PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

VCP-DCV for vSphere 8.x

JOHN A. DAVIS
STEVE BACA

FREE SAMPLE CHAPTER

VCP-DCV for vSphere 8.x Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **www.pearsonitcertification.com/register**.
2. Enter the **print book ISBN: 9780138169886**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

This page intentionally left blank

VCP-DCV for vSphere 8.x Cert Guide

John A. Davis, Steve Baca

Pearson

Hoboken, New Jersey

VCP-DCV for vSphere 8.x Cert Guide

ISBN-13: 978-0-13-816988-6

ISBN-10: 0-13-816988-8

Library of Congress Cataloging-in-Publication Data: 2023914336

$PrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

VICE PRESIDENT, IT PROFESSIONAL
Mark Taub

DIRECTOR, ITP PRODUCT MANAGEMENT
Brett Bartow

EXECUTIVE EDITOR
Nancy Davis

DEVELOPMENT EDITOR
Ellie Bru

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Mandie Frank

COPY EDITOR
Kitty Wilson

INDEXER
Erika Millen

PROOFREADER
Donna E. Mulder

TECHNICAL EDITOR
Joseph Cooper

PUBLISHING COORDINATOR
Cindy Teeters

DESIGNER
Chuti Prasertsith

COMPOSITOR
codeMantra

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Contents at a Glance

Table of Contents

About the Authors

John A. Davis, now an independent contractor and senior integration architect at MEJEER, LLC, became a VMware Certified Instructor (VCI) and VMware Certified Professional (VCP) in 2004. Since then, all of his work has focused on VMware-based technologies. He has experience in teaching official VMware curriculum in five countries and delivering VMware professional services throughout the United States. Recently, his work has involved designing and implementing solutions for hybrid clouds, cloud automation, disaster recovery, and virtual desktop infrastructure (VDI). He has authored several white papers and co-authored *VCP-DCV for vSphere 7.x Cert Guide*, *VCP6-DCV Cert Guide*, *and VCAP5-DCA Cert Guide* (VMware Press). He holds several advanced certifications, including VCAP-DCV 2021, VCP-NV 202, and VCP-DTM 2020. He has been a vExpert since 2014. He is the author of the vLoreBlog.com and can be found on Twitter @johnnyadavis.

Steve Baca, VCAP, VCI, VCP, and NCDA, has been in the computer industry for more than 20 years. Originally a computer programmer and a system administrator working on Unix and Windows systems, he migrated over to technical training and wrote a course for Sun Microsystems. After teaching various courses for Sun, he eventually transitioned to VMware about 10 years ago, to do technical training. Currently he is a badged employee for VMware and lives in Omaha, Nebraska. He thoroughly enjoys teaching and writing and believes that the constant evolution of the computer industry requires continuously learning to stay ahead. Steve can be found on Twitter @scbaca1.

Dedication

Dedicated to Madison, Emma, Jaxon, Ethan, Eli, and Robbie, the six wonderful children to whom I am blessed to be known as "Grampy." They fill my days with joy and fun, especially after a hard day of writing or working for their namesake, MEJEER, LLC.

—John Davis

First and foremost, I would like to dedicate this book to my loving wife, Sharyl. Without your support, I would not be able to commit the time necessary to co-author a book. Thank you for believing in me and allowing me to have the time for my many endeavors. I would also like to dedicate this book to my children: Zachary, Brianna, Eileen, Susan, Keenan, and Maura.

—Steve Baca

Acknowledgments

Thanks to my wife and best friend, Delores, who tolerates my late-night writing, supports my recent business venture, and makes me happy every day. Thanks to my parents, Monica and Norman Davis, who provided me with a great education and taught me the importance of hard work. Thanks to God for placing me in an environment with unmeasurable blessings and opportunities.

I would like to thank my co-authors and partners, Steve Baca and Owen Thomas. Thanks to our technical editor, Joe Cooper, for his hard work and dedication. Special thanks to Nancy Davis (executive editor) and Ellie Bru (development editor) for coordinating everything and keeping this project moving.

—John Davis

There are so many people to acknowledge and thank for making this book possible. First, thanks to my wife and family for supporting me while writing this book. I would also like to thank my co-authors, John Davis and Owen Thomas, who deserve much of the credit for this book. Thank you to the production team and editors at Pearson, who do a tremendous amount of work from the initial planning of the book to the final printing.

—Steve Baca

About the Technical Reviewer

Joseph Cooper is a Principal Instructor and a member of America's Tech Lead Team with VMware's Education Department. Joe has spoken at several VMworld conferences, VMUG events, and vForum events, and is a featured instructor in the VMware Learning Zone. Prior to joining VMware, Joe was an instructor at the State University of New York, College at Cortland, where he taught technology courses to sport management and kinesiology students. You can find him on Twitter @joeicooper and on YouTube at https://youtube.com/channel/UCYrPi0AqS8f8QxChAgZa5Sg.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *VCP-DCV for vSphere 8.x Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780138169886 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

This book focuses on one major goal: helping you prepare to pass the VMware vSphere 8.x Professional (2V0-21.23) exam, which is a key requirement for earning the VCP-DCV 2023 certification. This book may be useful for secondary purposes, such as learning how to implement, configure, and manage a vSphere environment or preparing to take other VCP-DCV qualifying exams.

The rest of this introduction provides details on the VCP-DCV certification, the 2V0-21.23 exam, and this book.

VCP-DCV Requirements

The primary objective of the VCP-DCV 2023 certification is to demonstrate that you have mastered the skills to successfully install, configure, and manage VMware vSphere 8 environments. You can find the exam requirements, objectives, and other details on the certification web portal, at http://mylearn.vmware.com/portals/certification/. On the website, navigate to the Data Center Virtualization track and to the VCP-DCV certification. Examine the VCP-DCV 2023 requirements based on your qualifications. For example, if you select that you currently hold no VCP certifications, then the website indicates that your path to certification is to gain experience with vSphere 8.0, attend one of the following required training courses, and pass the Professional vSphere 8.0 (2V0-21.23) exam:

- VMware vSphere: Install, Configure, Manage [V8]
- VMware vSphere: Optimize, Scale, and Secure [V8]
- VMware vSphere: Troubleshooting [V8]
- VMware vSphere: Fast Track [V8]

If you select that you currently hold a VCP-DCV 2020 or newer certification, the website indicates that your path includes a recommendation, but not a requirement, to take a training course.

VMware updates the VCP-DCV certification requirements each year. So, the requirements for the VCP-DCV 2024 certification may differ slightly from VCP-DCV 2023 certification. Likewise, VMware updates the qualifying exams. Each year, as VMware updates the Professional VMware vSphere 8.x exam, the authors of this book will create an appendix to supplement the original book. To prepare for a future version of the exam, download the corresponding online appendix from the book's companion website and use it to supplement the original book.

After you identify your path to certification, you can select the Professional VMware vSphere 8.x (2V0-21.23) exam to closely examine its details and to download the Exam Preparation Guide (also known as the exam blueprint).

Details on the 2V0-21.23 Exam

The 2V0-21.23 exam blueprint provides details on exam delivery, minimum qualifications for candidates, exam objectives, recommended courses, and references to supporting VMware documentation. It also contains 10 sample exam questions. The 2V0-21.23 exam is a proctored exam delivered through Pearson VUE. See Chapter 15, "Final Preparation," for details on registering and taking the exam.

A minimally qualified candidate (MQC) has 6 to 12 months of hands-on experience implementing, managing, and supporting a vSphere environment. The MQC has knowledge of storage, networking, hardware, security, business continuity, and disaster recovery concepts.

