2017 5:03:55 PM
ModifiedTime          : 9/14/2017 5:03:55 PM
MostRecentTask        :
ServerConnection      :
Microsoft.SystemCenter.VirtualMachineManager.Remoting.ServerConnection
ID                    : 3a7c72c4-cab2-44fc-88e4-4f03edd95912
MarkedForDeletion     : False
IsFullyCached         : True
MostRecentTaskIfLocal :
```

5. In VMMPowerShell use the following command to create the storage provider:

```
Add-SCStorageProvider -Name V7k71 -RunAsAccount $runas -NetworkDeviceName
https://9.115.246.71 -TCPPort 5989
```

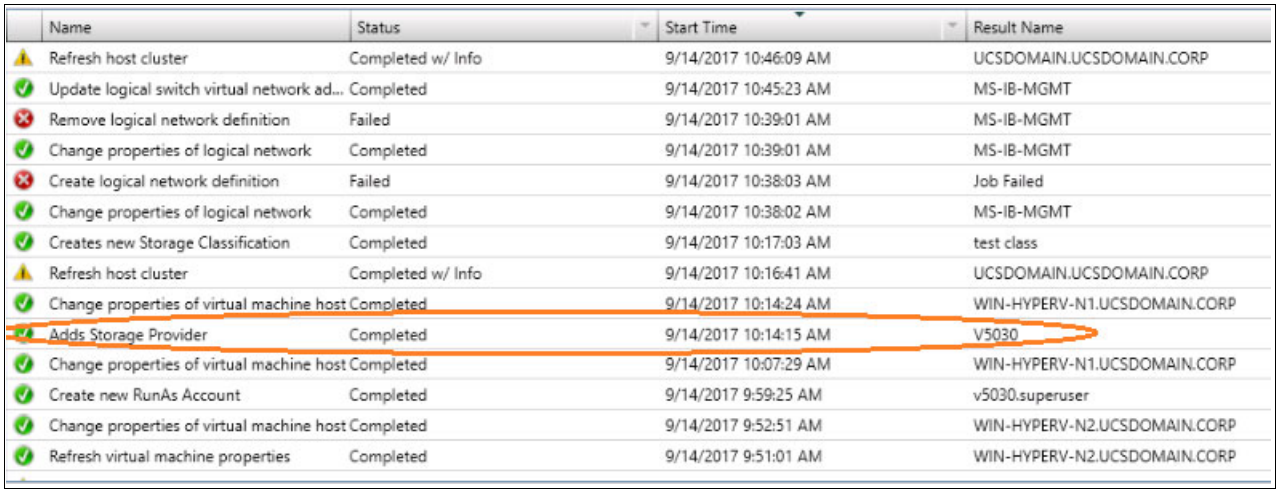
Example 10-2 lists the expected output.

Example 10-2 Expected output

```
NetworkAddress        : https://9.115.246.71
TCPPort               : 5989
ProviderType          : SmisCimXml
ProviderFlags         : StorageArray, StorageFileServer
Status                : Responding
RunAsAccount          : svc.superuser
IsNonTrustedDomain    : False
StorageArrays         : {cim71}
StorageFabrics        : {}
StorageSwitches       : {}
StorageFileServers    : {}
ObjectType            : StorageProvider
Accessibility         : Public
Name                  : V7k71
IsViewOnly            : False
Description           :
AddedTime             : 9/14/2017 5:04:55 PM
ModifiedTime          : 9/14/2017 5:06:24 PM
Enabled               : True
MostRecentTask        : Adds Storage Provider
ServerConnection      :
Microsoft.SystemCenter.VirtualMachineManager.Remoting.ServerConnection
```

