

Implementing a VersaStack Solution by Cisco and IBM with IBM Storwize V5030, 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







International Technical Support Organization

Implementing a VersaStack Solution by Cisco and IBM with IBM Storwize V5030, Cisco UCS Mini, Hyper-V, and SQL Server

November 2017

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.

© Copyright International Business Machines Corporation 2017. All rights reserved. Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	
Preface Authors Now you can become a published author, too! Comments welcome Stay connected to IBM Redbooks	. xi xiv xiv
Chapter 1. Introduction	
1.1 Overview	
1.2 The VersaStack solution described in this book	
1.3 VersaStack synopsis	
1.4 Common VersaStack use cases	
1.4.1 Remote and branch office	
1.4.2 Data center	
1.4.3 Private cloud	. 4
1.4.4 Hybrid cloud	
1.5 Optional and complementary products	. 5
1.5.1 Cisco application centric infrastructure	. 5
1.5.2 IBM Spectrum Control Storage Insights	. 6
1.5.3 IBM Spectrum Protect and IBM Spectrum Protect Plus	. 7
1.5.4 IBM Spectrum Copy Data Management	. 7
1.6 Assumptions made in this book	. 7
1.7 For more information	. 8
Chapter 2. Architecture of the solution	
2.1 VersaStack architecture	
2.1.1 Physical topology	
2.2 Software versions	
2.3 Configuration guidelines	
2.3.1 List of tables	
2.3.2 VersaStack build process	
2.4 VersaStack cabling	
2.5 Microsoft SQL Server on the VersaStack architecture	20
Chapter 3. Design considerations for Microsoft Hyper-V and SQL Server	23
3.1 Microsoft Hyper-V considerations	24
3.1.1 Root partition considerations	24
3.1.2 Child partition considerations	24
3.2 Microsoft SQL Server design considerations	25
3.2.1 Sizing and design planning for Microsoft SQL Server	25
3.2.2 Database applications and workload	26
3.2.3 Storage, RAID type and disk selection	
3.2.4 IOPS requirements for Microsoft SQL Server.	
3.2.5 Server virtualization	
3.2.6 Database availability	
3.2.7 Quality of service and network segregation	
	~ 1

Chapter 4. VersaStack Cisco Nexus 9000 network configuration	29
4.1 Initial terminal connection	
4.2 Configuring the Cisco Nexus switch A	30
4.3 Configuring the Cisco Nexus switch B	
4.4 Enabling the Cisco Nexus 9000 features and settings	
4.5 Creating the VLANs for the VersaStack traffic	
4.6 Configuring the Virtual PortChannel domain	
4.6.1 Configure the vPC for the Cisco Nexus switch A	
4.6.2 Configure the vPC for the Cisco Nexus switch B	
4.7 Configuring the network interfaces for the vPC peer links	
4.7.1 Configure the network interface for the Cisco Nexus switch A	
4.7.2 Configure the network interface for the Cisco Nexus switch B	
4.8 Configuring network interfaces to the Cisco UCS Fabric Interconnects	
4.8.1 Configure the Cisco Nexus switch A to FI-A	
4.8.2 Configure the Cisco Nexus switch B to FI-B	37
Chapter 5. The Cisco Unified Computing System Mini configuration	41
5.1 Completing the initial setup of the Cisco UCS 6324 Fabric Interconnects	
5.1.1 Cisco UCS Fabric Interconnects 6324 A.	
5.1.2 Cisco UCS Fabric Interconnects 6324 B.	
5.2 VersaStack Cisco UCS base setup.	
5.2.1 Logging in to the Cisco UCS Manager	
5.2.2 Adding a block of IP addresses for access to a kernel-based virtual machir	
44	
5.2.3 Synchronizing the Cisco UCS Mini chassis to NTP	45
5.2.4 Configuring the UCS Servers discovery policy	46
5.2.5 Acknowledging the Cisco UCS Mini chassis.	47
5.3 Enabling the server and uplink ports in the Fabric Interconnects	48
5.3.1 Creating an UUID suffix pool	
5.3.2 Creating a server pool	51
5.3.3 Creating a host firmware package	
5.3.4 Creating a local disk configuration policy	
5.3.5 Creating a power control policy	
5.3.6 Creating a server pool qualification policy (optional)	
5.3.7 Creating a Server BIOS policy	
5.3.8 Creating a vNIC/vHBA placement policy for the VM infrastructure hosts	
5.3.9 Updating the default Maintenance Policy	
5.4 Configuring UCS SAN connectivity	
5.4.1 Configuring unified ports	
5.4.2 Configure Fabric Interconnects in FC switching mode	
5.4.3 Creating storage virtual storage area networks	
5.4.4 Configuring the FC storage ports	
5.4.5 Creating WWNN pools	
5.4.6 Creating WWPN pools	
5.4.7 Creating virtual HBA templates for Fabric A and Fabric B	
5.4.8 Creating boot policies	
5.5 Configuring UCS LAN connectivity	
5.5.1 Creating uplink port channels to Cisco Nexus switches	
5.5.2 Creating MAC address pools	
5.5.3 Creating a virtual local area network	
5.5.4 Setting jumbo frames in Cisco UCS Fabric.	
5.5.5 Creating a network control policy for Cisco discovery protocol.	
5.5.6 Creating virtual network interface card templates	

 5.5.7 Creating LAN connectivity policy. 5.5.8 Creating service profile templates. 5.5.9 Creating service profiles . 5.6 Back up the Cisco UCS Manager configuration . 	83 90
Chapter 6. SAN Boot in a Cisco UCS Mini environment 6.1 Overview of a SAN Boot using Cisco UCS Mini 6.2 Preparing the SAN Boot for Windows Server 2016 6.2.1 Boot policy	
6.2.2 Unified Extensible Firmware Interface boot mode6.2.3 UEFI secure boot	95
6.3 Preparing and performing SAN Boot.6.4 Provisioning IBM LUN as a SAN Boot volume	
6.5 Setting up Microsoft Windows Server 2016	
6.5.1 Installing Intel chipset and Cisco eNIC drivers for Microsoft Windows .	
6.5.2 Cloning an OS volume	103
Chapter 7. Failover cluster and Hyper-V configuration	105
7.1 Introduction to Hyper-V Cluster for high availability	106
7.2 Physical topology for Hyper-V	
7.3 Microsoft Windows 2016 Failover Clustering feature requirements	
7.4 Configuring features and tools for failover cluster nodes	
7.4.1 Installing Data Center Bridging and multipath I/O	
7.4.2 Installing the IBM SDDDSM multipathing software	
7.5 Creating a host attachment in IBM Storwize V5030	
7.6 Creating a host cluster in the IBM Storwize V5030	
7.7 Provisioning IBM Storwize Volume for Cluster Shared Volumes7.8 Rescanning and assigning the cluster shared volumes	
7.9 Configuring the Failover Clustering feature.	
7.10 Adding the Hyper-V feature.	
7.11 Microsoft Virtual Machine Manager.	
7.12 Configuring the Hyper-V virtual network using Microsoft Virtual Machine M	
7.12.1 Network settings	
7.12.2 Configuring Run As account	
7.12.3 Host group containers	
7.12.4 Adding the Hyper-V Cluster to host groups.	133
7.12.5 Hyper-V networking	
7.12.6 Adding the IBM Storwize V5030 to VMM	
7.12.7 Storage classifications	
7.12.8 Configuring virtual switches on Hyper-V hosts	
7.13 Hardware profiles	
7.14 Creating virtual machines using hardware profiles	158
Chapter 8. Microsoft SQL Server setup and failover cluster implementation	
8.1 Before you begin	
8.1.1 Review the virtual machine configuration	
8.1.2 Review the OS configuration	
8.2 Provisioning storage volumes for Hyper-V cluster nodes	
8.2.1 Creating easy-tiered volumes on the IBM Storwize V5000 for data files,	•
system files	
8.2.2 Creating volumes on the v5030 for the tempob and log files	
8.3 Creating CSV on a Hyper-V cluster	
8.3.1 Initializing disks using the Disk Management facility.	

8.3.2 Create a file system volume on the disks	
8.3.3 Adding disks into the Hyper-V cluster	
8.4 Assigning the V5030 volumes as shared drives to SQL VMs	
8.4.1 Creating shared drives and assigning them to first SQL VM	
8.4.2 Assigning shared drives to a second SQL VM	
8.5 Preparing the Cluster Shared Volumes on SQL VMs for Windows Failover Cluster $$.	
8.5.1 Initializing disks using the Disk Management facility.	
8.5.2 Creating a file system volume on the disks	
8.6 Installing the Windows Failover Clustering feature on SQL virtual machines	
8.7 Installing a Microsoft SQL Server failover cluster	
8.7.1 Installing the Microsoft SQL Server on the first SQL VM	
8.7.2 Adding a second node to the SQL Server Failover Cluster instance	
8.7.3 Installing SQL Server Management Studio	
8.7.4 Connecting to SQL Server using SSMS	
8.8 Creating a sample database	
8.9 Configure Hyper-V level redundancy for SQL VMs.	
8.9.1 Setting Preferred Owner and Possible Owner for VMs	
8.10 Database tuning	202
Chapter 9. The IBM Storwize V5030 advanced functions	202
9.1 IBM Easy Tier	
9.1.1 IBM Easy Tier overview	
9.1.2 Easy Tier limitations and requirements.	
9.2 IBM HyperSwap	
9.3 Remote copy	
9.4 IBM FlashCopy	
9.5 Encryption	
9.6 Volume mirroring.	
9.7 Thin provisioning.	
9.8 IBM Real Time Compression	
9.9 Microsoft offloaded data transfer	
Chapter 10. Managing the VersaStack solution	
10.1 Management application integration	
10.1.1 Microsoft System Center Virtual Machine Manager	
10.1.2 Microsoft System Center Operations Manager.	
10.2 The IBM Storwize V5030 Manager	
10.2.1 Accessing the management software	
10.2.2 Monitoring	
10.2.3 Pools	
10.2.4 Volumes	
10.2.5 Hosts	
10.2.6 Copy Services	
10.2.7 Access	-
10.2.8 Settings	
10.3 The Cisco UCS GUI manager	
10.3.2 Server management	
10.3.3 LAN management	
10.3.4 SAN management. 10.4 Microsoft System Center Virtual Machine Manager	
10.4.1 SCVMM VMs and services	
10.4.1 SCVMM VMS and services	
	∠ວ∪

10.4.3 SCVMM library management	. 231
Chapter 11. Validation testing	
11.1 IBM Storwize V5030 node failure	. 234
11.1.1 Fibre Channel cable failure	. 234
11.1.2 Node failure	. 237
11.2 Fabric Interconnect failure	. 239
11.3 Microsoft WSFC and Microsoft SQL Server AlwaysOn FCI validation	. 243
11.3.1 Test procedure	. 243
11.3.2 Test observations	. 244
11.4 Cisco Nexus Virtual PortChannel peer switch failure	. 245
11.4.1 Test procedure	. 246
11.4.2 Test observation	. 246
11.5 Cisco UCS service profile migration validation	. 246
11.5.1 Test procedure	. 247
11.5.2 Test observations	
11.6 Hyper-V virtual machine failover	
Related publications	. 251
IBM Redbooks	. 251
Online resources	. 251
Help from IBM	. 252

viii Implementing a VersaStack Solution with IBM Storwize V5030, Cisco UCS Mini, Hyper-V, and SQL Server

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® C3® DS8000® Easy Tier® FlashCopy® Global Technology Services® HyperSwap® IBM® IBM FlashSystem® IBM Spectrum™ IBM Spectrum Control™ IBM Spectrum Protect™ IBM Spectrum Storage™ IBM Spectrum Virtualize™ POWER® Real-time Compression™ Redbooks® Redbooks (logo) @® Storwize® System Storage® 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® V9000 and IBM Storwize® 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 Storwize V5000 Gen2, 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 Storwize V5000 Gen2 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 Storwize V5000 Gen2 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 Storwize, 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 Storwize 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 Storwize V7000. His areas of expertise include planning, configuring, and troubleshooting DS8000, IBM Spectrum Virtualize and IBM Storwize 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" on page 2
- ▶ 1.2, "The VersaStack solution described in this book" on page 2
- ► 1.3, "VersaStack synopsis" on page 2
- ▶ 1.4, "Common VersaStack use cases" on page 3
- ► 1.5, "Optional and complementary products" on page 5
- ▶ 1.6, "Assumptions made in this book" on page 7
- ► 1.7, "For more information" on page 8

1.1 Overview

VersaStack is an innovative, validated design combining IBM Storwize 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 reliability, 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 Storwize V5030.The Cisco UCS Mini is a medium performance version of the UCS. The IBM Storwize V5030 is a mid-range storage array. The hypervisor installed is Hyper-V, and the software installed includes Microsoft SQL Server.

In this design, the Cisco UCS Mini and IBM Storwize V5030 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 Storwize V5030 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.

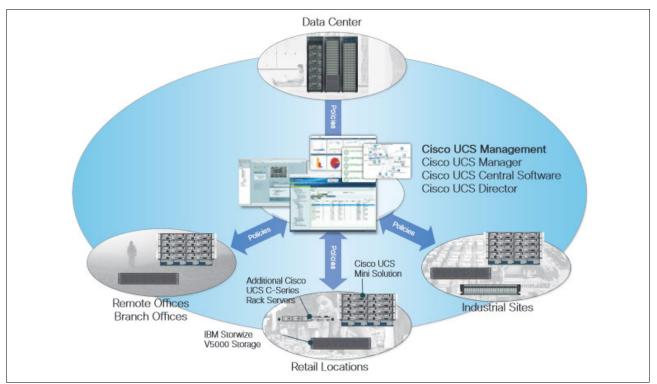


Figure 1-1 VersaStack as a remote and branch office solution

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.

Compute (UCS)	Network (Nexus and MDS)	Storage (Storwize & AllFlash)
Fabric Interconnect	Nexus 9372	Storwize V5000
		- Standard Constant - Storwize V7000
		-
	Nexus 9336	
C220 M4	MDS 9396S	AllFlash V9000
		SAN Volume Controller
	MDS 9148S	SAN VOIUME COntroller

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.

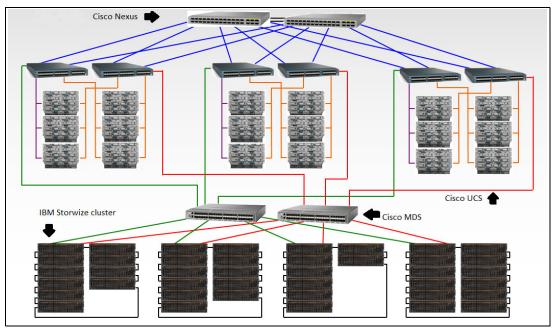


Figure 1-3 VersaStack design ready for a hypervisor for the private cloud

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.

	Cisco CloudCenter	
vCenter		SDX API
ultalla cisco UCS Servers	aluilo Nexus Switches	
IBM Spectrum Virtualize CDM	dialis MDS Switches	BM Bluemix"
SAN Volume IBM. Controller	torwize FlashSystem	Amazon Web Services (AWS)
VersaStack	Data Center	Public Clouds

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.

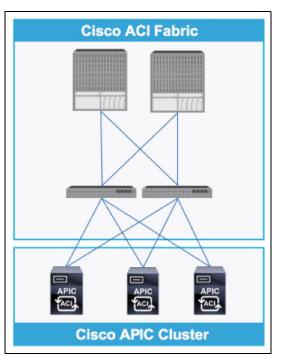


Figure 1-5 depicts the Cisco ACI Fabric design.

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 Storwize V5030 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 Storwize V5030 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" on page 10
- ► 2.2, "Software versions" on page 12
- ► 2.3, "Configuration guidelines" on page 12
- ► 2.4, "VersaStack cabling" on page 17
- ▶ 2.5, "Microsoft SQL Server on the VersaStack architecture" on page 20

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.

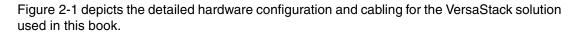
2.1.1 Physical topology

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 Storwize V5030 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.



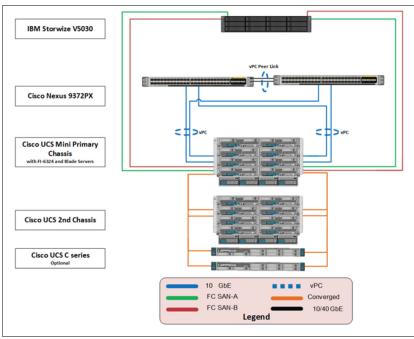


Figure 2-1 Hardware configuration and cabling for the VersaStack solution used in this book

An IBM Storwize V5030 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 Storwize V5030, 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 Storwize V5030 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.

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)14(7)	Operating system version
Storage	IBM Storwize V5030	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

Table 2-1 Software versions

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.

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 2-2 VLANs used in this solution

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>></var_node01_mgmt_ip>	Out-of-band management IP for V5000 node 01	
< <var_node01_mgmt_mask>></var_node01_mgmt_mask>	Out-of-band management network netmask	
< <var_node01_mgmt_gateway>></var_node01_mgmt_gateway>	Out-of-band management network default gateway	
< <var_node02_mgmt_ip>></var_node02_mgmt_ip>	Out-of-band management IP for V5000 node 02	
< <var_node02_mgmt_mask>></var_node02_mgmt_mask>	Out-of-band management network netmask	
< <var_node02_mgmt_gateway>></var_node02_mgmt_gateway>	Out-of-band management network default gateway	
< <var_cluster_mgmt_ip>></var_cluster_mgmt_ip>	Out-of-band management IP for V5000 cluster	
< <var_cluster_mgmt_mask>></var_cluster_mgmt_mask>	Out-of-band management network netmask	
< <var_cluster_mgmt_gateway>></var_cluster_mgmt_gateway>	Out-of-band management network default gateway	
< <var_password>></var_password>	Global default administrative password	
< <var_dns_domain_name>></var_dns_domain_name>	DNS domain name	
< <var_nameserver_ip>></var_nameserver_ip>	DNS server IP or IPs	
< <var_timezone>></var_timezone>	VersaStack time zone (for example, America/New_York)	
< <var_global_ntp_server_ip>></var_global_ntp_server_ip>	NTP server IP address	
< <var_email_contact>></var_email_contact>	Administrator email address	
< <var_admin_phone>></var_admin_phone>	Local contact number for support	
< <var_mailhost_ip>></var_mailhost_ip>	Mail server host IP	
< <var_country_code>></var_country_code>	Two-letter country code	
< <var_state>></var_state>	State or province name	
< <var_city>></var_city>	City name	
< <var_org>></var_org>	Organization or company name	
< <var_unit>></var_unit>	Organizational unit name	
< <var_street_address>></var_street_address>	Street address for support information	
< <var_contact_name>></var_contact_name>	Name of contact for support	
< <var_admin>></var_admin>	Secondary Admin account for storage login	
< <var_nexus_a_hostname>></var_nexus_a_hostname>	Cisco Nexus A host name	
< <var_nexus_a_mgmt0_ip>></var_nexus_a_mgmt0_ip>	Out-of-band Cisco Nexus A management IP address	
< <var_nexus_a_mgmt0_netmask>></var_nexus_a_mgmt0_netmask>	Out-of-band management network netmask	

Variable	Description	Implementation value
< <var_nexus_a_mgmt0_gw>></var_nexus_a_mgmt0_gw>	Out-of-band management network default gateway	
< <var_nexus_b_hostname>></var_nexus_b_hostname>	Cisco Nexus B host name	
< <var_nexus_b_mgmt0_ip>></var_nexus_b_mgmt0_ip>	Out-of-band Cisco Nexus B management IP address	
< <var_nexus_b_mgmt0_netmask>></var_nexus_b_mgmt0_netmask>	Out-of-band management network netmask	
< <var_nexus_b_mgmt0_gw>></var_nexus_b_mgmt0_gw>	Out-of-band management network default gateway	
< <var_ib-mgmt_vlan_id>></var_ib-mgmt_vlan_id>	In-band management network VLAN ID	
< <var_native_vlan_id>></var_native_vlan_id>	Native VLAN ID	
< <var_lvmn_vlan_id>></var_lvmn_vlan_id>	Windows Live Migration VLAN ID	
< <var_cluster_vlan_id>></var_cluster_vlan_id>	Windows Cluster VLAN ID	
< <var_vm-traffic_vlan_id>></var_vm-traffic_vlan_id>	VM traffic VLAN ID	
< <var_nexus_vpc_domain_id>></var_nexus_vpc_domain_id>	Unique Cisco Nexus switch VPC domain ID	
< <var_ucs_clustername>></var_ucs_clustername>	Cisco UCS Manager cluster host name	
< <var_ucsa_mgmt_ip>></var_ucsa_mgmt_ip>	Cisco UCS Fabric Interconnect A out-of-band management IP address	
< <var_ucs_mgmt_mask>></var_ucs_mgmt_mask>	Out-of-band management network netmask	
< <var_ucs_mgmt_gateway>></var_ucs_mgmt_gateway>	Out-of-band management network default gateway	
< <var_ucs_cluster_ip>></var_ucs_cluster_ip>	Cisco UCS Manager cluster IP address	
< <var_ucsb_mgmt_ip>></var_ucsb_mgmt_ip>	Cisco UCS Fabric Interconnect B out-of-band management IP address	
< <var_cimc_mask>></var_cimc_mask>	Out-of-band management network netmask	
< <var_cimc_gateway>></var_cimc_gateway>	Out-of-band management network default gateway	
< <var_ftp_server>></var_ftp_server>	IP address for FTP server	
< <var_utc_offset>></var_utc_offset>	UTC time offset for your area	
< <var_vsan_a_id>></var_vsan_a_id>	VSAN ID for FC FI-A (101 is used)	
< <var_vsan_b_id>></var_vsan_b_id>	VSAN ID for FC FI-B (102 is used)	
< <var_fabric_a_fcoe_vlan_id>></var_fabric_a_fcoe_vlan_id>	Fabric ID for FCoE A (101 is used)	
< <var_fabric_b_fcoe_vlan_id>></var_fabric_b_fcoe_vlan_id>	Fabric ID for FCoE B (102 is used)	
< <var_in-band_mgmtblock_net>></var_in-band_mgmtblock_net>	Block of IP addresses for KVM access for UCS	
< <var_hyperv_host_infra_01_ip>></var_hyperv_host_infra_01_ip>	Windows Hyper-V host 01 in-band Mgmt IP	
< <var_lvmn_ip_host-01>></var_lvmn_ip_host-01>	LVMN VLAN IP address for Hyper-V host 01	
< <var_lvmn_mask_ host-01="">></var_lvmn_mask_>	LVMN VLAN netmask for Hyper-V host 01	
< <var_hyperv_hos t_infra_02_ip="">>></var_hyperv_hos>	VMware Hyper-V host 02 in-band Mgmt IP	

Variable	Description	Implementation value
< <var_lvmn_vlan_id_ip_host-02>></var_lvmn_vlan_id_ip_host-02>	LVMN VLAN IP address for Hyper-V host 02	
< <var_csv_vlan_id_mask_host-02>></var_csv_vlan_id_mask_host-02>	LVMN VLAN netmask for Hyper-V host 02	
< <var_cluster_ip_ host-01="">></var_cluster_ip_>	Cluster VLAN IP address for Hyper-V host 01	
< <var_cluster_mask_host-01>></var_cluster_mask_host-01>	Cluster VLAN netmask for Hyper-V host 01	
< <var_cluster_ip_host-02>></var_cluster_ip_host-02>	CSV VLAN IP address for Hyper-V host 02	
< <var_cluster_mask_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>></var_wwpn_fc_nodea-fabrica>	
FC_NodeA-fabricB	Switch B FC3	< <var_wwpn_fc_nodea-fabricb>></var_wwpn_fc_nodea-fabricb>	
FC_NodeB-fabricA	Switch A FC4	< <var_wwpn_fc_nodeb-fabrica>></var_wwpn_fc_nodeb-fabrica>	
FC_NodeB-fabricB	Switch B FC4	< <var_wwpn_fc_nodeb-fabricb>></var_wwpn_fc_nodeb-fabricb>	
HyperV-Host-infra-01-A	Switch A	< <var_wwpn_vm-host-infra-01-a>></var_wwpn_vm-host-infra-01-a>	
HyperV-Host-infra-01-B	Switch B	< <var_wwpn_vm-host-infra-01-b>></var_wwpn_vm-host-infra-01-b>	
HyperV-Host-infra-02-A	Switch A	< <var_wwpn_vm-host-infra-02-a>></var_wwpn_vm-host-infra-02-a>	
HyperV-Host-infra-02-B	Switch B	< <var_wwpn_vm-host-infra-02-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.

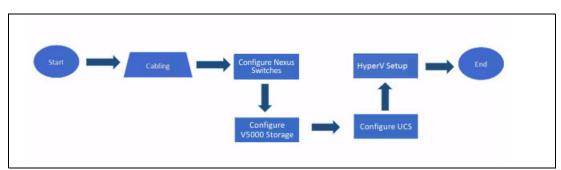


Figure 2-2 The process used to build the solution detailed in this book

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 Storwize V5030 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 Storwize V5030 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 18 illustrates the cabling diagrams for VersaStack configurations using the Cisco Nexus 9000 and IBM Storwize V5030. For SAS cabling information, connect the IBM Storwize V5030 control enclosure and expansion enclosure according to the cabling guide listed in IBM Knowledge Center.

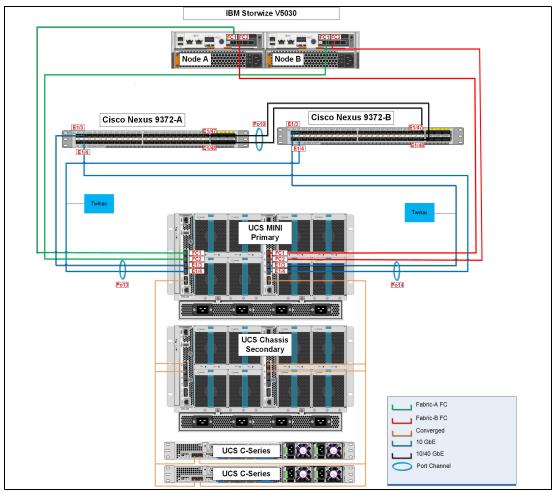


Figure 2-3 VersaStack cabling diagram

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 Storwize V5030 storage system that is used in the solution that is described in this book.

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 2-7 Cabling for Node A of the IBM Storwize V5030 storage system used in this solution

Table 2-8 lists the cabling for Node B of the IBM Storwize V5030 storage system that is used in the solution that is described in this book.

Table 2-8 Cabling for Node B of the IBM Storwize V5030 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.