The exam characteristics are as follows:

- **Format**: Proctored exam
- **Question type**: Multiple choice
- **Number of questions**: 70
- **Duration**: 135 minutes
- **Passing score**: 300
- **Cost**: $250 (in the United States)

2V0-21.23 Exam Objectives

The 2V0-21.23 exam blueprint lists the exam objectives, which are summarized here:

Section 1: Architectures and Technologies

- Objective 1.1: Identify the pre-requisites and components for a VMware vSphere 8.x implementation
- Objective 1.2: Describe the components and topology of a VMware vCenter architecture

- Objective 1.3: Describe storage concepts
  - 1.3.1: Identify and differentiate storage access protocols for VMware vSphere (NFS, iSCSI, SAN, etc.)
  - 1.3.2: Describe storage datastore types for VMware vSphere
  - 1.3.3: Explain the importance of advanced storage configurations (vStorage APIs for Array Integration (VAAI), vStorage APIs for Storage Awareness (VASA), multipathing, etc.)
  - 1.3.4: Describe storage policies
  - 1.3.5: Describe basic storage concepts in VMware vSAN and VMware Virtual Volumes (vVOLs)
  - 1.3.6: Identify use cases for raw device mapping (RDM), Persistent Memory (PMem), Non-Volatile Memory Express (NVMe), NVMe over Fabrics (NVMe-oF), and RDMA (iSER)
  - 1.3.7: Describe datastore clusters
  - 1.3.8: Describe Storage I/O Control (SIOC)
- Objective 1.4: Describe VMware ESXi cluster concepts
  - 1.4.1: Describe VMware Distributed Resource Scheduler (DRS)
  - 1.4.2: Describe vSphere Enhanced vMotion Compatibility (EVC)
  - 1.4.3: Describe how DRS scores virtual machines
  - 1.4.4: Describe VMware vSphere High Availability (HA)
  - 1.4.5: Identify use cases for fault tolerance
- Objective 1.5: Explain the difference between VMware standard switches and distributed switches
  - 1.5.1: Describe VMkernel networking
  - 1.5.2: Manage networking on multiple hosts with vSphere Distributed Switch (VDS)
  - 1.5.3: Describe networking policies
  - 1.5.4: Manage Network I/O Control (NIOC) on a vSphere Distributed Switch (VDS)
  - 1.5.5: Describe Network I/O Control (NIOC)

- Objective 1.6: Describe VMware vSphere Lifecycle Manager concepts
- Objective 1.7: Describe the basics of VMware vSAN as primary storage
  - 1.7.1: Identify basic vSAN requirements (networking, disk count, and type)
  - 1.7.2: Identify Express Storage Architecture (ESA) concepts for vSAN 8
- Objective 1.8: Describe the role of Virtual Machine Encryption in a data center
  - 1.8.1: Describe vSphere Trust Authority
  - 1.8.2: Describe the role of a Key Management Services (KMS) server in vSphere
- Objective 1.9: Recognize methods of securing virtual machines
  - 1.9.1: Recognize use cases for a virtual Trusted Platform Module (vTPM)
  - 1.9.2: Differentiate between Basic Input or Output System (BIOS) and Unified Extensible Firmware Interface (UEFI) firmware
  - 1.9.3: Recognize use cases for Microsoft virtualization-based security (VBS)
- Objective 1.10: Describe identity federation
  - 1.10.1: Describe the architecture of identity federation
  - 1.10.2: Recognize use cases for identity federation
- Objective 1.11: Describe VMware vSphere Distributed Services Engine
  - 1.11.1: Describe the role of a data processing unit (DPU) in vSphere
- Objective 1.12: Identify use cases for VMware Tools
- Objective 1.13: Describe the high-level components of VMware vSphere with Tanzu
  - 1.13.1: Identify the use case for a Supervisor Cluster and Supervisor Namespace
  - 1.13.2: Identify the use case for vSphere Zones
  - 1.13.3: Identify the use case for a VMware Tanzu Kubernetes Grid (TKG) cluster

Section 2: VMware Products and Solutions

- Objective 2.1: Describe the role of VMware vSphere in the Software-Defined Data Center
- Objective 2.2: Identify use cases for VMware vSphere+
- Objective 2.3: Identify use cases for VMware vCenter Converter
- Objective 2.4: Identify disaster recovery (DR) use cases
  - 2.4.1: Identify VMware vCenter replication options
  - 2.4.2: Identify use cases for VMware Site Recovery Manager (SRM)

Section 3: Planning and Designing (There are no testable objectives for this section.)

Section 4: Installing, Configuring, and Setup

- Objective 4.1: Describe single sign-on (SSO)
  - 4.1.1: Configure a single sign-on (SSO) domain
  - 4.1.2: Join an existing single sign-on (SSO) domain
- Objective 4.2: Configure vSphere distributed switches
  - 4.2.1: Create a distributed switch
  - 4.2.2: Add ESXi hosts to the distributed switch
  - 4.2.3: Examine the distributed switch configuration
- Objective 4.3: Configure Virtual Standard Switch (VSS) advanced virtual networking options
- Objective 4.4: Set up identity sources
  - 4.4.1: Configure identity federation
  - 4.4.2: Configure LDAP integration
- Objective 4.5: Deploy and configure VMware vCenter Server Appliance (VCSA)
- Objective 4.6: Create and configure VMware HA and DRS advanced options (Admission Control, Proactive HA, etc.)

- Objective 4.7: Deploy and configure VMware vCenter High Availability
- Objective 4.8: Set up content library
  - 4.8.1: Create a content library
  - 4.8.2: Add content to the content library
  - 4.8.3: Publish a local content library
- Objective 4.9: Subscribe to content library
  - 4.9.1: Create a subscribed content library
  - 4.9.2: Subscribe to a published content library
  - 4.9.3: Deploy virtual machines (VMs) from a subscribed content library
- Objective 4.10: Manage virtual machine (VM) template versions
  - 4.10.1: Update template in content library
- Objective 4.11: Configure VMware vCenter file-based backup
- Objective 4.12: Configure vSphere Trust Authority
- Objective 4.13: Configure vSphere certificates
  - 4.13.1: Describe Enterprise PKIs role for SSL certificates
- Objective 4.14: Configure vSphere Lifecycle Manager
- Objective 4.15: Configure different network stacks
- Objective 4.16: Configure host profiles
- Objective 4.17: Identify ESXi boot options
  - 4.17.1: Configure Quick Boot
  - 4.17.2: Securely Boot ESXi hosts
- Objective 4.18: Deploy and configure clusters using the vSphere Cluster Quickstart workflow
  - 4.18.1: Use Cluster Quickstart workflow to add hosts
  - 4.18.2: Use Cluster Quickstart workflow to configure a cluster
  - 4.18.3: Use Quickstart to expand clusters
- Objective 4.19: Set up and configure VMware ESXi
  - 4.19.1: Configure Time Configuration
  - 4.19.2: Configure ESXi services

- 4.19.3: Configure Product Locker
- 4.19.4: Configure Lockdown Mode
- 4.19.5: Configure ESXi firewall

- Objective 4.20: Configure VMware vSphere with Tanzu
  - 4.20.1: Configure a Supervisor Cluster & Supervisor Namespace
  - 4.20.2: Configure a Tanzu Kubernetes Grid Cluster
  - 4.20.3: Configure vSphere Zones
  - 4.20.4: Configure Namespace permissions

Section 5: Performance-tuning, Optimization, Upgrades

- Objective 5.1: Identify resource pools use cases
  - 5.1.1: Explain shares, limits, and reservations (resource management)
- Objective 5.2: Monitor resources of a VMware vCenter Server Appliance (VCSA) and vSphere 8.x environment
- Objective 5.3: Identify and use resource monitoring tools
- Objective 5.4: Configure Network I/O Control (NIOC)
- Objective 5.5: Configure Storage I/O Control (SIOC)
- Objective 5.6: Configure a virtual machine port group to be offloaded to a data processing unit (DPU)
- Objective 5.7: Explain the performance impact of maintaining virtual machine snapshots
- Objective 5.8: Use Update Planner to identify opportunities to update VMware vCenter
- Objective 5.9: Use vSphere Lifecycle Manager to determine the need for upgrades and updates
  - 5.9.1: Update virtual machines
  - 5.9.2: Update VMware ESXi
- Objective 5.10: Use performance charts to monitor performance
- Objective 5.11: Perform proactive management with VMware Skyline
- Objective 5.12: Use VMware vCenter management interface to update VMware vCenter