```
ID                    : 2c3bf218-6bae-49e6-9ca1-754d7f52d66c
MarkedForDeletion     : False
IsFullyCached         : True
MostRecentTaskIfLocal : Adds Storage Provider
```

6. Open the VMM Management Console.
7. Click **Jobs** → **History**, and then search for a job with the name *Add Storage Provider*. Figure 10-1 depicts a successful integration of the V5030 to SCVMM. If it is not successful, it is marked as failed.



Name	Status	Start Time	Result Name
Refresh host cluster	Completed w/ Info	9/14/2017 10:46:09 AM	UCSDOMAIN.UCSDOMAIN.CORP
Update logical switch virtual network ad...	Completed	9/14/2017 10:45:23 AM	MS-IB-MGMT
Remove logical network definition	Failed	9/14/2017 10:39:01 AM	MS-IB-MGMT
Change properties of logical network	Completed	9/14/2017 10:39:01 AM	MS-IB-MGMT
Create logical network definition	Failed	9/14/2017 10:38:03 AM	Job Failed
Change properties of logical network	Completed	9/14/2017 10:38:02 AM	MS-IB-MGMT
Creates new Storage Classification	Completed	9/14/2017 10:17:03 AM	test class
Refresh host cluster	Completed w/ Info	9/14/2017 10:16:41 AM	UCSDOMAIN.UCSDOMAIN.CORP
Change properties of virtual machine host	Completed	9/14/2017 10:14:24 AM	WIN-HYPERV-N1.UCSDOMAIN.CORP
Adds Storage Provider	Completed	9/14/2017 10:14:15 AM	V5030
Change properties of virtual machine host	Completed	9/14/2017 10:07:29 AM	WIN-HYPERV-N1.UCSDOMAIN.CORP
Create new RunAs Account	Completed	9/14/2017 9:59:25 AM	v5030.superuser
Change properties of virtual machine host	Completed	9/14/2017 9:52:51 AM	WIN-HYPERV-N2.UCSDOMAIN.CORP
Refresh virtual machine properties	Completed	9/14/2017 9:51:01 AM	WIN-HYPERV-N2.UCSDOMAIN.CORP

Figure 10-1 Successful integration of the V5030 to SCVMM

Cisco UCS integration

SCVMM can be used to manage some of the configuration on the Cisco UCS. Cisco has provided a plug-in for integration. You can find the plug-in and documentation online.

The plug-in does not implement all of the functions that are available in the Cisco UCS Manager, but it does allow you to view the equipment that is part of a UCS domain, assign service profiles to blades, view and copy service profiles and templates, and create templates from service profiles. For any functions not implemented in the plug-in, the plug-in provides a link to the UCS GUI manager that can be launched directly from SCVMM.

10.1.2 Microsoft System Center Operations Manager

Microsoft System Center Operations Manager (SCOM) is a component of Microsoft System Center. SCOM provides centralized reporting and alerting capabilities for servers, storage, and other components in the storage area network (SAN). SCOM can also monitor services and applications. You can find more information about Operations Manager Key Concepts at Microsoft TechNet.

This book does not cover SCOM in detail. However, integration with the IBM FlashSystem 5030 and other IBM Storwize products and with the Cisco UCS is available. The latest version of IBM Storage integration information, including IBM Storwize products is available in IBM Knowledge Center.

You can find information about Cisco UCS Integration and the SCOM Management Pack in the Cisco UCS Management Pack Suite Installation and Deployment Guide.

10.2 The IBM FlashSystem 5030 Manager

This section assumes that you have completed the initial configuration of the V5030 described in *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

The V5030 can be managed either through the web-based management GUI or by using CLI. This book does not discuss the CLI in detail. For more information about managing the V5030 by using the CLI, see *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

10.2.1 Accessing the management software

To access the management software open a new tab in your web browser, and in the address bar enter the IP address that was set during the initial setup process. The log in window shown in Figure 10-2 opens.

Figure 10-2 IBM FlashSystem 5030 Manager login window

Enter the user name and password that was set during initial setup. When a successful login is completed, the main page shown in Figure 10-3 on page 220 opens. The following menu options are available from the main page:

- *Monitoring*: Monitor the system, including performance.
- *Pools*: Create and delete storage pools and migrate pools to a new system.
- *Volumes*: Create and delete volumes.
- *Hosts*: Add and remove hosts and configure host mappings.
- *Copy Services*: Configure copy services. For more information about Copy Services options see Chapter 9, “The IBM FlashSystem 5030 advanced functions” on page 205.
- *Access*: Configure users and view the audit log.
- *Settings*: Configure the V5030 System Settings such as date and time, upgrade the system, and collect support data when requested by IBM Storwize Support.

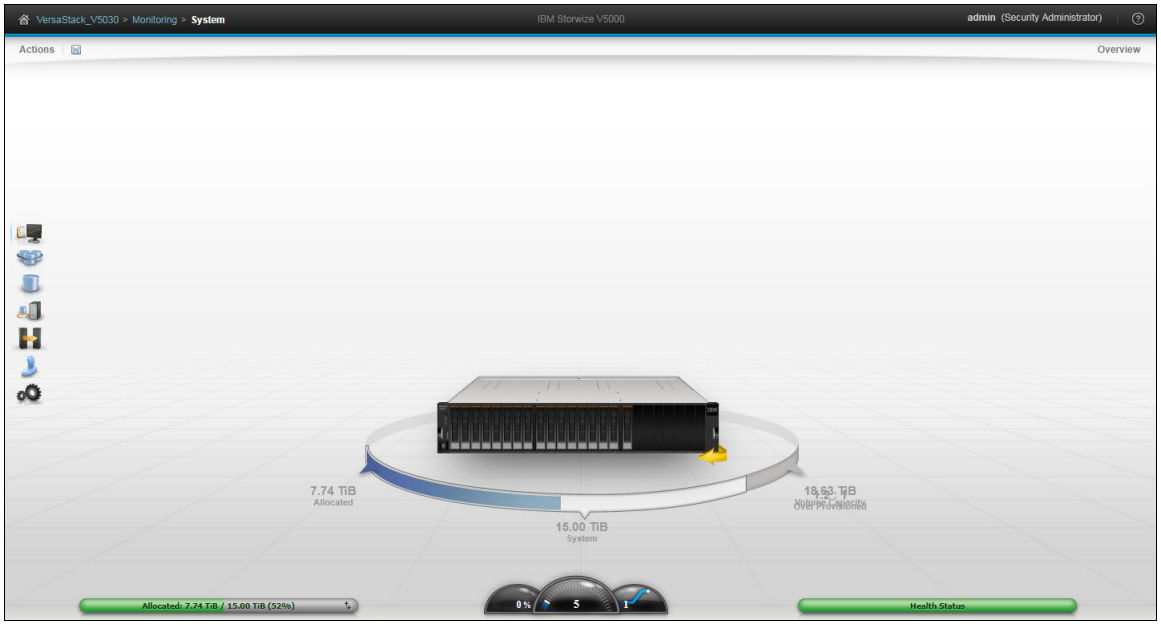


Figure 10-3 Main page

The next sections provide an overview of each menu item in the V5030 Management GUI. For complete details about each menu item, see *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

10.2.2 Monitoring

Hovering over the *Monitoring* menu displays the menu shown in Figure 10-4.

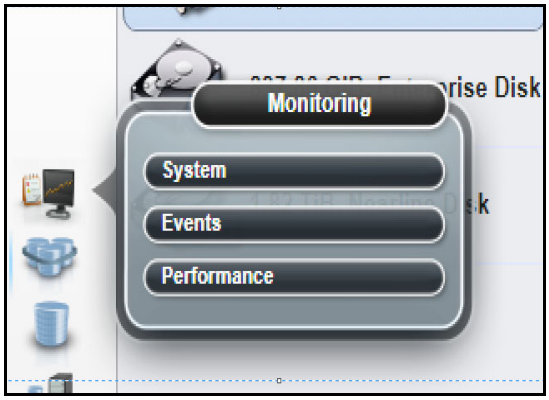


Figure 10-4 Monitoring menu

The Monitoring menu includes the following options:

- The *System* menu displays an overview of the V5030, the main page of the GUI management tool, which includes all components in the rack with the V5030, if any.
- The *Events* menu opens the system event viewer for the storage system. The event viewer is in table format. Events can be sorted and filtered. You can use the event viewer to customize the columns shown in the table, and you can save events to a CSV file.

- The *Performance* menu opens the Performance Monitoring page for the storage system. The default Performance view shows the following graphs for data rates in Mbps for Volumes, Interfaces, and MDisks as well as CPU utilization. Each graph has options that can be selected or deselected to display the statistics:
  - Within the *Volumes* graph, you can select or deselect Write throughput, Read throughput, Write latency, and Read latency. Write and Read data rates are in Mbps. Write and Read latency are expressed in milliseconds (ms).
  - Within the *Interfaces* graph, you can select the type of interface. Options are Fibre Channel (FC), Internet Small Computer System Interface (iSCSI), serial-attached SCSI (SAS), IP Remote Copy, and IP Compressed remote copy.
  - Within the *MDisks* graph, you have the same options as the Volumes. Both the MDisks and Volumes graphs display statistics for all MDisks and Volumes in the system.

  The Performance Monitoring page includes one additional option on the overall System Statistics to display statistics on a per-node basis for the storage system. If a single node is selected, the graphs listed previously are updated to include only the statistics for the selected node.

10.2.3 Pools

The Pools menu option is the second menu option in Figure 10-3 on page 220. Hovering over the Pools menu displays the menu shown in Figure 10-5.

Figure 10-5 Pools menu

The Pools menu gives the option for creating pools and lists the pools. Within the list of pools, you can click a pool and get additional options for the pool. These options include adding additional storage to the pool. The Actions tab on the Pools listing also includes some actions. These actions include adding storage to the pool and renaming the pool. For a full list of the options and their description, see *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

The following options are also available in the Pools menu:

- The *Volumes By Pool* menu option displays a list of pools on the system, in a Pool Filter. For each pool there is a list of the volumes contained in that pool. You can add volumes to the selected pool. To see a additional options for the volume, right-click a volume in the list of volumes for that pool.

When a pool is first selected in the pool filter, the Actions tab in the list of volumes displays actions for the pool. The actions include the following options:

- Estimating the space that is saved if compression is enabled on one or more volumes
- Generating a report on the estimated savings

When a volume is selected, the Actions tab changes to include the actions for a volume. There are numerous actions available on this menu. A full list of the actions options for volumes is available in *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

- The *Internal Storage* menu opens a page that lists the internal storage that is available on the V5030. The list can be filtered by the following drive types:
  - Flash
  - Enterprise Disk
  - Nearline

  You can also display all drives. The drives are listed in a table format. Right-click a drive in the table to open additional options for that drive.
- The *External Storage* option opens a page that lists the external storage that is available to the V5030, including any SAN disk systems that are attached to the IBM Storwize V5000. When a new external storage system is zoned to the IBM FlashSystem 5030, it automatically displays in the list. To use it, you must first run the *Discover storage* procedure from the Actions menu in the table header.
- The *MDisks by Pool* option opens a page that lists all managed disks and arrays of disks in the V5030. The list includes all disks, whether they are internally or externally connected, and associated with one of the defined pools. It also lists all unassigned MDisks separately. Unassigned MDisks are those disks that are not assigned to a pool. For details about assigning an MDisk to a pool, see *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.
- The *System Migration* option opens a page that gives options for migrating data from older storage subsystems to the V5030 to be able to use advanced features of the V5030, such as IBM Easy Tier, Space Efficient volumes, an intuitive management GUI, and advanced storage replication functions, that better support applications.

To migrate existing data, use the IBM Spectrum Virtualize storage migration wizard found under System Migration to guide you through the procedure. The migration of external volumes to the IBM Storwize V5000 system is one of the key benefits and features of external storage virtualization that are provided by the V5030. As such, an entire chapter of the implementation guide covers data migration. You can find details about the process and using the wizard in *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

10.2.4 Volumes

A *volume* is a logical disk that the system presents to the attached host. Application servers access volumes, not MDisks or drives. Volumes have additional characteristics. Volumes can be automatically expanded, mirrored, or pre-allocated. Volumes can also be generic, thin-provisioned, or compressed. For a full description of thin provisioned and compressed volumes see 9.7, “Thin provisioning” on page 212 and 9.8, “IBM Real Time Compression” on page 213.

Hovering over the Volumes menu displays the menu shown in Figure 10-6.

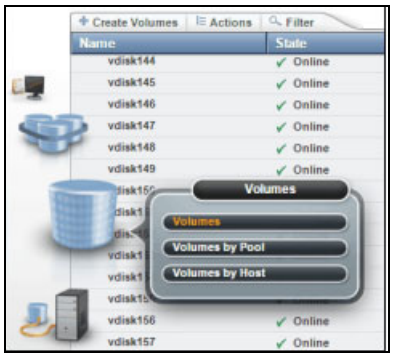


Figure 10-6 Volumes menu