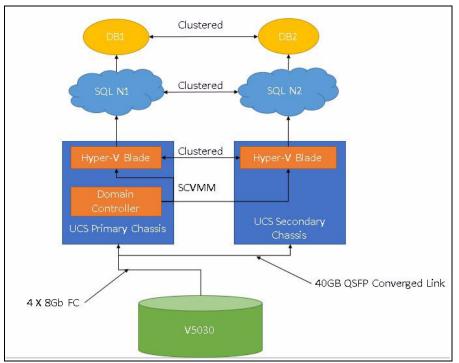


Figure 2-4 High-level architecture diagram of Microsoft SQL Server on VersaStack

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 Storwize V5030 storage controller. The UCS chassis is direct connected to the Storwize V5030 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 Storwize V5030 system, which is composed of an IBM Storwize V5030 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" on page 24
- ► 3.2, "Microsoft SQL Server design considerations" on page 25

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" on page 30
- 4.2, "Configuring the Cisco Nexus switch A" on page 30
- 4.3, "Configuring the Cisco Nexus switch B" on page 31
- 4.4, "Enabling the Cisco Nexus 9000 features and settings" on page 32
- ► 4.5, "Creating the VLANs for the VersaStack traffic" on page 33
- ► 4.6, "Configuring the Virtual PortChannel domain" on page 33
- 4.7, "Configuring the network interfaces for the vPC peer links" on page 34
- ▶ 4.8, "Configuring network interfaces to the Cisco UCS Fabric Interconnects" on page 36

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]:
```

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

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 (mgmtO) 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 <<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]:
```

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>>

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

role priority 10

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:

 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
```

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
```

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:

 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
```

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
```

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>>
```

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

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:

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:

 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>>
```

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
```

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
```

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:

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" on page 42
- ► 5.2, "VersaStack Cisco UCS base setup" on page 43
- ► 5.3, "Enabling the server and uplink ports in the Fabric Interconnects" on page 48
- ► 5.4, "Configuring UCS SAN connectivity" on page 60
- ► 5.5, "Configuring UCS LAN connectivity" on page 72
- 5.6, "Back up the Cisco UCS Manager configuration" on page 91

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 Storwize V5030 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]: yEnter 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 MgmtO IPv4 address: <<var ucsa mgmt ip>> Physical switch MgmtO 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 Storwize V5030 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.
- 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**.

Cisco Systems, Inc. will be collecting feature co	nfiguration and usage statistics which will be
sent to Cisco Smart Call Home server anonymou	
and improvements that will most benefit our cus	tomers.
If you decide to enable this feature in future, you	a can do so from the "Anonymous Reporting"
in the Call Home settings under the Admin tab.	
View Sample Data	
Do you authorize the disclosure of this inform	nation to Cisco Smart CallHome?
Yes No	
Don't show this message again.	

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.
- As shown in Figure 5-2 on page 45, click Pools → root → IP Pools ext-mgmt. Then, in the Actions pane, select Create Block of IPv4 Addresses.

UCS Manager	🛞 👽 🔔 🚸 0 46 1 32	• • • • • • • • •
← LAN → LAN Cloud	LAN / Pools / root / IP Pools / IP Pool ext-mgmt General IP Addresses IP Blocks Faults	Events
 Appliances Internal LAN Internal Fabric A Internal Fabric B Threshold Policies Policies Pools 	Actions Delete Create Block of IPv4 Addresses Create Block of IPv6 Addresses Create DNS Suffix Create IPV4 WINS Server Show Pool Usage	Properties Name : ext-mgmt Description : GUID : 0000000-0000-0000-00000000000 Size : 15 Assigned : 14 Assignment Order : : Default _ Sequential
root IP Pools IP Pool sct-mgmt IP Pool iSCSL_initiator_A IP Pool iSCSL_initiator_B		

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 \rightarrow Time Zone Management, as shown in Figure 5-3.

UCS Manager	😢 👽 么 📀 0 40 1 32
All All	All / Time Zone Management Time Zone Management + - + Export Print Name Timezone NTP Server 192.168.160.254
 Time Zone Management Timezone Capability Catalog License Management Device Connector 	

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.

192.168.160.254		
		Cancel
	192.168.160.254	192.168.160.254

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.

 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.

quipment							
Main Topology View	w Fabric Interconn	ects Servers	Thermal	Decommissioned	Firmware Manageme	ent Policies	Faults
Global Policies	Autoconfig Policies	Server Inheritanc	e Policies	Server Discovery Polic	sies SEL Policy	Power Groups	12
Chassis/FEX Disco	wery Policy						
Action	: 2 Link		*				
		0.0-+ 0					
Link Grouping Prefe							
Multicast Hardware	e Hash : 💿 Disab	led O Enabled					
Rack Server Disco	unn Dollou						
nauk derver DISCO	setà soncà						
Action : 💿	Immediate 🔿 User Ad	knowledged					
Scrub Policy :	not set> 🔻						
Rack Management	Connection Policy						
Action : Auto A	Acknowledged 🔘 Use	r Acknowledged					
Power Policy							
Redundancy :	Non Redundant N+	1 O Grid					
MAC Address Tabl	le Aging						
							Save Changes Reset Value

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.

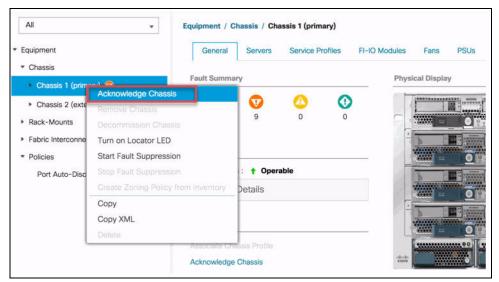


Figure 5-6 Acknowledge the UCS Mini chassis

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.

Ali	٠	Equipment	/ Fabric Interconne / Fabric In	sterconnec / Fixed Module / Ethernet Ports / Port 3 /
* Equipment		General	Faults Events FSM	Statistics
Chassis Rack-Mounts Servers Fabric Intercon Fabric Interco Fixed Mod	Configure as Server Port Configure as Server Port Configure as Uplink Port Configure as FCoE Uplin Configure as FCoE Stora Configure as Appliance I	k Port ige Port	mary 0 0 0	Physical Display
Etherner Port 1 Port 2 Port 2 Port 2	Uncentigure Unconfigure FCoE UoShi Unconfigure Uplink Port Unconfigure FCoE Store Unconfigure Appliance F		atus : 4 Admin Down Info : Administratively down Ite : Disabled	Up Admin Down Fail Link Down Properties ID : 4 Sior ID : 1
 Scalabi FC Ports 	ility Port 5	Enablis Pe Deutitie P Reconfigu Unconfigu Show Inte	urt ne *	User Label : MAC : 8C:60:4F:A3:D4:88 Mode : Access Port Type : Physical Role : Unconfigured Transceiver Type : H10GB CU3M Model : 1-2053783-2 Vendor : CISCO-TYCO

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** \rightarrow **root**.

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

▼ Servers	UUID Suffix Poo	ls		
 Service Profiles 	+ - 🏷 Ad	vanced Filter 🛉 Export	int Print	
 Service Profile Templates 	Name	Pool Name	UUID Prefix	From
 Policies 				
▼ Pools				
💌 root 👽				
 Server Pools 				
UUID Suffix Pools				
Sub-Organizations	JID Suffix Pool			
▼ Schedules				
▶ default				
 exp-bkup-outdate 				
▶ fi-reboot				
▶ infra-fw				

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.

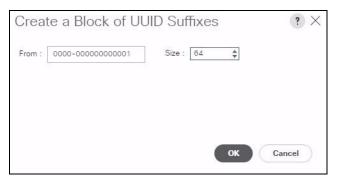


Figure 5-9 Add a block of UUIDs

11.Click OK.

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

All	Servers / Pools / root / UUID S	umx Poois			
Servers	UUID Suffix Pools				
 Service Profiles 	+ - 🏹 Advanced Filter 🔶 E	ixport 🚔 Print			¢
 Service Profile Templates 	Name	Pool Name	UUID Prefix	From	To
Policies	Pool default	default	3620136A-E47	2	
Pools	▼ Pool UUID_Pool	UUID_Pool	3620136A-E47		
💌 root 😗	[0000-0000000001 - 00	000-0000		0000-000000	0000-000000
 Server Pools 					
UUID Suffix Pools					
 Sub-Organizations 	_				
 Schedules 					
 default 					
Construction of the second					
 exp-bkup-outdate 					

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** \rightarrow **root**.
- 3. Right-click Server Pools and select Create Server Pool, as shown in Figure 5-11.

All	Servers / Pools / root /	Server Pools	
▼ Servers	Server Pools		
 Service Profiles 	+ - Ty Advanced Filter	r 🔶 Export 🚔 Print	
 Service Profile Templates 	Name	Size	Assigned
 Policies 	Server Pool default	0	0
▼ Pools			
🔻 root 👽			
Server Pools			
► UUID Suffix Pools	reate Server Pool		
 Sub-Organizations 			
 Schedules 			

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** \rightarrow **root**.
- Right-click Host Firmware Packages and select Create Host Firmware Package, as shown in Figure 5-12.

All	Servers / Poli Host Firmware	cies / root / Ho	st Firmwa			
 Service Profile Templates Policies 	2		Export 🚔 Print			¢
 root ♥ Adapter Policies 	Name	Туре	Vendor	Model	Presence	Version
 BIOS Defaults BIOS Policies Boot Policies Diagnostics Policies 						
 Graphics Card Policies Host Firmware Packages 	st Firmware Packaş	ne				
 IPMI Access Profiles KVM Management Policies Local Disk Config Policies 						
 Maintenance Policies Management Firmware Packages Memory Policy 			① Add	n Delete 👩 Info		
 Power Control Policies Power Sync Policies 						

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.

Description : Iow would you like to configure the Host Firmware Package? • Simple Advanced Blade Package : 3.2(1d)B * Rack Package : anot set> * Service Pack : enot set> * Service Pack : enot set> * The images from Blade or Rack Package Excluded Components: Adapter BloS Board Controller CMC FC Adapters Plax Flash Controller Plax Flash Controller BloS Blade of Rack Package	
Simple Advanced Blade Package : 3.2(1d)8 Rack Package : <not set=""> Service Pack : <not set=""> The images from Service Pack will take precedence over the images from Blade or Rack Package Excluded Components: Adapter BloS Board Controller CIMC FC Adapters Flex Flash Controller GPUs</not></not>	
Blade Package : 3.2(1d)B Rack Package : <not set=""> Service Pack : <not set=""> He images from Service Pack will take precedence over the images from Blade or Rack Package Excluded Components: Adapter BIOS Board Controller CIMC CAdapters Flex Flash Controller GPUs</not></not>	
Rack Package : <not set=""> Service Pack : <not set=""> He images from Service Pack will take precedence over the images from Blade or Rack Package Excluded Components: Adapter BIOS Board Controller CIMC CMC CAdapters Flex Flash Controller GPUs</not></not>	
Rack Package : <not set=""> Service Pack : <not set=""> He images from Service Pack will take precedence over the images from Blade or Rack Package Excluded Components: Adapter BIOS Board Controller CIMC CMC CAdapters Flex Flash Controller GPUs</not></not>	
Service Pack : <not set=""></not>	
he images from Service Pack will take precedence over the images from Blade or Rack Package Excluded Components: Adapter BIOS Board Controller CIMC CIMC Flox Flash Controller GPUs	
he images from Blade or Rack Package Excluded Components: Adapter BIOS Board Controller CIMC F6x Adapters Flash Controller GPUs GPUs	
CIMC FC Adapters Flex Flash Controller GPUs	
CIMC FC Adapters Flex Flash Controller GPUs	
Flex Flash Controller GPUs	
GPUs	
HBA Option ROM	
Host NIC	
Host NIC Option ROM	
✓ Local Disk	
PSU	
SAS Expander	

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** \rightarrow **root**.

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

All	Servers / Policies / root / Local D	isk Con	
Servers	Local Disk Config Policies		
Service Profiles	+ - Ty Advanced Filter 🛉 Exp	ort 🚔 Print	¢
 Service Profile Templates 	Name	Mode	
▼ Policies	default	Any Configuration	
🔻 root 😲			
 Adapter Policies 			
 BIOS Defaults 			
 BIOS Policies 			
 Boot Policies 			
 Diagnostics Policies 			
 Graphics Card Policies 			
 Host Firmware Packages 			
 IPMI Access Profiles 			
 KVM Management Policies 			
Local Disk Config Policies			
 Maintenance Policies 	e Local Disk Configuration Policy		
 Management Firmware Packages 			
 Memory Policy 			

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.

ctions	Properties	
elete	Name	SAN-Boot
how Policy Usage	Description	x
Use Global	Owner	: Local
	Mode	: No Local Storage
	FlexFlash	
	FlexFlash State	: Oisable C Enable
		ibled, SD cards will become unavailable immediately. are not in use before disabling the FlexFlash State.
	FlexFlash RAID Reportin	ng State : 💿 Disable 🔘 Enable

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** \rightarrow **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.

Name :	No-Power-Cap	
Description :		
Fan Speed Policy :	Any 🔻	
Power Capping		
	the server is allocated a certain amount of power ba	10 SANG CA CA SAN 1-40
within its power gro	the server is allocated a certain amount of power ba oup. Priority values range from 1 to 10, with 1 being p, the server is exempt from all power capping.	10 SANG CA CA SAN 1-40
within its power gro	bup. Priority values range from 1 to 10, with 1 being p, the server is exempt from all power capping.	10 SANG CA CA SAN 1-40

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** \rightarrow **root**.
- 3. Right-click Server Pool Policy Qualifications and select Create Server Pool Policy Qualification.

 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.

Create Server Pool P	olicy Qualification	? >
Naming		
Name : UCSB-B200-M5 Description :	will apply to new or re-discovered servers. Existing servers are not qualified until they are re-discovered	
Actions Create Adapter Qualifications	Qualifications + — ¬_v Advanced Filter + Export + Print	¢
Create Chassis/Server Qualifications	Name Max Model From To Architect Speed Stepping F	Power G
Create Memory Qualifications Create CPU/Cores Qualifications Create Storage Qualifications Create Server PID Qualifications Create Power Group Qualifications Create Rack Qualifications	No data available	
	🕀 Add 👔 Delete 🕕 Info	
	ОК Са	ncel

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** \rightarrow **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.

Create BIOS		
Name	: HyperV-Hosts	
Description	2	
Reboot on BIOS Settir	igs Change : 🔲	

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

Main	Advanced	Boot Op	ions	Server Managemer	nt Events			
Action	IS							
Delete								
Show	Policy Usage							
Prope	rties							
Name			: Hyp	erV-Hosts				
	intion							
Descr	iption		1					
Descr Owne			: : Loc	al				
Owne		tings Chang	: Loca	al				
Owne	r	tings Chang	: Loca	al				
Owne Reboo	r		: Loca	al				≎
Owne Reboo	r ot on BIOS Set		: Loca	al		Settings		¢
Owne Reboo Adva BIOS	r ot on BIOS Set inced Filter 4		: Loca	al			Ţ.	☆
Owne Reboo Adva BIOS	or ot on BIOS Set Inced Filter 4 Tokens	Export	: Loca	ai		Settings	<u>ष्</u> र 	\$
Owne Reboo Adva BIOS CDN Fron	r ot on BIOS Set inced Filter 4 Tokens I Control	Export	: Loca	al		Settings Enabled		\$
Owne Reboo BIOS CDN Fron POS	r ot on BIOS Set inced Filter Tokens I Control t panel lockou	Export	: Loca	al	_	Settings Enabled Platform Default) 	≎

Figure 5-19 Main properties of BIOS policy

- 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*.

Policies / root / BIOS Policies / HyperV-Hosts					
Main Advanced Boot Options Server Management Events					
Processor Intel Directed IO RAS Memory Serial Port USB PI	CI QPI LOM and PCIe Slots Trusted Platform Graphics Configuration				
Advanced Filter 🔶 Export 🖷 Print					
BIOS Tokens	Settings				
DRAM Clock Throttling	Performance *				
Direct Cache Access	Platform Default				
Energy Performance Tuning	Platform Default				
Enhanced Intel SpeedStep Tech	Platform Default				
Execute Disable Bit	Platform Default				
Frequency Floor Override	Enabled				
Intel HyperThreading Tech	Platform Default				
Intel Turbo Boost Tech	Platform Default				
Intel Virtualization Technology	Platform Default				
Channel Interleaving	Platform Default				
IMC Inteleave	Platform Default				
Memory Interleaving	Platform Default				
Rank Interleaving	Platform Default				
Sub NUMA Clustering	Platform Default				
Local X2 Apic	Platform Default				
Max Variable MTRR Setting	Platform Default				
P STATE Coordination	Platform Default				
Package C State Limit	Platform Default				
Processor C State	Disabled				
Processor C1E	Platform Default				

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*.

fain Adv	Ivanced Boot Opt	ons	Server Management	Events			
Actions							
Delete							
Show Policy	/ Usage						
Use Global							
Properties							
Name		Hype	rV-Hosts				
Description		:					
Description							
Owner		: Loca	I				
Owner		: Loca	I				
Owner		: Loca	I				
Owner	BIOS Settings Change	: Loca	I				\$
Owner Reboot on E	BIOS Settings Change	: Loca	1		Settings		\$
Owner Reboot on E	BIOS Settings Change Filter 🛧 Export 🚔 Is	: Loca				¥.	\$
Owner Reboot on B // Advanced F BIOS Token	BIOS Settings Change Filter 🔶 Export 👼 15 trol	: Loca			Settings	¥. ¥.	\$
Owner Reboot on B Advanced F BIOS Token CDN Contr	BIOS Settings Change Filter + Export -	: Loca			Settings Enabled		\$
Owner Reboot on B Advanced F BIOS Token CDN Contri Front pane	BIOS Settings Change Filter	: Loca			Settings Enabled Platform Default	₹	\$

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.

Main Advanced Boot Options Server Management Event	s						
Processor Intel Directed IO RAS Memory Serial Port USE	PCI	QPI	LOM and PCIe Slots	Trusted Platform	Graphics Configuration		
Advanced Filter 🕆 Export 🚔 Print							\$
BIOS Tokens			Settings				
DDR3 Voltage Selection			Platform Default			•	
DRAM Refresh Rate			Platform Default			X	
LV DDR Mode			Performance Mode			₹,	
Mirroring Mode			Platform Default			₹.	
NUMA optimized			Platform Default			Ψ.	
Memory RAS configuration			Platform Default			Ŧ	

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** \rightarrow **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**.

Actions	Properties		
Delete	Name Owner	: HyperV-Hosts : Local	
Show Policy Usage Jse Global		Round Robin C Linear Ordered	
	▼ Advanced Filter 🛉 Exp	ort 🖷 Print	¢
	Virtual Slot	Selection Preference	
	1	Assigned Only	
	2	All	
	3	All	
	4	All	

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** \rightarrow **root**.
- 3. Click Maintenance Policies \rightarrow default.
- 4. Change the Reboot Policy to User Ack. See an example in Figure 5-24.

Maintenance Polic	сy	
General Events		
Actions	Properties	
	Name	: default
Show Policy Usage	Description	i l
	Owner	: Local
	Soft Shutdown Timer	: 150 Secs 🔻
	Storage Config. Deployment Pol	licy : 🚫 Immediate 💿 User Ack
	Reboot Policy	: O Immediate
	✓ On Next B	oot (Apply pending changes at next reboot.)
		OK Cancel Help

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:

 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 61. Click Yes.

æ	All	Equipment / Fabric Interconnects / Fabric	Interconnect A (subordinate)	
Equipment	▼ Equipment	General Physical Ports Physical I	Display FSM Faults Events Neighbors	Statistics
Servers	Chassis Rack-Mounts Servers Fabric Interconnects	Fault Summary Image: Constraint of the second se	Physical Display	
LAN	 Fabric Interconnect A (subordinate) 	Status		
		Overall Status :	Up Admin Down Fail Link Down Properties Name : A Product Name : Cisco UCS 6324	
Storage		Actions	Vendor : Cisco Systems, Inc.	PID : UCS-FI-M-6324
		Configure Evacuation	Revision : 0	Serial : FCH19337NS1
		Configure Unified Ports	Available Memory : 4.894 (GB)	Total Memory : 7.869 (GB)
Chassis		Internal Fabric Manager LAN Uplinks Manager	\oplus Local Storage Information	
Admin		NAS Appliance Manager SAN Uplinks Manager	 Access 	

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.

Configure U	nified Ports		? >
	ider determines the type of the p		
		ports (Purple), while the ports to the right are Etherne	t ports (Blue).
		If Dala or Dart Channel Momhership	Desired If Dala
Port	Transport	If Role or Port Channel Membership	Desired If Role
		FC Storage	Desired If Role
Port FC Port 1	fc Transport		Desired If Role
Port FC Port 1 FC Port 2 Port 3	fc fc	FC Storage FC Storage	Desired If Role
Port FC Port 1 FC Port 2 Port 3	Transport fc fc ether	FC Storage FC Storage Ethernet Uplink Port Channel Member	Desired If Role
Port FC Port 1 FC Port 2	Transport fc fc ether	FC Storage FC Storage Ethernet Uplink Port Channel Member Ethernet Uplink Port Channel Member	Desired If Role
Port FC Port 1 FC Port 2 Port 3	Transport fc fc ether	FC Storage FC Storage Ethernet Uplink Port Channel Member Ethernet Uplink Port Channel Member	Desired If Role
Port FC Port 1 FC Port 2 Port 3	Transport fc fc ether	FC Storage FC Storage Ethernet Uplink Port Channel Member Ethernet Uplink Port Channel Member	Desired If Role
Port FC Port 1 FC Port 2 Port 3	Transport fc fc ether	FC Storage FC Storage Ethernet Uplink Port Channel Member Ethernet Uplink Port Channel Member	Desired If Role
Port FC Port 1 FC Port 2 Port 3	Transport fc fc ether	FC Storage FC Storage Ethernet Uplink Port Channel Member Ethernet Uplink Port Channel Member	Desired If Role

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.

a	All	Equipment / Fabric Interconnects / Fabric In	tterconnect A (primary)
Equipment	* Equipment	General Physical Ports Physical Dis	play FSM Faults Events Neighbors Statistics
0	Chassis	Actions	Product Name : Cisco UCS 6324 Vendor : Cisco Systems, Inc. PID : UCS-FI-M-6324
	 Rack-Mounts 		
Servers	Servers	Configure Evacuation	Revision : 0 Serial : FCH19337NS1
몲	 Fabric Interconnects 	Configure Unified Ports	Available Memory : 4.824 (GB) Total Memory : 7.869 (GB)
LAN	Fabric Interconnect A (primary)	Internal Fabric Manager	Local Storage Information
SAN SAN	 Fabric Interconnect B (subordinate) 	NAS Appliance Manager SAN Uplinks Manager	⊕ Access
0		SAN Storage Manager	🛞 High Availability Details
VM		Enable Ports Disable Ports Set Ethernet End-Host Mode Set Ethernet Switching Mode	(+) VLAN Port Count
			⊕ FC Zone Count
Storage		Set FC End-Heat Mode Set FC Switching Mode	Firmware
Chassis		Activate Firmware	Boot-loader Version : v1.022.0

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 63, 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.

Create Storage VSAN	; ×
Name : VSAN_A	
FC Zoning Settings	
FC Zoning : Olisabled Enabled	
Do NOT enable local zoning if fabric interconnect is connected	ed to an upstream FC/FCoE switch.
○ Common/Global ● Fabric A ○ Fabric B ○ Both Fabrics C You are creating a local VSAN in fabric B that maps to a VSAN ID that exists only in fabric B.	Configured Differently A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.
Enter the VSAN ID that maps to this VSAN.	Enter the VLAN ID that maps to this VSAN.
VSAN ID: 101	FCoE VLAN : 101
	OK Cancel

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.

Create Storage VSAN	? ×
Name : VSAN_B	
FC Zoning Settings	
FC Zoning : Olisabled Enabled	
Do NOT enable local zoning if fabric interconnect is connected	d to an upstream FC/FCoE switch.
◯ Common/Global ◯ Fabric A ④ Fabric B ◯ Both Fabrics C	Configured Differently
You are creating a local VSAN in fabric B that maps to a VSAN ID that exists only in fabric B.	A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.
Enter the VSAN ID that maps to this VSAN.	Enter the VLAN ID that maps to this VSAN.
VSAN ID: 102	FCoE VLAN : 102
	OK Cancel

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:

- 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.

Port 4 + Scalabil		Admin State : Disabled		
* FC Ports	E	Enable Port		
FC Port				
FC Po	Enable	pre las Uplice. Port		
Fabric Interco		ure as FC Storage Port		
		Interface		
	Configure as FC Storage Po	α		
	Сору			
	Copy XML			
		L.		

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**.
- 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** \rightarrow **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.
- Keep the default block of WWNNs, or specify a base WWNN.
- 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 65. Then, click OK.

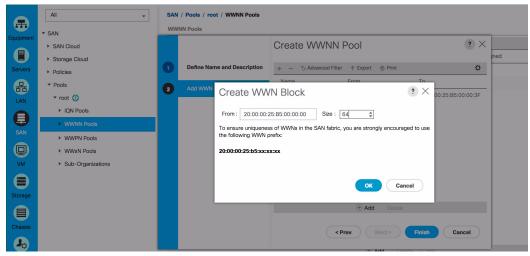


Figure 5-31 Create WWNN block

10.Click Finish.

Figure 5-32 shows the properties of WWNN created.

Properties f	or: [20:00:00:25:B5:00:00:00 -	X
20:00:00:25	5:B5:00:00:3F]	
General Even	its	
Actions	Properties	
Delete	From : 20:00:00:25:B5:00:00:00	
2439-82 202 min	To : 20:00:00:25:B5:00:00:3F	
	OK Cancel Help	2

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** \rightarrow **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.

	All	SAN	/ Pools / root / WWPN Pools		
	▼ SAN	ww	PN Pools		
Equipment	SAN Cloud			Create WWPN Pool	? ×
0	Storage Cloud				ined
Servers	Policies	0	Define Name and Description	Name : WWPN_Pool_A	
品	▼ Pools	2	Add WWN Blocks	Description :	
LAN	🔻 root 🕔			Assignment Order : Default Sequential 	
8	IQN Pools				
SAN	WWNN Pools				
	WWPN Pools				
	WWxN Pools				
VM	 Sub-Organizations 				
Storage					
Chassis					
				< Prev Next > Finish	Cancel
40				(+) Add 👘 Delete 🤲 Into	_

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.

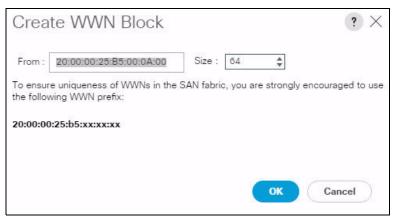


Figure 5-34 Creating the WWN Block

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.