- Objective 5.13: Complete lifecycle activities for VMware vSphere with Tanzu
  - 5.13.1: Update Supervisor cluster
  - 5.13.2: Back up and restore VMware vSphere with Tanzu

Section 6: Troubleshooting and Repairing

- Objective 6.1: Identify use cases for enabling vSphere Cluster Services (vCLS) retreat mode
- Objective 6.2: Differentiate between the main management services in VMware ESXi and vCenter and their corresponding log files
- Objective 6.3: Generate a log bundle

Section 7: Administrative and Operational Tasks

- Objective 7.1: Create and manage virtual machine snapshots
- Objective 7.2: Create virtual machines using different methods (Open Virtualization Format (OVF) templates, content library, etc.)
- Objective 7.3: Manage virtual machines (modifying virtual machine settings, VMware per-VM EVC, latency sensitivity, CPU affinity, etc.)
- Objective 7.4: Manage storage
  - 7.4.1: Configure and modify datastores
  - 7.4.2: Create virtual machine storage policies
  - 7.4.3: Configure storage cluster options
- Objective 7.5: Create DRS affinity and anti-affinity rules for common use cases
- Objective 7.6: Migrate virtual machines
  - 7.6.1: Identify requirements for Storage vMotion, Cold Migration, vMotion, and Cross vCenter Export
- Objective 7.7: Configure role-based access control
- Objective 7.8: Manage host profiles
- Objective 7.9: Utilize VMware vSphere Lifecycle Manager
  - 7.9.1: Describe firmware upgrades for VMware ESXi
  - 7.9.2: Describe VMware ESXi updates
  - 7.9.3: Describe component and driver updates for VMware ESXi

- 7.9.4: Describe hardware compatibility check
- 7.9.5: Describe ESXi cluster image export functionality
- 7.9.6: Create VMware ESXi cluster image

- Objective 7.10: Use predefined alarms in VMware vCenter
- Objective 7.11: Create custom alarms
- Objective 7.12: Deploy an encrypted virtual machine
  - 7.12.1: Convert a non-encrypted virtual machine to an encrypted virtual machine
  - 7.12.2: Migrate an encrypted virtual machine
  - 7.12.3: Configure virtual machine vMotion encryption properties

NOTE For future exams, download and examine the objectives in the updated exam blueprint. Be sure to use the future Pearson-provided online appendix specific to the updated exam.

NOTE Section 3 does not apply to the 2V0-21.23 exam, but it may be used for other exams.

Who Should Take This Exam and Read This Book?

The VCP-DCV certification is the most popular certification at VMware; more than 100,000 professionals around the world hold this certification. This book is intended for anyone who wants to prepare for the 2V0-21.23 exam, which is a required exam for VCP-DCV 2023 certification. The audience includes current and prospective IT professionals such as system administrators, infrastructure administrators, and virtualization engineers.

Book Features and Exam Preparation Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass the exam only by memorization but by truly learning and understanding the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it but do not study it any further, you probably will not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you don't know, and be well prepared for the exam. These tools include:

- **"Do I Know This Already?" Quizzes**: Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter.
- **Foundation Topics**: These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Exam Preparation Tasks**: This section of each chapter lists a series of study activities that should be done after reading the "Foundation Topics" section. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include the following:
  - **Key Topics Review**: The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The "Key Topics Review" section lists the key topics from the chapter and their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed for each key topic. Review these topics carefully.
  - **Memory Tables**: To help you exercise your memory and memorize some important facts, memory tables are provided. The memory tables contain only portions of key tables provided previously in the chapter, enabling you to complete the table or list. Appendix B, "Memory Tables," provides the incomplete tables, and Appendix C, "Memory Tables Answer Key," includes the completed tables (answer keys). These appendixes are also provided on the companion website that is provided with your book.
  - **Define Key Terms:** The VCP-DCV exam requires you to learn and know a lot of related terminology. This section lists some of the most important terms from the chapter and asks you to write a short definition and compare your answer to the glossary.
- **Practice Exams**: The companion website contains an exam engine.

Book Organization

The chapters in this book are organized such that Chapters 1 through 7 provide in-depth material on vSphere concepts, and Chapters 8 through 14 describe procedures

for the installation, configuration, and management of vSphere components and features. The authors recommend that you read the entire book from cover to cover at least once. As you read about any topic in Chapters 1 to 7, keep in mind that you can find corresponding "how to" steps in Chapters 8 to 14. As you read about any specific procedure in Chapters 8 to 14, keep in mind that you can find associated details (concepts) in Chapters 1 to 7.

Optionally, you can prepare for the exam by studying for the exam objectives in order, using Table I-1 as a guide. As you prepare for each exam objective, you can focus on the most appropriate chapter and section. You can also refer to related chapters and sections. For example, as you prepare for Objective 1.2 (Describe the components and topology of a VMware vCenter architecture), you should focus on the "vCenter Server Topology" section in Chapter 1, but you may also want to review the "Deploying vCenter Server Components" section in Chapter 8 and the "vSphere Managed Inventory Objects" section in Chapter 5.

When preparing for a specific exam objective, you can use Table I-1 to identify the sections in the book that directly address the objective and the sections that provide related information.

Table I-1 Mapping of Exam Objectives to Book Chapters and Sections

Objective	Description	Chapter/Section	Supporting Chapter/Section
1	**Architectures and Technologies**		
1.1	Identify the prerequisites and components for a VMware vSphere 8.x implementation	1: vSphere Overview, Components, and Requirements ■ Infrastructure Requirements ■ Other Requirements	8: vSphere Installation ■ Installing ESXi Hosts ■ Deploying vCenter Server Components
1.2	Describe the components and topology of a VMware vCenter architecture	1: vSphere Overview, Components, and Requirements ■ vCenter Server Topology	8: vSphere Installation ■ Deploying vCenter Server Components 5: vCenter Server Features and Virtual Machines ■ vSphere Managed Inventory Objects

Objective	Description	Chapter/Section	Supporting Chapter/Section
1	**Architectures and Technologies**		
1.3	Describe storage concepts	2: Storage Infrastructure ■ Storage Models and Datastore Types	
1.3.1	Identify and differentiate storage access protocols for VMware vSphere (NFS, iSCSI, SAN, etc.)	2: Storage Infrastructure ■ Storage Virtualization: Traditional Model	
1.3.2	Describe storage datastore types for VMware vSphere	2: Storage Infrastructure ■ Software-Defined Storage Models ■ Datastore Types	11: Managing Storage ■ Managing Datastores
1.3.3	Explain the importance of advanced storage configurations (vStorage APIs for Array Integration (VAAI), vStorage APIs for Storage Awareness (VASA), multipathing, etc.)	2: Storage Infrastructure ■ VASA ■ VAAI	11: Managing Storage ■ VASA: Registering a Storage Provider ■ VASA: Managing Storage Providers
1.3.4	Describe storage policies	2: Storage Infrastructure ■ Storage Policies	11: Managing Storage ■ Managing Storage Policies
1.3.5	Describe basic storage concepts in VMware vSAN and VMware Virtual Volumes (vVOLs)	2: Storage Infrastructure ■ vSAN Concepts ■ Virtual Volumes (vVols)	2: Storage Infrastructure ■ Storage Virtualization: Traditional Model ■ Software-Defined Storage Models ■ Datastore Types ■ Storage in vSphere with Kubernetes 11: Managing Storage ■ Managing vSAN ■ Managing Datastores ■ Configuring and Managing vVols