The Volumes menu provides a list of all the volumes in the storage system. The list is displayed alphabetically by default but can be changed. The list also has a function to create new volumes. Selecting a volume in the list and then right-clicking that volume opens a menu with the following additional volume functions:

- Mapping and unmapping volumes to hosts
- Renaming, shrinking, or expanding existing volumes
- Migrating to a different pool
- Defining a volume copy

The Volumes listing also includes an option to create new volumes, as shown in Figure 10-7. You use this option to create the volumes for the solution that is detailed in this book. See *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162 for details about creating volumes on the V5030.

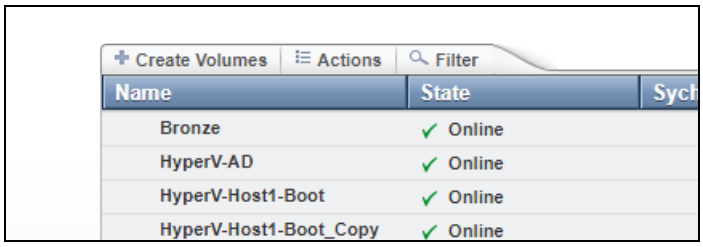


Figure 10-7 Creating volumes

The *Volumes by Pool* and *Volumes by Host* options offer views of the volumes that can be filtered by pool and host, respectively. After a pool or host is selected, a list of volumes is displayed for that pool or host. The volumes listed have the same options as described in the previous list.

For more details about each of these options, see *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

10.2.5 Hosts

Selecting the *Hosts* menu displays the menu shown in Figure 10-8.

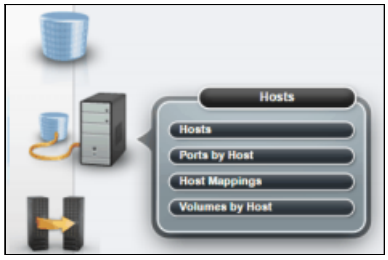


Figure 10-8 Hosts menu

This option provides an overview about all the hosts that are connected (zoned) to the system, detected, and configured to be ready for storage allocation. This overview shows the following information about the hosts:

- The name of the host as defined in the IBM Spectrum Virtualize
- The type of the host
- Its access status
- The number of ports that are used for host mapping
- Whether host mapping is active

From the same pane, you can create a new host, rename a host, delete a host, or modify a host mapping.

From the Hosts menu, you have the following options:

- *Ports By Host* displays a list of hosts. This overview shows hosts with active, inactive, or degraded ports. You can delete or add a port or modify its characteristics. Also, in this pane, you can create a new host or rename the existing host.
- *Host Mappings* displays a list of the Host mappings. The list identifies the host name, SCSI identifier, volume name, and volume identifier for all mapped volumes. Right-clicking a host map in the list opens a menu that has options for viewing the volume properties and viewing the host properties. When viewing the host properties, a settings page can be enabled. When it is enabled, some host details can be edited. You can find a full description of the available options in *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.
- *Volumes By Host* opens the same listing as described in 10.2.4, “Volumes” on page 222.

10.2.6 Copy Services

The Copy Services menu is shown in Figure 10-9. You can find a detailed description of each of the features in this menu in Chapter 9, “The IBM FlashSystem 5030 advanced functions” on page 205.

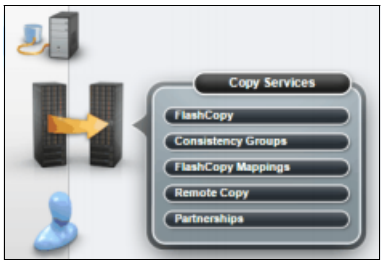


Figure 10-9 Copy Services menu

10.2.7 Access

Selecting the *Access* menu displays the menu shown in Figure 10-10.

Figure 10-10 Access menu

The Access menu offers the following options:

- The *Users* menu displays a list of the users on the system. From this list you can create and delete new users, change and remove passwords, and add and remove Secure Shell (SSH) keys for users.
- The *Audit Log* menu displays a list of the changes made to the storage system and which user made the changes. It also displays a time and date for each change.

You can find details about each of these menu option *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

10.2.8 Settings

Selecting the *Settings* menu displays the menu shown in Figure 10-11 on page 226. The details of each of the menu items are covered in *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162.

This book does not cover all of the items that available in the Settings menu. Instead, it highlights the options in Settings that you need to check or configure when implementing the solution from this book.

Figure 10-11 Settings menu

If you are using Microsoft Directory Server to manage users on the Windows Server, you can integrate authentication on the V5030 with your existing Directory Server. Follow these steps:

1. Select **Security** from the menu in Figure 10-11. Select **Configure Remote Authentication** → **LDAP** (Figure 10-12).

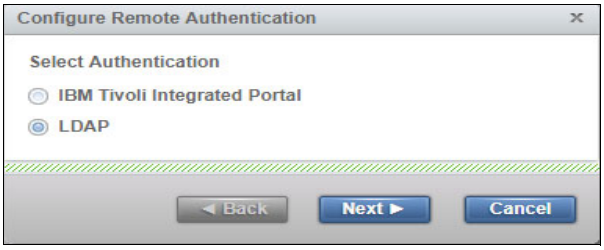


Figure 10-12 Authentication configuration

2. Select **Microsoft Active Directory** (Figure 10-13), and then click **Next** to continue configuration of your Microsoft Active Directory server and complete the integration.

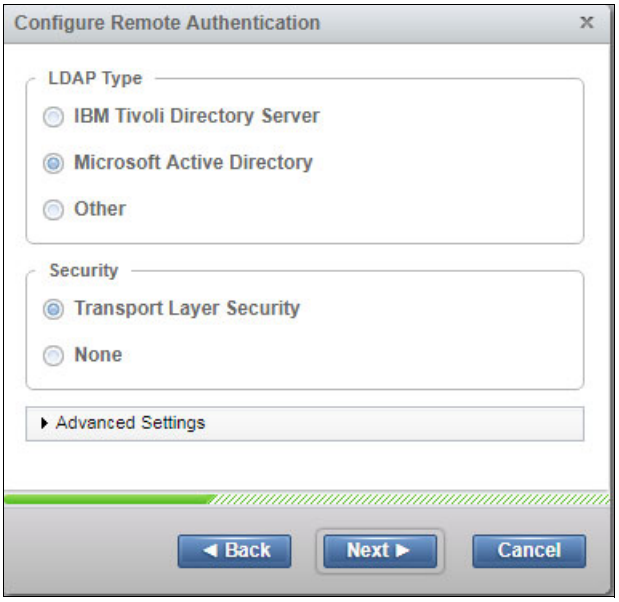


Figure 10-13 Configuring the Active Directory

3. Next, check the Service IP addresses. You can find this menu option in the Network Settings menu, as shown in Figure 10-14.

   You configure two addresses, one per Node canister, if they were not configured as part of the initial setup of the V5030. Setting the Service IP addresses on the Node canisters enables communication directly with the Node canisters and provides a backup mechanism to connect to the storage system if managing the system via the management port becomes inaccessible.

Figure 10-14 Network Settings menu

4. Update the V5030 to the latest system code as part of implementing this solution. You can update the system by clicking **System** → **Update System** from the System option on the menu shown in Figure 10-11 on page 226.
5. Lastly, check and review any licensed features that you might need by clicking **System** → **Licensed Functions** from the System option on the menu pictured in Figure 10-11 on page 226. This option displays the available licenses that you have. You can review this list to determine if you need to install any additional licenses.

10.3 The Cisco UCS GUI manager

The Cisco UCS is managed via a GUI application. The application can be accessed either via a web-based application or a downloadable Java application. The examples and images used in this book are taken from the web application. As with the V5030 Management tool covered in 10.1, “Management application integration” on page 216, this book assumes that basic setup of the UCS was completed. This book does not cover all of the options that are available in the UCS management tool in detail. Instead, it focuses on the sections of the Management GUI that are used to configure the UCS for this specific solution.

Cisco UCS Administration Guides: You can find more information about Cisco UCS in each of the UCS Administration Guides. Note that each function of the UCS is listed as a separate Administration guide.

This book focuses on the UCS Equipment, Server Management, LAN Management, and SAN Management pages of the UCS Manager. Answers to any other questions on the other components of the management GUI are found in the Administration guides available at the Cisco link.

10.3.1 Equipment management

Figure 10-15 shows the Equipment management main page from the UCS Manager Main Menu.

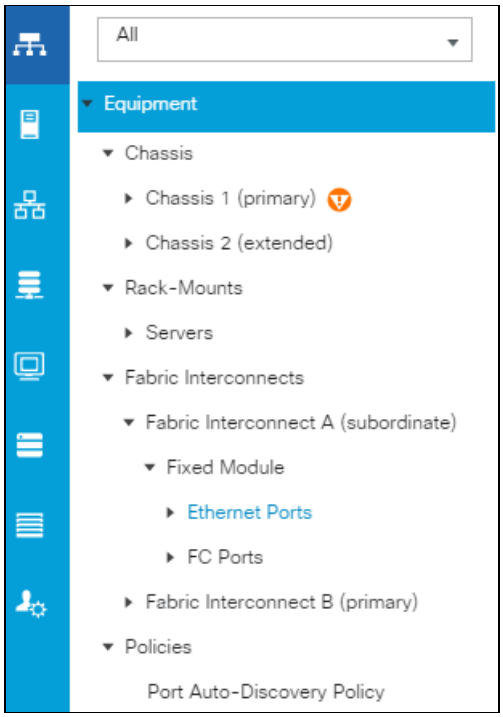


Figure 10-15 UCS Equipment Management page

The menu of icons on the left side represents the functions of the UCS that can be managed. The icons are as follows:

- Equipment management
- Server management
- LAN management
- SAN management

These functions are the functions for which this book provides more detail.

Continuing down the menu, the remaining menus include the following choices:

- Virtual machine management
- Storage
- Chassis management
- Options for administration

For more information about these selections, see the UCS Administrator's guide noted in 10.3, "The Cisco UCS GUI manager" on page 227.

The *Equipment* management menu provides options for managing the UCS hardware. From this menu, you can configure and view status on the chassis, blades (both in the chassis and rack-mount), and the Fabric Interconnects. There are also options to view any alerts on the physical components of the UCS.

Figure 10-16 shows the Equipment top menu. It displays in the UCS Management GUI across the top of the management page when you select the Equipment tab. This menu is set by context and changes depending on what selection is made from the choices under the Equipment selection on the menu. The menu also changes if you select **Servers**, **LAN management**, or any of the other main functions. This book does not discuss each of the menu selections in detail. For a full explanation of the menu, visit the link to the UCS administration guide at the start of this section.

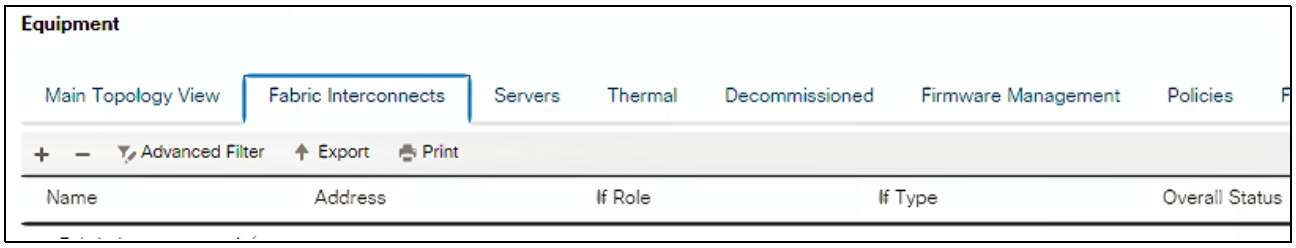


Figure 10-16 UCS Equipment top menu

Filtering the menu options: The drop-down menu under *All* in the main menu is a filter. Selecting one of the options from that filter sets the menu in Figure 10-16 to the same options as selecting that component in the main menu.

10.3.2 Server management

The *Server* management menu option displays the options for configuring UCS servers. As with the Equipment management menu option, you can filter the Server management menu to the options listed in Figure 10-17, Server management is accomplished primarily using *Service Profiles*, which are generated using *Service Profile Templates*. The templates are profiles that have some predefined options that are the same across multiple servers.

Using a profile template, a UCS Administrator can rapidly deploy a new server by customizing the necessary options for the new server and assigning the new profile to a physical blade. You can find details about the process in the UCS Administrator's guide. You can also use this menu to create pools of servers that the UCS pulls from when creating servers, and you can schedule events, such as system firmware upgrades.

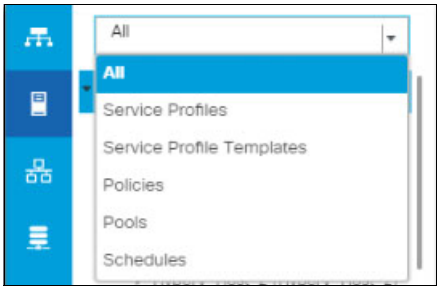


Figure 10-17 UCS Server menu

10.3.3 LAN management

If you select the *LAN management* option, the menu shown in Figure 10-18 displays. You can use these options to manage LAN connectivity for the servers in the chassis.

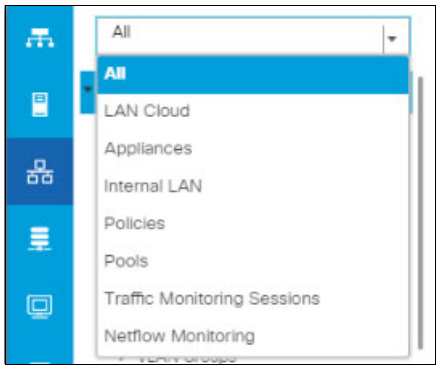


Figure 10-18 LAN management

In addition to configuring options related to LAN settings, you can monitor LAN traffic using the *Traffic Monitoring Sessions* and *Netflow Monitoring* options. As with the Server configuration, configure your LAN connections using LAN connectivity policies that are defined under the LAN management menu. You can use the *Pools* menu to define IP and MAC address pools. UCS Manager auto-assigns IP and MAC addresses as you create new virtual NICs. You can find details about configuring the LAN settings on the vNICs for the solution in this book in 5.1, “Completing the initial setup of the Cisco UCS 6324 Fabric Interconnects” on page 44.

10.3.4 SAN management

If you select the *SAN management* option, the menu shown in Figure 10-19 displays. The SAN management menu includes options for managing SAN attachment of the servers both internal and external to the UCS chassis.

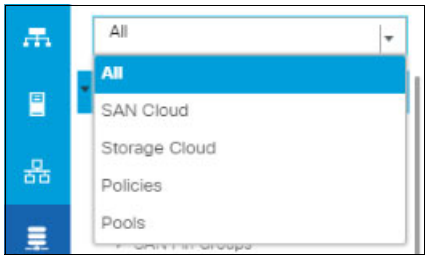


Figure 10-19 SAN management