- 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.

General	Events
Actions	Properties
Delete	From : 20:00:00:25:B5:01:0A:00
	To : 20:00:00:25:B5:01:0A:3F

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.

All • SAN	SAN / Pools / root / WWPN Pools WWPN Pools	
 SAN Cloud 	+ - 🏷 Advanced Filter 🛧 Export 🚔 Print	
 Storage Cloud 	Name	Size
 Policies 	WWPN Pool default	0
▼ Pools	WWPN Pool WWPN_Pool_A	64
🔹 root 👽	[20:00:00:25:B5:01:0A:00 - 20:00:00:25:B5:01:0A:3F]	
 IQN Pools 	WWPN Pool WWPN_Pool_B	64
 WWNN Pools 	[20:00:00:25:B5:01:0B:00 - 20:00:00:25:B5:01:0B:3F]	
WWPN Pools		
 WWxN Pools 		
 Sub-Organizations 		

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** \rightarrow **root**.
- 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 69:
 - 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.

Create vHBA	Template	? ×
Name	: vHBA_Template_A	
Description	2	
Fabric ID	: • A O B	
Redundancy		
Redundancy Type	: No Redundancy Primary Template Secondary Template	
Select VSAN	: VSAN_A v Create VSAN	
Template Type	: 🔘 Initial Template 💿 Updating Template	
Max Data Field Size	: 2048	
WWPN Pool	: WWPN_Pool_A(53/64) V	
QoS Policy	: <not set=""> V</not>	
Pin Group	: <not set=""></not>	
Stats Threshold Policy	: default 🔻	
	ОК	Cancel

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** \rightarrow **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 70:
 - 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.

Create vHBA	Template	? ×
Name	: vHBA_Template_B	
Description	3	
Fabric ID Redundancy	E ○A ⊙ B	20
Redundancy Type	: O No Redundancy O Primary Template O Secondary Template	
Select VSAN	: VSAN_B Create VSAN	
Template Type	: 🔘 Initial Template 💿 Updating Template	
Max Data Field Size	: 2048	
WWPN Pool	: WWPN_Pool_B(53/64) 🔻	
QoS Policy	: <not set=""> V</not>	
Pin Group	<pre>< <not set=""> </not></pre>	
Stats Threshold Policy	r: default 🔻	
	ОК С	ancel

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 Storwize V5030 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 Storwize V5030 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.

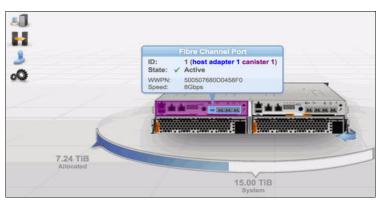


Figure 5-39 Visualizing WWPN of IBM Storwize FC ports

Use Table 5-1 to record the WWPN information.

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

Table 5-1 IBM Storwize V5030 WWPN information

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** \rightarrow **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.

Name :	Boot-Fabric-A	*										
Description :												
Reboot on Boot Order Change :	0											
Enforce vNIC/vHBA/iSCSI Name :												
Boot Mode :	Legacy	Uefi										
The type (primary/secondary) does The effective order of boot devices if Enforce vNIC/vHBA/ISCSI Name if it is not selected, the vNICs/vHBA	within the sam is selected and is are selected	e device d the vNI	class (LAN/Storag IC/vHBA/ISCSI doe xist, otherwise the	es not exis	t, a config e	error will b	e reported.		ed.			
See more	4		Ty Advanced Filter	+ Export	t 💮 Print							<
Add Local Disk	-	Name		Or +	vNIC/	Туре	WWN	LUN N.	Slot N	Boot	Boot	Descr
Add Local LUN	-	CD/DV	(D	1								
Add Local JBOD		00/04	0	<u>.</u>								
Add SD Card												
Add Internal USB												
Add External USB												
Add Embedded Local LUN												
Add Embedded Local Disk												
					1 Move	n Np 👎 1	Move Down	Deleti	8));			
Add Local CD/DVD												
Add Remote CD/OVD												
Add Floppy												
Add Floppy Add Local Floppy												

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.

Add	SAN Boot	? ×
VHBA :	Fabric-A	
Type :	Primary Secondary Any	

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.

Add SAN Bo	ot Target	? ×
		. A
Boot Target WWPN :	50:05:07:68:0D:04:58:F0	

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**.

		Create Port Channel
0	Set Port Channel Name	ID : 13
2	Add Ports	Name: VPC-13-Nexus
		Next > Finish Cancel

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.

2	Set Port Channel Name		P	orts				Ports in the	port char	nel
	Add Ports	Slot ID	Aggr. Po	Port	MAC		Slot ID	Aggr. Po	Port	MAC
1		-	No data	available			1	0	3	8C:60:4
						2.2	1	0	4	8C:60:4
						ec.				

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 $\text{LAN} \rightarrow \text{LAN}$ 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.

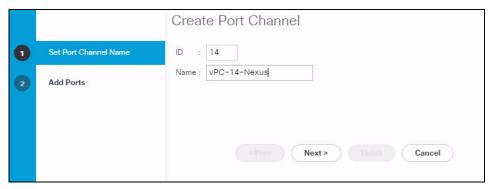


Figure 5-45 Set Port Channel Name

- 4. Select the following ports to be added to the port channel:
 - Slot ID 1 and port 3
 - Slot ID 1 and port 4
- 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** \rightarrow **root**.

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

- 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**.

		Create MAC Pool ?	Х
0	Define Name and Description	Name : MAC_Pool_A	
2	Add MAC Addresses	Description : Assignment Order : ① Default ○ Sequential	
		Next > Finish Cancel	

Figure 5-46 Creating a new MAC pool

 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.
- Enter MAC_Pool_B as the name of the MAC pool, and enter a description for the MAC pool (optional). Then, click Next.
- 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.

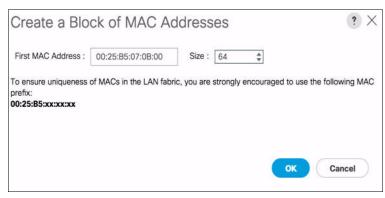


Figure 5-48 Adding a MAC address size pool (2)

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.

+ - 🏹 Advanced Filter 🔶 Exp	port 🖷 Print	
Name	Size	Assigned
MAC Pool default	0	0
MAC Pool MAC_Pool_A	32	15
[00:25:B5:07:0A:00 - 00:25:B	35:	
MAC Pool MAC_Pool_B	32	15

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.
- 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.

Create VLANs	Ĺ			Create VLANs	? ×
VLAN Name/Prefix :	IB-MGMT-VLAN				
Multicast Policy Name :	<not set=""></not>	Create Multicast	t Policy		
You are creating global VI Enter the range of VLAN I VLAN IDs : 11	abric A () Fabric B () Both F LANs that map to the same VI Ds.(e.g. * 2009-2019*, * 29,3 e () Primary () Isolated ()	LAN IDs in all available fabrics 35,40-45" , " 23" , " 23,34-45	s.		
			Check Overlap	ОК Са	ncel

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.
- 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.
- 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.
- 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 \rightarrow LAN Cloud \rightarrow 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.

General E	vents FSN	1					
Actions		Properties					
Jse Global		Owner : Local					
Priority	Enabled	CoS	Packet Drop	Weight		Weight (%)	МТU
Platinum		5		10	T	N/A	normal
Gold		4		9	v	N/A	normal
Silver		2		8	T	N/A	normal
Bronze		1		7	v	N/A	normal
Best Effort		Апу	()	5	T,	50	9216
Fibre Channel	1	3		5	v	50	fc

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** \rightarrow **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.

Name :	Enable_CDP	
Description :		
CDP :	Olisabled Enabled	
MAC Register Mode :	Only Native Vlan All Host Vlans	
Action on Uplink Fail :	● Link Down ◯ Warning	
MAC Security		
Forge : Allow	Deny	
1100		
LLDP		

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** \rightarrow **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.

Name	: vNIC-Ho	ost-A		
Description	:			
Fabric ID Redundancy	: 🖲 Fa	abric A	○ Fabric B	Enable Failover
Redundancy Ty	ре : 🖸	No Redundancy (Primary Template Secondary	Template
Peer Redundan	v Template :			
Peer Redundan	cy Template :	<not set=""> V</not>		
	cy Template :	<not set=""> ¥</not>		
arget Adapter	cy Template :	<not set=""> V</not>		

Figure 5-53 Creating the vNIC template

- 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.

		VLAN Groups	VLANS
	Print	d Filter 🔶 Export 👘 Pr	▼ Advanced
Native VLAN	Name		Select
۲	IB-MGMT-VLAN		~
0	MS-Cluster-VLAN		~

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** again.

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

- 1. In the navigation pane, go to the LAN tab.
- 2. Click **Policies** \rightarrow **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.

Description	3			
Redundancy	: 0	Fabric A	Fabric B	Enable
Redundancy Type Peer Redundancy arget Adapter VM		No Redundancy	Primary Template Secondary	Template
Warning				
If VM is selected, a		by the same name will ne exists, and updating	be created. template is selected, it will be over	rwrit

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 \rightarrow Policies \rightarrow 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.

Jame : 00-Host-A	
Jse vNIC Template : 🛃	
Redundancy Pair :	Peer Name :
NIC Template : vNIC-Host-A *	Create vNIC Template
Adapter Performance Proñie	
Adapter Policy : Windows *	Create Ethernet Adapter Policy

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

- 7. Click OK to add this vNIC to the policy.
- 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.

Create vNIC		? ×
Name : 01-Host-B		
Use vNIC Template : 🗹		
Redundancy Pair :	Peer Name :	
vNIC Template : vNIC-Host-B •	Create vNIC Template	
Adapter Performance Profile		
Adapter Policy : Windows •	Create Ethernet Adapter Policy	

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.

Mama	It was to LAN ON	
Name :	HyperV-LAN-CP	
Description :		
lick Add to sp	pecify one or more vNICs th	hat the server should use to connect to the LAN
Name		MAC Address
Name vNIC 01-F	lost-B	

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 \rightarrow 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 Storwize V5030, Node 1 on Fabric A.
 - b. Select the **Updating Template** option.
 - c. Under UUID, select the UUID_Pool as the UUID pool.

		Create Service Profile Template	? ×		
1	Identify Service Profile Template	You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to the template and enter a description.	his		
2	Storage Provisioning	Name : HyperV-Host-Infra			
3	Networking	The template will be created in the following organization. Its name must be unique within this organization. Where : org-root			
4	SAN Connectivity	he template will be created in the following organization. Its name must be unique within this organization. Type : Initial Template Outpdating Template Specify how the UUID will be assigned to the server associated with the service generated by this template.			
5	Zoning				
6	vNIC/vHBA Placement	UUID Assignment: UUID_Pool(26/32)			
7	vMedia Policy	The UUID will be assigned from the selected pool. The available/total UUIDs are displayed after the pool name.			
8	Server Boot Order				
9	Maintenance Policy	Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used	ι.		
10	Server Assignment				
11	Operational Policies				
		< Prov Next > Finish Can	cel		

Figure 5-59 Identify the service profile template

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

 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.

		Create Service Profile Template					
0	Identify Service Profile Template	Optionally specify or create a Storage Profile, and select a local disk configuration policy.					
		Specific Storage Profile Storage Profile Policy Local Disk Configuration Policy					
2	Storage Provisioning	Local Storage: SAN-Boot V					
3	Networking	Select Local Storage Policy to use					
~		Create Loca Create a Specific Storage Policy Protect Configuration Yes					
0	SAN Connectivity	Storage Policies If Protect Configuration is set, the local disk configuration is preserved if the service profile is disassociated					
5	Zoning	SAN-Boot with the server. In that case, a configuration error will be raised when a new service profile is associated with					
		Test that server if the local disk configuration in that profile is					
6	vNIC/vHBA Placement	default different. FlexFlash					
0	vMedia Policy	FlexFlash State : Disable If FlexFlash State is disabled, SD cards will become unavailable immediately.					
8	Server Boot Order	Please ensure SD cards are not in use before disabling the FlexFlash State. FlexFlash RAID Reporting State : Disable					
0	Maintenance Policy						
10	Server Assignment						
0	Operational Policies						
		< Prev Next > Finish	Cancel				

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.

		Create Service Profile Template ?			
0	Identify Service Profile	Optionally specify LAN configuration information.			
	Template Storage Provisioning	Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by default) *			
2	Storage Provisioning	Create Dynamic vNIC Connection Policy			
3	Networking				
4	SAN Connectivity	How would you like to configure LAN connectivity?			
5	Zoning	LAN Connectivity Policy : HyperV-LAN-CP Create LAN Connectivity Policy			
6	vNIC/vHBA Placement	Initiator Name Initiator Name Assignment: <pre><not set=""> </not></pre>			
7	vMedia Policy	Create IQN Suffix Pool			
8	Server Boot Order	WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.			
9	Maintenance Policy				
10	Server Assignment				
1	Operational Policies				
		< Prev Next > Finish Ca	ncel		

Figure 5-61 Create the service profile template

- 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**.

<u>.</u>		Create Service Profile Template	X				
1	Identify Service Profile	Optionally specify disk policies and SAN configuration information.					
	Template	How would you like to configure SAN connectivity?	Ĩ				
2	Storage Provisioning	○ Simple					
3	Networking	A server is identified on a SAN by its World Wide Node Name (WWNN). Specify how the system should assign a WWNN to the server associated this profile. World Wide Node Name	witr				
0	SAN Connectivity	WWNN Assignment: WWNN Pool(56/64)					
6	Zoning	www.casymenc.					
6	vNIC/vHBA Placement	The WWNN will be assigned from the selected pool. The available/total WWNNs are displayed after the pool name.					
0	vMedia Policy						
8	Server Boot Order						
0	Maintenance Policy						
10	Server Assignment						
0	Operational Policies	Name WWPN No data available					
		< Prev Next > Finish Cancel	\supset				

Figure 5-62 SAN Connectivity for Service Profile

- 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.

Create vHBA		? ×
Name : Fabric-A		
Use vHBA Template : 🗹		
Redundancy Pair :	Peer Name :	
vHBA Template : vHBA_Template_A 🔻	Create vHBA Template	
Adapter Performance Profile		
Adapter Policy : Windows 🔻	Create Fibre Channel Adapter Policy	
	ОК	Cancel

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.

		Create Service Pro	ofile Template ? ×
0	Identify Service Profile	Optionally specify disk policies a	and SAN configuration information.
	Template	WWNN Assignment:	WWNN_Pool(56/64)
2	Storage Provisioning		
3	Networking	The WWNN will be assigne The available/total WWNNs	ed from the selected pool. s are displayed after the pool name.
0	SAN Connectivity		
5	Zoning		
6	vNIC/vHBA Placement		
0	vMedia Policy	Name	WWPN
8	Server Boot Order	vHBA Fabric-B	Derived
9	Maintenance Policy	vHBA If default	
		▼ vHBA Fabric-A	Derived
10	Server Assignment	vHBA If default	
11	Operational Policies		
			Delete (1) Add (1) Modify
			< Prev Next > Finish Cancel

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 87. Click Next for vNIC/vHBA Placement.

		Create Service Pro	file Template		(? ×
0	Identify Service Profile	Specify zoning information				
Template Storage Provisioning		Zoning configuration involves the 1 1. Select vHBA Initiator(s) (vHi 2. Select vHBA Initiator Group 3. Add selected Initiator(s) to s	BAs are created on storage page) s)			
3	Networking	Select vHBA initiators		Select vHBA Initiator	Groups	
	SAN Connectivity	Name		Name	Storage Connection Policy Na	ame
6	Zoning	Fabric-A	>> Add To >>		No data available	
6	vNIC/vHBA Placement	Fabric-B				
0	vMedia Policy					
8	Server Boot Order				Delete Add Modify	
9	Maintenance Policy					
10	Server Assignment					
0	Operational Policies					
				< Prev	Next > Finish Cance	ł)

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.

		Create Service Profile Template	? ×
0	Identify Service Profile	Optionally specify the boot policy for this service profile template.	
	Template	Select a boot policy.	
2	Storage Provisioning	Boot Policy: Boot-fabric-A V Create Boot Policy	
3	Networking	Name : Boot-fabric-A Description :	
0	SAN Connectivity	Reboot on Boot Order Change : No Enforce vNIC/VHBA/ISCSI Name : Yes	
5	Zoning	Boot Mode : Legacy WARNINGS: The type (primary/secondary) does not indicate a boot order presence.	
6	vNIC/vHBA Placement	The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order. If Enforce vNIC/VHBA/ISCSI Name is selected and the vNIC/VHBA/ISCSI does not exist, a comfg error will be reported. If it is not selected, the vNIC/SVHBA as elected if they exist, otherwise the vNIC/VHBA with the lowest PCIe bus scan order is used.	
0	vMedia Policy	Boot Order + - Y _e Advanced Filter ↑ Export. ⊜ Print	¢
0	Server Boot Order		ription
0	Maintenance Policy	CD/DVD 1 > San 2	
10	Server Assignment		
Ð	Operational Policies		
		< Prev Next > Finish Cr	ancel

Figure 5-66 Server Boot Order

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

	Create Sen	vice Profile Template		?
Identify Service Profile Template	Specify how disrup service profile.	tive changes such as reboots, network in	terruptions, and firmware upgrades should be applied to the server asso	ciated with I
Storage Provisioning	 Maintenance 	e Policy		
1217 - 122			or create a new maintenance policy that will be accessible to all service	profiles.
Networking	Maintenance Policy:	Select (no policy used by default) 🔹	Create Maintenance Policy	
SAN Connectivity		Select (no policy used by default)		
		Domain Policies		
Zoning		default		
vNIC/vHBA Placement				
Server Boot Order				
Server Boot Order Maintenance Policy				
Maintenance Policy				
Maintenance Policy Server Assignment			< Prev Next> Finish	Cancel

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 89:
 - 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.

		Create Service P	Profile Te	mplate)	? ×
0	Identify Service Profile	Optionally specify a server pe	ool for this serv	ice profile te	mplate.	
	Template	You can select a server pool y	ou want to asso	ciate with th	is service profile template.	
2	Storage Provisioning	Pool Assignment: Infra_Pool	•	Create Se	rver Pool	
3	Networking			Select the with the se	power state to be applied when this profile is associated erver.	
4	SAN Connectivity			● Up (Down	
5	Zoning				of the servers in the selected pool.	
6	vNIC/vHBA Placement	If desired, you can specify an the list. Server Pool Qualification :		ver pool poli	cy qualification that the selected server must meet. To do so	i, select the qualification from
7	vMedia Policy	Restrict Migration :	<not set=""> <not set=""></not></not>]	
8	Server Boot Order	+ Firmware Managem	Domain Pol		er, Adapter)	
9	Maintenance Policy		UCSB-B20			
	Occurs Accimentation		all-chassis			
10	Server Assignment					
11	Operational Policies					
					< Prev Next >	Finish Cancel

Figure 5-68 Server assignment for the service profile

 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.

		Create Service Profile Template	? ×			
0	Identify Service Profile Template	Optionally specify information that affects how the system operates.				
2	Storage Provisioning	 BIOS Configuration If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile 				
3	Networking	BIOS Policy : HyperV-Hosts 🔻				
4	SAN Connectivity	⊕ External IPMI Management Configuration				
5	Zoning	Management IP Address				
6	vNIC/vHBA Placement	Monitoring Configuration (Thresholds)				
0	vMedia Policy	Power Control Policy Configuration				
8	Server Boot Order	Power control policy determines power allocation for a server in a given power group.				
9	Maintenance Policy	Power Control Policy: default Create Power Control Policy <not set=""></not>				
10	Server Assignment	Scrub Policy Domain Policies				
1	Operational Policies	KVM Managem				
		(+) Graphics Card Policy	Finish Cancel			

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 \rightarrow root \rightarrow Service Template HyperV-Host-Infra.
- 3. Right-click **HyperV-Host-Infra** and select **Create Service Profiles from Template**, as shown in Figure 5-70.

All	Servers / Service Profile Templa / root / Service			
▼ Servers	General Storage Network iSCSI vNICs			
 Service Profiles Service Profile Templates 	Actions			
 Service Profile Templates root () 	Create Service Profiles From Template			
 Service Template AAAAA 	Create a Clone			
 Service Template HyperV-Ho. 	Create Service Profiles From Template			
 Service Template Template-C 	Create a Clone			
 Service Template Test () 	Disassociate Template			
 Service Template Testinghhhł 	Associate with Server Pool			
 Service Template VM-Host-H 	Change UUID			
 Service Template VM-Host-In 	Change World Wide Node Name			
 Service Template VM-Host-In 	Change Local Disk Configuration Policy			
Service Template VM-Host-In	Change Dynamic vNIC Connection Policy			
 Service Template VM-Host-iS 	Change Serial over LAN Policy			
 Service Template VM-Host-Till 	Modify vNIC/vHBA Placement			
 Service remplate vivi-HOSt-11 	Copy			

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.

Create Service Profiles From Template $? \times$
Naming Prefix : HyperV-Host-Infra-0
Name Suffix Starting Number: 1
Number of Instances : 2
OK Cancel

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" on page 94
- 6.2, "Preparing the SAN Boot for Windows Server 2016" on page 94
- ► 6.3, "Preparing and performing SAN Boot" on page 96
- ► 6.4, "Provisioning IBM LUN as a SAN Boot volume" on page 97
- ► 6.5, "Setting up Microsoft Windows Server 2016" on page 99

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 Storwize V5030 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 Storwize V5030. 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 70.

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 Storwize V5030, you must add hosts and map the boot volumes on the IBM Storwize V5030:

- 1. Open the IBM Storwize V5030 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.

🗥 Versa	aStack_V5030 > Hosts > Hosts	IBM Storwi
	Add Host	х
	Required Fields Name: Host connections: Host port (WWPN): Optional Fields Host type: I/O groups: Host cluster:	Fibre Channel iSC SI Image: Comparison of the second of the sec
		Add Cancel

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 Storwize V5030.

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 Storwize V5030:

1. Log on to IBM Storwize V5030, click **Volumes** (from the left side menu), and then select **Volumes** as shown in Figure 6-2.

☆ VersaStack_V5030 > Monitoring > System
Actions 🛛 🔀
Volumes Volumes Volumes by Pool Volumes by Host

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.

Basic	Mirrored	Quick Volume Creation			Advanced —
Pool: Quantity: Ca 1 🗘	EasyTier_POOL pacity: 128 GiB	Capacity savings: None	Name: HYPERV-N1_OS	Total 15.0	0 TIB
I/O group:	Automatic	•			
1	ummary volume ⁄olume name: HYPERV-	N1_OS			
Need Help		Create Create	and Map Cancel		

Figure 6-3 Provisioning a new volume using IBM Storwize V5030 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.

Create Mapping					×
Create Mappings to:					
Hosts					
Host Clusters					
Select hosts to map to	oTest				
Q Filter				Showing 9 hosts Selecting 1 host	
Name 🔻	Status	Host Type	Host Mappings	IJ	
WIN-HYPERV-N1	✓ Online	Generic	Yes		
Would you like the sys	stem to assign SCSI L	UN IDs or manually	assign these IDs?		
System Assign					_
Self Assign					-
					annan <mark>an</mark>
		< Back	Next ►		Cancel

Figure 6-4 Creating a host cluster mapping

- Scroll down to select the SCSI ID assignment. When selecting System Assign, the IBM Storwize V5030 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.
- 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 100.

General	Storage	Network	iSCSI vNICs	Boot Order	Virtual Machines	FC Zones	Policies	Server Details	CIMC Sessions	FSM	VIF P
Global Boot P	Policy										
Name		: Boot-f	fabric-A								
Boot Policy In	nstance	: org-ro	ot/boot-policy-B	oot-fabric-A							
Description		:									
Reboot on Bo	oot Order Cha	nge : No									
Enforce vNIC;	/vHBA/iSCSI	Name : Yes									
/ARNINGS: he type (prim he effective o	order of boot (devices within t	icate a boot orde	lass (LAN/Storage							
VARNINGS: he type (prim he effective o Enforce vNI it is not selec	order of boot	y) does not ind devices within t I Name is sele	icate a boot orde the same device cted and the vNK		not exist, a config	error will be rep	ported.	used.			
VARNINGS: The type (prim The effective of Enforce VNIO it is not select	order of boot	y) does not ind devices within t i l Name is sele ss/vHBAs are so	icate a boot orde the same device cted and the vNIG elected if they ex	class (LAN/Storage C/vHBA/iSCSI does	not exist, a config	error will be rep	ported.	used.			
VARNINGS: he type (prim he effective o Enforce vNIC it is not selec oot Order	order of boot of C/vHBA/ISCS cted, the vNIC	y) does not ind devices within t il Name is selec is/vHBAs are so the Export	icate a boot orde the same device cted and the vNIG elected if they ex	class (LAN/Storage C/vHBA/iSCSI does	not exist, a config	error will be rep	ported.		Boot Path	Descri	
VARNINGS: the type (prim the effective of Enforce vNik it is not select toot Order + - Ty A	order of boot of C/vHBA/iSCS cted, the vNIC Advanced Filter	y) does not ind devices within t il Name is selec is/vHBAs are so the Export	icate a boot orde the same device cted and the vNK elected if they ex	class (LAN/Storage C/vHBA/iSCSI does ist, otherwise the vf	not exist, a config	error will be rep lowest PCle bu	ported. s scan order is		Boot Path	Descri	
VARNINGS: the type (prim the effective of Enforce vNI(it is not select the ot Order +	Order of boot of C/vHBA/ISCS cted, the vNIC Advanced Filter Order	y) does not ind devices within t il Name is selec is/vHBAs are so the Export	icate a boot orde the same device cted and the vNK elected if they ex	class (LAN/Storage C/vHBA/iSCSI does ist, otherwise the vf	not exist, a config	error will be rep lowest PCle bu	ported. s scan order is		Boot Path	Descrij	
The effective of Enforce vNIG Finforce vNIG f it is not select Boot Order + - Ty A Name CD/DVD	Advanced Filter	y) does not ind devices within t il Name is selec is/vHBAs are so the Export	Licate a boot orde the same device cted and the vNIG elected if they ex	class (LAN/Storage /vHBA/iSCSI does st, otherwise the vf	not exist, a config	error will be rep lowest PCle bu	ported. s scan order is		Boot Path	Descrij	ption

Figure 6-5 Boot Order details

- 3. To proceed with the Windows OS installation, return to the main menu, and click Servers.
- 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.
- 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.
- 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**.
- 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.

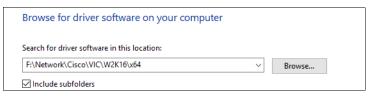


Figure 6-6 Browsing for the Cisco fNIC driver ISO

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.