Objective	Description	Chapter/Section	Supporting Chapter/Section
1	**Architectures and Technologies**		
1.3.6	Identify use cases for raw device mapping (RDM), Persistent Memory (PMem), Non-Volatile Memory Express (NVMe), NVMe over Fabrics (NVMe-oF), and RDMA (iSER).	2: Storage Infrastructure ■ Raw Device Mappings (RDMs) ■ vVols ■ VMware NVMe	11: Managing Storage ■ Managing RDMs ■ Managing Storage Policies ■ Managing VMware NVMe ■ Managing PMem
1.3.7	Describe datastore clusters	2: Storage Infrastructure ■ Storage DRS (SDRS)	11: Managing Storage ■ Configuring and Managing SDRS
1.3.8	Describe Storage I/O Control (SIOC)	2: Storage Infrastructure ■ NIOC, SIOC, and SDRS	11: Managing Storage ■ Configuring and Managing SIOC
1.4	Describe VMware ESXi cluster concepts	4: Clusters and High Availability ■ Cluster Concepts and Overview ■ Distributed Resources Scheduler (DRS) ■ High Availability (HA)	10: Managing and Monitoring Clusters and Resources ■ Creating and Configuring a vSphere Cluster ■ Creating and Configuring a vSphere DRS Cluster ■ Creating and Configuring a vSphere HA cluster
1.4.1	Describe VMware Distributed Resource Scheduler (DRS)	4: Clusters and High Availability ■ Cluster Concepts and Overview ■ Distributed Resources Scheduler (DRS)	10: Managing and Monitoring Clusters and Resources ■ Creating and Configuring a vSphere DRS Cluster
1.4.2	Describe vSphere Enhanced vMotion Compatibility (EVC)	4: Clusters and High Availability ■ Enhanced vMotion Compatibility (EVC)	10: Managing and Monitoring Clusters and Resources ■ EVC Mode

Objective	Description	Chapter/Section	Supporting Chapter/Section
1	**Architectures and Technologies**		
1.4.3	Describe how DRS scores virtual machines	4: Clusters and High Availability ■ How DRS Scores VMs	10: Managing and Monitoring Clusters and Resources ■ Creating and Configuring a vSphere DRS Cluster
1.4.4	Describe VMware vSphere High Availability (HA)	4: Clusters and High Availability ■ vSphere High Availability (HA)	10: Managing and Monitoring Clusters and Resources ■ Creating and Configuring a vSphere HA cluster
1.4.4.1	Describe Admission Control	4: Clusters and High Availability ■ vSphere HA Admission Control	10: Managing and Monitoring Clusters and Resources ■ Creating and Configuring a vSphere HA cluster
1.4.4.2	Describe vSphere Cluster Services (vCLS)	4: Clusters and High Availability ■ vSphere Cluster Services (vCLS)	
1.4.5	Identify use cases for fault tolerance	4: Clusters and High Availability ■ Fault Tolerance (FT)	10: Managing and Monitoring Clusters and Resources ■ Configuring vSphere Fault Tolerance
1.5	Explain the difference between VMware standard switches and distributed switches	3: Network Infrastructure ■ vSphere Standard Switch (vSS) ■ vSphere Distributed Switch (vDS) ■ vDS Settings and Features	9: Configuring and Managing Virtual Networks ■ Creating and Configuring vSphere Standard Switches ■ Creating and Configuring vSphere Distributed Switches
1.5.1	Describe VMkernel networking	3: Network Infrastructure ■ VMkernel Networking and TCP/IP Stacks	9: Configuring and Managing Virtual Networks ■ Configuring and Managing VMkernel Adapters ■ Configuring TCP/IP Stacks

Objective	Description	Chapter/Section	Supporting Chapter/Section
1	**Architectures and Technologies**		
1.5.2	Manage networking on multiple hosts with vSphere Distributed Switch (VDS)	9: Configuring and Managing Virtual Networks ■ Managing Host Networking with vDS	3: Network Infrastructure ■ vSphere Distributed Switch (vDS)
1.5.3	Describe networking policies	3: Network Infrastructure ■ vSS Networking Policies ■ vDS Networking Policies	9: Configuring and Managing Virtual Networks ■ Networking Policies and Advanced Features
1.5.4	Manage Network I/O Control (NIOC) on a vSphere Distributed Switch (VDS)	9: Configuring and Managing Virtual Networks ■ Configuring Network I/O Control (NIOC)	3: Network Infrastructure ■ Network I/O Control
1.5.5	Describe Network I/O Control (NIOC)	3: Network Infrastructure ■ Network I/O Control	9: Configuring and Managing Virtual Networks ■ Configuring Network I/O Control (NIOC)
1.6	Describe VMware vSphere Lifecycle Manager concepts	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	8: vSphere Installation ■ VMware vSphere Lifecyle Manager Implementation
1.7	Describe the basics of VMware vSAN as primary storage	2: Storage Infrastructure ■ vSAN Concepts	
1.7.1	Identify basic vSAN requirements (networking, disk count, and type)	2: Storage Infrastructure ■ vSAN Requirements	11: Managing Storage ■ Configuring and Managing vSAN
1.7.2	Identify Express Storage Architecture (ESA) concepts for vSAN 8	2: Storage Infrastructure ■ vSAN Concepts	

Objective	Description	Chapter/Section	Supporting Chapter/Section
1	**Architectures and Technologies**		
1.8	Describe the role of Virtual Machine Encryption in a data center	7: vSphere Security ■ Virtual Machine Encryption	
1.8.1	Describe vSphere Trust Authority	7: vSphere Security ■ vSphere Trust Authority (vTA)	12: Managing vSphere Security ■ Configuring and Managing vSphere Trust Authority (vTA)
1.8.1.1	Describe the vSphere Trust Authority architecture	7: vSphere Security ■ vSphere Trust Authority (vTA)	12: Managing vSphere Security ■ Configuring and Managing vSphere Trust Authority (vTA)
1.8.1.2	Recognize use cases for vSphere Trust Authority	7: vSphere Security ■ vSphere Trust Authority (vTA)	
1.8.2	Describe the role of a Key Management Services (KMS) server in vSphere	1: vSphere Overview, Components, and Requirements ■ Infrastructure Requirements	
1.9	Recognize methods of securing virtual machines	7: vSphere Security ■ Virtual Machine Security	
1.9.1	Recognize use cases for a virtual Trusted Platform Module (vTPM)	7: vSphere Security ■ Virtual Trusted Platform Module (vTPM)	
1.9.2	Differentiate between Basic Input or Output System (BIOS) and Unified Extensible Firmware Interface (UEFI) firmware	7: vSphere Security ■ ESXi Secure Boot and TPM	12: Managing vSphere Security ■ Configuring UEFI Secure Boot for ESXi Hosts

Objective	Description	Chapter/Section	Supporting Chapter/Section
1	**Architectures and Technologies**		
1.9.3	Recognize use cases for Microsoft virtualization-based security (VBS)	14: Managing Virtual Machines ■ Virtualization-Based Security	
1.10	Describe identity federation	8: vSphere Installation ■ Configuring Identity Federation	
1.10.1	Describe the architecture of identity federation	8: vSphere Installation ■ Configuring Identity Federation	
1.10.2	Recognize use cases for identity federation	8: vSphere Installation ■ Configuring Identity Federation	
1.11	Describe VMware vSphere Distributed Services Engine	3: Network Infrastructure ■ Network Offloads Compatibility	
1.11.1	Describe the role of a data processing unit (DPU) in vSphere	1: vSphere Overview, Components and Requirements ■ Compute and System Requirements 3: Network Infrastructure ■ Traditional Networking Terminology ■ Network Offloads Compatibility	
1.12	Identify use cases for VMware Tools	5: vCenter Server Features and Virtual Machines ■ VMware Tools	
1.13	Describe the high-level components of VMware vSphere with Tanzu	6: VMware Product Integration ■ vSphere with Tanzu	

Objective	Description	Chapter/Section	Supporting Chapter/Section
1	**Architectures and Technologies**		
1.13.1	Identify the use case for a Supervisor Cluster and Supervisor Namespace	6: VMware Product Integration ■ vSphere with Tanzu ■ vSphere with Tanzu Use Cases	
1.13.2	Identify the use case for vSphere Zones	6: VMware Product Integration ■ vSphere with Tanzu	
1.13.3	Identify the use case for a VMware Tanzu Kubernetes Grid (TKG) cluster	6: VMware Product Integration ■ vSphere with Tanzu	
2	**VMware Products and Solutions**		
2.1	Describe the role of VMware vSphere in the Software-Defined Data Center	1: vSphere Overview, Components, and Requirements ■ VMware SDDC	
2.2	Identify use cases for VMware vSphere+	6: VMware Product Integration ■ vSphere+	
2.3	Identify use cases for VMware vCenter Converter	6: VMware Product Integration ■ vCenter Converter	
2.4	Identify disaster recovery (DR) use cases	6: VMware Product Integration ■ vSphere Replication ■ Site Recovery Manager (SRM)	
2.4.1	Identify VMware vCenter replication options	6: VMware Product Integration ■ vSphere Replication	
2.4.2	Identify use cases for VMware Site Recovery Manager (SRM)	6: VMware Product Integration ■ Site Recovery Manager (SRM)	