The *SAN Cloud* menu contains options for viewing information about and managing parts of the SAN that are contained within the UCS chassis. This menu selection contains options for creating and managing FC and FCoE uplinks both within the UCS and from the Fabric Interconnects to the rest of the SAN. This menu also contains options for managing virtual storage area networks (VSANs).

The *Storage Cloud* menu contains options for managing SAN settings as they pertain to Storage. Ports for direct-attached storage can be defined in this menu for both FC and FCoE ports. Zoning policies and profiles can also be configured from this menu. The option to have the UCS manage zoning is available when creating VSANs from the Storage Cloud menu.

Enable this option only when the Fabric Interconnects are not connected to an upstream FC switch.

Other UCS Manager main menu options: The remaining menu selections depicted in the UCS Manager main menu, shown in Figure 10-15 on page 228, are not covered in this book. You can find details about those menus in the Administrator's guide at the link provided at the beginning of this section.

10.4 Microsoft System Center Virtual Machine Manager

Microsoft Virtual Machine Manager (VMM) is part of the Microsoft System Center (SC) management suite. SCVMM is a data center management tool that can provide a unified management experience for the following components:

- *Data center*: Configure and manage your datacenter components as a single fabric in VMM. Data center components include virtualization servers, networking components, and storage resources.
- *Virtualization hosts*: VMM can add, provision, and manage Hyper-V and VMware virtualization hosts and clusters.
- *Networking*: Add networking resources to the VMM fabric, including network sites defined by IP subnets, virtual local area networks (VLANs), logical switches, static IP address and MAC pools.
- *Storage*: VMM can discover, classify, provision, allocate, and assign local and remote storage.
- *Library resources*: The VMM fabric retains a library of file-based and non file-based resources that are used to create and deploy VMs and services on virtualization hosts.

As noted in 10.1, "Management application integration" on page 216, SCVMM can also be used to managed the V5030 and the UCS, provided it is configured to do so. Figure 10-20 displays the top-level menu in SCVMM. This book will give a brief overview of the VMs and Services, Fabric, and Library menus pictured in Figure 10-20. Covering these options in detail is beyond the scope of this book. You can find details about all of the capabilities and functions of SCVMM in the Microsoft article, "What is Virtual Machine Manager?"

The *How To* menu provides details about using SCVMM and all of its functions. See Figure 10-20.

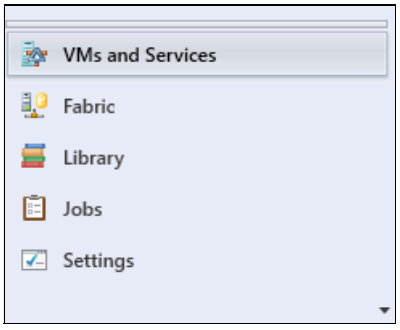


Figure 10-20 SCVMM main menu

10.4.1 SCVMM VMs and services

You can use SCVMM to create and deploy virtual machines and manage Windows Services. Selecting this option from the main menu brings up additional menu selections for managing virtual machines. The VMs and Services menu is depicted in Figure 10-21.

SCVMM can manage Microsoft Tenants, Cloud Services, Azure Subscriptions, the Virtual Networks used by the VMs, Storage, and Hosts. When the Cisco UCS Manager plug-in is installed, you can manage the UCS by selecting **All Hosts**, and then selecting the **UCS plug-in** from the tool ribbon at the top of the SCVMM window.

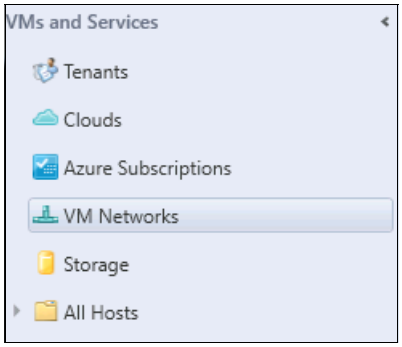


Figure 10-21 VMs and Services menu

10.4.2 SCVMM fabric management

Selecting the *Fabric* menu opens the SCVMM Fabric Management menu. You can use the menu selections here to manage the Network and Storage Network related components in SCVMM. The Fabric menu also has selections that include configuring Logical Networks, configuring MAC and IP Address Pools, and configuring Storage Network and IP Network resources. If the Storage Device management has been integrated into SCVMM you can use the Storage options under the Fabric menu to configuring and manage storage. You can find a complete list of the functions available under Fabric Management online.

When selected, the Fabric menu (Figure 10-22) offers the following menu options:

- Servers
- Networking
- Storage

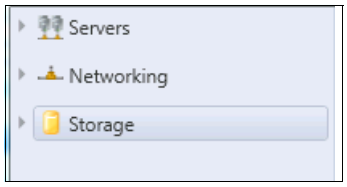


Figure 10-22 The Fabric menu

The *Servers* menu includes actions that are used to manage both virtual machines and other servers that comprise your VMM infrastructure. These infrastructure servers can include Library servers that contain items from the VMM library, PXE servers, servers that manage and deploy updates and VMWare VCenter servers.

Additionally you can define host groups, Hyper-V clusters and hosts, and stand-alone hosts using the Servers menu.

The *Networking* menu displays tasks for managing the Networking components of your virtual machine environment. This management includes Logical Switches and Logical Networks, MAC and IP address pools for auto-assignment to VMs as they are created, Port Profiles, Port Classifications, and Network Services.

Logical networks allow VMM to match virtual network properties to the physical networks in your datacenter. They allow you to specify connectivity properties, such as the VLAN ID, the management network, and other properties. Logical networks also allow you to group hosts together that should share the same network properties. When a new host is created and assigned to a logical network, it is assigned all of the network properties for that logical network.

Logical switches bring virtual switch extensions, port profiles, and port classifications together so that you can configure each network adapter with the settings you need and have consistent settings on network adapters across multiple hosts. You can team multiple network adapters by applying the same logical switch and uplink port profile to them.

Port Profiles and Port Classifications are used to automatically assign settings on virtual adapters. You can use several predefined Port Profiles to set default settings for the intended use of the adapter. For example, if the adapter is used for iSCSI, you can edit the iSCSI Port Profile to assign default settings to all adapters. You can also create your own Port Profiles. Port Classifications are used to tune the virtual adapter for the type of workload. For the iSCSI workload the adapter physical parameters might be different than for a Cluster interconnect. This is configured using the Port Profile.

Network Services is a container where you can add Windows and non-Windows network gateway and IP address management and monitoring information. For example, you can add a Microsoft IP Address Management server (IPAM) to the Network Services Container. You can use the IPAM server to configure and monitor logical networks and their associated network sites and IP address pools. You can also use the IPAM server to monitor the usage of VM networks that you have configured or changed in VMM.

10.4.3 SCVMM library management

The VMM library is a file share that includes a catalog of resources that are used to deploy virtual machines and services in the VMM fabric. The Library menu is shown in Figure 10-23.

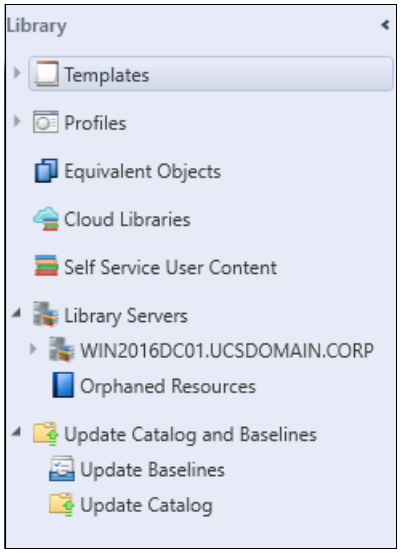


Figure 10-23 SCVMM Library

The library stores the following resources:

- File-based resources, such as virtual hard disks, ISO images, and scripts, driver files, and application packages (SQL Server data-tier applications and Web Deploy)
- Non-file-based resources, such as virtual machine templates and service templates that are used to create VMs and services
- Offline virtual machines that are stored in the library

You can find a complete list of what the library stores and information about how to add objects to the library online. File-based resources that can be added to the library include PowerShell scripts, SQL Server scripts, ISO images, hard disk images, driver files, and more. Non-file resources that can be added to the library include Virtual Machine templates, hardware templates and application templates. Lastly, any virtual machines that are offline are stored in the library. Offline VMs can be added to the stored node section of the library.

11

Validation testing

This chapter covers validation testing for the VersaStack design and includes the following failure and failover scenarios:

11.1 IBM FlashSystem 5030 node failure

The pair of nodes within a single IBM FlashSystem 5030 control enclosure is known as an *I/O group*. When a write operation is performed to a volume, the node that processes the I/O duplicates the data to the cache of the partner node in the I/O group. After the data is mirrored on the partner, the node acknowledges the write operation as complete to the host. The data in cache is physically written to disk later.

A host accesses its assigned volumes through either of the nodes in the I/O group. Each volume has a preferred node. Many multi-pathing driver implementations direct I/O to the preferred node. The other node in the I/O group is used only if the preferred node is not accessible. Most array configurations split volumes' preferred nodes across both nodes in order to balance performance.

You can specify a preferred node for a volume. The default is the node in the I/O group that has the fewest volumes.

Read I/O is processed by referencing the cache in the node that receives the I/O. If the data is not found in cache, it is read from the back-end MDisks. The read cache can provide better performance if the same node is chosen to service I/O for a particular volume. In volumes with volume mirrors, you can set one mirror as the primary or "preferred read" mirror. This configuration can improve performance when the preferred read mirror is of faster technology than the secondary mirror.

I/O traffic for a particular volume is managed exclusively by the nodes in a single I/O group. Although a clustered IBM Storwize or SVC can have two to eight nodes, the nodes manage I/O in independent pairs. When a node fails within an I/O group, the other node in the I/O group assumes the I/O responsibilities of the failed node. Mirroring the write cache between the two nodes prevents data loss during a node failure.

If only one node is assigned to an I/O group or if a node fails in an I/O group, the cache is flushed to the disk and then goes into write-through mode. Any writes for the volumes that are assigned to this I/O group are not cached; they are sent directly to the storage device. If both nodes in an I/O group go offline, the volumes assigned to the I/O group cannot be accessed.

11.1.1 Fibre Channel cable failure

Fibre Channel (FC) cable failure is a relatively common failure in storage environments. To simulate this failure, one can remove the FC cables from one node in the IBM FlashSystem 5030 storage system. This removal causes all the I/O traffic to go through the host interface card on the other node, but I/O continues and both nodes are still used. Example 11-1 shows the output of the **lsportfc** command, where you can see that all eight FC ports are active.

Example 11-1 The lsportfc command listing