🥥 🔩 Windows Setup	22
Select the driver to install	
Cisco VIC-FCoE Storport Miniport (C\\driver\fnic2k16.inf)	
Hide drivers that aren't compatible with this computer's hardware.	
Br <u>o</u> wse <u>R</u> escan	At

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 102. 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**.

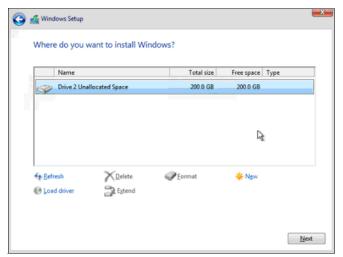


Figure 6-8 Selecting the LUN to install Windows

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** \rightarrow **Chipset** \rightarrow **"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** \rightarrow **Computer Management**. In the Computer Manager, select **System Tools** \rightarrow **Device Manager** \rightarrow **Other devices**.

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

Device Manager		
File Action View He	- F	
🗧 🔿 🛛 📰 🖉 🛛	📰 🖳 🖡 🗙 🖲	
VIN-R9N0Q4K0KKI-	4	
> 🗃 Batteries		
> 🔜 Computer		
> Disk drives		
> 🤜 Display adapters		
> 🔐 DVD/CD-ROM d	lrives	
> 📲 Floppy disk driv	es	
> 🐺 Human Interfac	e Devices	
> Keyboards		
> II Mice and other	pointing devices	
> 🤜 Monitors		
Other devices		
🚺 Ethernet 🛀		
🚺 Ethernet 🤇	Update Driver Software	
> 🧧 Portable Devi	Disable	
Ports (COM &	Uninstall	
> Image: Print queues		
> Processors	Scan for hardware changes	
> 🎥 Storage conti	Properties	
> bystem devic		
> Ü Universal Serial I	Bus controllers	

Figure 6-9 Updating driver software

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

ð	Dev	ice Ma	inager	и	
Fil	e /	Action	View	ew Help	
(m	nþ			🖬 📷 🖳 🖡 🗙 💿	
3		WIN-R Bat Cor Disl D	4	Update Driver Software - Cisco VIC Ethernet Interface Windows has successfully updated your driver software Windows has finished installing the driver software for this device: Cisco VIC Ethernet Interface	×
		Por Prir Prio Sto Sys			Close

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 Storwize V5030 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 Storwize V5030.

This chapter has the following sections:

- ► 7.1, "Introduction to Hyper-V Cluster for high availability" on page 106
- 7.2, "Physical topology for Hyper-V" on page 106
- > 7.3, "Microsoft Windows 2016 Failover Clustering feature requirements" on page 107
- ▶ 7.4, "Configuring features and tools for failover cluster nodes" on page 108
- ► 7.5, "Creating a host attachment in IBM Storwize V5030" on page 111
- ▶ 7.6, "Creating a host cluster in the IBM Storwize V5030" on page 113
- ▶ 7.7, "Provisioning IBM Storwize Volume for Cluster Shared Volumes" on page 115
- 7.8, "Rescanning and assigning the cluster shared volumes" on page 119
- 7.9, "Configuring the Failover Clustering feature" on page 121
- 7.10, "Adding the Hyper-V feature" on page 125
- ► 7.11, "Microsoft Virtual Machine Manager" on page 129
- 7.12, "Configuring the Hyper-V virtual network using Microsoft Virtual Machine Manager" on page 129
- ► 7.13, "Hardware profiles" on page 153
- 7.14, "Creating virtual machines using hardware profiles" on page 158

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 Storwize V5030 direct-attached through redundant Fabric Interconnects. The IBM Storwize V5030 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.

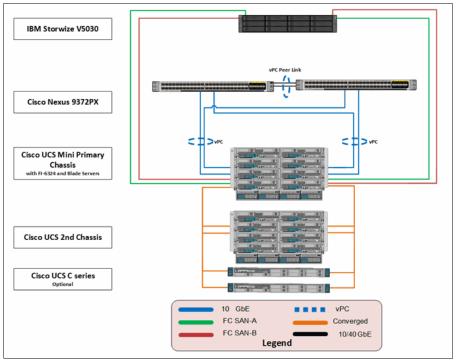


Figure 7-1 shows the physical topology used in this deployment.

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** \rightarrow **Add Roles and Features**, as shown in Figure 7-2.

ᡖ Server Manager		- 🗆 X
Server Manag	er • Dashboard	
Image: Dashboard Image: Local Server Image: All Servers Image: File and Storage Services Image: File and Storage Services	Roles: 1 Server groups: 1 Servers total: 1 Image Services 1 Image Se	1 Image ability Image ability Events Services Performance BPA results

Figure 7-2 Add Roles and Features

 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.

📥 Add Roles and Features Wizard				-		×
Select destination	i server		WIN-HYPERV		TION SERV	
Before You Begin Installation Type Server Selection Server Roles	 Select a server from the Select a virtual hard disk 		oles and features.			
Features Confirmation	Server Pool					
Results	Name WIN-HYPERV-N1.UCSD	IP Address 192.168.161.177,192.168	Operating System Microsoft Windows Serv	ver 2016	Datacent	er
	and that have been added h	at are running Windows Serve by using the Add Servers com which data collection is still in	mand in Server Manager.			
		< Previous	Next > Inst	all	Cance	2

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.

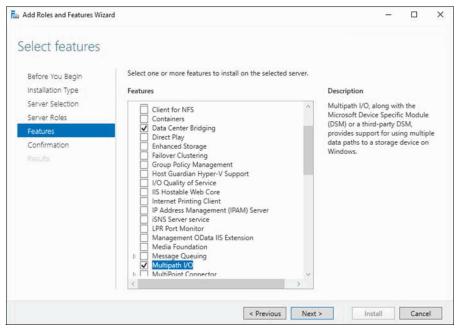


Figure 7-4 Installing DCB and Multipath I/O

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 Storwize V5030.

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:

- The examples in this book use the IBM SDDSDM package for IBM Storwize V5030, for OS platform Microsoft Windows 2016. You can download the software package from the IBM Support website.
- 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.

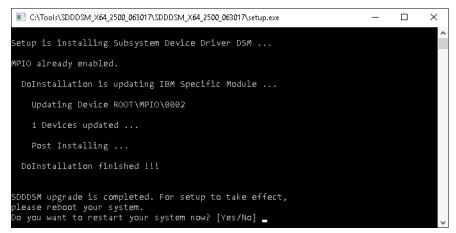


Figure 7-6 Completion of the IBM SDDDSM installation

4. After 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 Storwize V5030. 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 PortO:	20000025B5010A2E
Scsi Port1:	20000025B5010B2E

C:\Program Files\IBM\SDDDSM>

7.5 Creating a host attachment in IBM Storwize V5030

This section guides you through the host configuration procedures that are required to attach supported hosts to the IBM Storwize V5030 attached to the Cisco UCS Mini environment. The IBM Storwize V5030 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 Storwize V5030 system by using FC protocol must be zoned appropriately, as described in 5.4, "Configuring UCS SAN connectivity" on page 60.

To create a host in the IBM Storwize V5030:

1. Log in to IBM Storwize V5030 and open the host configuration panel, as shown in Figure 7-7.

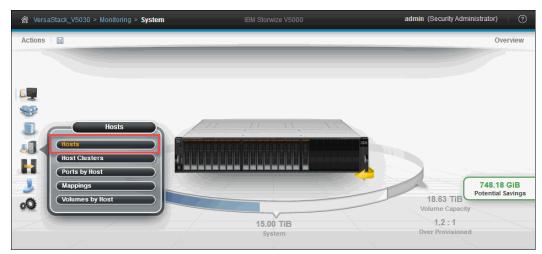


Figure 7-7 Creating a host in IBM Storwize V5030

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

🔺 Versa	☆ VersaStack_V5030 > Hosts > Hosts			vize V5000	
Г	+ Add Host 🗄 Action				
	name	Status	Host Type	# of Ports	Host Map
Q					

Figure 7-8 Adding new host to IBM Storwize V5030

 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.

Add Host		х
Required Fields Name: Host connections: Host port (WWPN):	The value entered is not valid. () () () () () () () () () () () () ()	
Optional Fields Host type:	Generic	
I/O groups:	All	
Host cluster:	No Host Cluster Selected	
	Add Cancel	

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 Storwize V5030" on page 113 (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 Storwize V5030.

7.6 Creating a host cluster in the IBM Storwize V5030

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 Storwize V5030:

1. Log on to IBM Storwize V5030 and select **Host Clusters** from the **Host** menu, as shown in Figure 7-10.

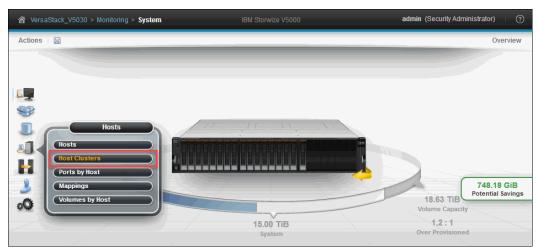


Figure 7-10 Creating a host cluster

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

☆ Vers	aStack_V5030	> Hosts >	Host Clusters		IBM Storwize V5000
	Create H	ost Cluster Name	E Actions	C Filter	
1					
3					
00					

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.

Optional: Select hosts to as Il the hosts in the host clust		ster. Any current volur	ne mappings become the shared mappings for
It is recommended that a	ill nosts in a nost clust	er have access to the	same I/O Groups.
🔍 Filter 🔚			Showing 6 hosts Selecting 0 hosts
Name	▲ Status	Host Type	Host Mappings
HyperV-AD	✓ Online	Generic	Yes
VM-Host-INfra-iSCSI-02	😣 Offline	Generic	No
VM-Host-Infra-01	✓ Online	Generic	Yes
VM-Host-Infra-02	✓ Online	Generic	Yes
VM-Host-Infra-iSCSI-01	🔕 Offline	Generic	No
VersaStack-SVC	✓ Online	Generic	Yes

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.

lanta kalanging ta l	thus a shift		
Hosts belonging to I	Hyperv:		
🔍 Filter 🛛 🔚			Showing 2 hosts Selecting 0 h
	▲ Status	Host Type Ho	Showing 2 hosts Selecting 0 h
	▲ Status ✓ Online	Host Type Ho Generic Yes	

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 Storwize V5030 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 Storwize V5030 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 Storwize V5030:

1. Log on to IBM Storwize V5030, click the **Volumes** icon and select the **Volumes** menu, as shown in Figure 7-14.

☆ VersaStack_V5030 > Monitoring > System
Actions
12
Volumes
Volumes
Volumes by Pool
Volumes by Host
ī

Figure 7-14 Assigning new volume

 The wizard starts, as shown in Figure 7-15 on page 117, 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 Storwize V5030 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 Storwize V5030 advanced functions" on page 203.

When using the Quick Volume Creation, the IBM Storwize V5030 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

Create Vo	olumes	x
	Basic	Quick Volume Creation Advanced
	Pool:	Pool0 Total 15.00 TiB Capacity: Capacity savings: Name:
1		Capacity: Capacity savings: Name: 1 GiB None HyperV_MSC_QUORUM
I/	O group:	Automatic
1	Sime 7	Summary
		1 volume Volume name: HyperV_MSC_QUORUM
		1 volume in pool Pool0
		Caching I/O group: Automatic Accessible I/O group: Automatic
		Total real capacity: 1.00 GiB Total virtual capacity: 1.00 GiB

Figure 7-15 Provisioning a new volume using IBM Storwize V5030 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.

Create Ma	pping					х
						_
Cr	reate Mappings to:					
0	Hosts					
۲	Host Clusters					
Se	elect host clusters to map t	io.				
_	Silter			Showing 1 host	cluster Selecting 1 host cluster	
	Name 🔺	Status	Host Count	Mappings Count	Ports Count	
ŀ	HyperV	✓ Online	2	0	4	
						-
					_	
			A Back	ext ►		Cancel

Figure 7-16 Creating a host cluster mapping

- 5. Scroll down to select the SCSI ID assignment. When selecting System Assign, the IBM Storwize V5030 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 118. Click **Map Volumes** to map the volume. Wait for the wizard to complete the disk assignment, and then close the wizard.

The following volumes will be m	apped to HyperV:			
Name	SC SI ID	Caching I/O Group ID	New Mapping	
HyperV_MSC_QUORUM	Auto	0	New	

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** \rightarrow **Computer Management**.
- 3. Switch to Disk Management as shown in Figure 7-18 on page 119.

🔝 Computer Management				_		×
File Action View Help						
🗢 🔿 🖄 🖬 🛛 🖬 🗩 🗙 🖓 🔒	<u>,</u>					
🜆 Computer Management (Local)	Volume Layout	Type File System	Status	Actions		
 System Tools O Task Scheduler 	🛲 (C:) Simple	Basic NTFS	Healthy (System, Boot, Page File, Active, Crash Dump, Pr	Disk Managem	nent	
 Jask Scheduler Jask Scheduler Shared Folders Shared Folders Local Users and Groups Performance Device Manager Storage Windows Server Backup Disk Management Services and Applications 	٢		>	More Acti	ons	۲.
	Disk 0 Basic 128.00 GB Online Unallocated	501 MB Unallocated Primary partition	1C:1 127.51 GB NTFS Healthy (System, Boot, Page File, Active, Crash E			

Figure 7-18 Windows Disk Management utility

 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.

🛃 C	omputer Management		
File	Action View Help		
= 🧇	Refresh	X 🖸 🔒	
🛃 Ci	Rescan Disks		Volume Layout Type File System Status
~ 1	Create VHD		👄 (C:) Simple Basic NTFS Healthy (System, Boot, Page File, Active, Crash Dump, Pr
>	Attach VHD		
>	All Tasks >		
>	Help		
	🚠 Device Manager		
× 🕾	Storage		
>	🐞 Windows Server Backup		
	📅 Disk Management		
> 🗟	Services and Applications		<>

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 120.

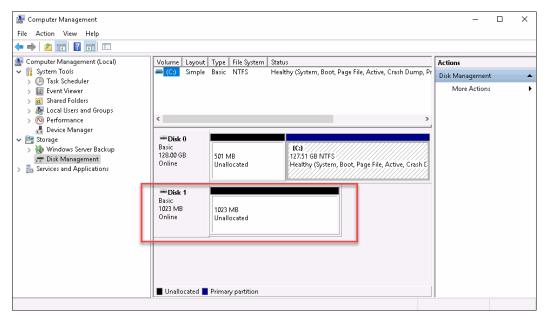


Figure 7-20 Disk rescanning operation

 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.

New Simple Volume Wizard		×
	Completing the New Simple Volume Wizard	
	You have successfully completed the New Simple Volume Wizard.	
	You selected the following settings:	
	Volume type: Simple Volume	
	Disk selected: Disk 11	
	Volume size: 1021 MB Drive letter or path: None	
	File system: NTFS	
	Allocation unit size: Default Volume label: QUORUM Quick format: Yes	
	To close this wizard, click Finish,	
	< Back Finish Cance	

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:

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

ᡖ Server Manager				- 🗆 X
Server Manager	 Dashboard 	Ţ	© 🚩 м	anage Tools View Help Add Roles and Features
Dashboard	ROLES AND SERVER GROUPS Roles: 1 Server groups: 1 Servers total: 1		,	Remove Roles and Features Add Servers Create Server Group
■ All Servers ■ File and Storage Services ▷	File and Storage 1 Services	Local Server 1	All S	Server Manager Properties
The and storage services	 Manageability 	 Manageability 	Manage	ability
	Events	Events	Events	
	Performance	Services	Services	
	BPA results	Performance	Perform	ance
		BPA results	BPA resu	ults

Figure 7-22 Starting the wizard

 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.

🍓 Failover Cluster Manager					-	×
File Action View Help						
🖛 🔿 📅 🔽 🖬						
📲 Failover Cluster Manager	Failover Cluster Manager		^	Actions		
	Create failover clusters, validate hardware for pot changes to your failover clusters.	ential failover clusters, and perform	configuration	1	Manager onfiguration	•
	A failover cluster is a set of independent computers that roles. The clustered servers (called nodes) are connect nodes fails, another node begins to provide services. Th	ed by physical cables and by softwa	ability of server re. If one of the	Create Clu Connect to View Refresh		•
	Clusters Name No.tems.	Role Status	Node Stati	Properties		
	Management To begin to use failover clustering, first validate your ha After these steps are complete, you can manage the clu to it from a cluster running Windows Server 2016 or sup	dware configuration, and then creat ster. Managing a cluster can include ported previous versions of Window	te a cluster. e copying roles rs Server.			

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 122. Click **Next** to move to the next step.

💐 Validate a Config	uration Wizard		×
Select Se	ervers or a Cluster	r	
Before You Begin Select Servers or a Cluster		vers, add the names of all the servers. er, add the name of the cluster or one of its nodes.	
Testing Options Confirmation Validating Summary	Enter name: Selected servers:	U WIN-HYPERV-N1.UCSDOMAIN.CORP WIN-HYPERV-N2.UCSDOMAIN.CORP	Browse Add Remove
		< Previous Next :	Cancel

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

 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.

👹 Validate a Configuration Wizard					
Testing (Options				
Before You Begin Select Servers or a Cluster	Choose between running all tests or running selected tests. The tests examine the Cluster Configuration, Hyper-V Configuration, Inventory, Network, Storage, and System Configuration.				
Testing Options Confirmation Validating Summary	ng Options Microsoft supports a cluster solution only if the complete configuration (servers, network, and storag pass all tests in this wizard. In addition, all hardware components in the cluster solution must be "Ce for Windows Server 2016."				
	 Run all tests (recommended) Run only tests I select 				
	More about cluster validation tests Cancel				

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.

🝓 Failover Cluster Manager			-	×
File Action View Help				
🦛 🔿 🔲 🖬				
🍓 Failover Cluster Manager	Failover Cluster Manager	^	Actions	
	Create failover clusters, validate hardware for potential failover clusters, and perform		Failover Cluster Manager	•
	configuration changes to your failover clusters.		💐 Validate Configuration	
			🍓 Create Cluster	
	Overview A failover cluster is a set of independent computers that work together to increase the	1	📲 Connect to Cluster	
	availability of server roles. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node beins to provide services. This		View	•
	process is known as failover.		💿 Refresh	
	· · · · · · · · · · · · · · · · · · ·		Properties	
	Clusters		🕜 Help	
	Name Role Status			
	No items found.			
	O Management			
	To begin to use failover clustering, first validate your hardware configuration, and then create a cluster. After these steps are complete, you can manage the cluster. Managing a cluster can include copying roles to it from a cluster running Windows Server 2016 or supported previous versions of Windows Server.	~		

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.

💐 Create Cluster Wizard					
Select Se	ervers				
Before You Begin Select Servers	Add the names of all the s	servers that you want to have in the cluster. You must add at least one server.			
Validation Warning					
Access Point for Administering the	Enter server name:	Browse]		
Cluster	Selected servers:	Add			
Confirmation		Remove			
Creating New Cluster		Trendve			
Summary					
		< Previous Next> Cancel			

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.

🍓 Create Cluster Wi	zərd	×
Access P	oint for Administering the Cluster	
Before You Begin Select Servers Access Point for Administering the	Type the name you want to use when administering the cluster. Cluster Name:]
Cluster Confirmation	automatically. For each network to be used, make sure the network is selected, and then type an address.	_
Creating New Cluster	Networks Address	
Summary	☑ 192.168.160.0/22 Click here to type an address	
	< Previous Next> Cancel	

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.

Create Cluster Wi	
Before You Begin Select Servers Access Point for Administering the Cluster Confirmation Creating New Cluster Summary	You are ready to create a cluster. The wizard will create your cluster with the following settings: Cluster USCDOMAIN Node WIN-HYPERV-N1.UCSDOMAIN.CORP WIN-HYPERV-N2.UCSDOMAIN.CORP Cluster registration DNS and Active Directory Domain Services Add all eligible storage to the cluster. To continue, click Next.
	< Previous Next > Cancel

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.

🍓 Failover Cluster Manager										-	٥
File Action View Help											
♦ ♦ 2											
📲 Failover Cluster Manager	Disks (1)								Actio	ons	
✓ 噌 UCSDOMAIN.UCSDOMAIN.CORP	Search						🔎 Queries 🔻		Disks		
🍯 Nodes	Name	Status	Assigned To	Owner Node	Disk Number	Partition Style	Capacity	Replication	3	Add Disk	
V 📇 Storage	📇 Cluster Disk 1	Online	Available Storage	WIN-HYPERV-N1	1	MBR	1.00 GE		3	Move Available Storage	
Pools									·	View	
Enclosures									Q	Refresh	
Networks Cluster Events									?	Help	
									Clust	ter Disk 1	
										Bring Online	
										Take Offline	
									a .	Add to Cluster Shared Vol	umes
									8	Information Details	
									8	Show Critical Events	
	<							>	8	Replication	
	🗸 🦣 Cluster D	iisk 1								More Actions	
										Remove	
	Volumes (0)									Properties	
									?	Help	

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 \rightarrow Add Role and Features, as shown in Figure 7-31.

server Manager €⊙ ▼ Server Manage	er • Dashboard	
Dashboard Local Server All Servers File and Storage Services	ROLES AND SERVER GROUPS Roles: 1 Server groups: 1 Servers total: 1 Image: File and Storage Services 1 Image: Local Server Image: Services 1 Services Imag	1 Add Koles and reatures Remove Roles and Features Add Severs Create Server Group Server Manager Properties Manageability Events Services Performance BPA results

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.

Defere Veu Decie	Select a server or a	ı virtual hard disk on which to i	nstall roles and features.
Before You Begin Installation Type Server Selection	 Select a server Select a virtual 	from the server pool hard disk	
Server Roles Features	Server Pool		
	Name WIN-HYPERV-N1	IP Address UCSD 192.168.161.177,192	Operating System 2.168 Microsoft Windows Server 2016 Datace
	1 Computer(s) four	nd	
			vs Server 2012 or a newer release of Windows Ser ers command in Server Manager. Offline servers a

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.

📥 Add Roles and Features Wizard		– 🗆 X
Select server roles		DESTINATION SERVER WIN-HYPERV-N1.UCSDOMAIN.CORP
Before You Begin Installation Type Server Selection	Select one or more roles to ir Roles	Add features that are required for Hyper-V?
Server Roles Features Confirmation Results	Active Directory Dom Active Directory Fede Active Directory Ligh Active Directory Righ Device Health Attest DHCP Server DNS Server Fax Server File and Storage Serv Hots Guardian Servic	have to be installed on the same server. A Remote Server Administration Tools A Role Administration Tools A Hyper-V Management Tools [Tools] Hyper-V Module for Windows PowerShell [Tools] Hyper-V GUI Management Tools
	MultiPoint Service MultiPoint Services Network Controller Network Policy and A Print and Document Remote Access Remote Desktop Sen Volume Activation Se Web Server (IIS)	✓ Include management tools (if applicable)
		< Previous Next > Install Cancel

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.

📥 Add Roles and Features Wizar	d	>			
Create Virtual Sv	vitches	DESTINATION SERVER WIN-HYPERV-N1.UCSDOMAIN.CORP			
Before You Begin		tual switches to communicate with other computers. After you install this nachines and attach them to a virtual switch.			
Installation Type Server Selection	One virtual switch will be created for each network adapter you select. We recommend that you crea at least one virtual switch now to provide virtual machines with connectivity to a physical network. Yo				
Server Roles	can add, remove, and modify your virtual switches later by using the Virtual Switch M				
Features	Network adapters:				
Hyper-V	Name	Description			
Virtual Switches	✓ Ethernet	Cisco VIC Ethernet Interface			
Migration	✓ Ethernet 2	Cisco VIC Ethernet Interface			
Default Stores	<	>			
Confirmation Results		u reserve one network adapter for remote access to this server. To reserve a t select it for use with a virtual switch.			

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**.

ᡖ Add Roles and Features Wizard		_		Х
Virtual Machine N	Aigration WIN-HYPERV		ATION SERV OMAIN.CC	
Before You Begin Installation Type Server Selection Server Roles Features Hyper-V Virtual Switches Migration Default Stores Confirmation Results	 Hyper-V can be configured to send and receive live migrations of virtual machines Configuring Hyper-V now enables any available network on this server to be used you want to dedicate specific networks for live migration, use Hyper-V settings aftr ✓ Allow this server to send and receive live migrations of virtual machines Authentication protocol Select the protocol you want to use to authenticate live migrations. ● Use Credential Security Support Provider (CredSSP) This protocol is less secure than Kerberos, but does not require you to set up delegation. To perform a live migration, you must be logged on to the source O Use Kerberos This protocol is more secure but requires you to set up constrained delegation environment to perform tasks such as live migration when managing this server for live migration, including specifying networks, when you create the comparison of the server for live migration, including specifying networks, when you create the comparison of the server for live migration, including specifying networks, when you create the comparison of the server for live migration, including specifying networks, when you create the comparison of the server for live migration, including specifying networks, when you create the comparison of the server for live migration is performed and the server for live migration is performed and the server for live migration is performed and the server for live migration including specifying networks, when you create the comparison of the server for live migration, including specifying networks, when you create the comparison of the server for live migration, including specifying networks, when you create the comparison of the server for live migration is performed and the server for live migration for the server for live migratio	for live m er you in: o constrai e server. on in you ver remo	nigration: stall the r ined ir ytely.	ole.
	< Previous Next > Inst	all	Cance	I

Figure 7-35 Hyper-V for live migration setup

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.

📥 Add Roles and Features Wizard	-	D X
Default Stores	DESTINA WIN-HYPERV-N1.UCSD	TION SERVER OMAIN.CORP
Before You Begin Installation Type Server Selection Server Roles Features Hyper-V Virtual Switches Migration Default Stores Confirmation Results	Hyper-V uses default locations to store virtual hard disk files and virtual machine configurat unless you specify different locations when you create the files. You can change these defau now, or you can change them later by modifying Hyper-V settings. Default location for virtual hard disk files: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks Default location for virtual machine configuration files: C:\ProgramData\Microsoft\Windows\Hyper-V	
	< Previous Next > Install	Cancel

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

 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 129) to allow the wizard to complete the installation of the Hyper-V feature.

📥 Add Roles and Features Wizard		-		Х
Confirm installation	on selections with	DESTINA HYPERV-N2.UCSD	ATION SERV OMAIN.CC	
Before You Begin	To install the following roles, role services, or features on selected server, clic	:k Install.		
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this p			
Server Roles	been selected automatically. If you do not want to install these optional feat their check boxes.	ures, click Prev	ious to cl	ear
Features				
Hyper-V	Hyper-V			
Virtual Switches	Remote Server Administration Tools			
Migration	Role Administration Tools Hyper-V Management Tools			
Default Stores	Hyper-V Module for Windows PowerShell			
Confirmation	Hyper-V GUI Management Tools			
Results				
	e a e a a			
	Export configuration settings Specify an alternate source path			
	· · ·			
	< Previous Next >	Install	Cance	I

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.