Objective	Description	Chapter/Section	Supporting Chapter/Section
3	**Planning and Designing**		
4	**Installing, Configuring, and Setup**		
4.1	Configure single sign-on (SSO)	1: vSphere Overview, Components and Requirements ■ vCenter Server Topology 8: vSphere Installation ■ Configuring Single Sign-On (SSO)	12: Managing vSphere Security ■ Managing SSO
4.1.1	Configure an SSO domain	8: vSphere Installation ■ Deploying vCenter Server Components ■ Configuring Single Sign-On (SSO)	1: vSphere Overview, Components, and Requirements ■ vCenter Server Topology 12: Managing vSphere Security ■ Managing SSO
4.1.2	Join an existing SSO domain	8: vSphere Installation ■ Deploying vCenter Server Components ■ Configuring Single Sign-On (SSO)	1: vSphere Overview, Components, and Requirements ■ vCenter Server Topology 12: Managing vSphere Security ■ Managing SSO
4.2	Configure vSphere distributed switches	9: Configuring and Managing Virtual Networks ■ vSphere Distributed Switches (vDS)	
4.2.1	Create a distributed switch	9: Configuring and Managing Virtual Networks ■ Creating and Configuring vSphere Distributed Switches	
4.2.2	Add ESXi hosts to the distributed switch	9: Configuring and Managing Virtual Networks ■ Adding Hosts to a vDS	

Objective	Description	Chapter/Section	Supporting Chapter/Section
4	**Installing, Configuring, and Setup**		
4.2.3	Examine the distributed switch configuration	9: Configuring and Managing Virtual Networks ■ Creating and Configuring vSphere Distributed Switches	
4.3	Configure Virtual Standard Switch (VSS) advanced virtual networking options	9: Configuring and Managing Virtual Networks ■ Creating and Configuring vSphere Standard Switches ■ Creating and Configuring Standard Port Groups	3: Network Infrastructure ■ vSphere Standard Switch (vSS)
4.4	Set up identity sources	8: vSphere Installation ■ Adding, Editing, and Removing SSO Identity Sources	12: Managing vSphere Security ■ Managing SSO
4.4.1	Configure identity federation	8: vSphere Installation ■ Configuring Identity Federation	12: Managing vSphere Security ■ Managing SSO
4.4.2	Configure LDAP integration	8: vSphere Installation ■ Adding, Editing, and Removing SSO Identity Sources ■ How to Add an LDAP Authentication Source	12: Managing vSphere Security ■ Managing SSO
4.5	Deploy and configure VMware vCenter Server Appliance (VCSA)	8: vSphere Installation ■ vCenter Server Appliance	1: vSphere Overview, Components, and Requirements ■ vCenter Server Topology 13: Managing vSphere and vCenter Server ■ Upgrading to vSphere 7.0 ■ Repointing a vCenter Server to Another Domain

Objective	Description	Chapter/Section	Supporting Chapter/Section
4	**Installing, Configuring, and Setup**		
4.6	Create and configure VMware HA and DRS advanced options (Admission Control, Proactive HA, etc.)	10: Managing and Monitoring Clusters and Resources ■ Creating and Configuring a vSphere DRS Cluster ■ Creating and Configuring a vSphere HA Cluster	4: Clusters and High Availability ■ Distributed Resource Scheduler (DRS) ■ vSphere High Availability (HA)
4.7	Deploy and configure VMware vCenter High Availability	8: vSphere Installation ■ Implementing VCSA HA	1: vSphere Overview, Components, and Requirements ■ vCenter Server Topology ■ vCenter High Availability Requirements 4: Clusters and High Availability ■ vCenter Server High Availability 13: Managing vSphere and vCenter Server ■ Managing the vCenter HA Cluster
4.8	Set up content library	14: Managing Virtual Machines ■ Content Libraries	5: vCenter Server Features and Virtual Machines ■ Content Libraries
4.8.1	Create a content library	14: Managing Virtual Machines ■ Creating a Content Library	
4.8.2	Add content to the content library	14: Managing Virtual Machines ■ Adding Items to a Content Library	
4.8.3	Publish a local content library	14: Managing Virtual Machines ■ Publishing a Content Library	

Objective	Description	Chapter/Section	Supporting Chapter/Section
4	**Installing, Configuring, and Setup**		
4.9	Subscribe to content library	14: Managing Virtual Machines ■ Subscribing to a Content Library	
4.9.1	Create a subscribed content library	14: Managing Virtual Machines ■ Publishing a Content Library	
4.9.2	Subscribe to a published content library	14: Managing Virtual Machines ■ Subscribing to a Content Library	
4.9.3	Deploy virtual machines (VMs) from a subscribed content library	14: Managing Virtual Machines ■ Deploying VMs by Using a Content Library	
4.10	Manage virtual machine (VM) template versions	14: Managing Virtual Machines ■ Managing VM Templates in a Content Library	
4.10.1	Update template in content library	14: Managing Virtual Machines ■ Managing VM Templates in a Content Library	
4.11	Configure VMware vCenter file-based backup	13: Managing vSphere and vCenter Server ■ vCenter Server Backup	
4.12	Configure vSphere Trust Authority	12: Managing vSphere Security ■ Configuring and Managing vSphere Trust Authority (vTA)	7: vSphere Security ■ vSphere Trust Authority (vTA)

Objective	Description	Chapter/Section	Supporting Chapter/Section
4	**Installing, Configuring, and Setup**		
4.13	Configure vSphere certificates	12: Managing vSphere Security ■ Configuring and Managing vSphere Certificates	7: vSphere Security ■ ESXi Host Certificates 13: Managing vSphere and vCenter Server ■ Verifying SSL Certificates for Legacy Hosts
4.13.1	Describe Enterprise PKIs role for SSL certificates	7: vSphere Security ■ vSphere Certificates Overview	12: Managing vSphere Security ■ Configuring and Managing vSphere Certificates
4.14	Configure vSphere Lifecycle Manager	8: vSphere Installation ■ Implementing VMware vSphere Lifecycle Manager	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager ■ About VMware Update Manager ■ Update Manager Download Service (UMDS)
4.15	Configure different network stacks	9: Configuring and Managing Virtual Networks ■ Configuring TCP/IP Stacks	3: Network Infrastructure ■ VMkernel Networking and TCP/IP Stacks
4.16	Configure host profiles	8: vSphere Installation ■ Configuring ESXi Using Host Profiles	
4.17	Identify ESXi boot options	8: vSphere Installation ■ ESXi Kernel Options	
4.17.1	Configure Quick Boot	13: Managing vSphere and vCenter Server ■ ESXi Quick Boot	
4.17.2	Securely Boot ESXi hosts	12: Managing vSphere Security ■ Configuring UEFI Secure Boot for ESXi Hosts	7: vSphere Security ■ ESXi Secure Boot and TPM ■ vSphere Trusted Authority (vTA)