```
0,1,1,fc,8Gb,3,node1,500507680D0458F0,CE0020,active,switch,local_partner,1,1
1,2,2,fc,8Gb,3,node1,500507680D0858F0,770001,active,switch,local_partner,1,2
2,3,3,fc,16Gb,3,node1,500507680D0C58F0,400200,active,switch,local_partner,1,3
3,4,4,fc,16Gb,3,node1,500507680D1058F0,7701C0,active,switch,local_partner,1,4
16,1,1,fc,8Gb,2,node2,500507680D0458F1,CE0002,active,switch,local_partner,1,1
17,2,2,fc,8Gb,2,node2,500507680D0858F1,770000,active,switch,local_partner,1,2
18,3,3,fc,16Gb,2,node2,500507680D0C58F1,400220,active,switch,local_partner,1,3
19,4,4,fc,16Gb,2,node2,500507680D1058F1,770220,active,switch,local_partner,1,4
```

To simulate FC cable failure, complete the following steps:

1. Remove the two FC cables from node 2 to create an error message on the IBM FlashSystem 5030 CLI and GUI.
2. Click **System** → **Events** to show the Event log depicted in Figure 11-1.

Error Code	Last Time Stamp	Status	Description	Object Type	Object ID	Object Name
1450	9/20/17 10:27:38 AM	Alert	Fibre Channel I/O ports not operational	node	2	node2
1061	9/20/17 10:27:33 AM	Alert	Fibre Channel ports not operational	node	2	node2
1450	9/20/17 10:24:48 AM	Alert	Fibre Channel I/O ports not operational	node	2	node2
1061	9/20/17 10:24:48 AM	Alert	Fibre Channel ports not operational	node	2	node2
1450	9/20/17 10:22:03 AM	Alert	Fibre Channel I/O ports not operational	node	3	node1
1061	9/20/17 10:22:03 AM	Alert	Fibre Channel ports not operational	node	3	node1
1450	9/20/17 10:21:58 AM	Alert	Fibre Channel I/O ports not operational	node	2	node2
1061	9/20/17 10:21:43 AM	Alert	Fibre Channel ports not operational	node	2	node2
	9/20/17 1:00:03 AM	Message	SAS discovery occurred	io_grp	0	io_grp0
	9/20/17 1:00:03 AM	Message	SAS discovery occurred	io_grp	0	io_grp0
	9/19/17 5:16:27 PM	Message	Volume copy format completed	vdisk	9	San-Policy-Test
1450	9/19/17 1:59:22 PM	Alert	Fibre Channel I/O ports not operational	node	2	node2

Figure 11-1 The V5030 event log

3. Figure 11-2 shows two errors inside the event log. You can run a directed maintenance procedure (DMP) by clicking the event in question and then clicking **Run Fix**. Click **Run Fix** for the top error to start a DMP for that error.

1450	9/20/17 10:21:58 AM	Alert	Fibre Channel I/O ports not operational	node	2	node2
1061	9/20/17 10:21:43 AM	Alert	Fibre Channel ports not operational	node	2	node2

Figure 11-2 Alert to downed ports

You are asked if the change is purposeful, and if not, what you want to do to fix the issue. Figure 11-3 shows the window that explains the error. In this case, two FC ports are inactive.

Fibre Channel ports not operational

Fibre Channel ports status changed

There has been a change of status on the Fibre Channel ports.

The Fibre Channel ports are located on this node

Machine Type and Model	Node Identifier	Node Name	Enclosure Identifier	Enclosure Serial Number	Panel Name	Canister Position In Enclosure
2078-324	2	node2	1	781B546	01-2	Right

The current status of the Fibre Channel ports

Adapter slot ID	Port ID	Port WWPN	Current status	Expected status
1	1	500507680D0458F1	Inactive	Active
1	2	500507680D0858F1	Inactive	Active
1	3	500507680D0C58F1	Active	Active
1	4	500507680D1058F1	Active	Active

If this change is intentional due to administration or maintenance, click this box: ☑ then click **Next**.

Note: this event could also be caused by a hardware change on this node that has not yet been accepted into configuration. Click **Cancel** to exit this fix procedure and check if any unfixed event with error code 1198 or 1199 is logged against this node, and run fix procedure for that event first. If there is no such event or it has already been fixed, click **Next** to proceed.

Figure 11-3 Port status after simulated failure

4. Click **Next**. The DMP shows you possible ways to fix the issue. Figure 11-4 shows how the DMP directs you to fix the error by checking the FC cabling.

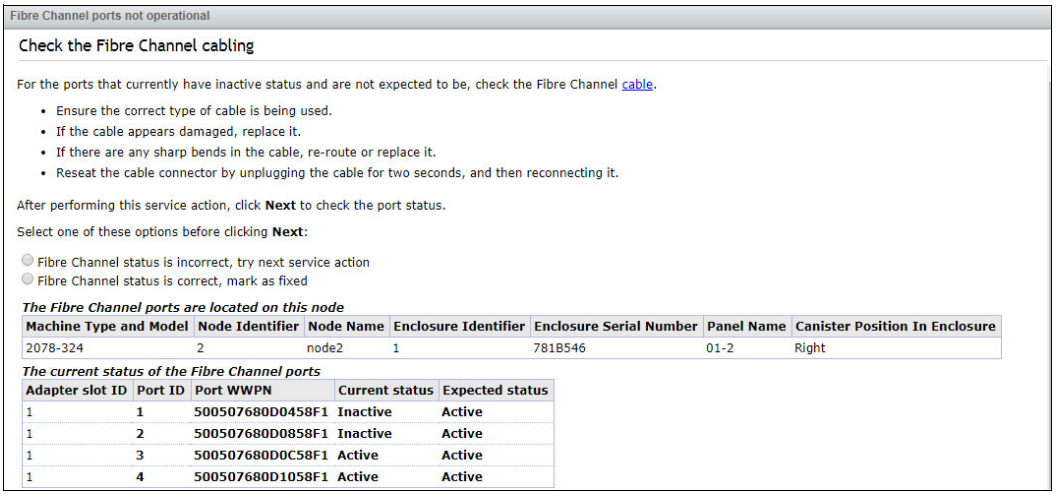


Figure 11-4 Fix procedure for inactive ports

5. If you plug in the FC cables that were removed from node 2 and refresh this window, you see the status of the ports go to *Active* and the event is marked as fixed. Figure 11-5 shows that the problem is solved and the event is marked as fixed.

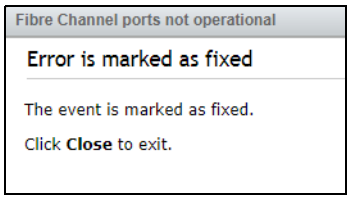


Figure 11-5 Error is fixed

11.1.2 Node failure

An IBM FlashSystem 5030 storage system uses a dual controller architecture with active/active node configuration to allow for continued operation in case of a node failure. Figure 11-6 shows the performance window on the IBM FlashSystem 5030 GUI. I/O is running, and the health status is *green*. The IBM FlashSystem 5030 performance window shows only 5 minutes of data.

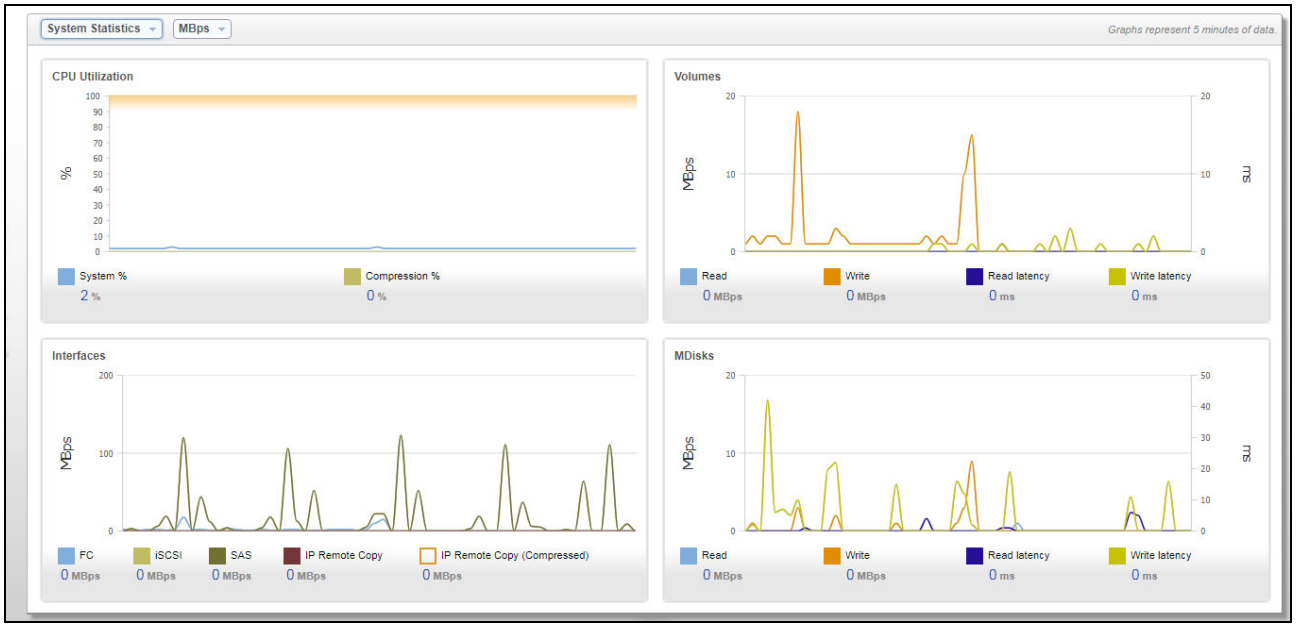


Figure 11-6 V5030 Performance Monitor

To simulate this failure, complete the following steps:

1. Remove the control node (node 2 in this case), which causes the cluster IP to fail over from node 2 to node 1. You briefly lose access to the GUI.
2. Access the GUI again by refreshing the GUI after a few minutes. There are errors in the event log. For more information, go to the System tab in Monitoring. Figure 11-7 shows the errors in the event log.

Error Code	Last Time Stamp	Status	Description	Object Type	Object ID	Object Na
	9/20/17 11:45:18 AM	Message	SAS discovery occurred	io_grp	0	io_grp0
1196	9/20/17 11:45:18 AM	Alert	Node is offline	node	3	node1

Figure 11-7 Event Log showing node offline

3. Rotate the enclosure by using the red arrow, and hover your cursor over the canister to see more information. Figure 11-8 shows the node offline.

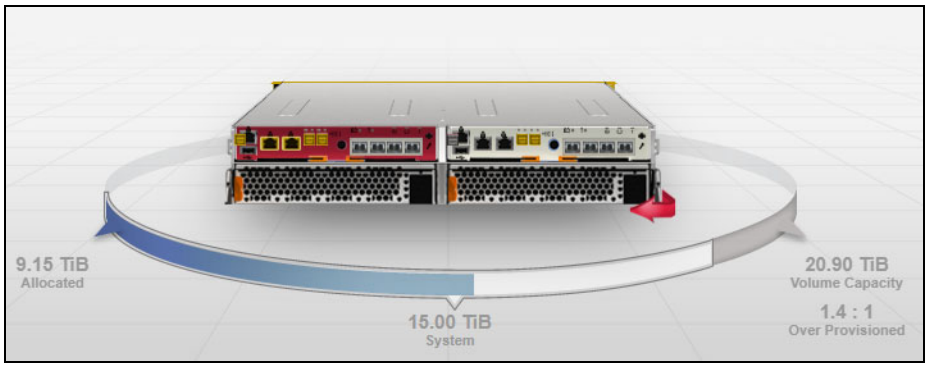


Figure 11-8 System view showing node offline

With only one node active, the cache is immediately flushed to disk. This is to eliminate the possibility of data loss while the hardware is not protected by redundancy, and so the host does not write over data on cache that has yet to be destaged. This means that you have a write cache hit rate of 0% when a node is removed.

4. Reinsert node 2. When it starts, it seamlessly joins the cluster, and the systems window updates to show that it joined the cluster. Figure 11-9 shows the fully recovered cluster, which shows no errors.

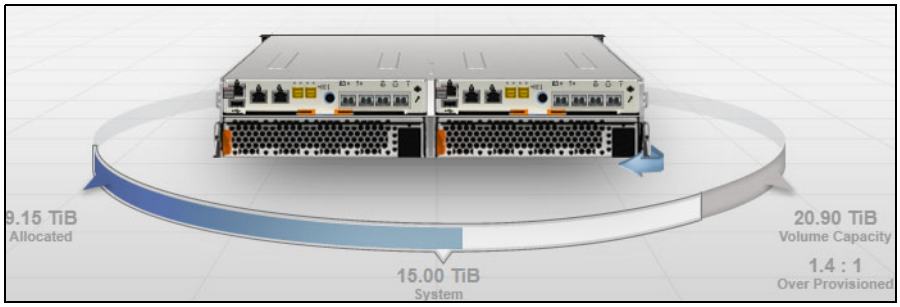


Figure 11-9 System view showing the node online

11.2 Fabric Interconnect failure

To simulate a failure of the Fabric Interconnect interface, disable all the ports on one interface:

1. Connect to the cluster IP over SSH and check which Fabric Interconnect is Primary or Subordinate as shown in Figure 11-10.