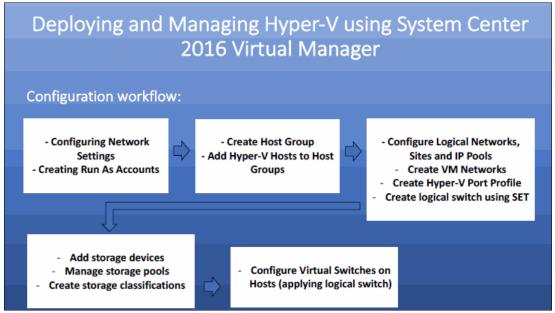


Figure 7-38 Deploying a virtual environment using System Center 2016

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**.

🔳 Network Settings			×
Network settings			
Specify the options for logic	al and virtual switches.		
Logical network matching			
Match logical networks by:	First DNS Suffix Label		
If the above fails, match by:	Virtual Network Switch Name 🛛 👻		
Automatic creation of logi	tal networks		
In case the host network ada network matching.	pter is not associated with a logical net	work, a new one will be created based	on the above choice made for
Create logical networks a	automatically		
View Script			Finish Cancel

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 Storwize V5030 and many other tasks. To create a Run As account:

- 1. Click Settings, and in the Create menu, click Create Run As account.
- 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 132 shows an example of this dialog box.

🔳 Create Run As	s Account	×
Provide the	details for this Run As account	
Name: Ver	rsaStack Domain Account	
Description:		
User name:	UCSDOMAIN\Administrator Example: contoso\domainuser or localuser	
Password:	•••••	
Confirm passwor	ord: ••••••	
✓ Validate dom	nain credentials	

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 Storwize V5030 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.

Fabric <	Hosts (2)		
A 👰 Servers			
🔺 🚞 All Hosts	Name	Host Status	Role
VS_Hyper-V			
Infrastructure			
Metworking			
🔺 逼 Storage			
Classifications and Pools			
🜉 Providers			
🥬 Arrays			
📑 File Servers			
Fibre Channel Fabrics			
🔓 QoS Policies			

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 121 and 7.10, "Adding the Hyper-V feature" on page 125. 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**.

👌 Discovery S	Scope
Resource Location Credentials Discovery Scope Target Resources Host Settings Summary	Specify the search scope for virtual machine host candidates Search for computers by whole or partial names, FQDNs, and IP addresses. Alternatively, you may generate an Active Directory query to discover the desired computers. Specify Windows Server computers by names Specify an Active Directory query to search for Windows Server computers Enter the computer names of the hosts or host candidates that you want VMM to manage. Each computer name must be on a separate line. Computer names: WIN-HYPERV-N1.UCSDOMAIN.CORP WIN-HYPERV-N2.UCSDOMAIN.CORP Skip AD verification Examples: server1 server1.contoso.com 10.0.1.1 2a01:110:1e:3:f8ffcfe44:23
	Previous Next Cancel

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

 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 121, you might see the cluster name as shown in Figure 7-43 on page 134.

背 Target Resc	burces		
Resource Location	Select the computers that you	want to add as hosts	
	Discovered computers:		
Discovery Scope	Computer Name	Operating System	Hypervisor
Target Resources	UCSDOMAIN.UCSDOMAIN.CO.	. Windows Server 2016 Datacenter	Hyper-V
Host Settings	WIN-HYPERV-N1.UCSDOMAIN.	. Windows Server 2016 Datacenter	Hyper-V
Host Settings	WIN-HYPERV-N2.UCSDOMAIN.	. Windows Server 2016 Datacenter	Hyper-V
Summary			
	Select all Refresh Stop		
		Previous	Next Cancel

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.

🗎 Host Settir	ngs
Resource Location Credentials Discovery Scope Target Resources Host Settings Summary	Specify a host group and virtual machine placement path settings for hosts Assign the selected computers to the following host group: Host group: VS_Hyper-V If any of the selected hosts are currently managed by another Virtual Machine Manager (VMM) environment, select this option to reassociate the hosts with this VMM management server. Reassociate this host with this VMM environment
	Previous Next Cancel

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.

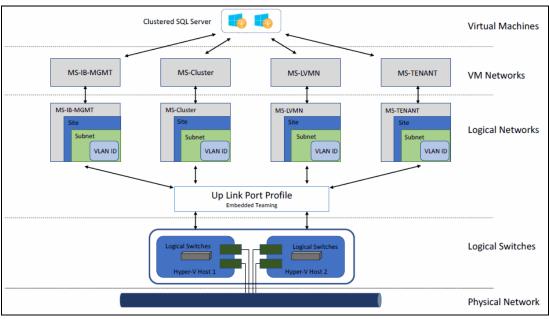


Figure 7-45 Hyper-V logical representation

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.

🁬 Create Logical Network V	/izard	Х		
🐫 Settings				
Name	Specify logical network settings			
Settings	Select the option which describes this logical network:			
Network Site	O One connected network			
Summary	The network sites within this network are equivalent and routable to one another and can be used as a single connected network.	5		
	Allow new VM networks created on this logical network to use network virtualization			
	Create a VM network with the same name to allow virtual machines to access this logical network directly	¢		
	VLAN-based independent networks			
	The subnet-VLAN pairs defined by the sites in this logical network are used as independent network. They might or might not be routable to one another.	s,		
	O Private VLAN (PVLAN) networks			
	The network sites within this logical network contain independent networks consisting of primary an secondary VLAN pairs in isolated mode.	d		
	Previous Next Cancel			

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 135. See the complete list of all logical networks created in Figure 7-47 on page 137.

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.

ame	Network Complia Subne
👬 MS-Cluster	Fully compliant
m MS-IB-MGMT	Fully compliant
m MS-LVMN	Fully compliant
m MS-Tenant-VM	Fully compliant

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 135, 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.

龞 Create Static IP Address P	ool Wizard		Х
🧱 Name			
Name	Specify the IF	address pool name and logical network	
Network Site	Enter the name o available.	f the IP address pool and select the logical network to which you want to make the po	ol
IP address range	available.		
Gateway	Name:	MS-IB-MGMT	
DNS	Description:		
WINS			
Summary	Logical network:	MS-IB-MGMT	~
		Previous Next Cancel	

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**.

🤓 Create Static IP Address Po	iol Wizard		×
🦉 Network Si	te		
Name	Specify a r	etwork site and the IP subnet	
Network Site		ing network site and IP subnet from the logical network you have chosen or create a ne	w
IP address range	one. Specify t 192.168.1.0/2	ne IP subnet using classless inter-domain routing (CIDR) notation; for example 4.	
Gateway	Use an exi	sting network site	
DNS	O Create a n	etwork site	
WINS	Network site:	MS-IB-MGMT	~
Summary	IP subnet:	192.168.160.0/22 · VLAN: 11	
Junnary		hat can use this network site:	
		Hosts VS_Hyper-V	_
	· · ·	v3_пуры-v	_
		Previous Next Cance	el a constant

Figure 7-49 Creating IP Pool for existing logical network

5. The next dialog box (Figure 7-50 on page 139) 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.

🤷 Create Static IP Address Po	pol Wizard	×
🦉 IP address	range	
Name	IP address range	
Network Site	Specify the range of IP addresses from the subnet to be managed by this pool.	
IP address range	IP subnet: 192.168.160.0/22	
Gateway	Starting IP address: 192.168.162.91	
DNS	Ending IP address: 192.168.162.96	
WINS	Total addresses: 6	
Summary	VIPs and reserved IP addresses You can specify one or more IP addresses from the address range in the IP subnet to use for creating virtual IP (VIP) addresses or to reserve for other purposes. Use commas to separate multiple IP addresses Ranges in the format IP1-IP2 are allowed.	
	IP addresses reserved for load balancer VIPs:	
	IP addresses to be reserved for other uses:	
	Previous Next Cancel],,

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**.

🚟 Create Static IP Address Poo	ol Wizard						\times
🧱 Gateway							
Name	Specify default gate	way addresses a	and netwo	ork routes			
Network Site	Gateway addresses must b	elong to the range b	etween 192.	168.160.1 and 192	2.168.163.254		
IP address range	Network routes:						_
Gateway	Destination Prefix	Gateway Addres	s	Metric		Insert	
DNS						Delete	
WINS							
Summary							
Summary							
	Default gateways:						
	Gateway Address		Metric			Insert	
	192.168.160.1		Automatic		v	Delete	
				Previous	Next	Cancel	

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**.

🤷 Create Static IP Address Po	ool Wizard	×
🚟 DNS		
Name	Specify one or more DNS servers	
Network Site	DNS server addresses in the order of use:	
IP address range	DNS Server Address	Insert
Gateway	192.168.162.130	Delete
DNS		Move Up
WINS		Move Down
Summary		
	Connection specific DNS suffix: Enter DNS suffix	
	DNS search suffixes to append (in order):	
	DNS Suffix	Insert
		Delete
		Move Up
		Move Down
	Previous Next	Cancel

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 141.

🧱 Create Static IP Address Po	ool Wizard		×
🧱 Summary			
Name Network Site	Confirm the settings		View Script
IP address range	Name: Description:	MS-IB-MGMT	
Gateway DNS	IP subnet: IP address range:	192.168.160.0/22 192.168.162.91-192.168.162.96	
WINS	Connection specific DNS s		
Summary	Gateways:	0 Network routes 1 Gateways	
	DNS servers:	1 DNS servers 0 DNS suffixes	
	WINS servers:	0 WINS servers	
		Previous	Finish Cancel

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 135).

- 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.

VM Networks and IP Pools (4)					
Name	Subnet	Gateway Connection			
📥 MS-Cluster		No			
📥 MS-IB-MGMT		No			
📥 MS-LVMN		No			
🚢 MS-TENANT		No			

Figure 7-54 VM networks

 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.

VM Networks and IP Pools (5)					
Name	Subnet	Gateway Connection	Available Addresses		
🗉 📥 MS-Cluster		No			
🚟 MS-Cluster	172.17.72.0/24		253		

Figure 7-55 VM Network IP Pool

6. Click Next to 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 \rightarrow 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 143. 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.

💼 Create Virtual Network Ad	dapter Port Profile	×
💼 General		
General Network configuration Summary	Select the type of Hype You can create virtual network profiles for use on uplink ports Name: Up-Lin-Port-Profi Description: Type of Hyper-V port profile: Virtual network adapter por	adapter port profiles for use by hosts and virtual machines, or uplink port
	Uplink port profile	
	Load balancing algorithm:	Host Default ~
	Teaming mode:	Switch Independent ~
		Previous Next Cancel

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**.

	twork Adapter Port Profile		>
General	Select the network sites su	oported by this uplink port profile	
Network configurati	on Network sites:		
Summary	Network Site	Logical Network	
	MS-Cluster	MS-Cluster	
	MS-IB-MGMT	MS-IB-MGMT	
	MS-LVMN	MS-LVMN	
	MS-Tenant-VM	MS-Tenant-VM	
		zation Network Virtualization filter on hosts running Windows Sen R2, Hyper-V Network Virtualization is always enabled on ho	
		Previous Next C	Cancel

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.
- 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.

Create Logical Switch Wiz	ard		×
🐔 General			
Getting Started	Enter name	e and description for the logical switch	
General	Vou can use a	logical switch to apply settings to virtual switches across multiple hosts. A logical switch	
Settings		profiles from the native Hyper-V switch and port profiles for any extensions that you use	
Extensions	Name:	Cluster_Logical_Switch	
Virtual Port	Description:		
Uplinks			
Summary	Uplink mode:	Embedded Team	Ŷ
		Previous Next Cancel	

Figure 7-58 Creating a logical switch

- 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**.

General	Specify the port classifications for virtual ports part of this logical switch				
ettings	The port classifications configured virtual machines.	l here will be av	ailable for use by virtual network	adapters in a host or	
ixtensions	Virtual ports:				
/irtual Port	Port Classification	Default	Marked For Deletion	Add	
	High bandwidth	False	No	Edit	
Jplinks	Host Cluster Workload	False	No		
	Host management	False	No	Remove	
	Live migration workload	False	No		
	Medium bandwidth	False	No	Set Default	
				Clear Defau	

Figure 7-59 Port classification

 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.

🔳 Add Uplin	k Port Profile		×
Select a p	ort profile		
	file selected here will connect to this logica	be available for use by the host physical al switch.	
Port profile:	Up-Link-Port-Profile		~
- Summary -			
Host group	os:	All Hosts	
Network sites:		MS-Cluster, MS-IB-MGMT, MS-LVMN, MS- Tenant-VM	
Network v	irtualization enabled:	No	
Description	n:		
		OK Cancel	

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.

🐈 Add 💐 New virtual netwo	ork adapter 🗙	Remove	
Up-Link-Port-Profile SwitchIndependent	Name:	MS-Cluster	
MS-Cluster MS-Cluster	Connectivity VM Network:	MS-Cluster	Browse
MS-Cluster	VM Subnet:		
	🗸 Enable VL	AN	
	VLAN ID:	3172	v
	managem	I network adapter will be used for ho ent : connection settings from host netwo	
	IP address co	onfiguration	
	O DHCP		
	 Static 		
	IPv4 pool:	MS-Cluster (172.17.72.91 - 172.17.7	72.96) 🗸 🗸
	IPv6 pool:	Not Applicable	~
	Port profile		
	Classification:		Ý
1			

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.

🐈 Add 💐 New virtual netwo	rk adapter 🟋 Remove	
UP-Link-Port-Profile SwitchIndependent	Name:	UP-Link-Port-Profile
MS-LVMN MS-LVMN	Description:	
MS-Cluster MS-Cluster	Load balancing algorithm:	Host Default \checkmark
MS-IB-MGMT MS-IB-MGMT	Teaming mode:	Switch Independent
MS-Tenant-VM MS-Tenant-VM	Network sites:	Logical Network
	MS-Cluster	MS-Cluster
	MS-IB-MGMT	MS-IB-MGMT
	MS-LVMN	MS-LVMN
	MS-Tenant-VM	MS-Tenant-VM
	on hosts running Wind	rk Virtualization • Hyper-V Network Virtualization filter ows Server 2012 only. As of Windows V Network Virtualization is always

Figure 7-62 UP Link port profile

Add 🛁 New Virtual netw	vork adapter 🗙	Remove	
UP-Link-Port-Profile SwitchIndependent	Name:	MS-LVMN	
MS-LVMN MS-LVMN	Connectivity VM Network:	MS-LVMN	Browse
MS-Cluster	VM Subnet:		U
MS-Cluster	🗸 Enable VL	AN	
MS-IB-MGMT MS-IB-MGMT	VLAN ID:	3173	L.
MS-Tenant-VM MS-Tenant-VM	managem	I network adapter will be used for he ent connection settings from host netw	
		2	ork adapter
	IP address co	5	ork adapter
		5	ork adapter
	IP address co	5	ork adapter
	IP address co O DHCP Static	5	
	IP address co O DHCP Static IPv4 pool:	nfiguration	
	IP address co O DHCP Static IPv4 pool:	nfiguration MS-LVMN (172.17.73.91 - 172.17.7	· 73.96)

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.

🐈 Add 💐 New virtual netwo	ork adapter 🗡	Remove	
UP-Link-Port-Profile SwitchIndependent MS-LVMN MS-LVMN	Name: Connectivity VM Network:	MS-Cluster	Browse
MS-Cluster MS-Cluster	VM Subnet:	AN	v
MS-IB-MGMT MS-IB-MGMT	VLAN ID:	3172	v
MS-Tenant-VM MS-Tenant-VM	managem	I network adapter will be used for he ent : connection settings from host netw	
	IPv6 pool: Port profile	MS-Cluster (172.17.72.91 - 172.17. Not Applicable	72.96) ~
	Classification:	Host Cluster Workload	Ŷ

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.

General	📲 Add 💐 New virtual netv	vork adapter X Remove
Settings	Up-Link-Port-Profile SwitchIndependent	Name: MS-IB-MGMT-NIC
Extensions	MS-TENANT-NIC MS-TENANT	VM Network: MS-IB-MGMT Browse
/irtual Port	MS-CLUSTER-NIC MS-Cluster	VM Subnet:
Jplinks	MS-IB-MGMT-NIC MS-IB-MGMT	VLAN ID:
	MS-LVMN MS-LVMN	 This virtual network adapter will be used for host management Inherit connection settings from host network adapter
		IP address configuration
		DHCP
		Static IPv4 pool: Not Applicable
		IPv6 pool: Not Applicable V
		Port profile

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

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

🐈 Add 💐 New virtual netwo	ork adapter 🗙	Remove	
UP-Link-Port-Profile SwitchIndependent MS-LVMN	Name: Connectivity	MS-Tenant-VM	
MS-LVMN MS-Cluster MS-Cluster	VM Network: VM Subnet:	MS-Tenant-VM	Browse
MS-IB-MGMT MS-IB-MGMT	VLAN ID:	3174	Ŷ
MS-Tenant-VM MS-Tenant-VM	manageme	I network adapter will be used for ho ent connection settings from host netw	
	IP address co DHCP Static	nfiguration	
	IPv4 pool: IPv6 pool:		17.74.96) ¥
	Port profile		
	Classification:	High bandwidth	~

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 Storwize V5030 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 Storwize V5030 storage array in VMM, see Chapter 4, "VersaStack Cisco Nexus 9000 network configuration" on page 29.

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 Storwize V5030 Gold* or a system that does not hold SSDs but HDDs only as *IBM Storwize V5030 Silver*.

Before creating or renaming the storage classifications, we assume the IBM Storwize V5030 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 Storwize V5030 is listed.

4. Rename the classification that is related to IBM Storwize V5030 by clicking in **Properties**, as shown in Figure 7-67.

🔳 IBM Storwize V5030 Propert	ies					×
General	Storage C	Classification Info	rmation			
File Shares	Name:	IBM Storwize V5030				
Disks	Description:					
	Associated s	torage pools:				
	Name	torage pools.	Manufacturer	Mod	lel	
	Pool0					
View Script					OK	Cancel

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.

🔳 New Class	ification	×
Create a s	storage classification	
Name:	IBM Storwize V5030	
Description:	IBM Storwize V5030 - Hybrid Storage Pool	
View Script	Add Cancel	

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.
- Click Virtual Switches from the menu, and then select New Virtual Switch → New Logical Switch.
- Select the Virtual Switch that you created in "Configuring Hyper-V logical switch using SET" on page 144. Under Adapter, select the Hyper-V physical adapters by clicking the Add button those to the logical switch, as shown in Figure 7-69.

🐈 New Virtual Switch 💐 New	w Virtual Network Adapter ᅟ 🏋 De	lete
Cluster_Logical_Switch Logical Switch	Logical switch: Cluster_Logical_S	
	more than one physical adapter t single uplink.	5
	Physical adapters:	
	Adapter	Uplink Port Pro Add
	Ethernet - Cisco VIC Ether 🗡	Up-Link-Port-F Remove
	Ethernet 2 - Cisco VIC Eth 🗡	Up-Link-Port-F
	III The teaming mode supported physical adapters to use the s	

Figure 7-69 Selecting the physical adapters

 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

 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. 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.

Port profile	
Classification:	Host management ~
IP address confi	guration
O DHCP	
 Static 	
IPv4 pool:	IB-MGMT (192.168.162.91 - 192.168.162.96) *
IPv4 address:	
IPv6 pool:	Not Applicable V
IPv6 address:	
MAC address	
 Dynamic 	
Static:	00:1D:D8:B7:1C:52

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.

Port profile	
Classification:	Host Cluster Workload ~
IP address confi	guration
○ DHCP	
 Static 	
IPv4 pool:	MS-Cluster (172.17.72.91 - 172.17.72.96)
IPv4 address:	172.17.72.92
IPv6 pool:	Not Applicable
IPv6 address:	
MAC address	
 Dynamic 	
Static:	00:1D:D8:B7:1C:54

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.

🕂 New Virtual Switch 💐 New	w Virtual Network Adapter ᅟ 🏋 De	elete	
Cluster_Logical_Switch Logical Switch	Logical switch: Cluster_Logical_S		v
MS-IB-MGMT-NIC MS-IB-MGMT	The logical switch supports teamin more than one physical adapter th single uplink.		
💐 MS-TENANT-NIC	Physical adapters:		
MS-TENANT	Adapter	Uplink Port Pro	Add
MS-CLUSTER-NIC MS-Cluster	Ethernet - Cisco VIC Ether 👻	Up-Link-Port-F	Remove
MS-LVMN-NIC MS-LVMN	Ethernet 2 - Cisco VIC Eth 💙	Up-Link-Port-F	
	۰ III	4	
	The teaming mode supported physical adapters to use the s		

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.
- 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.

🔳 New Hardware Profile			×
General	Name:	HW_PROFILE-MSSQL_CLUSTER	
Hardware Profile	Description:		
	Generation:	Generation 2	~
	Туре:	Generation 1 Generation 2	
	Added:	9/18/2017 12:17:04 PM	
a second second	Modified:	9/18/2017 12:17:04 PM	
View Script			OK Cancel

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.

🐈 New 🗡 Remove		
Compatibility	^	Processor
Cloud Capabilit Hyper-V		Number of processors: 8
General Processor		Compatibility
8 processors		To improve compatibility with different processor versions, VMM by
Memory 1024 MB		default limits the processor features that a virtual machine can use. Allow migration to a virtual machine host with a different
Bus Configuration		processor version

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.

2	New 🗙 Remove					
*	Compatibility	^	📷 Memory			
×	Cloud Capabilit Hyper-V General		Specify how much memory (32.00 MB - 1,024.00 GB) to allocate to the virtual machine, or specify a range to allow the virtualization host to allocate memory dynamically.			
	Processor 8 processors		● Static			
	Memory <i>32768 MB</i>		Virtual machine memory: 32 🛖 GB 🗸			
*	Bus Configuration		O Dynamic			
	SCSI Adapter 0 1 Device attached					
	💿 Virtual DVD		Startup memory: 1024 🙀 MB 🗸			
	No Media Ca		Minimum memory: 32 📮 MB 🗸			
^						
	Network Adapt Not connected		Maximum memory: 1048576 🗼 MB 🗸			
×	Fibre Channel Adapt		Memory buffer percentage: 20 🜩			
*	Advanced					
	🦆 Checkpoints					
	 Availability Normal Firmware 					
	rinnware	~				

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 156.

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** \rightarrow **Select the Library Server FQDN** \rightarrow **Add to Library Server**.

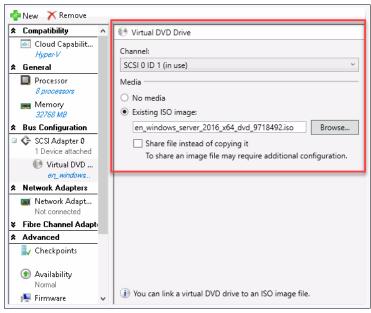


Figure 7-77 Bus configuration

 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.

4	new 🗙 Remove					
*	Compatibility 🔨	Metwork Adapter 2				
*	Cloud Capabilit Hyper-V General	Connectivity O Not connected				
	Processor <i>8 processors</i> Memory	 Connected to a VM VM network: 	network MS-IB-MGMT	Browse		
	32768 MB	VM subnet:	None	~		
*	Bus Configuration	IP address				
	SCSI Adapter 0 1 Device attached	O Dynamic IP				
	💿 Virtual DVD	 Static IP (from a static IP pool) 				
	en_windows	IP protocol version:	IPv4 only	¥		
*		MAC address				
	Network Adapt Connected to M	 Dynamic 				
	📷 Network Adapt	 Static 				
	Connected to M	Port profile				
	Network Adapt Connected to M	Classification:	Host management	¥		
×	Fibre Channel Adapt	Enable virtual switch optimizations				
*	Advanced	Enable spoofing of I	MAC addresses			
	🚽 Checkpoints	Enable guest specifi	ed IP addresses			
	×					

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.

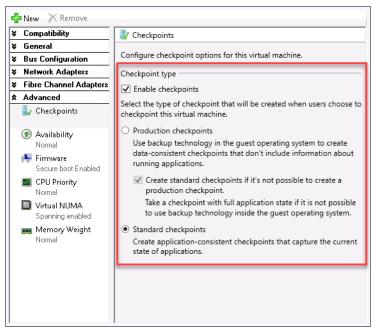


Figure 7-79 Hardware profile checkpoint

• *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 158.

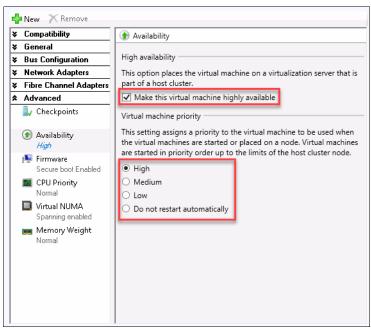


Figure 7-80 Hardware profile high availability sets

- 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 \rightarrow Create Virtual Machine \rightarrow 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**.
- 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 153, and click Next (Figure 7-81).

Configure Hardware						
Select Source Identity	Configure hardware for the virtual machine. You can import settings from a hardware profile or save a new profile based on your settings. Hardware profile: [Default - create new hardware configuration settings]					
Configure Hardware						
Select Destination Select Host Configure Settings	Compatibility Solution Cloud Capability Pr General Processor	Ate new hardware configuration ROFILE Compatibility Select the capability profile to VMM will ensure that the set profile.	hat will be used to create th			
Add Properties Summary	1 processor Memory 1024 MB Bus Configuration Configuration CSCSI Adapter 0 2 Devices attached	Name	Description The built-in fabric capabi The built-in fabric capabi			

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 153, 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 160 as example.

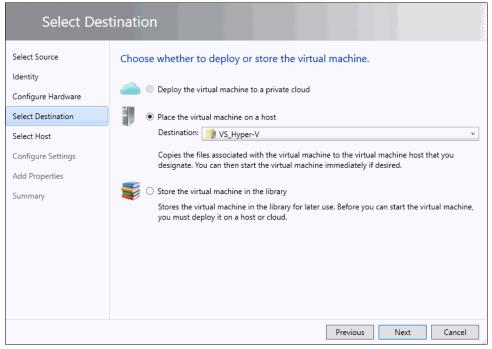


Figure 7-82 Destination of virtual machine

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.