Objective	Description	Chapter/Section	Supporting Chapter/Section
4	**Installing, Configuring, and Setup**		
4.18	Deploy and configure clusters using the vSphere Cluster Quickstart workflow	10: Managing and Monitoring Clusters and Resources ■ Creating a Cluster	
4.18.1	Use Cluster Quickstart workflow to add hosts	10: Managing and Monitoring Clusters and Resources ■ Configuring a Cluster with Quickstart	
4.18.2	Use Cluster Quickstart workflow to configure a cluster	10: Managing and Monitoring Clusters and Resources ■ Configuring a Cluster with Quickstart	
4.18.3	Use Quickstart to expand clusters	10: Managing and Monitoring Clusters and Resources ■ Configuring a Cluster with Quickstart	
4.19	Set up and configure VMware ESXi	8: vSphere Installation ■ vSphere Lifecycle ■ Installing ESXi Hosts ■ Initial vSphere Configuration	12: Managing vSphere Security ■ Configuring and Managing ESXi Security
4.19.1	Configure Time Configuration	12: Managing vSphere Security ■ Customizing ESXi Services ■ Configuring ESXi Using Host Profiles 8: vSphere Installation ■ ESXi Configuration Settings	10: Managing and Monitoring Clusters and Resources ■ Configuring a Cluster with Quickstart

Objective	Description	Chapter/Section	Supporting Chapter/Section
4	**Installing, Configuring, and Setup**		
4.19.2	Configure ESXi services	12: Managing vSphere Security ■ Customizing ESXi Services	
4.19.2.1	Configure ESXi Shell	12: Managing vSphere Security ■ SSH and ESXi Shell Security	
4.19.2.2	Configure SSH	12: Managing vSphere Security ■ SSH and ESXi Shell Security	
4.19.3	Configure Product Locker	8: vSphere Installation ■ Configuring ESXi Using Host Profiles	
4.19.4	Configure Lockdown Mode	12: Managing vSphere Security ■ Using Lockdown Mode	7: vSphere Security ■ ESXi Host Access
4.19.5	Configure ESXi firewall	12: Managing vSphere Security ■ Configuring the ESXi Firewall	7: vSphere Security ■ Security Profiles
4.20	Configure VMware vSphere with Tanzu	6: VMware Product Integration ■ vSphere with Tanzu Integration	
4.20.1	Configure a Supervisor Cluster & Supervisor Namespace	6: VMware Product Integration ■ vSphere with Tanzu	
4.20.2	Configure a Tanzu Kubernetes Grid Cluster	6: VMware Product Integration ■ vSphere with Tanzu	

Objective	Description	Chapter/Section	Supporting Chapter/Section
4	**Installing, Configuring, and Setup**		
4.20.3	Configure vSphere Zones	6: VMware Product Integration ■ vSphere with Tanzu	
4.20.4	Configure Namespace permissions	6: VMware Product Integration ■ vSphere with Tanzu	
5	**Performance-tuning, Optimization, Upgrades**		
5.1	Identify resource pools use cases	4: Clusters and High Availability ■ Resource Pools	10: Managing and Monitoring Clusters and Resources ■ Creating a Resource Pool ■ Monitoring and Managing Resource Pool Resources
5.1.1	Explain shares, limits, and reservations (resource management)	4: Clusters and High Availability ■ Shares, Limits, and Reservations	10: Managing and Monitoring Clusters and Resources ■ Shares, Limits, and Reservations ■ Creating a Resource Pool ■ Monitoring and Managing Resource Pool Resources
5.2	Monitor resources of a VMware vCenter Server Appliance (VCSA) and vSphere 8.x environment	10: Managing and Monitoring Clusters and Resources ■ Monitoring and Managing vSphere Resources	4: Clusters and High Availability ■ Cluster Concepts and Overview ■ Distributed Resource Scheduler (DRS)
5.3	Identify and use resource monitoring tools	10: Managing and Monitoring Clusters and Resources ■ Monitoring and Managing vSphere Resources	
5.4	Configure Network I/O Control (NIOC)	9: Configuring and Managing Virtual Networks ■ Configuring Network I/O Control (NIOC)	3: Network Infrastructure ■ Network I/O Control

Objective	Description	Chapter/Section	Supporting Chapter/Section
5	**Performance-tuning, Optimization, Upgrades**		
5.5	Configure Storage I/O Control (SIOC)	11: Managing Storage ■ Configuring and Managing SIOC	2: Storage Infrastructure ■ NIOC, SIOC, and SDRS
5.6	Configure a virtual machine port group to be offloaded to a data processing unit (DPU)	9: Configuring and Managing Virtual Networks ■ vSphere Distributed Switches (vDS)	
5.7	Explain the performance impact of maintaining virtual machine snapshots	5: vCenter Server Features and Virtual Machines ■ Virtual Machine Snapshots	14: Managing Virtual Machines ■ Creating and Managing Virtual Machine Snapshots
5.8	Use Update Planner to identify opportunities to update VMware vCenter	13: Managing vSphere and vCenter Server ■ Using Update Planner	
5.9	Use vSphere Lifecycle Manager to determine the need for upgrades and updates	13: Managing vSphere and vCenter Server ■ Using Lifecycle Manager ■ Upgrading to vSphere 7.0 ■ Using Update Planner	
5.9.1	Update virtual machines	4: Managing Virtual Machines ■ Installing and Upgrading VMware Tools	
5.9.2	Update VMware ESXi	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	
5.10	Use performance charts to monitor performance	10: Managing and Monitoring Clusters and Resources ■ Monitoring and Managing vSphere Resources	

Objective	Description	Chapter/Section	Supporting Chapter/Section
5	**Performance-tuning, Optimization, Upgrades**		
5.11	Perform proactive management with VMware Skyline	10: Managing and Monitoring Clusters and Resources ■ Monitoring and Managing Host Resources and Health	6: VMware Product Integration ■ VMware Skyline
5.12	Use VMware vCenter management interface to update VMware vCenter	13: Managing vSphere and vCenter Server ■ Patching with VAMI	
5.13	Complete lifecycle activities for VMware vSphere with Tanzu	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	
5.13.1	Update Supervisor cluster	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	
5.13.2	Back up and restore VMware vSphere with Tanzu	13: Managing vSphere and vCenter Serve ■ vCenter Server	
6	**Troubleshooting and Repairing**		
6.1	Identify use cases for enabling vSphere Cluster Services (vCLS) retreat mode	4: Clusters and High Availability ■ vSphere Cluster Services (vCLS)	
6.2	Differentiate between the main management services in VMware ESXi and vCenter and their corresponding log files	10: Managing and Monitoring Clusters and Resources ■ ESXi Logs ■ vCenter Server Logs	

Objective	Description	Chapter/Section	Supporting Chapter/Section
6	**Troubleshooting and Repairing**		
6.3	Generate a log bundle	10: Managing and Monitoring Clusters and Resources ■ ESXi Logs ■ vCenter Server Logs ■ Uploading System Logs to VMware 13: Managing vSphere and vCenter Server ■ Monitoring and Managing vCenter Server with the VAMI	
7	**Administrative and Operational Tasks**		
7.1	Create and manage virtual machine snapshots	14: Managing Virtual Machines ■ Creating and Managing Virtual Machine Snapshots	5: vCenter Server Features and Virtual Machines ■ Virtual Machine Snapshots
7.2	Create virtual machines using different methods (Open Virtualization Format (OVF) templates, content library, etc.)	14: Managing Virtual Machines ■ Managing VMs by Using PowerCLI ■ Deploying OVF/OVA Templates ■ Deploying VMs by Using a Content Library	5: vCenter Server Features and Virtual Machines ■ Virtual Machine Cloning 14: Managing Virtual Machines ■ Managing OVF Templates ■ Content Libraries
7.3	Manage virtual machines (modifying virtual machine settings, VMware per-VM EVC, latency sensitivity, CPU affinity, etc.)	14: Managing Virtual Machines ■ Managing EVC Mode and CPU Affinity 10: Managing and Monitoring Clusters and Resources ■ Latency Sensitivity	5: vCenter Server Features and Virtual Machines ■ Virtual Machine Migration