```
login as: admin
Cisco UCS Mini 6324 Series Fabric Interconnect
Using keyboard-interactive authentication.
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

VersaStack-V5030-UCSmini-B# show cluster state
Cluster Id: 0x3620136ae47e11e0-0x8f978c604fa3d482

B: UP, PRIMARY
A: UP, SUBORDINATE

HA READY
VersaStack-V5030-UCSmini-B#
```

Figure 11-10 Logging in to the Fabric Interconnect

Getting more information: The **`show cluster extended-state`** command provides more detailed information.

2. Confirm that the *B* fabric switch is the primary connect to Fabric Interconnect B management CLI interface, as shown in Figure 11-11.

```
B: memb state UP, lead state PRIMARY, mgmt services state: UP
A: memb state UP, lead state SUBORDINATE, mgmt services state: UP
   heartbeat state PRIMARY_OK

INTERNAL NETWORK INTERFACES:
eth2, UP

HA READY
Detailed state of the device selected for HA storage:
Chassis 1, serial: FOX1929GEDL, state: active
VersaStack-V5030-UCSmini-B# connect local-mgmt B
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

VersaStack-V5030-UCSmini-B(local-mgmt)#
```

Figure 11-11 Connecting with connect local-management B

3. From the Fabric Interconnect B local-management interface, issue the **`reboot`** command, as shown in Figure 11-12.

```
   heartbeat state PRIMARY_OK

INTERNAL NETWORK INTERFACES:
eth2, UP

HA READY
Detailed state of the device selected for HA storage:
Chassis 1, serial: FOX1929GEDL, state: active
VersaStack-V5030-UCSmini-B# connect local-mgmt B
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

VersaStack-V5030-UCSmini-B(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):
```

Figure 11-12 Reboot the Fabric Interconnect

4. If you reboot the primary Fabric Interconnect, it disconnects and is briefly unavailable until the other switch takes over as the primary switch. Connect again, and run the **cluster state** command to check the status of the Fabric Interconnect B switch, as shown in Figure 11-13.

```
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

VersaStack-V5030-UCSmini-A# show cluster extended-state
Cluster Id: 0x3620136ae47e11e0-0x8f978c604fa3d482

Start time: Thu Dec 13 16:27:36 2012
Last election time: Tue Sep 19 13:33:49 2017

A: UP, PRIMARY
B: DOWN, INAPPLICABLE

A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state DOWN, lead state INAPPLICABLE, mgmt services state: DOWN
   heartbeat state SECONDARY_FAILED

INTERNAL NETWORK INTERFACES:
eth2, UP

HA NOT READY
Peer Fabric Interconnect is down
Detailed state of the device selected for HA storage:
Chassis 1, serial: FOX1929GEDL, state: active
VersaStack-V5030-UCSmini-A#
```

Figure 11-13 Logging in to the other Fabric Interconnect with show cluster extended-state

5. After the cluster enters the *HA READY* status, connect to the Fabric Interconnect A local-management, and make the Fabric Interconnect B the *primary* switch in order to reboot Fabric Interconnect A, as shown in Figure 11-14.

```
HA NOT READY
Peer Fabric Interconnect is down
Detailed state of the device selected for HA storage:
Chassis 1, serial: FOX1929GEDL, state: active
VersaStack-V5030-UCSmini-A# show cluster extended-state
Cluster Id: 0x3620136ae47e11e0-0x8f978c604fa3d482

Start time: Thu Dec 13 16:27:36 2012
Last election time: Tue Sep 19 13:42:08 2017

A: UP, PRIMARY
B: UP, SUBORDINATE

A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP
   heartbeat state PRIMARY_OK

INTERNAL NETWORK INTERFACES:
eth2, UP

HA READY
Detailed state of the device selected for HA storage:
Chassis 1, serial: FOX1929GEDL, state: active
VersaStack-V5030-UCSmini-A#
```

Figure 11-14 Show cluster extended-state

6. Connect to Fabric Interconnect A, and change the cluster lead to B to make Fabric Interconnect B the primary switch, as shown in Figure 11-15.

```
Detailed state of the device selected for HA storage:
Chassis 1, serial: FOX1929GEDL, state: active
VersaStack-V5030-UCSmini-A# connect local-mgmt A
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

VersaStack-V5030-UCSmini-A(local-mgmt)# cluster lead b
If the system is at 'infrastructure firmware' auto-install 'pending user Ack' st
age,this action will result in upgrading and rebooting current primary. Please c
heck the outstanding faults (scope monitoring <enter> show new-faults) and make
sure the data-paths on FI-B are established properly before making it primary to
 ensure there is no data outage.
Do you want to continue? (yes/no):yes
Cluster Id: 0x3620136ae47e11e0-0x8f978c604fa3d482
VersaStack-V5030-UCSmini-A(local-mgmt)#
```

Figure 11-15 Change Fabric Interconnect B to the primary switch

7. Connect to local management A and reboot Fabric Interconnect A, as shown in Figure 11-16.

```
VersaStack-V5030-UCSmini-B# connect local-mgmt a
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

VersaStack-V5030-UCSmini-A(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
nohup: ignoring input and redirecting stderr to stdout

Broadcast message from root (Tue Sep 19 13:57:14 2017):