Select Hos	t			
Select Source	Select a destination for the virtual machine			
Identity	Destinations are rated based on the virtual machine requirements and on the default placement options.			
Configure Hardware	Expected Utilization			
Select Destination	Search P v in All Hosts\VS_Hyper-V v			
Select Host	Rating Destination Warnings Transfer Type Network 🔿			
Configure Settings	🛠 🛠 🛠 🛠 🚦 WIN-HYPERV-N1.UCSDOMAIN.CORP 🛛 👞 Network			
Add Properties	🚖 🚖 🚖 🚔 🚦 WIN-HYPERV-N2.UCSDOMAIN.CORP 🔹 Network 🗸			
Summary Placement has finished calculating ratings for each potential destination of this virtual machine. Summary Placement has finished calculating ratings for each potential destination of this virtual machine. Summary Details Details Details				
	Description			
	Status OK			
	Operating system Microsoft Windows Server 2016 Datacenter			
	Virtualization software Microsoft Hyper-V			
	Status Backbon and Same Sectors - United Sectors			

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 161.

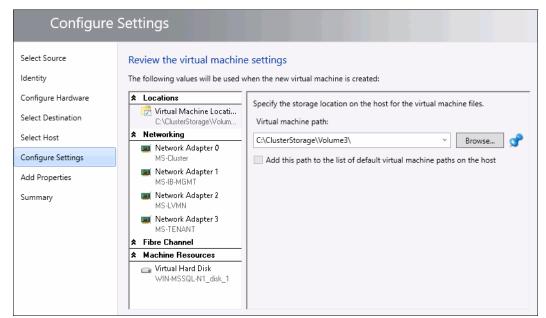


Figure 7-84 Configuring settings for the new virtual machine

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.

Identity	Select an action to perform automatically when the virtualization server starts:			
Configure Hardware	Always turn on the virtual machine			
Select Destination	Delay start up (seconds):			
Select Host	Action to take when the virtualization server stops:			
Configure Settings	Shut down guest OS v			
Add Properties	Operating system			
Summary	Specify the operating system you will install in the virtual machine: Windows Server 2016 Standard ×			

Figure 7-85 Virtual Machine virtualization properties

 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.

162 Implementing a VersaStack Solution with IBM Storwize V5030, Cisco UCS Mini, Hyper-V, and SQL Server

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" on page 164
- 8.2, "Provisioning storage volumes for Hyper-V cluster nodes" on page 164
- 8.3, "Creating CSV on a Hyper-V cluster" on page 167
- 8.4, "Assigning the V5030 volumes as shared drives to SQL VMs" on page 170
- 8.5, "Preparing the Cluster Shared Volumes on SQL VMs for Windows Failover Cluster" on page 178
- 8.6, "Installing the Windows Failover Clustering feature on SQL virtual machines" on page 179
- 8.7, "Installing a Microsoft SQL Server failover cluster" on page 187
- 8.8, "Creating a sample database" on page 200
- 8.9, "Configure Hyper-V level redundancy for SQL VMs" on page 201
- ▶ 8.10, "Database tuning" on page 202

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 153. 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.

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
WIN-MSSQL-N2	WIN-HYPERV-N2	8	32 GB	100 GB	2016 STD

 Table 8-1
 Virtual machine configuration

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 42 for information about creating the volumes using V5030 GUI.

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-O	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

Table 8-2 Volumes to be created on V5030

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 **1smdisk** 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 167.

Name	SCSI ID	Caching I/O Group ID	New Mapping
HyperV-MSSQL-UserData-1	7	0	New
HyperV-MSSQL-System	5	0	New
HyperV-MSSQL-UserData-3	9	0	New
HyperV-MSSQL-UserData-2	8	0	New
HyperV-MSSQL-UserData-0	6	0	New
HyperV-MSSQL-Quorum	4	0	New
HyperV-MSSQL-UserLog	10	0	New
HyperV-MSSQL-TempDB	11	0	New
Hyper-V_CSV02	3	0	
Hyper-V_CSV01	2	0	
HyperV_MSC_QUORUM	1	0	

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).
- 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 \rightarrow Tools and select Failover Cluster Manager.
- 2. Click Connect to Cluster, and select Cluster on this server. Then click OK.
- 3. Navigate to Storage \rightarrow Disks. Then, click Actions \rightarrow 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.

Name	Status	Assigned To	Owner Node	Disk Number	Partition Style	Capacity
📇 Cluster Disk 1	Online	Disk Witness in Quorum	WIN-HYPERV-N1	1	MBR	10.0 GB
📇 Cluster Disk 2	Online	Available Storage	WIN-HYPERV-N1	12	MBR	100 GB
HyperV-MSSQL-Quorum	(1) Online	Cluster Disk 2 Properties			× MBR	1.20 GB
HyperV-MSSQL-System	(Online	cluster bisk 2 Properties			MBR	103 GB
HyperV-MSSQL-TempDB	Online	General Dependencies P	olicies Advanced Policies	Shadow Copies	MBR	103 GB
HyperV-MSSQL-UserDat	Online	Name: Clus	ter Disk 2		MBR	203 GB
HyperV-MSSQL-UserDat	Online		sical Disk		MBR	203 GB
HyperV-MSSQL-UserDat_	Online	Status: Onlin	ne		MBR	203 GB
HyperV-MSSQL-UserDat	Online				MBR	203 GB
HyperV-MSSQL-UserLog	Online				MBR	103 GB
A OS_BINS-1	1 Online	Disk number: 12			MBR	500 GB
BINS-2	Online	Volume Ca	apacity Free S	pace	MBR	500 GB
		D: 10	10.0 GB 99.9 G	βB		
				<u>R</u> epair		
V Cluster Disk 2			OK Cano	el Apply		

Figure 8-2 Rename the cluster disk resource

 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	Canaahu
All OS BINS-2	Online	Cluster Shared Volume	WIN-HYPERV-N1	Disk Number	MBR	500 GI
BOS BINS-1	Online	Cluster Shared Volume	WIN-HYPERV-N1	2	MBR	500 GI
HyperV-MSSQL-UserLog	(Online	Cluster Shared Volume	WIN-HYPERV-N2	10	MBR	103 GI
HyperV-MSSQL-UserData-3	(Online	Cluster Shared Volume	WIN-HYPERV-N1	6	MBR	203 GI
HyperV-MSSQL-UserData-2	Online	Cluster Shared Volume	WIN-HYPERV-N2	8	MBR	203 GE
HyperV-MSSQL-UserData-1	(Online	Cluster Shared Volume	WIN-HYPERV-N2	4	MBR	203 GI
HyperV-MSSQL-UserData-0	(Online	Cluster Shared Volume	WIN-HYPERV-N1	8	MBR	203 GI
HyperV-MSSQL-TempDB	(Online	Cluster Shared Volume	WIN-HYPERV-N1	11	MBR	103 GE
HyperV-MSSQL-System	() Online	Cluster Shared Volume	WIN-HYPERV-N1	4	MBR	103 GE
📇 HyperV-MSSQL-Quorum	(f) Online	Cluster Shared Volume	WIN-HYPERV-N2	5	MBR	1.20 GI
📇 Cluster Disk 1	Online	Disk Witness in Quorum	WIN-HYPERV-N1	1	MBR	10.0 GE

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\Volumenn 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.V.ClusterCt			
C:\ClusterSt Volume in d		na labal	
		is 5A69-FAA0	
Vorume Seri	ar Number	15 5A09-FAA0	
Directory o	f C.\Clust	enStonage	
bireccory o		cr scor uge	
09/19/2017	05:51 AM	<dir></dir>	
09/19/2017	05:51 AM	<dir></dir>	
09/19/2017	05:21 AM	<junction></junction>	Volume3 [\??\Volume{839699f1-f684-4396-8bf5-96dd7d6973a7}\]
09/19/2017	05:21 AM	<junction></junction>	Volume4 [\??\Volume{0b9c7ef1-708a-46a4-96cc-704371c810e0}\]
09/19/2017	05:21 AM	<junction></junction>	Volume5 [\??\Volume{ca1f7f04-d0b2-41a7-870b-92f4cc1ae3cd}\]
09/19/2017	05:21 AM	<junction></junction>	Volume6 [\??\Volume{a5d5fb18-9c86-47e9-9f72-6fac24e4aacd}\]
09/19/2017	05:21 AM	<junction></junction>	Volume7 [\??\Volume{5bca7221-d3d1-479a-8f65-6a4cb94831f0}\]
09/19/2017	05:21 AM	<junction></junction>	Volume8 [\??\Volume{83a9fea3-dc76-4ae8-be7b-845db639b045}\]
09/19/2017		<junction></junction>	Volume9 [\??\Volume{230c918d-5079-4e31-b31b-a77150360116}\]
	0 File(0 bytes
	9 Dir(s	5) 91,690,311,0	580 bytes free
C:\ClusterSt	orage>ren	Volume3 HyperV-	-MSSQL-System
c.) c]+c+		Malling & House M	NCCOL TamaDD
C:\ClusterSt	orage>ren	Volume4 HyperV	-MSSQL-TempDB
C.) ClustonSt		VolumeE HunonV	-MSSQL-UserData-0
c. (crusterst	onagezhen	vorumes Hyperv-	-MSSQL-USEIDaca-0
C:\ClusterSt	orage\ren	Volume6 HyperV.	-MSSOL-UserData-1
e. (eruster se	or age /r en	vorumeo nyperv	
C:\ClusterSt	orage>ren	Volume7 HyperV-	-MSSQL-UserData-2
C:\ClusterSt	orage>ren	Volume8 HyperV-	-MSSQL-UserData-3
		1.31	
C:\ClusterSt	orage≻ren	Volume9 HyperV-	-MSSQL-UserLog
	-	" 001/	

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 \rightarrow 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.

192.168.162.92 - Remote Desktop Conn	ection		Test and the	an Thinks		
Railover Cluster Manager						
File Action View Help						
🗢 🔿 🖄 📰 🛛 🖬						
Railover Cluster Manager	Roles (2)					
VUCSDOMAIN.UCSDOMAIN.CORP	Search					
Roles	Name		Status	Туре	Owner Node	Priority
> 🛃 Storage	SCVMM WIN-MSSO	I MI Passuras	O.maina	Virtual Machine	WIN-HYPERV-N1	Medium
Networks	SCVMM WIN-N	Connect		Virtual Machine	WIN-HYPERV-N2	Medium
Elister Events	0	Start				
	0	Save				
	0	Shut Down				
		Turn Off				
	1	Settings				
	34	Manage				
	20	Replication	•			
		Move	•			
	3	Cancel Live Migra	tion			
	3	Change Startup Pr	iority 🕨			
	6	Information Detai	S			
		Show Critical Ever	ts			
	2	Add Storage				
		Add Resource				
		More Actions	•			
	×	a and a state of the				
		Properties				

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.

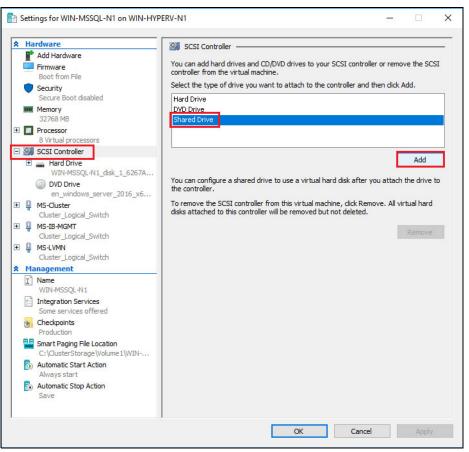


Figure 8-6 Add shared drives to the VM

6. Click **New** as indicated in Figure 8-7 to start the wizard. Click **Next** if you are prompted with an introduction.

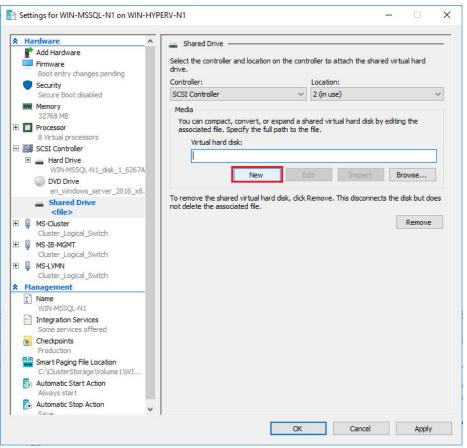


Figure 8-7 Create a new VHD file

7. Click VHDX to choose the VHDX format for the virtual hard disk, as shown in Figure 8-8.

 New Virtual Hard Disk Wiz Choose Disk 	
Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location Configure Disk Summary	What format do you want to use for the virtual hard disk? Image: WHDX This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012. VHD Set This format is for shared virtual hard disks only, and enables backup of virtual machine groups using shared virtual hard disks. This format is not supported in operating systems earlier than Windows 10.
	< Previous Next > Finish Cancel

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.

🚢 New Virtual Hard Disk Wiz	tard X
🚢 Choose Disk	к Туре
Before You Begin Choose Disk Format	What type of virtual hard disk do you want to create?
Choose Disk Format Choose Disk Type Specify Name and Location	Fixed size This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
Configure Disk Summary	Opynamically expanding This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.
	< Previous Next > Finish Cancel

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.

🚢 New Virtual Hard Disk Wizard		×
Specify Name and Loo	cation	
	the name and location of the virtual hard disk file.	
Choose Disk Format Name:	HyperV-MSSQL-Quorum vhdx	
Choose Disk Type Specify Name and Location	: C:\ClusterStorage\HyperV-MSSQL-Quorum\	Browse
Configure Disk		
Summary		
	< Previous Next > Finish	Cancel

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.

Before You Begin	You can create a blank virtual hard disk or copy the c	ontents of an existing physical disk.	
Choose Disk Format Choose Disk Type Specify Name and Location	Create a new blank virtual hard disk Size: GB (Maximum: 64 TB)		
Configure Disk	Copy the contents of the specified physical disk: Physical Hard Disk	Size	^
Summary	\\.\PHYSICALDRIVE0	127 GB	
	\\.\PHYSICALDRIVE1	9 GB	
	\\. PHYSICALDRIVE2	499 GB	
	\\. PHYSICALDRIVE3	499 GB	
	\\.\PHYSICALDRIVE4	101 GB	
	\\. \PHYSICALDRIVE5	201 GB	
	\\.\PHYSICALDRIVE6	201 GB	¥
	O Copy the contents of the specified virtual hard di	sk	
	Path:	B	rowse

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.

 New Virtual Hard Disk Wiz Completing 	the New Virtual Hard Disk Wizard	×
Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location Configure Disk Summary	You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk. Description: Format: VHDX Type: fixed size Net Creating the new virtual hard disk Siz Cancel To create the virtual hard disk and close this wizard, click Finish.	
	< Previous Next > Finish Cance	

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 \rightarrow 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.

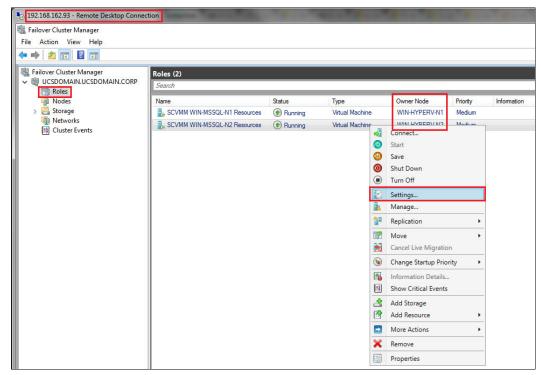


Figure 8-13 Change the VM role settings

5. Navigate to SCSI Controller, select Shared Drive from the selection, and click Add, as shown in Figure 8-14.

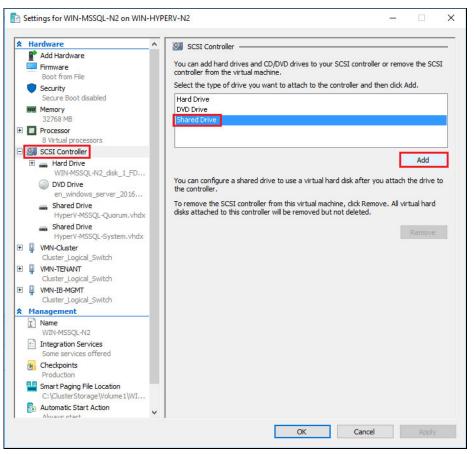


Figure 8-14 Add shared drives to the VM

6. Click **Browse**, and select the location of shared drive (VHDX file), as shown in Figure 8-15.

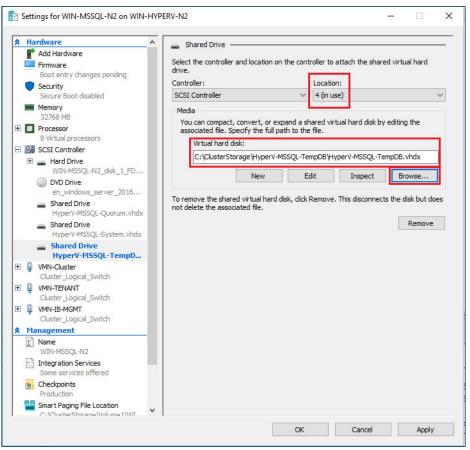


Figure 8-15 Provide VHDX location

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 167. 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.
- 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 \rightarrow 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.

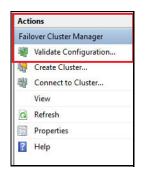


Figure 8-16 Start the cluster validation wizard

4. Enter the host names of the nodes, or browse and select them. Then, click **Next**, as shown in Figure 8-17.

Cluster Testing Options Enter name:	
Confirmation	Browse
Validating Selected servers: WIN-MSSQL-N1.UCSDOMAIN.CORP WIN-MSSQL-N2.UCSDOMAIN.CORP	Add
Summary	Remove

Figure 8-17 Enter host names

5. Select the Run all tests (recommended) option, and click Next as shown in Figure 8-18.

💐 Validate a Config	uration Wizard	×
Testing (Options	
Before You Begin Select Servers or a Cluster	Choose between running all tests or running selected tests. The tests examine the Cluster Configuration, Hyper-V Configuration, Inventory, Network, Storage, and System Configuration.	
Testing Options Confirmation Validating Summary	Microsoft supports a cluster solution only if the complete configuration (servers, network, and storage) can pass all tests in this wizard. In addition, all hardware components in the cluster solution must be "Certified for Windows Server 2016."	
	Run all tests (recommended) Run only tests I select	
	More about cluster validation tests	
	< Previous Next > Cancel]

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.

Validate a Config			
Before You Begin Select Servers or a Cluster	Testing has completed for the tests you selected. To confi you must run all tests. A cluster solution is supported by Mi validation tests, and all tests succeed (with or without war	crosoft only if you run all clu	
Testing Options	Node		^
Confirmation	WIN-MSSQL-N1.UCSDOMAIN.CORP	Validated	
alidating	WIN-MSSQL-N2.UCSDOMAIN.CORP	Validated	
	Result		
ummary	List BIOS Information	Success	
	List Disks	Success	
	List Disks To Be Validated	Success	
	List Environment Variables	Success	
	List Files Channel Hest Rus Adapton	Success	~
	Create the cluster now using the validated nodes		
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.	Viev	v Report
			Finish

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**.

 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.

Before You Begin	Type the name yo	u want to use v	when administering the cluster.	
Select Servers	Cluster Name:	MSSQLCLU	JS	
Access Point for Administering the Cluster Confirmation				IPv4 addresses could not be configured network is selected, and then type an
reating New Cluster		Net	works	Address
ummary			192.168.160.0/22	192 . 168 . 162 . 96

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.

Create Cluster Wi		×
Before You Begin Select Servers Access Point for	You are ready to create a cluster. The wizard will create your cluster with the following settings:	
Administering the Cluster	Cluster	^
Confirmation	MSSQLCLUS	_
Creating New Cluster Summary	Node WIN-MSSQL-N1.UCSDOMAIN.CORP WIN-MSSQL-N2.UCSDOMAIN.CORP	ъ
	Cluster registration DNS and Active Directory Domain Services	~
	Add all eligible storage to the cluster. To continue, click Next.	
	< Previous Next > Car	ncel

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.

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 GI
AS_BINS-1	(f) Online	Cluster Shared Volume	WIN-HYPERV-N1	2	MBR	500 Gi
HyperV-MSSQL-UserLog	(f) Online	Cluster Shared Volume	WIN-HYPERV-N2	10	MBR	103 G
HyperV-MSSQL-UserData-3	(Online	Cluster Shared Volume	WIN-HYPERV-N1	6	MBR	203 G
HyperV-MSSQL-UserData-2	(Online	Cluster Shared Volume	WIN-HYPERV-N2	8	MBR	203 G
HyperV-MSSQL-UserData-1	Online	Cluster Shared Volume	WIN-HYPERV-N2	4	MBR	203 G
HyperV-MSSQL-UserData-0	(Online	Cluster Shared Volume	WIN-HYPERV-N1	8	MBR	203 G
📇 HyperV-MSSQL-TempDB	(Online	Cluster Shared Volume	WIN-HYPERV-N1	11	MBR	103 G
HyperV-MSSQL-System	Online	Cluster Shared Volume	WIN-HYPERV-N1	4	MBR	103 Gi
📇 HyperV-MSSQL-Quorum	(Online	Cluster Shared Volume	WIN-HYPERV-N2	5	MBR	1.20 G
📇 Cluster Disk 1	(Online	Disk Witness in Quorum	WIN-HYPERV-N1	1	MBR	10.0 G

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 \rightarrow Configure Cluster Quorum Settings, as shown in Figure 8-23.

-	n View Help					
Failover (퀳 M	Cluster Manager Disks (a Configure <u>R</u> ole	B)				
	Validate Cluster		Status	Assigned To		
v 📒	View Validation Report	Disk 1	(Online	Available Stora	age	
ę	Add <u>N</u> ode	Disk 2	(Online	Available Stora	age	
	Close Connection	Disk 3	(Online	Available Stora	age	
	-	-	— Disk 4	Disk 4	(Online	Available Storage
14	<u>R</u> eset Recent Events	eset Recent Events		Available Stora	Storage	
	More Actions	> 0	Configure Cluster <u>Q</u> uorum :	Settings	je	
	Re <u>f</u> resh	<u>(</u>	opy Cluster Roles		je	
	P <u>r</u> operties	Shut Down Cluster				
	<u>H</u> elp	Destroy Cluster				
		N	Nove Core Cluster <u>R</u> esource	es >		
			Cluster-Aware Updating			

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.

Configure Cluster	Quorum Wizard	×
Select Qu	Jorum Configuration Option	
Before You Begin	Select a guorum configuration for your cluster.	
Select Quorum Configuration Option	O Use default quorum configuration	
Select Quorum Witness	The cluster determines quorum management options, including the quorum witness.	
Confirmation	Select the quorum witness	
Configure Cluster Quorum Settings	You can add or change the quorum witness. The cluster determines the other quorum management options.	
Summary	 Advanced quorum configuration You determine the quorum management options, including the quorum witness. Failover Cluster Quorum and Witness Configuration Options	
	< Previous Next > Cancel	

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.

🐮 Configure Cluste	r Quorum Wizard	х
Select Q	uorum Witness	
Before You Begin Select Quorum Configuration Option	Select a quorum witness option to add or change the quorum witness for your cluster configuration. As a best practice, configure a quorum witness to help achieve the highest availability of the cluster.	
Select Quorum Witness	Configure a disk witness Adds a quorum vote of the disk witness	
Configure Storage Witness Confirmation Configure Cluster Quorum Settings Summary	Configure a file share witness Adds a quorum vote of the file share witness Configure a cloud witness Adds a quorum vote of the cloud witness Do not configure a quorum witness Failover Cluster Quorum and Witness Configuration Options	
	< Previous Next > Cancel	

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.

Before You Begin	Select the storage volume the	nat you want to assign a	s the disk witness.		
Select Quorum Configuration Option					
Select Quorum Witness	Name	Status	Node	Location	^
Configure Storage	🔲 🕀 🔠 Cluster Disk 1	(Online	WIN-MSSQL-N1	Available Storage	
Vitness	🔲 🗄 进 Cluster Disk 2	Online	WIN-MSSQL-N1	Available Storage	
onfirmation	🔲 🗄 📇 Cluster Disk 3	🕥 Online	WIN-MSSQL-N1	Available Storage	
onfigure Cluster	🗹 🗆 🔠 Cluster Disk 4	🕥 Online	WIN-MSSQL-N1	Available Storage	
auorum Settings	Volume: (\\?\	File System: NTFS	950 MB free of 990 MB		
	🔲 🗄 🏭 Cluster Disk 5	① Online	WIN-MSSQL-N1	Available Storage	~
iummary	<			3	

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.

Configure Cluste	er Quorum Wizard	×
Summar	y .	
Before You Begin Select Quorum Configuration Option	You have successfully configured the quorum settings for the cluster	
Select Quorum Witness	Cluster Managed Voting Enabled	
Configure Storage Witness	Witness Type Disk Witness	
Confirmation	Witness Resource	
Configure Cluster Quorum Settings	Cluster Disk 4	
Summary		
	To should a second and a factor of a fact Mars Decod	
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.	View Report
		Finish

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.