Objective	Description	Chapter/Section	Supporting Chapter/Section
7	**Administrative and Operational Tasks**		
7.4	Manage storage	11: Managing Storage ■ Managing Datastores ■ Managing Storage Policies ■ Managing Multipathing ■ Managing Paths with the vSphere Client	2 : Storage Infrastructure ■ Datastore Types ■ Storage Policies ■ Storage Multipathing and Failover
7.4.1	Configure and modify datastores	11: Managing Storage ■ Managing Datastores	2: Storage Infrastructure ■ Datastore Types
7.4.2	Create virtual machine storage policies	11: Managing Storage ■ Managing Storage Policies	2: Storage Infrastructure ■ Storage Policies
7.4.3	Configure storage cluster options	11: Managing Storage ■ Configuring and Managing Storage DRS ■ Configuring and Managing vSAN	2: Storage Infrastructure ■ SDRS
7.5	Create DRS affinity and anti-affinity rules for common use cases	10: Managing and Monitoring Clusters and Resources ■ Creating Affinity/ Anti-Affinity Rules	4: Clusters and High Availability ■ DRS Rules
7.6	Migrate virtual machines	14: Managing Virtual Machines ■ Migrating Virtual Machines	5: vCenter Server Features and Virtual Machines ■ Virtual Machine Migration ■ vMotion Details ■ Storage vMotion Details
7.6.1	Identify requirements for Storage vMotion, Cold Migration, vMotion, and Cross vCenter Export	14: Managing Virtual Machines ■ Migrating Virtual Machines	5: vCenter Server Features and Virtual Machines ■ Virtual Machine Migration ■ vMotion Details ■ Storage vMotion Details

Objective	Description	Chapter/Section	Supporting Chapter/Section
7	**Administrative and Operational Tasks**		
7.7	Configure role-based access control	12: Managing vSphere Security ■ Configuring and Managing Authentication and Authorization	7: vSphere Security ■ vSphere Permissions 8: vSphere Installation ■ Applying Permissions to ESXi Hosts Using Host Profiles
7.8	Manage host profiles	8: vSphere Installation ■ Configuring ESXi by Using Host Profiles	5: vCenter Server Features and Virtual Machines ■ Host Profiles
7.9	Utilize VMware vSphere Lifecycle Manager	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	8: vSphere Installation ■ Implementing VMware vSphere Lifecycle Manager 14: Managing Virtual Machines ■ Installing and Upgrading VMware Tools
7.9.1	Describe firmware upgrades for VMware ESXi	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	8: vSphere Installation ■ Implementing VMware vSphere Lifecycle Manager
7.9.2	Describe ESXi updates	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	8: vSphere Installation ■ Implementing VMware vSphere Lifecycle Manager
7.9.3	Describe component and driver updates for ESXi	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	8: vSphere Installation ■ Implementing VMware vSphere Lifecycle Manager Implementation
7.9.4	Describe hardware compatibility check	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	8: vSphere Installation ■ Implementing VMware vSphere Lifecycle Manager 5: vCenter Server Features and Virtual Machines ■ VM Hardware/Compatibility 14: Managing Virtual Machines ■ Configuring Virtual Machine Hardware

Objective	Description	Chapter/Section	Supporting Chapter/Section
7	**Administrative and Operational Tasks**		
7.9.5	Describe ESXi cluster image export functionality	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	8: vSphere Installation ■ Implementing VMware vSphere Lifecycle Manager 4: Clusters and High Availability ■ Cluster Concepts and Overview
7.9.6	Create ESXi cluster image	13: Managing vSphere and vCenter Server ■ Using vSphere Lifecycle Manager	
7.10	Use predefined alarms in VMware vCenter	10: Managing and Monitoring Clusters and Resources ■ Alarms	
7.11	Create custom alarms	10: Managing and Monitoring Clusters and Resources ■ Advanced Use Cases for Alarms ■ Creating Alarm Definitions	
7.12	Deploy an encrypted virtual machine	12: Managing vSphere Security ■ Encrypting a Virtual Machine	
7.12.1	Convert a non-encrypted virtual machine to an encrypted virtual machine	12: Managing vSphere Security ■ Encrypting a Virtual Machine	
7.12.2	Migrate an encrypted virtual machine	7: vSphere Security ■ Encrypted vSphere vMotion	
7.12.3	Configure virtual machine vMotion encryption properties	7: vSphere Security ■ Encrypted vSphere vMotion	

Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the authors that provide further insight into the more troublesome topics on the exam. Be sure to check the box indicating that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

Step 1. Go to **www.pearsonITcertification.com/register** and log in or create a new account.

Step 2. Enter the ISBN **9780138169886**.

Step 3. Answer the challenge question as proof of purchase.

Step 4. Click on the **Access Bonus Content** link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

NOTE Keep in mind that many of the companion content files—especially image and video files—are very large.

If you are unable to locate the files for this title by following these steps, please visit www.pearsonITcertification.com/contact and select the Site Problems/Comments option. Our customer service representatives will assist you.

How to Access the Pearson Test Prep Practice (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- You can get your access code by registering the print ISBN (9780138169886) on pearsonitcertification.com/register. Make sure to use the print book ISBN, regardless of whether you purchased an eBook or the print book. After you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.

- Premium Edition: If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at pearsonitcertification.com, click Account to see details of your account, and click the digital purchases tab.

NOTE After you register your book, your code can always be found in your account under the Registered Products tab.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

Step 1. Open this book's companion website as shown earlier in this Introduction under the heading, "Companion Website."

Step 2. Click the **Practice Exams** button.

Step 3. Follow the instructions listed there for both installing the desktop app and using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all test banks or just from one individual bank by selecting the desired banks in the exam bank area. There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the Tools tab and click the Update Products button. Again, this is only an issue with the desktop Windows application. If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the Tools tab and click the Update Application button. This ensures that you are running the latest version of the software engine.

Credits

Cover: FrameRatio/Shutterstock

Figure 5-1, Figure 5-2, Figure 5-3, Figure 5-4, Figure 8-1, Figure 10-1, Figure 10-2, Figure 10-3, Figure 10-4, Figure 13-1, Figure 13-2: VMware, Inc.

Clusters and High Availability

This chapter provides details on clusters and high availability in vSphere 8.0.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should study this entire chapter or move quickly to the "Exam Preparation Tasks" section. In any case, the authors recommend that you read the entire chapter at least once. Table 4-1 outlines the major headings in this chapter and the corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 4-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Cluster Concepts and Overview	1
Distributed Resource Scheduler (DRS)	2–4
vSphere High Availability (HA)	5–7
Other Resource Management and Availability Features	8–10

1. You want to implement EVC to ensure that vMotion is enabled across a specific set of ESXi hosts. Which of the following are requirements? (Choose two.)
   a. Hosts must be connected to a DRS cluster.
   b. Hosts must be connected to a vCenter Server.
   c. CPUs must be configured with a custom compatibility mask.
   d. You must select either Enable EVC for AMD Hosts or Enable EVC for Intel Hosts.

2. In vSphere 8.0, you want to configure the DRS migration threshold such that it is at the minimum level at which virtual machine happiness is considered. Which of the following values should you choose?
    a. Level 1
    b. Level 2
    c. Level 3
    d. Level 4
    e. Level 5

3. Which of the following is not a good use for resource pools in DRS?
    a. To delegate control and management
    b. To impact the use of network resources
    c. To impact the use of CPU resources
    d. To impact the use of memory resources

4. You want to use shares to give high-priority resource access to a set of virtual machines in a resource pool, without concern for the relative number of objects in the pool compared to other pools. Which feature is helpful?
    a. Limits
    b. Standard shares
    c. Scalable shares
    d. DRS advanced settings

5. You are configuring vSphere HA in a cluster. You want to configure the cluster to use a specific host as a target for failovers. Which setting should you use?
    a. Host Failures Cluster Tolerates
    b. Define Host Failover Capacity By set to Cluster Resource Percentage
    c. Define Host Failover Capacity By set to Slot Policy (Powered-on VMs)
    d. Define Host Failover Capacity By set to Dedicated Failover Hosts
    e. Define Host Failover Capacity By set to Disabled

6. You are enabling VM Monitoring in a vSphere HA cluster. You want to set the monitoring level such that its failure interval is 60 seconds. Which of the following options should you choose?
    a. High
    b. Medium

c. Low

d. Normal

7. You are configuring Virtual Machine Component Protection (VMCP) in a vSphere HA cluster. Which of the following statements is true?

   a. For PDL and APD failures, you can control the restart policy for virtual machines by setting it to Conservative or Aggressive.

   b. For PDL failures, you can control the restart policy for virtual machines by setting it to Conservative or Aggressive.

   c. For APD failures, you can control the restart policy for virtual machines by setting it to Conservative or Aggressive.

   d. For PDL and APD failures, you cannot control the restart policy for virtual machines.