All shells being terminated due to system /sbin/reboot
bash: line 1: 16007 Killed                  /isan/bin/ucssh --ucs-local-mgmt -t
30 -p "admin"
VersaStack-V5030-UCSmini-B#
```

Figure 11-16 Rebooting the secondary Fabric Interconnect

11.3 Microsoft WSFC and Microsoft SQL Server AlwaysOn FCI validation

A *Microsoft WSFC cluster* is a group of independent servers that work together to increase the availability of applications and services, such as File and Print Services and SQL Server Failover Cluster Instances.

An *AlwaysOn FCI* is a SQL Server instance that is installed across nodes in a WSFC cluster. If there is a failover, the WSFC service transfers ownership of resources to another available designated node in the cluster. The SQL Server instance is then restarted on the failover node, and databases are recovered as usual.

This validation scenario describes the impact of a manual failure of the WSFC active node and the SQL Server FCI. This scenario highlights the high availability for the SQL Server database instance.

11.3.1 Test procedure

The virtual machine hosting the primary instance of the SQL Server FCI is identified. Figure 11-17 shows the Failover Cluster Manager with the owner node Node 1.

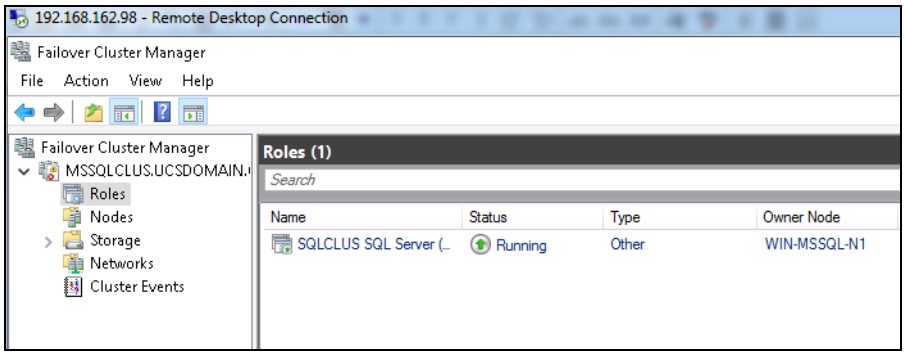


Figure 11-17 Owner Cluster Node

Complete the following steps:

1. Start an OLTP workload from a machine outside the VersaStack environment. The tool to generate an OLTP workload is called *HammerDB*. This is a tool that is used to put load on databases for performance testing. Figure 11-18 shows the HammerDB OLTP workload running on the SQL Server FCI.

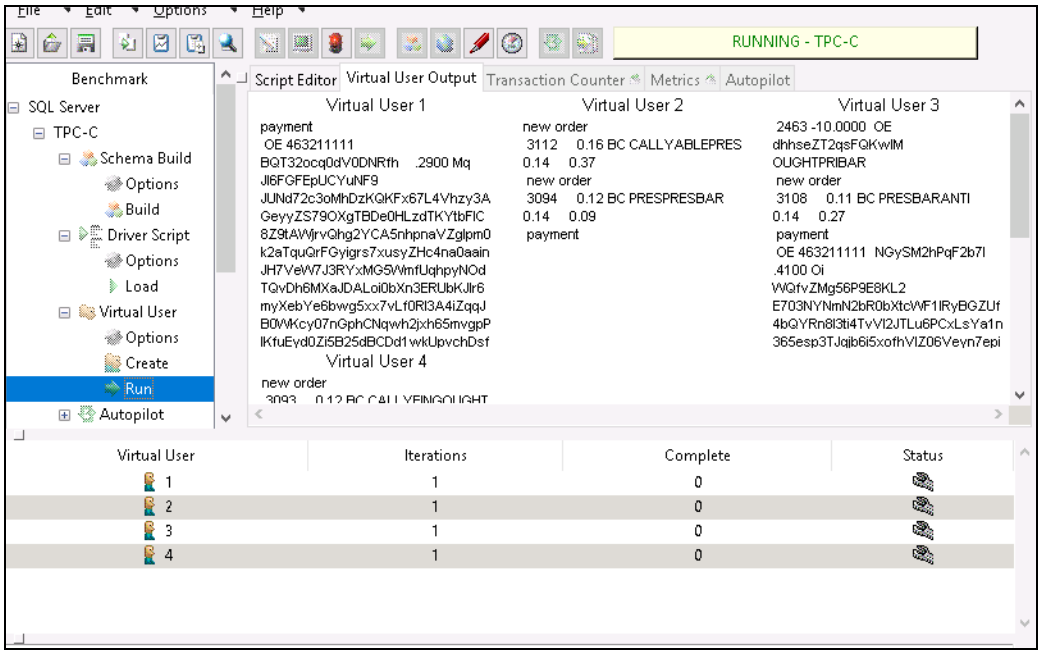


Figure 11-18 HammerDB workload running

2. From the Failover Cluster Manager window, right-click the virtual machine that is an owner node and stop the cluster service.

11.3.2 Test observations

The status of the node whose cluster service was stopped is *Down* after moving the roles to the other node. Figure 11-19 shows the node's cluster service as *Down*.

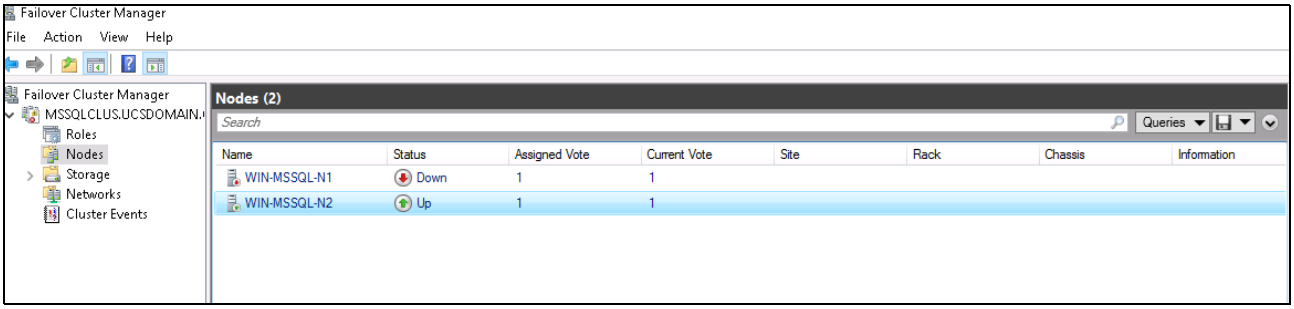


Figure 11-19 Node's cluster service is down

The client machine from where the OLTP workload was started loses connectivity during the failover. Figure 11-20 shows the client losing connectivity when the owner node cluster service is down.

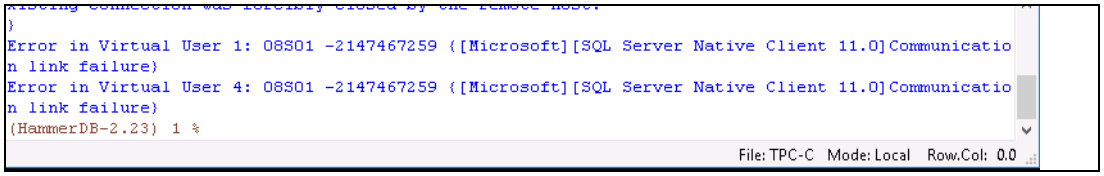


Figure 11-20 Lost connection to SQL Server cluster

Important: HammerDB is a tool that is used to put load on databases for performance testing. It lost its connection to the SQL cluster because it is not a cluster-aware application. Production applications that are cluster-aware and configured correctly do not lose database connectivity in the event of a cluster node failure.

The cluster service and the SQL Server FCI came online quickly on the other node and reconnected the clients successfully. During this exercise, all the instance-level entities of SQL Server, including the security objects, are made to fail over to the passive virtual machine. After the manual failover, the standby instance of the failover cluster instance is made the active instance that hosts the FCI. After the test is complete, the cluster service of the node is restarted to put all the cluster nodes online.

Figure 11-21 shows the Failover Cluster Manager after the resources are moved from the failed cluster node to the available cluster node 2.

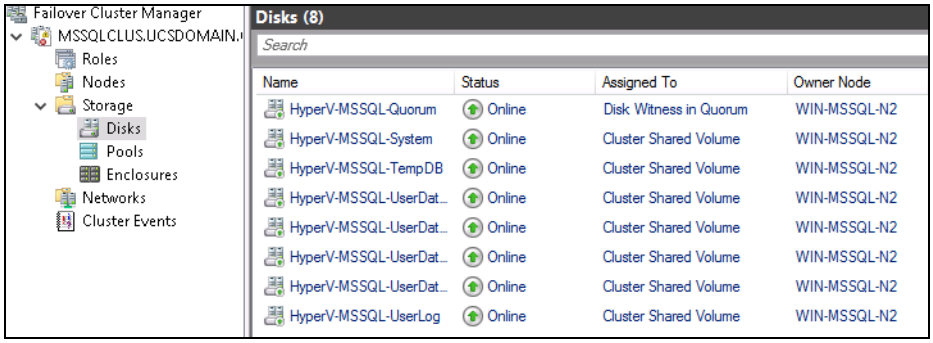


Figure 11-21 Resources moved to available node

11.4 Cisco Nexus Virtual PortChannel peer switch failure

A Virtual PortChannel (vPC) allows links that are physically connected to two different Cisco Nexus 9000 Series devices to appear as a single PortChannel to a third device. The third device can be a Cisco Nexus 2000 Series Fabric Extender or a switch, server, or any other networking device. A vPC can provide Layer 2 multi-pathing, which allows you to create redundancy by increasing bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

Figure 11-22 shows the Cisco Nexus vPC physical and logical topology.

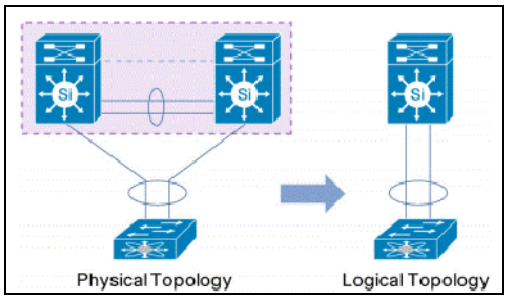


Figure 11-22 Cisco Nexus vPC topologies

A vPC provides the following benefits:

- Allows a single device to use a PortChannel across two upstream devices
- Eliminates Spanning Tree Protocol blocked ports
- Provides a loop-free topology
- Uses all available uplink bandwidth
- Provides fast convergence if either the link or a device fails
- Provides link-level resiliency
- Helps ensure high availability

This validation scenario describes a vPC peer switch failure by bringing down one of the Nexus 9372 PX switches. This scenario highlights the high availability and redundancy of Nexus switches in the VersaStack environment.

11.4.1 Test procedure

Connect to the Nexus 9372 switch with the vPC role as the primary through Secure Shell and run the **reload** command, as shown in Figure 11-23.