File Action View Help							
🗢 🔿 🔁 📆 🖬							
🝓 Failover Cluster Manager	Disks (8)						
MSSQLCLUS.UCSDOMAIN.CORP	Search						
Roles	Name	Status	Assigned To 🔺	Owner Node Disk	Number	Partition Style Capac	ty
✓ A Storage B Disks	🔠 Cluster Disk 5	(Online	Available Storage	WIN-MSSQL-N1	5	GPT	200 0
	킍 Cluster Disk 6	(Online	Available Storage	WIN-MSSQL-N1	8	GPT	100 0
Pools Enclosures	킍 Cluster Disk 7	(Online	Available Storage	WIN-MSSQL-N1	2	GPT	100 0
Networks	El Cluster Disk 8	(Online	Available Storage	WIN-MSSQL-N1	6	GPT	200 0
III Cluster Events	Cluster Disk 1	(Online	Available Storage	WIN-MSSQL-N1	7	GPT	200 0
	Eluster Disk 2	() Online	Available Storage	WIN-MSSQL-N1	4	GPT	200 0
	긙 Cluster Disk 3	(Online	Available Stora	WIN MCCOL NA	3	GPT	100 0
	E Cluster Disk 4	() Online	Disk Witness ir	Bring Online Take Offline Simulate Failure	1	GPT	1.00 0
			<u></u>	Add to Cluster Shared Volumes			
				More Actions	•		
				Remove			

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\Volumenn 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 in drive C has no label. Volume Serial Number is 5A69-FA	
Volume Serial Number 15 5A69-FA	Að
Directory of C:\ClusterStorage	
Directory of C. (Clusterstorage	
09/19/2017 05:51 AM <dir></dir>	
09/19/2017 05:51 AM <dir></dir>	
09/19/2017 05:21 AM <junctio< td=""><td>N> Volume3 [\??\Volume{839699f1-f684-4396-8bf5-96dd7d6973a7}\]</td></junctio<>	N> Volume3 [\??\Volume{839699f1-f684-4396-8bf5-96dd7d6973a7}\]
09/19/2017 05:21 AM <junctio< td=""><td></td></junctio<>	
09/19/2017 05:21 AM <junctio< td=""><td>이야지 않는 것은 것은 것이 집에 가장 것을 하는 것이 같은 것이 있는 것이 같은 것이 있는 것은 것이 같은 것이 같은 것이 같이 많이 있는 것이 없는 것이 없</td></junctio<>	이야지 않는 것은 것은 것이 집에 가장 것을 하는 것이 같은 것이 있는 것이 같은 것이 있는 것은 것이 같은 것이 같은 것이 같이 많이 있는 것이 없는 것이 없
09/19/2017 05:21 AM <junctio< td=""><td></td></junctio<>	
09/19/2017 05:21 AM <junctic< td=""><td></td></junctic<>	
09/19/2017 05:21 AM <junctic< td=""><td><pre>W> Volume8 [\??\Volume{83a9fea3-dc76-4ae8-be7b-845db639b045}\]</pre></td></junctic<>	<pre>W> Volume8 [\??\Volume{83a9fea3-dc76-4ae8-be7b-845db639b045}\]</pre>
09/19/2017 05:21 AM <junctic< td=""><td><pre>W> Volume9 [\??\Volume{230c918d-5079-4e31-b31b-a77150360116}\]</pre></td></junctic<>	<pre>W> Volume9 [\??\Volume{230c918d-5079-4e31-b31b-a77150360116}\]</pre>
0 File(s)	0 bytes
9 Dir(s) 91,690,	311,680 bytes free
C:\ClusterStorage≻ren Volume3 Hy	perV-MSSQL-System
over status i povo da menurata i den el matematica el como povo se como	
C:\ClusterStorage≻ren Volume4 Hy	perV-MSSQL-TempDB
C:\ClusterStorage≻ren Volume5 Hy	perv-MSSQL-UserData-0
C:\ClusterStorage≻ren Volume6 Hy	Dept MEEOL LicesDate 4
C:\ClusterStorage>ren Volume6 Hy	perv-MSSQL-USerbala-1
C:\ClusterStorage≻ren Volume7 Hy	nenV-MSSOI-licenData-2
c. (cruster stor age/ren vorume/ ny	
C:\ClusterStorage≻ren Volume8 Hy	perV-MSSOI-UserData-3
erter bereinigert en vorameo ny	
C:\ClusterStorage≻ren Volume9 Hy	perV-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 153 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.

📸 SQL Server Installation Center	– 🗆 X	
Planning Installation	New SQL Server stand-alone installation or add features to an existing installation Launch a wizard to install SQL Server 2016 in a non-clustered environment or to add features to an existing SQL Server 2016 instance.	^
Maintenance Tools Resources Advanced	 Install SQL Server Management Tools Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Databases Tuning Advisor. An internet connection is required to install these tools. Install SQL Server Data Tools Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Azure 	
Options	SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT. New SQL Server failover cluster installation Launch a wizard to install a single-mode SQL Server 2016 failover cluster.	
	Add node to a SQL Server failover cluster Launch a wizard to add a node to an existing SQL Server 2016 failover cluster. Upgrade from a previous version of SQL Server Launch a vizard to upgrade a previous version of SQL Server to SQL Server 2016.	
	New R Server (Standalone) installation Launch a wizard to install R Server (Standalone) on a Windows machine. This is typically used by data scientists as a standalone analysis server or as a SQL Server R Services client.	

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**.
- 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.
- 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.

🃸 Install a SQL Server Failover Clust	ter		- 🗆 X
Feature Selection Select the Standard features to	install.		
Product Key License Terms Global Rules Microsoft Update Install Sedup Files Install Failover Cluster Rules Feature Selection Feature Rules Instance Configuration Cluster Resource Group Cluster Disk Selection Cluster Network Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress Complete	Features: Instance features ☑ Database Engine Services ☑ SQL Server Replicatio ☑ Full-Text and Semant ☑ Data Quality Services □ PolyBase Query Servi □ Analysis Services - Nation □ Stata Quality Client □ Client Tools Connectivity Select All Unselect All Instance root directory: Shared feature directory Shared feature directory	n ic Extractions for Sec ce for External Data ve ePoint n for SharePoint Proc r C:\Program Files\W C:\Program Files\W	Feature description: The configuration and operation of each isolated from other SQL Server instance. Subject isolated from other SQL Server. Already installed: Wirrosoft. NFT Framework 4.6 Disk Space Requirements Dirke C: 1482 MB required, 87746 MB available Microsoft SQL ServerA Servering isolated from other isola
	1		< Back Next > Cancel

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.

髋 Install a SQL Server Failover Clus	ter				1 <u>-</u> 3		×
Instance Configuration	n						
Specify the name and instance	e ID for the instance of SQL Ser	ver. Instance ID be	ecomes part of	the installation path			
Product Key License Terms	Specify a network name for your failover cluster on the		er failover clus	ter. This will be the r	name used to	identify	
Global Rules	SQL Server Network Name:	SQLCLUS					
Microsoft Update Install Setup Files Install Failover Cluster Rules	Default instance						
Feature Selection	O Named instance:	MSSQLSERVER					
Feature Rules			R.				
Instance Configuration	Instance ID:	MSSQLSERVER					
Cluster Resource Group Cluster Disk Selection Cluster Network Configuration	SQL Server directory:	C:\Program Files	· ∖Microsoft SQL	. Server\MSSQL13.M	SSQLSERVER		
Server Configuration	Detected SQL Server instance	es and features or	n this computer	:			
Database Engine Configuration	Instance Cluster	Network Name	Features	Edition	Version		Inst
Feature Configuration Rules Ready to Install							
Installation Progress							
Complete							
	<						>
	1			< Back	lext >	Cance	el

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.

🐮 Install a SQL Server Failover Clus						<u>-</u>		×
Cluster Resource Grou	р							
Create a new cluster resource	group for your	SQL Server failover cluste	r.					
Product Key License Terms Global Rules	failover clu	ame for the SQL Server cl ster resources will be plac sew cluster resource group	ed. You	can choose to use an exi				
Microsoft Update	SQL Ser	ver cluster resource group	name:	SQLCLUS SQL Server (N	ASSQLSERVER)			~
Install Setup Files								
Install Failover Cluster Rules	Qualified	Name	м	essage				
Feature Selection		Available Storage	-	e cluster group 'Available	e Storage' is resen	ved by I	Windows	Fai.
Feature Rules Instance Configuration		Cluster Group	Th	e cluster group 'Cluster (Group' is reserved	by Win	dows Fa	ilov
Cluster Resource Group								
Cluster Disk Selection								
Cluster Network Configuration								
Server Configuration								
Database Engine Configuration								
Feature Configuration Rules								
Ready to Install								
Installation Progress								
Complete							Refre	sh
				< Back	Next >		Cance	el

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**.

tinstall a SQL Server Failover Clu	ster					đ	-		×
Cluster Disk Selection	i								
Select shared cluster disk reso	ources for your S	QL Server failover clu	ster.						
Product Key License Terms Global Rules	used as the	shared disks to be in default drive for all o figuration pages.							
Microsoft Update Install Setup Files Install Failover Cluster Rules Feature Selection	HyperV- HyperV- HyperV- HyperV-	MSSQL-System MSSQL-TempDB MSSQL-UserData-0 MSSQL-UserData-1 MSSQL-UserData-2							*
Feature Rules Instance Configuration	Available sh		88						
Cluster Resource Group	Qualified	Disk HyperV-MSSQL-Qu	orum	Message The disk resou	rce 'HyperV-MSS(QL-Quorum' car	nnot b	oe used	^
Cluster Network Configuration Server Configuration		HyperV-MSSQL-Sys HyperV-MSSQL-Ten							
Database Engine Configuration	Ø	HyperV-MSSQL-Use	1						
Feature Configuration Rules Ready to Install		HyperV-MSSQL-Use							_
Installation Progress		HyperV-MSSQL-Use							~
Complete								Refres	h
					< Back	Next >	1	Cancel	

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.

髋 Install a SQL Server Failover Clust	er								×
Cluster Network Confi Select network resources for yo	-		lover clu:	ster.					
Product Key License Terms			twork <u>s</u> et DHCP	tings for this failo	ver cluster: Subnet Mask	6 hours		twork	
Global Rules		IP Ty				Subnet(s)			
Microsoft Update		IPv4		192.168.162.95	255.255.252.0	192.168.160.0/22	Clu	ster Netw	ork 1
Install Setup Files									
Install Failover Cluster Rules									
Feature Selection									
Feature Rules									
Instance Configuration									
Cluster Resource Group									
Cluster Disk Selection									
Cluster Network Configuration									
Server Configuration									
Database Engine Configuration									
Feature Configuration Rules									
Ready to Install									
Installation Progress									
Complete								<u>R</u> ef	resh
					[< Back Next	>	Cance	:

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.

Server Configuration					
Specify the service accounts a	nd collation configuration.				
Product Key	Service Accounts Collation				
License Terms Global Rules	Microsoft recommends that you use	a separate account for each	SQL Server serv	ice.	
Global Rules Microsoft Update	Service	Account Name	Password	Startup T	vne
Install Setup Files	SQL Server Agent	UCSDOMAIN.CORP\Ad	••••••	Manual	
install Failover Cluster Rules	SQL Server Database Engine	UCSDOMAIN.CORP\Ad		Manual	~
Feature Selection	SQL Full-text Filter Daemon Launc	NT Service\MSSQLFDLa		Manual	
Feature Rules	SQL Server Browser	NT AUTHORITY\LOCAL		Automati	c 🗸
Cluster Resource Group Cluster Disk Selection Cluster Network Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install Installation Progress	Grant Perform Volume Maintenan This privilege enables instant file to information disclosure by allow <u>Click here for details</u>	nitialization by avoiding zero	oing of data pag		ead
Complete					

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.

S Install a SQL Server Failover Clust	er		-		
Database Engine Confi	guration				
Specify Database Engine authe	ntication security mode,	administrators, data directories and TempDB settings.			
Product Key	Server Configuration	Data Directories TempDB FILESTREAM			
License Terms Global Rules	Specify the authent	ication mode and administrators for the Database Engin	e.		
Vicrosoft Update	Authentication Mod	de	1		
install Setup Files	O Windows authen	tication mode			
nstall Failover Cluster Rules	0				
Feature Selection	Mixed Mode (SQ	L Server authentication and Windows authentication)			
eature Rules	Specify the passwor	rd for the SQL Server system administrator (sa) account.	-		
nstance Configuration	Enter password:	•••••			_
Cluster Resource Group					_
Cluster Disk Selection	Confirm password:				
Cluster Network Configuration	Specify SQL Server a	administrators			
Server Configuration	UCSDOMAIN\Adm	inistrator (Administrator)	SQL Server adr	ministrato	ors
Database Engine Configuration			have unrestrict		
eature Configuration Rules			to the Databas	se Engine	63
leady to Install					
nstallation Progress					-
Complete	Add Current User	Add Remove			
		< Back	Next >	Cance	el

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.

髋 Install a SQL Server Failover Clust	er			×
Database Engine Confi				
Specify Database Engine authe	ntication security mode, administr	ators, data directories and TempDB settings.		
Product Key	Server Configuration Data Dir	rectories TempDB FILESTREAM		
License Terms			_	
Global Rules	Data root directory:	C:\ClusterStorage\HyperV-MSSQL-System\		
Microsoft Update	System database directory:	C:\ClusterStorage\HyperV-MSSQL-		
Install Setup Files		System\MSSQL13.MSSQLSERVER\MSSQL\Data		
Install Failover Cluster Rules	User database directory:	C:\ClusterStorage\HyperV-MSSQL-System\MSSQL13.MSSQLSEF	19	1
Feature Selection		C) ChurterSterrenzbille and // MSSOL StetrenzbMSSOL 12 MSSOL	-	1
Feature Rules	User database log directory:	C:\ClusterStorage\HyperV-MSSQL-System\MSSQL13.MSSQLSEF	o	
Instance Configuration	Backup directory:	C:\ClusterStorage\HyperV-MSSQL-System\MSSQL13.MSSQLSEF	R	
Cluster Resource Group				1
Cluster Disk Selection				
Cluster Network Configuration				
Server Configuration				
Database Engine Configuration				
Feature Configuration Rules				
Ready to Install				
Installation Progress				
Complete				
		< Back Next >	Cancel	
		S BACK INEXT >	cancer	

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.

📸 Install a SQL Server Failover Clust	er		-		×
Database Engine Confi Specify Database Engine authe	-	ministrators, data directories and TempDB settings.			
Product Key License Terms Global Rules Microsoft Update Install Setup Files Install Failover Cluster Rules Feature Selection Feature Rules	TempDB data files: te Number of files: 8 Initial size (MB): 8 Autogrowth (MB): 64	Total initial size (MB): 64		Add	
Instance Configuration Cluster Resource Group Cluster Disk Selection Cluster Network Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install	TempDB log file: te Initial size (MB): ⁶ Autogrowth (MB): ⁶⁴			Remove	
Installation Progress Complete	Log directory: C	:\ClusterStorage\HyperV-MSSQL-TempDB\TempDB			
		< Back Nex	t >	Cance	1

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.

Verify the SQL Server 2016 features to be installed. Product Key License Terms Global Rules Microsoft Update Install Failover Cluster Rules Install Failover Cluster Rules Instance Configuration Cluster Retwork Configuration Cluster Network Configuration Custer Network Configuration Database Engine Configuration Database Engine Configuration Database Engine Configuration Instance Configuration Database Engine Configuration Instante Configuration Instance Configuration Instance Configuration Configuration Instance Configuration Configuration Rules Instance Configuration Instance Configuration Instance Instance Configuration Instance Name: MSSQLSERVER Instance Name: MSSQLSERVER Instance Instance Configuration Configuration File path:	Des du és lusés II		
Global Rules Globa	Product Key	Ready to install the SQL Server 2016 failover cluster.	
Install Stup Files Prerequisites Already installed: Windows PowerShell 3.0 or higher Database Engine Services Server Configuration Database Engine Configuration Rules Instance Inh Micro (SERVER Installation Progress Configuration file path: Version Server Windows Power Shell 2.0 or higher Windows Power Shell 2.0 or higher Windows Power Shell 2.0 or higher Windows Power	Global Rules	Edition: Standard	Í
Complete	Install Setup Files Install Failover Cluster Rules Feature Selection Feature Rules Instance Configuration Cluster Resource Group Cluster Network Configuration Server Configuration Database Engine Configuration Feature Configuration Rules Ready to Install	Already installed: Windows PowerShell 3.0 or higher Windows PowerShell 3.0 or higher Microsoft Visual Studio 2010 Redistributables General Configuration Features Database Engine Services Sol. Server Replication Full-Text and Semantic Extractions for Search Data Quality Services Instance Configuration Instance Name: MSSQLSERVER Instance In: MSSQL SERVER	>
	Complete	C:\Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20170919_061354\ConfigurationFile.i	ni

Figure 8-40 Review installation summary

19. After the installation completes, verify the installation summary, and click **Close**, as shown in Figure 8-41.

🃸 Install a SQL Server Failover Clus	ter		_		×
Complete Your SQL Server 2016 failover	cluster installation is complete.				
Product Key License Terms	Information about the Setup operation or possible				
Global Rules	Feature	Status			^
Microsoft Update	Database Engine Services	Succeeded			
Install Setup Files	Data Quality Services	Succeeded			
Install Failover Cluster Rules	Full-Text and Semantic Extractions for Search SQL Server Replication	Succeeded			
Feature Selection	SOL Browser	Succeeded			
	SOL Writer	Succeeded			~
Feature Rules					
Instance Configuration					
Cluster Resource Group	Details:				
Cluster Disk Selection					
Cluster Network Configuration					
Server Configuration					
Database Engine Configuration					
Feature Configuration Rules					
Ready to Install					
Installation Progress	Summary log file has been saved to the following lo	ocation:			
Complete	C:\Program Files\Microsoft SQL Server\130\Setup E MSSQL-N1_20170919_072258.bt	300tstrap\Log\20170919_072258	Summar	y WIN-	
			E	Close	:

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 187, 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.

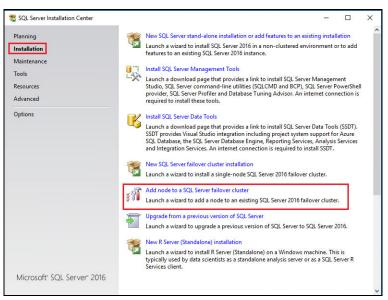


Figure 8-42 Add a node to SQL Server failover cluster

- 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.
- 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.
- 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.

📸 Add a Failover Cluster Node							×
Cluster Node Configure		er.					
Product Key License Terms Global Rules Microsoft Update Install Setup Files Add Node Rules Cluster Node Configuration	SQL Server ins Name of this I Disk Space Re	node:	MSSQLSERVER WIN-MSSQL-N2 Drive C: 1482 MB requi	red, 87701 MB availab	le		~
Cluster Network Configuration Service Accounts Feature Rules Ready to Add Node Add Node Progress Complete	Instance Name MSSQLSERVER	Cluster Network Name SQLCLUS	Features SQLEngine, SQ	Nodes WIN-MSSQL-N1			
				< Back	Next >	Cano	el .

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**.

Cluster Note		ulan.					-		>
Cluster Network Confi The current node that is being shown are the previously com	added	does not							
Product Key	Spec	ify the ne	twork se	tings for this failo	ver cluster:				
License Terms Global Rules		IP Ty	DHCP	Address	Subnet Mask	Subnet(s)	Ne	etwork	_
Giopai Rules Microsoft Update		IPv4		192.168.162.95	255.255.252.0	192.168.160.0/22	Clu	ister Netw	ork
Cluster Node Configuration Cluster Network Configuration Service Accounts Feature Rules Ready to Add Node Add Node Progress Complete									
								Ref	resh
						< Back Next	>	Cance	el

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.

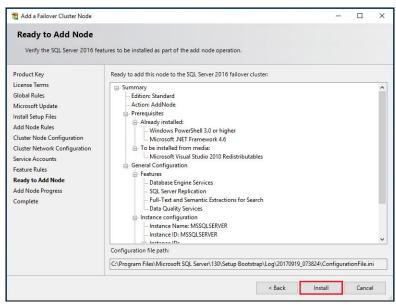


Figure 8-45 Ready to add the node

13. After the installation is complete, verify the installation summary, and click **Close**, as shown in Figure 8-46.

髋 Add a Failover Cluster Node		10			×
Complete Your SQL Server 2016 failover	cluster add node operation is complete.				
Product Key	Information about the Setup operation or possible	next steps:			
License Terms Global Rules	Feature	Status			^
Global rules Microsoft Update Install Setup Files Add Node Rules Cluster Node Configuration Cluster Network Configuration Service Accounts Feature Rules Ready to Add Node Add Node Progress Complete	Database Engine Services Data Quality Services Data Quality Services Sult Server Replication SQL Server Replication SQL Browser SQL Browser Details: Details: Summary log file has been saved to the following log C\Program. Files/Microsoft SQL Server\130.Setup 5 MSSQL-N2_20170919_073824.txt		mmaŋ	∠ WIN-	•
				Close	

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.

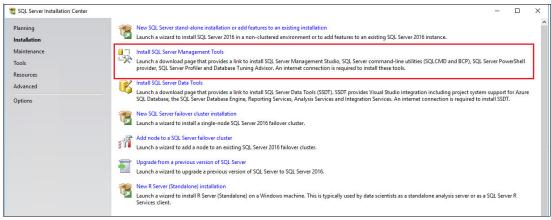


Figure 8-47 Download link for SSMS

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.

RELEASE 17.2 Microsoft SQL Server Management Studio	-
Welcome. Click "Install" to begin.	
By clicking the "Install" button, I acknowledge that I accept the <u>License Terms</u> and Privacy Statement.	
SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about SQL Server Management Studio data processing and privacy controls, see the privacy statement link above.	
Install Close	

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.

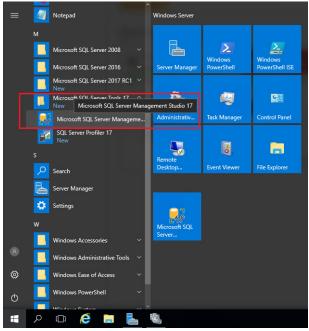


Figure 8-49 Launching SQL Server Management Studio

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 187.

name: SoluciUS	Connect to Server		×
name: SoluciUS		SQL Server	
tication: Windows Authentication rname: UCSDOMAIN/Administrator	erver type:	Database Engine	~
er name: UCSDOMAIN\Administrator	erver name:	SQLCLUS	~
	thentication:	Windows Authentication	~
teword.	User name:	UCSDOMAIN\Administrator	~
Remember password	Password:	Remember pageword	

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.
- 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.

ect Explorer								
nnect - 🛱 🎽 🔳 🔻	- 4 ×							
SQLCLUS (SQL Server								
SQLCLUS (SQL Server Databases	13.0.1001.5 - 0C5							
100								
New Database								
elect a page	🗐 Script 👻 😧 Help							
General Options								
Filegroups	Database name:	VERSADB						
	Owner:	<default></default>						1
		(adriadic)						
	Use full-text indexing							
	Database files:							1 -
	Logical Name	File Type	Filegroup	Initial Size (Autogrowth / Maxsize	Path	File Name	
	VERSADB-DATA-0	ROWS Data	PRIMARY	200	None	 C:\ClusterStorage\HyperV-MSSQL-UserData-0	VERSADB-DATA-0	
	VERSADB-DATA-1	ROWS Data	PRIMARY	200	None		VERSADB-DATA-1	
	VERSADB-DATA-2	ROWS Data	PRIMARY	200	None		VERSADB-DATA-2	
	VERSADB-DATA-3	ROWS Data	PRIMARY	200	None	C:\ClusterStorage\HyperV-MSSQL-UserData-3	WERSADB-DATA-3	
	VERSADB-LOG	LOG	Not Appli	100	None	 C:\ClusterStorage\HyperV-MSSQL-UserLog	VERSADB-LOG	
							Record of the second se	
onnection								
erver: QLCLUS								
Connection:								
CSDOMAIN\administrator								
View connection propert	ies							
ogress	< C							

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.

WIN-MSSQL-N2 Propertie	5	×
General	Self-Service	
Status	If the virtual machine will be assigned to a self-service user, specify the number of points to apply towar virtual machine quota while the virtual machine is deployed.	rd the owner's
Hardware Configuration	Quota points: 1	
Checkpoints	Preferred Owners	
Custom Properties	Select the preferred owners for this virtual machine. Use the buttons to list them in order from most pre to least preferred at the bottom:	ferred at the top
Settings	WIN-HYPERV-N2.UCSDOMAIN.CORP	Move Up
Settings	□ 🕽 WIN-HYPERV-N1.UCSDOMAIN.CORP	Move Down
Actions		
Servicing Windows		
Dependencies		
Validation Errors		
Access	Possible Owners	
Storage	Clear the checkbox if you don't want a node to host this virtual machine:	
Storage	WIN-HYPERV-N2.UCSDOMAIN.CORP	Select All
	VIN-HYPERV-N1.UCSDOMAIN.CORP	Clear All
	() VMM configures possible owners only for 'virtual machine resource'.	-
View Script	ОК	Cancel

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 Storwize V5030 advanced functions

This chapter describes the following advanced functions that are provided by the IBM Storwize V5030:

- ▶ 9.1, "IBM Easy Tier" on page 204
- ▶ 9.2, "IBM HyperSwap" on page 206
- ▶ 9.3, "Remote copy" on page 207
- ▶ 9.4, "IBM FlashCopy" on page 208
- ▶ 9.5, "Encryption" on page 209
- ▶ 9.6, "Volume mirroring" on page 210
- ▶ 9.7, "Thin provisioning" on page 210
- 9.8, "IBM Real Time Compression" on page 211
- 9.9, "Microsoft offloaded data transfer" on page 212

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

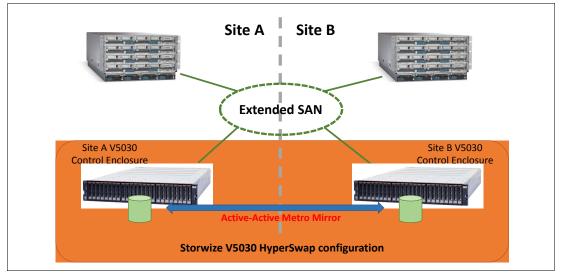


Figure 9-2 depicts a high-level design for a V5030 HyperSwap configuration.

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.

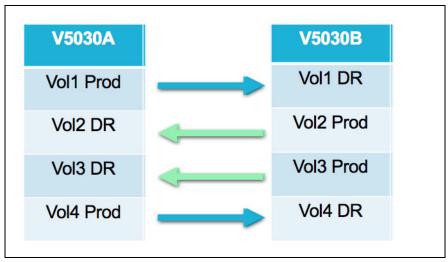


Figure 9-3 A mix of primary and secondary volumes

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.

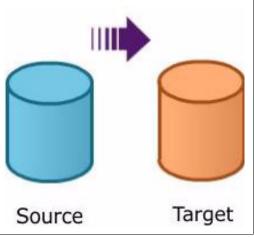


Figure 9-4 FlashCopy flow

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 Storwize V5030 supports encryption of data at rest, as shown in Figure 9-5.

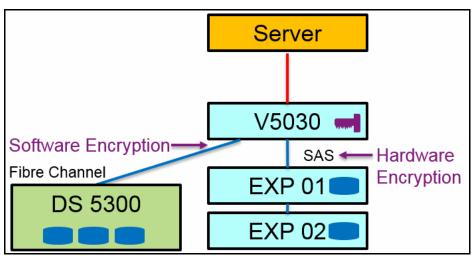


Figure 9-5 Encryption

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.

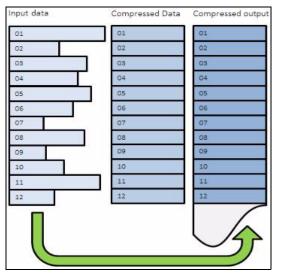


Figure 9-6 Compression operation diagram

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.