```
N9K-A# reload
This command will reboot the system. (y/n)?  [n] y
```

Figure 11-23 Reloading the Nexus 9372

11.4.2 Test observation

When the primary Nexus peer switch was reloading, the secondary peer switch that is running assumes the vPC role of operational primary. During the reload of the primary switch, half of the network bandwidth is lost and the remaining vPC switch maintains the network connectivity. There is no impact to the vPC operation or data forwarding.

11.5 Cisco UCS service profile migration validation

Conceptually, a service profile is an extension of the virtual machine abstraction that is applied to physical servers. The definition is expanded to include elements of the environment that span the entire data center, encapsulating the server identity (LAN and SAN addressing, I/O configurations, firmware versions, boot order, network virtual local area network (VLAN), physical port, and quality of service policies) in logical “service profiles.”

These profiles can be dynamically created and associated with any physical server in the system within minutes rather than hours or days. The association of service profiles with physical servers is performed as a simple, single operation. It enables migration of identities between servers in the environment without requiring any physical configuration changes, and facilitates rapid bare-metal provisioning of replacements for failed servers.

Service profiles also include operational policy information, such as information about firmware versions.

This highly dynamic environment can be adapted to meet rapidly changing needs in today's data centers with just-in-time deployment of new computing resources and reliable movement of traditional and virtual workloads. Data center administrators can now focus on addressing business policies and data access on the basis of application and service requirements, rather than physical server connectivity and configurations.

Service profiles can be abstracted from the specifics of a given server to create a service profile template, which defines policies that can be applied any number of times to provision any number of servers. Service profile templates help enable large-scale operations in which many servers are provisioned as easily as a single server.

In addition, by using service profiles, Cisco UCS Manager provides logical grouping capabilities for both physical servers and service profiles and their associated templates. This pooling or grouping, combined with fine-grained role-based access, allows businesses to treat a farm of compute blades as a flexible resource pool that can be reallocated in real time to meet their changing needs, while maintaining any organizational overlay on the environment that they want.

This validation scenario describes a use case of a Cisco UCS service profile migration in case there is an unplanned Cisco UCS B200 M4 hardware failure. This scenario is tested on a server that boots from SAN and needs spare hardware to replace the failed one.

11.5.1 Test procedure

Complete the following steps:

1. Power off the Cisco UCS B200 M4 server in slot 1 to simulate the hardware failure scenario. Figure 11-24 shows a decommissioned Server 1 in Cisco UCS Manager. Also note that Server 2 is unassociated.

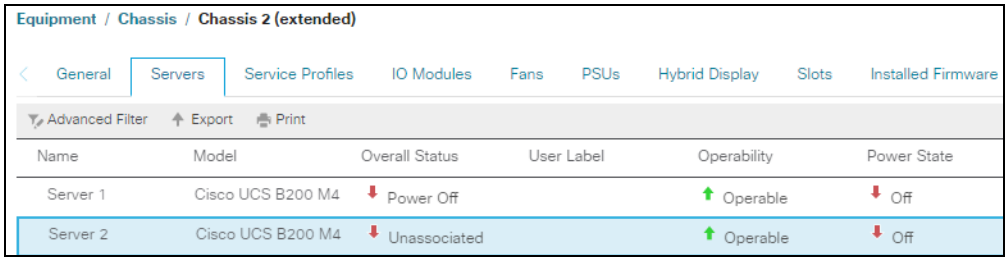


Figure 11-24 Chassis 2 unpowered servers

2. Reassociate the service profile to a new server to simulate hardware replacement. Figure 11-25 shows the service profile association to Server 2in Cisco UCS Manager.

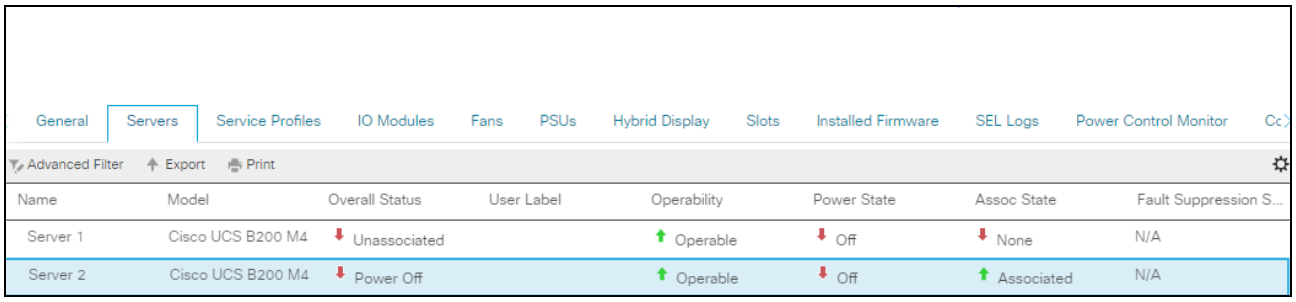


Figure 11-25 Associating the service profile

11.5.2 Test observations

The service profile migration from the failed hardware to the new hardware was successful and the new server booted from SAN successfully.

11.6 Hyper-V virtual machine failover

To test Hyper-V virtual machine failover, log in to the Windows Failover Cluster Manager. The virtual machine volumes are usually balanced across physical nodes in the cluster. This case involves the following nodes:

- WIN-HYPERV-N1
- WIN-HYPERV-N2

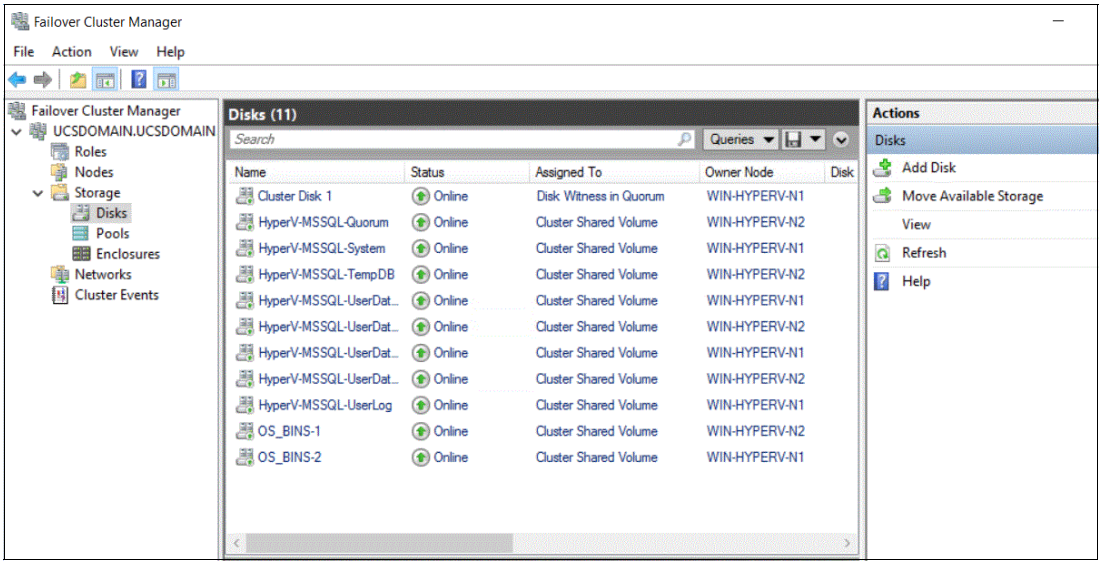


Figure 11-26 List of storage disks balanced across nodes

To show the application continues to run during a failover, this scenario uses a load simulator to run database transactions on the SQL Server's clustered IP address. In the Windows Failover Cluster Manager, highlight the volumes on the secondary node. Then, right-click and select **Move** → **Select Node**.

This scenario moves the `WIN-HYPERV-N2` volumes to `WIN-HYPERV-N1`, as shown in Figure 11-27.

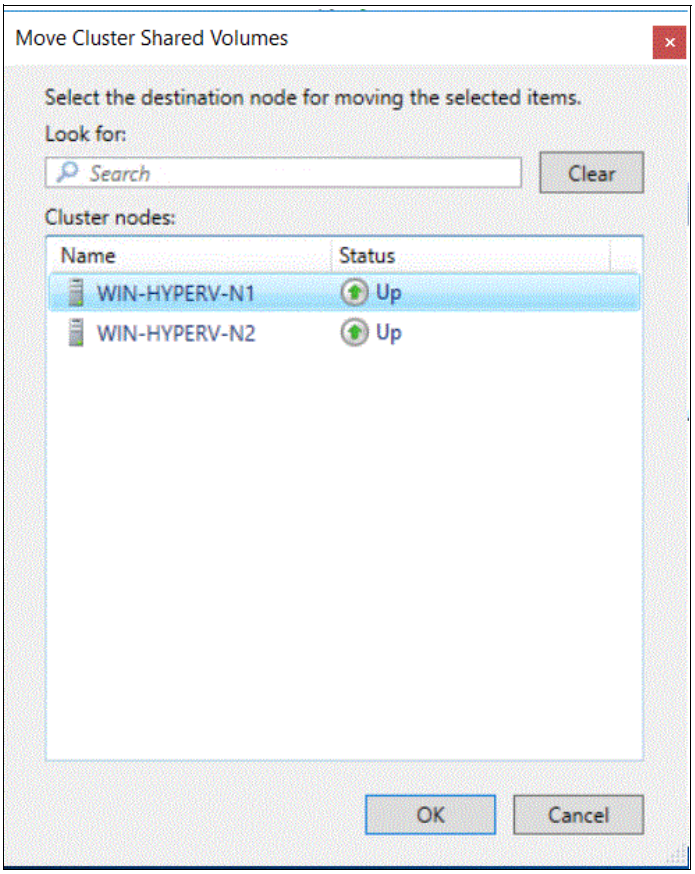


Figure 11-27 Selecting a node to move the cluster shared volumes to

Monitor the load on the application during the move, as shown in Figure 11-28.

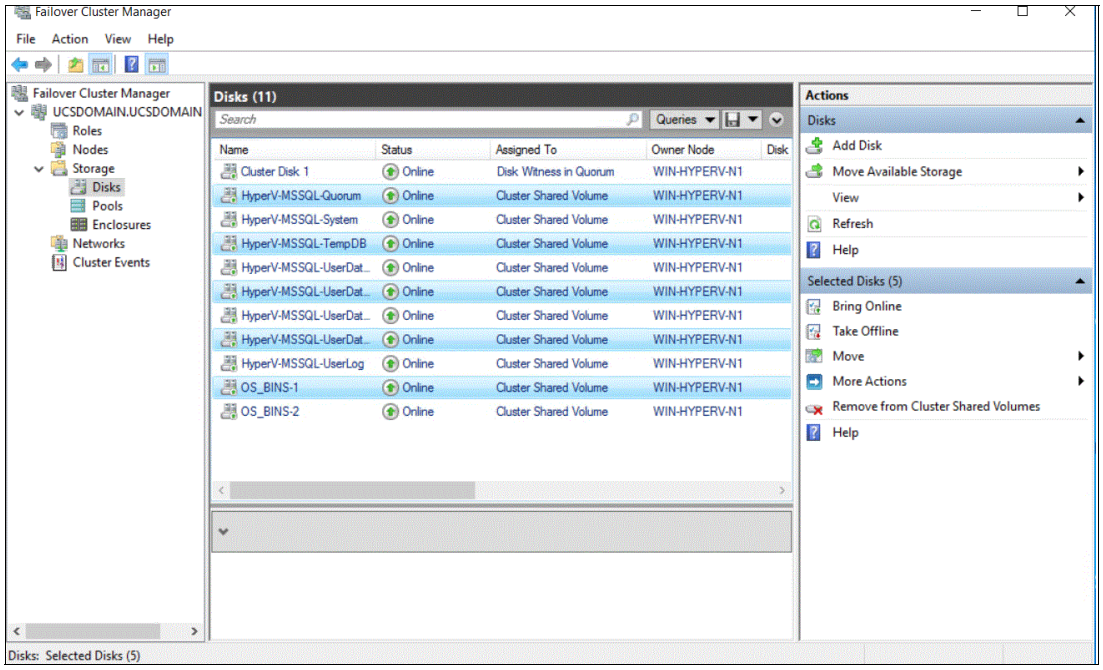


Figure 11-28 After moving the nodes

In this example the move at 12:59 was hardly noticeable if at all at the application layer, as shown in Figure 11-29.

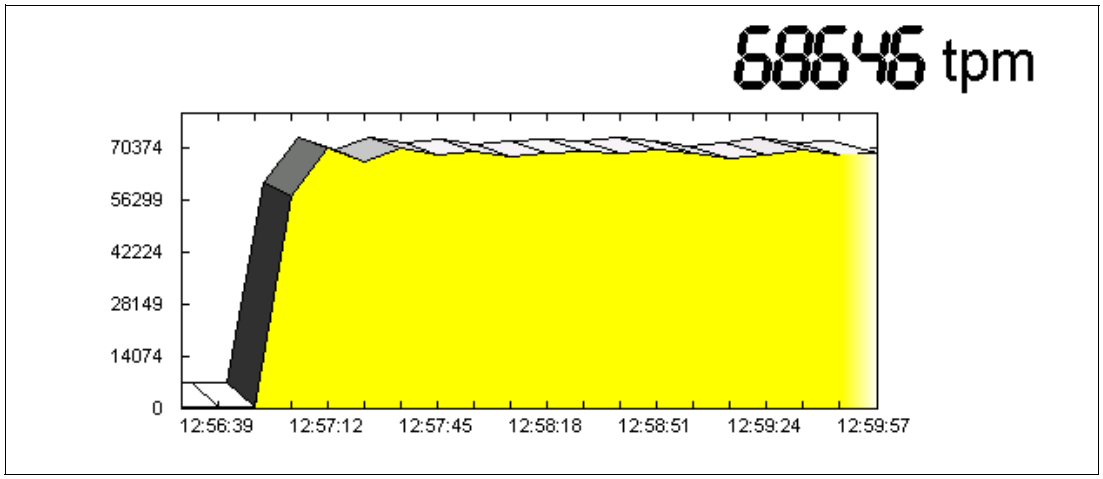


Figure 11-29 Application monitoring during the move at 12:59

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.

- *Implementing the IBM Storwize V5000 Gen2 (including the Storwize V5010, V5020, and V5030) with IBM Spectrum Virtualize V8.1*, SG24-8162

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 Storwize family:

  https://www.ibm.com/storage/storwize

- VersaStack Solution for Remote and Branch-Office Deployments:

  https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/versastack-solution-cisco-ibm/versastack-aag-storwize.pdf

- VersaStack Solutions: Based on Cisco UCS Integrated Infrastructure and IBM Storage Systems:

  https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/versastack-solution-cisco-ibm/le-brochure-versastack.pdf

- VersaStack Solution for Private Cloud:

  https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/versastack-solution-cisco-ibm/aag-versastack-iaas.pdf?cm_mc_uid=85898154834615046256647&cm_mc_sid_50200000=1505231729

- Solution Brief: Top 5 Reasons to Deploy Hybrid Cloud on VersaStack Solutions:

  https://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/versastack-solution-cisco-ibm/versastack-hybrid-cloud-top-5reasons.pdf

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Redbooks

Implementing a VersaStack Solution with IBM FlashSystem 5030, Cisco UCS Mini, Hyper-V, and SQL Server

SG24-8407-00

ISBN 073844278X

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

SG24-8407-00

ISBN 073844278X

Printed in U.S.A.