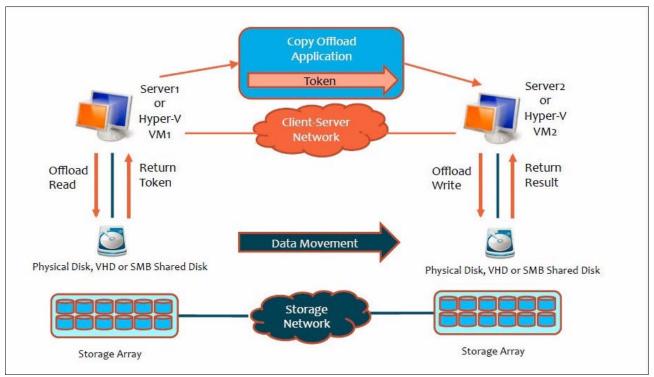


Figure 9-7 ODX operation

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 214
- ► 10.2, "The IBM Storwize V5030 Manager" on page 217
- ▶ 10.3, "The Cisco UCS GUI manager" on page 225
- ▶ 10.4, "Microsoft System Center Virtual Machine Manager" on page 229

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 Storwize V5030, 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)

 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	:	75700cd5-893e-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	r.'	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.SystemCent	er.VirtualMachineManager.Remoting.ServerConnection

ID	: 2c3bf218-6bae-49e6-9ca1-754d7f52d66c
MarkedForDeletion	: False
IsFullyCached	: True
MostRecentTaskIfLocal	: Adds Storage Provider

- 6. Open the VMM Management Console.
- 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
٨	Refresh host cluster	Completed w/ Info	9/14/2017 10:46:09 AM		UCSDOMAIN.UCSDOMAIN.CORP
0	Update logical switch virtual network ad	Completed	9/14/2017 10:45:23 AM		MS-IB-MGMT
8	Remove logical network definition	Failed	9/14/2017 10:39:01 AM		MS-IB-MGMT
0	Change properties of logical network	Completed	9/14/2017 10:39:01 AM		MS-IB-MGMT
8	Create logical network definition	Failed	9/14/2017 10:38:03 AM		Job Failed
Ø	Change properties of logical network	Completed	9/14/2017 10:38:02 AM		MS-IB-MGMT
Ø	Creates new Storage Classification	Completed	9/14/2017 10:17:03 AM		test class
٨	Refresh host cluster	Completed w/ Info	9/14/2017 10:16:41 AM		UCSDOMAIN.UCSDOMAIN.CORP
0	Change properties of virtual machine host	Completed	9/14/2017 10:14:24 AM		WIN-HYPERV-N1.UCSDOMAIN.CORP
4	Adds Storage Provider	Completed	9/14/2017 10:14:15 AM		V5030
Ø	Change properties of virtual machine host	Completed	9/14/2017 10:07:29 AM		WIN-HYPERV-N1.UCSDOMAIN.CORP
0	Create new RunAs Account	Completed	9/14/2017 9:59:25 AM		v5030.superuser
Ø	Change properties of virtual machine host	Completed	9/14/2017 9:52:51 AM		WIN-HYPERV-N2.UCSDOMAIN.CORP
0	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 Storwize V5030 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 Storwize V5030 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.

	ze [®] V5000 agement (VersaStack)	
User name: Password:	•••	
	Log in 🔿	H
	Corp. ⊚ IBM Corporation and other(s) 2016. IBM and Storwize a in the United States, other countries, or both.	re registered

Figure 10-2 IBM Storwize V5030 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 218 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 Storwize V5030 advanced functions" on page 203.
- 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.

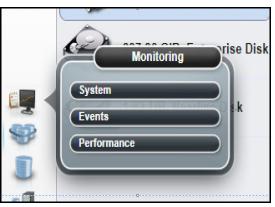


Figure 10-4 Monitoring menu

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 218. 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 Storwize V5030, 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 210 and 9.8, "IBM Real Time Compression" on page 211.

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.

+ Create Volumes	E Actions	Q Filter	
Name		State	Syc
Bronze		✓ Online	
HyperV-AD		✓ Online	
HyperV-Host1	-Boot	✓ Online	
HyperV-Host1	-Boot_Copy	✓ Online	

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.

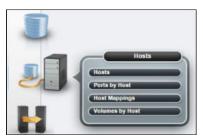


Figure 10-8 Hosts menu

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 220.

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 Storwize V5030 advanced functions" on page 203.



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 224. 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:

 Select Security from the menu in Figure 10-11. Select Configure Remote Authentication → LDAP (Figure 10-12).

Configure R	emote Authenti	cation	x
Select Aut	hentication		
IBM Tiv	oli Integrated P	ortal	
LDAP			
	< Back	Next	Cancel

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.

Configure Remote Authentication	×
LDAP Type	
IBM Tivoli Directory Server	
Microsoft Active Directory	
) Other	
Security	
Transport Layer Security	
O None	
► Advanced Settings	
	ancel

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.

e (15)	11000 - Satings - Network	1000 Marvana (15000 Begerinner (Security Administration)	۲
		los	test.
	Network	Management IP Addresses	1
	Management IP Addresses	The management IP address is assigned during the initialization of the system and represents a set of enclosurus on the system that contains the management OUI and the command-line interface which management (IP address). If you change management (IP address) to go to the management (IP address) to go to t	Ŀ
-	Service IP Addresses	A system uses the same management IP addresses for all control enclosures.	Ŀ
	Ethernet Ports		L
43.	ISCSI		
3	Fibre Channel Connectivity		
00	Fibre Channel Ports		
~			_
50	Alexand: 13.00.00 / 0.30		(II)

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 224.
- 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 224. 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 214, 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.

Æ	All
	▼ Equipment
	▼ Chassis
몲	🕨 Chassis 1 (primary) 👽
	 Chassis 2 (extended)
	▼ Rack-Mounts
	 Servers
▣	▼ Fabric Interconnects
_	▼ Fabric Interconnect A (subordinate)
	▼ Fixed Module
=	Ethernet Ports
	► FC Ports
20	 Fabric Interconnect B (primary)
	▼ Policies
	Port Auto-Discovery Policy

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 225.

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.

Equipment							
Main Topology View	Fabric Interconnects	Servers	Thermal	Decommissioned	Firmware Management	Policies	F
+ - Ty Advanced F	filter 🔶 Export 🚔 Print						
Name	Address		If Role	lf	Туре	Overall Sta	tus

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.

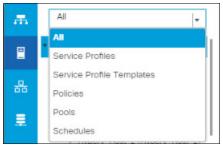


Figure 10-17 UCS Server menu

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.

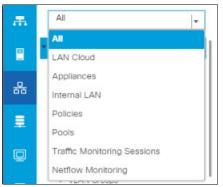


Figure 10-18 LAN management

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 42.

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.

æ	All	*
	All	
	SAN Cloud	
	Storage Cloud	
55 S	Policies	
	Pools	
	 omratin oroopa 	

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 226, 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 214, 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.

-	VMs and Services	
1	Fabric	
	Library	
Ē	Jobs	
-	Settings	
		•

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.

VMs and Services	<
🥵 Tenants	
i Clouds	
🚰 Azure Subscriptions	
📥 VM Networks	
🧧 Storage	
All Hosts	

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

•	👥 Servers
۶.	📥 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.

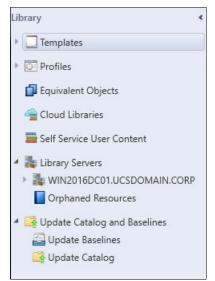


Figure 10-23 SCVMM Library

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 Storwize V5030 node failure" on page 234
- ► 11.2, "Fabric Interconnect failure" on page 239
- ▶ 11.3, "Microsoft WSFC and Microsoft SQL Server AlwaysOn FCI validation" on page 243
- ▶ 11.4, "Cisco Nexus Virtual PortChannel peer switch failure" on page 245
- ▶ 11.5, "Cisco UCS service profile migration validation" on page 246
- ▶ 11.6, "Hyper-V virtual machine failover" on page 248

11.1 IBM Storwize V5030 node failure

The pair of nodes within a single IBM Storwize V5030 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 Storwize V5030 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 **1sportfc** command, where you can see that all eight FC ports are active.

Example 11-1 The Isportfc 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,node2,500507680D0058F1,400220,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 Storwize V5030 CLI and GUI.
- 2. Click **System** \rightarrow **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

 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
Figuro	11-2 Alert to down	od norte				

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.

The Fibre Chann	el ports a	re located on this	node					
Machine Type a	nd Model	Node Identifier	Node Nam	e Enclos	ure Identifier	Enclosure Serial Number	Panel Name	Canister Position In Enclosure
2078-324		2	node2	1		781B546	01-2	Right
The current stat	us of the	Fibre Channel por	ts					
Adapter slot ID	Port ID	Port WWPN	Curre	nt status	Expected stat	us		
1	1	500507680D045	BF1 Inacti	/e	Active			
1	2	500507680D085	BF1 Inacti	/e	Active			
1	3	500507680D0C5	BF1 Active		Active			
1	4	500507680D105	F1 Active		Active			

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.

	not operatio	nal						
Theck the Fibre	e Channe	l cabling						
or the ports that o	currently h	ave inactive status	and are not e	expected	to be, check the	Fibre Channel cable.		
Ensure the c	orrect type	e of cable is being u	ised.					
 If the cable a 	appears da	maged, replace it.						
 If there are 	any sharp	bends in the cable,	re-route or r	eplace it.				
Reseat the c	able conne	ector by unplugging	the cable for	two seco	onds, and then n	econnecting it.		
fter performing th	is service	action, click Next t	o check the r	ort statu	15.			
10 JE 5				ore statu				
elect one of these	options b	efore clicking Next	6					
Fibre Channel s	tatus is ind	correct, try next ser	vice action					
_		correct, try next ser rrect, mark as fixed						
Fibre Channel s	tatus is co		1					
Fibre Channel s Fibre Channel s	tatus is co el ports a	rrect, mark as fixed re located on this	node	Enclos	sure Identifier	Enclosure Serial Number	Panel Name	Canister Position In Enclosure
Fibre Channel s Fibre Fibre Chann Machine Type a	tatus is co el ports a	rrect, mark as fixed re located on this Node Identifier	node	Enclos		Enclosure Serial Number 7818546	Panel Name 01-2	Canister Position In Enclosure Right
Fibre Channel s The Fibre Chann Machine Type a 2078-324	tatus is co el ports a nd Model	rrect, mark as fixed re located on this Node Identifier	node Node Name node2	Enclos				
Fibre Channel s The Fibre Chann Machine Type a 2078-324 The current state	tatus is co el ports a nd Model us of the	rrect, mark as fixed re located on this Node Identifier 2 Fibre Channel poo	node Node Name node2	1		781B546		
Fibre Channel s The Fibre Chann Machine Type a 2078-324 The current state	tatus is co el ports a nd Model us of the	rrect, mark as fixed re located on this Node Identifier 2 Fibre Channel poo	i node node2 rts Curren	1 t status		781B546		
Fibre Channel s The Fibre Chann Machine Type a 2078-324 The current state	tatus is co el ports a nd Model us of the Port ID 1	rrect, mark as fixed re located on this Node Identifier 2 Fibre Channel por Port WWPN	node Node Name node2 ts Curren 8F1 Inactiv	1 t status re	Expected stat	781B546		
Fibre Channel s The Fibre Chann Machine Type at 2078-324	tatus is co el ports a nd Model us of the Port ID 1 2	rrect, mark as fixed re located on this Node Identifier 2 Fibre Channel por Port WWPN 500507680D045	node Node Name node2 rts Curren 8F1 Inactiv 8F1 Inactiv	1 t status re	Expected stat	781B546		

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.

Error is marked	d as fixed
The event is mark	ed as fixed.
lick Close to exit	t.

Figure 11-5 Error is fixed

11.1.2 Node failure

An IBM Storwize V5030 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 Storwize V5030 GUI. I/O is running, and the health status is *green*. The IBM Storwize V5030 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.

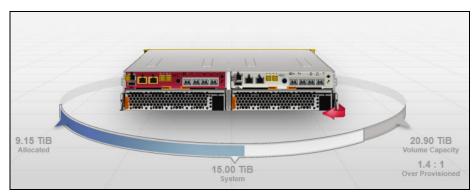


Figure 11-8 System view showing node offline

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.

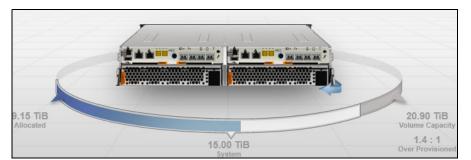


Figure 11-9 System view showing the node online

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.

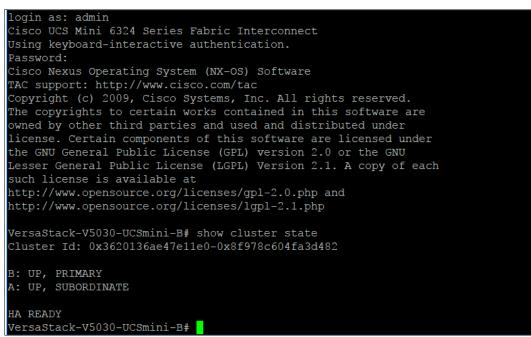


Figure 11-10 Logging in to the Fabric Interconnect

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.

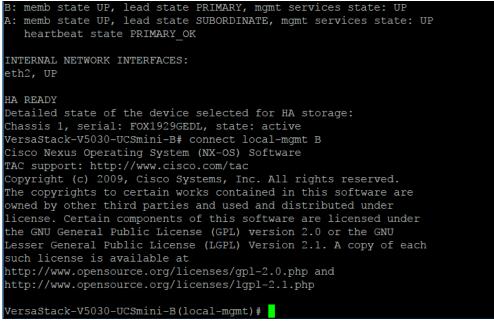


Figure 11-11 Connecting with connect local-management B

 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 10 Deheat the Febrie Interconnect

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
eer Fabric Interconnect is down
etailed 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.



Figure 11-15 Change Fabric Interconnect B to the primary switch

 Connect to local management A and reboot Fabric Interconnect A, as shown in Figure 11-16.

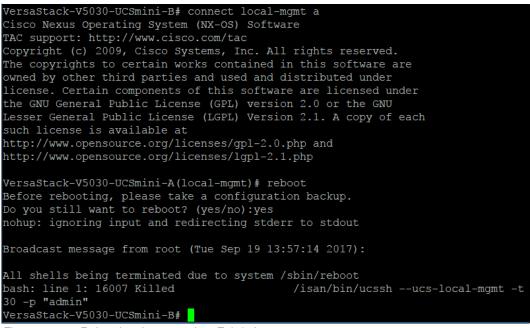


Figure 11-16 Rebooting the secondary Fabric Interconnect

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.

5 192.168.162.98 - Remote Deskto	p Connection	1970		1 1 8 11	
🍓 Failover Cluster Manager					
File Action View Help					
🗢 🄿 🖄 🖬 🚺					
File Action View Help File Action View Help Failover Cluster Manager Failover Cluster Manager MSSQLCLUS.UCSDOMAIN. File Roles Name					
Ligger	Name	Status	Туре	Owner Node	
Networks	SQLCLUS SQL Server (💿 Running	Other	WIN-MSSQL-N1	

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.

a) 🍙 🔜 🕺 🖾 🖾	3	[🔄 🍽 💈 🛸 🥖 🤇	3 🕙 🛞 _	RUN	NNING - TPC-C	
Benchmark	^_	Script Editor Virtual User Output Tra	insaction Counter	Metrics 🐴 Auto	pilot	
SQL Server		Virtual User 1	Virtual	l User 2	Virtual User 3	^
 TPC-C Schema Build Options Build Envice Script Options Load Virtual User Options Create 		payment OE 463211111 BIG1320cg04V0DNRth 2900 Mq JIGFGFEpUCYuNF9 JUN472c330MhDztKQkFx67L4Vhzy3A Geyr25790Xg15De0HLzdTKYtbFIC 8291AV/jrvQhg2YCA5hhpnaVZgipm0 K2aTquQrFGvjgrs7xusy2Hc4na0aain JH7VeN/73RYxMG5WmtUqhpyNOd TGvDhBMXaJDALo0bXn3ERUbKJr6 myXebYe6bwg5xx7vL10R13A4IZqqJ B0WKcy07nGphCNqwh2)xh65mvgpP IkfuEvd0215B25dBCDd1wkUpvchDst Virtual User 4	0.14 0.37 new order	CALLYABLEPRES PRESPRESBAR	2463 -10.0000 OE dhaseZT2qsFGKvWM OUGHTPRIBAR new order 3108 0.11 BC PRESBARANTI 0.14 0.27 payment OE 463211111 NGySM2hPqF2b7I 4100 Oi WQfvZMg56P9E8KL2 E703NYNmN2bR0bXtcVVF1IRyBGZUf 4bQYRn8/3ti4TvVI2JTLu6PCxLsYa1n 365esp3TJqib6i5xofhVIZ06Vevn7epi	1
🔷 Run 🖅 🐺 Autopilot		new order 3093 - 0.12 BC CALL VEINGOLIGHT				~
🗄 🥁 Autophot	~					
		Iterations		Complete	Status	1
<u> </u> 1		1		0	8	
🧧 2		1		0		
📱 3		1		0	and the second s	
4		1		0	a la	
_						

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*.

📱 Failover Cluster Manager File Action View Help 🃁 🛶 🛛 🙍 💼 🛛 🛐								
 Hailover Cluster Manager ✓ I MSSQLCLUS.UCSDOMAIN. I Roles 	Nodes (2) Search						P	Queries 🔻 拱 🗸 🗸
 Moles Norage 	Name	Status	Assigned Vote 1 1	Current Vote 1 1	Site	Rack	Chassis	Information

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.

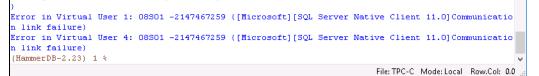


Figure 11-20 Lost connection to SQL Server cluster

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.

MSSQLCLUS.UCSDOMAI	Search			
🍯 Nodes	Name	Status	Assigned To	Owner Node
 Nodes Storage Disks Pools Enclosures Networks 	HyperV-MSSQL-Quorum	Online	Disk Witness in Quorum	WIN-MSSQL-N2
	HyperV-MSSQL-System	Online	Cluster Shared Volume	WIN-MSSQL-N2
	HyperV-MSSQL-TempDB	Online	Cluster Shared Volume	WIN-MSSQL-N2
🐴 Networks	HyperV-MSSQL-UserDat	() Online	Cluster Shared Volume	WIN-MSSQL-N2
🔢 Cluster Events	HyperV-MSSQL-UserDat	Online	Cluster Shared Volume	WIN-MSSQL-N2
	HyperV-MSSQL-UserDat	Online	Cluster Shared Volume	WIN-MSSQL-N2
	HyperV-MSSQL-UserDat	🕥 Online	Cluster Shared Volume	WIN-MSSQL-N2
	HyperV-MSSQL-UserLog	(Online	Cluster Shared Volume	WIN-MSSQL-N2

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.

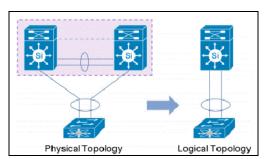


Figure 11-22 Cisco Nexus vPC topologies

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:

 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.

quipment / Cha	issis / Chassis 2 (extended)			
General	Servers Service Profiles	s IO Modules	Fans PSU	s Hybrid Display Slots	Installed Firmwa
Advanced Filter	r 🛉 Export 🚔 Print	Overall Status	User Label	Operability	Power State
Server 1	Cisco UCS B200 M4	Power Off		↑ Operable	↓ Off
Derver					

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.

						50 50		
General	Servers Service Profile	s IO Modules	Fans PSUs	Hybrid Display Slots	Installed Firmware	SEL Logs	Power Control Monitor	Cc>
Y Advanced Filter	r 🛉 Export 🚔 Print							₽
Name	Model	Overall Status	User Label	Operability	Power State	Assoc State	Fault Suppression	S
Server 1	Cisco UCS B200 M4	↓ Unassociated		1 Operable	↓ Off	↓ None	N/A	
Server 2	Cisco UCS B200 M4	↓ Power Off		Operable	↓ Off	1 Associate	d N/A	

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:

Disks (11)				Ac	tions
Search		J	👂 Queries 🔻 🔛 👻 👽	Dis	sks
Name	Status	Assigned To	Owner Node Dis	. 3	Add Disk
📇 Cluster Disk 1	🕥 Online	Disk Witness in Quorum	WIN-HYPERV-N1	3	Move Available Storage
ItyperV-MSSQL-Quorum	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N2		View
HyperV-MSSQL-System	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N1	a	Refresh
HyperV-MSSQL-TempDB	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N2	_	Help
ItyperV-MSSQL-UserDat	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N1		c.p
ItyperV-MSSQL-UserDat	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N2		
📇 HyperV-MSSQL-UserDat	Online	Cluster Shared Volume	WIN-HYPERV-N1		
进 HyperV-MSSQL-UserDat	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N2		
📇 HyperV-MSSQL-UserLog	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N1		
BINS-1	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N2		
BINS-2	🕥 Online	Cluster Shared Volume	WIN-HYPERV-N1		
	Search Name Cluster Disk 1 HyperV-MSSQL-Quorum HyperV-MSSQL-System HyperV-MSSQL-UserDat. HyperV-MSSQL-UserDat. HyperV-MSSQL-UserDat. HyperV-MSSQL-UserDat. HyperV-MSSQL-UserDat. HyperV-MSSQL-UserDat. HyperV-MSSQL-UserLog SS_BINS-1	Search Name Status Clutter Disk 1 ① Online HyperV-MSSQL-Quorum ④ Online HyperV-MSSQL-System ④ Online HyperV-MSSQL-System ④ Online HyperV-MSSQL-UserDat ④ Online HyperV-MSSQL-UserLog ④ Online HyperV-MSSQL-UserLog ④ Online HyperV-MSSQL-UserLog ④ Online HyperV-MSSQL-UserLog ④ Online	Search Assigned To Name Status Assigned To Intermediate Online Disk Witness in Quorum Intermediate HyperV-MSSQL-Quorum Intermediate HyperV-MSSQL-System Online Cluster Shared Volume HyperV-MSSQL-JuserDat Online Cluster Shared Volume HyperV-MSSQL-UserDat Online Cluster Shared Volume HyperV-MSSQL-UserLog Online Cluster Shared Volume OS_BINS-1 Online Cluster Shared Volume	Search Queries Image Name Status Assigned To Owner Node Disk Cluster Disk 1 Image Disk Witness in Quorum WIN-HYPERV-N1 Image HyperV-MSSQL-Quorum Online Cluster Shared Volume WIN-HYPERV-N2 Image HyperV-MSSQL-System Online Cluster Shared Volume WIN-HYPERV-N1 Image HyperV-MSSQL-UserDatOnline Cluster Shared Volume WIN-HYPERV-N1 Image HyperV-MSSQL-UserDatOnline Outline Cluster Shared Volume WIN-HYPERV-N1 Image HyperV-MSSQL-UserDatOnline Outline Cluster Shared Volume WIN-HYPERV-N2 Image HyperV-MSSQL-UserDatOnline Cluster Shared Volume WIN-HYPERV-N1 Image OS	Status Assigned To Owner Node Disk Name Status Assigned To Owner Node Disk ² Cluster Disk 1 [®] Online Disk Witness in Quorum WIN-HYPERV-N1 ² HyperV-MSSQL-Quorum [®] Online Cluster Shared Volume WIN-HYPERV-N1 ² HyperV-MSSQL-System [®] Online Cluster Shared Volume WIN-HYPERV-N1 ² HyperV-MSSQL-JoserDat. [®] Online Cluster Shared Volume WIN-HYPERV-N1 ⁸ HyperV-MSSQL-UserDat. [®] Online Cluster Shared Volume WIN-HYPERV-N1 ⁸ HyperV-MSSQL-UserDat. [®] Online Cluster Shared Volume ^{WIN-HYPERV-N1 [#] [#] HyperV-MSSQL-UserDat. [®] Online [®] Cluster Shared Volume ^{WIN-HYPERV-N1 [#] HyperV-MSSQL-UserDat. [®] Online [®] Cluster Shared Volume ^{WIN-HYPERV-N1 [#] HyperV-MSSQL-UserDat. [®] Online [®] Cluster Shared Volume ^{WIN-HYPERV-N1}}}}

- WIN-HYPERV-N1
- WIN-HYPERV-N2

5

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** \rightarrow **Select Node**.

This scenario moves the WIN-HYPERV-N2 volumes to WIN-HYPERV-N1, as shown in Figure 11-27.

P Search	Clear	
luster nodes:		
Name	Status	
WIN-HYPERV-N1	🕐 Up	
WIN-HYPERV-N2	🛞 Up	

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.

ailover Cluster Manager	Disks (11)				Actions	
UCSDOMAIN.UCSDOMAI	Search			Queries 🔻 🔛 👻 😪	Disks	
Nodes	Name	Status	Assigned To	Owner Node Disk	🛃 Add Disk	
	📇 Cluster Disk 1	🕥 Online	Disk Witness in Quorum	WIN-HYPERV-N1	💣 Move Available Storage	
Broad Provide State Stat	HyperV-MSSQL-Quorum	🕜 Online	Cluster Shared Volume	WIN-HYPERV-N1	View	
Enclosures	HyperV-MSSQL-System	Online	Cluster Shared Volume	WIN-HYPERV-N1	G Refresh	
 Nodes Storage Disks Pools 	HyperV-MSSQL-TempDB	🕜 Online	Cluster Shared Volume	WIN-HYPERV-N1	Help	
	HyperV-MSSQL-UserDat_	🕜 Online	Cluster Shared Volume	WIN-HYPERV-N1		
	HyperV-MSSQL-UserDat	1 Online	Cluster Shared Volume	WIN-HYPERV-N1	Selected Disks (5)	
	HyperV-MSSQL-UserDat	Online	Cluster Shared Volume	WIN-HYPERV-N1	Bring Online	
	HyperV-MSSQL-UserDat	🕜 Online	Cluster Shared Volume	WIN-HYPERV-N1	Take Offline	
	HyperV-MSSQL-UserLog	🛞 Online	Cluster Shared Volume	WIN-HYPERV-N1	Move Move	
	BINS-1	🕜 Online	Cluster Shared Volume	WIN-HYPERV-N1	More Actions	
	BINS-2	🕜 Online	Cluster Shared Volume	WIN-HYPERV-N1	Remove from Cluster Shared Volumes	
	C.			8	2 Help	
	•					

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.

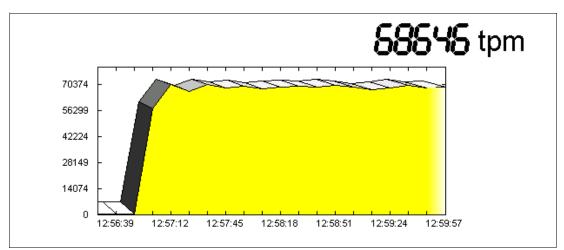


Figure 11-29 Application monitoring during the move at 12:59

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-virtualizati
on/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-virtualizati
on/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-virtualizati on/versastack-solution-cisco-ibm/aag-versastack-iaas.pdf?cm_mc_uid=858981548346 15046256647&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-virtualizati
on/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



ISBN 073844278X

UCS Mini, Hyper-V, and SQL Server ISBN 073844978X

Implementing a VersaStack Solution with IBM Storwize V5030, Cisco UCS Mini, Hyper-V, and SQL Server





SG24-8407-00

ISBN 073844278X

Printed in U.S.A.



Get connected