8. You want to configure your environment to use predictive metrics when making placement and balancing decisions. What feature is required?

   a. Predictive DRS

   b. Aria Automation

   c. Proactive HA

   d. Slot Policy

9. You are configuring vSphere Fault Tolerance (FT) in a vSphere 8.0 environment. What is the maximum number of virtual CPUs you can use with an FT-protected virtual machine?

   a. One

   b. Two

   c. Four

   d. Eight

10. You are concerned about service availability for your vCenter Server. Which of the following statements is true?

    a. If a vCenter service fails, VMware Service Lifecycle Manager restarts it.

    b. If a vCenter service fails, VMware Lifecycle Manager restarts it.

    c. If a vCenter service fails, vCenter Server HA restarts it.

    d. VMware Service Lifecycle Manager is a part of the PSC.

Foundation Topics

Cluster Concepts and Overview

A vSphere cluster is a set of ESXi hosts that are intended to work together as a unit. When you add a host to a cluster, the host's resources become part of the cluster's resources. vCenter Server manages the resources of all hosts in a cluster as one unit. In addition to creating a cluster, assigning a name, and adding ESXi objects, you can enable and configure features on a cluster, such as vSphere Distributed Resource Scheduler (DRS), VMware Enhanced vMotion Compatibility (EVC), Distributed Power Management (DPM), vSphere High Availability (HA), and vSAN.

In the vSphere Client, you can manage and monitor the resources in a cluster as a single object. You can easily monitor and manage the hosts and virtual machines in the DRS cluster.

If you enable VMware EVC on a cluster, you can ensure that migrations with vMotion do not fail due to CPU compatibility errors. If you enable vSphere DRS on a cluster, you can allow automatic resource balancing using the pooled host resources in the cluster. If you enable vSphere HA on a cluster, you can allow rapid virtual machine recovery from host hardware failures, using the cluster's available host resource capacity. If you enable DPM on a cluster, you can provide automated power management in the cluster. If you enable vSAN on a cluster, you use a logical SAN that is built on a pool of drives attached locally to the ESXi hosts in the cluster.

You can use the Quickstart workflow in the vSphere Client to create and configure a cluster. The Quickstart page provides three cards: Cluster Basics, Add Hosts, and Configure Cluster. For an existing cluster, you can use Cluster Basics to change the cluster name and enable cluster services, such as DRS and vSphere HA. You can use the Add Hosts card to add hosts to the cluster. You can use the Configure Cluster card to configure networking and other settings on the hosts in the cluster.

In addition, in vSphere 7.0 and later, you can configure a few general settings for a cluster. For example, when you create a cluster, even if you do not enable DRS, vSphere, HA, or vSAN, you can choose to manage all hosts in the cluster with a single image. With this option, all hosts in a cluster inherit the same image, which reduces variability between hosts, improves your ability to ensure hardware compatibility, and simplifies upgrades. This feature requires hosts to already be ESXi 7.0 or above. It replaces baselines. Once it is enabled, baselines cannot be used in this cluster.

NOTE Do not confuse a vSphere cluster with a datastore cluster. In vSphere, datastore clusters and vSphere (host) clusters are separate objects. Although you can directly enable a vSphere cluster for vSAN, DRS, and vSphere HA, you cannot directly enable it for datastore clustering. You create datastore clusters separately. See Chapter 2, "Storage Infrastructure," for details on datastore clusters.

vSphere Cluster Services (vCLS)

vCLS, which is implemented by default in all vSphere clusters, ensures that cluster services remain available even if vCenter Server becomes unavailable. When you deploy a new cluster in vCenter Server 7.0 Update 3 or upgrade a vCenter Server to Version 7.0 Update 3, vCLS virtual appliances are automatically deployed to the cluster. In clusters with three or more hosts, three vCLS appliances are automatically deployed with anti-affinity rules to separate the appliances. In smaller clusters, the number of vCLS VMs matches the number of hosts.

In vSphere 8.0, each vCLS VM is configured with one vCPU, 128 MB memory, and no vNIC. The datastore for each vCLS VM is automatically selected based on the rank of the datastores connected to the cluster's hosts, with preference given to shared datastores. You can control the datastore choice by using the vSphere Client to select the cluster, navigating to Configure > vSphere Cluster Service > Datastores, and clicking the Add button. vCLS VMs are always powered on and should be treated as system VMs, where only administrators perform selective operations on the vCLS VMs. vCenter Server manages the health of vCLS VMs. You should not back up or take snapshots of these VMs. You can use the Summary tab for a cluster to examine the vCLS health, which is either Healthy, Degraded, or Unhealthy.

If you want to place a datastore hosting a vCLS VM into Maintenance Mode, you must either manually migrate the vCLS VM with Storage vMotion to a new location or put the cluster in Retreat Mode. In Retreat Mode, the health of vCLS is degraded, DRS stops functioning, and vSphere HA does not perform optimal placement when responding to host failure events. To put a cluster in Retreat Mode, you need to obtain its cluster domain ID from the URL of the browser after selecting the cluster in the vSphere Client. Then you apply the cluster domain ID, which is in the form *domain*-c(*number*), to create a new vCenter Server advanced setting with the entry **config.vcls.clusters.*domain*-c(*number*).enabled** that is set to False.

Enhanced vMotion Compatibility (EVC)

EVC is a cluster setting that can improve CPU compatibility between hosts for supporting vMotion. vMotion migrations are live migrations that require compatible instruction sets for source and target processors used by the virtual machine. The source and target processors must come from the same vendor class (AMD or Intel)

to be vMotion compatible. The clock speed, cache size, and number of cores can differ between source and target processors. When you start a vMotion migration or a migration of a suspended virtual machine, the wizard checks the destination host for compatibility; it displays an error message if problems exist. By using EVC, you can allow vMotion between some processors that would normally be incompatible.

The CPU instruction set that is available to a virtual machine guest OS is determined when the virtual machine is powered on. This CPU feature set is based on the following items:

- The host CPU family and model
- Settings in the BIOS that might disable CPU features
- The ESX/ESXi version running on the host
- The virtual machine's compatibility setting
- The virtual machine's guest operating system

EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. If you enable the EVC cluster setting, you can configure the EVC Mode with a baseline CPU feature set. EVC ensures that hosts in a cluster use the baseline feature set when presenting an instruction set to a guest OS. EVC uses AMD-V Extended Migration technology for AMD hosts and Intel FlexMigration technology for Intel hosts to mask processor features; this allows hosts to present the feature set of an earlier processor generation. You should configure EVC Mode to accommodate the host with the smallest feature set in the cluster.

The EVC requirements for hosts include the following:

- ESXi 6.7 or later is required.
- Hosts must be attached to a vCenter Server.
- CPUs must be from a single vendor (either Intel or AMD).
- If the AMD-V, Intel-VT, AMD NX, or Intel XD features are available in the BIOS, they need to be enabled.
- Check the *VMware Compatibility Guide* to ensure that CPUs are supported for EVC Mode.

NOTE You can apply a custom CPU compatibility mask to hide host CPU features from a virtual machine, but VMware does not recommend doing so.

You can configure the EVC settings by using the Quickstart > Configure Cluster workflow in the vSphere Client. You can also configure EVC directly in the cluster settings. The options for VMware EVC are Disable EVC, Enable EVC for AMD

Hosts, and Enable EVC for Intel Hosts. You can also configure per-VM EVC, as described in Chapter 5, "vCenter Server Features and Virtual Machines."

If you choose Enable EVC for Intel Hosts, you can set the EVC Mode setting to one of the options described in Table 4-2.

Table 4-2 EVC Modes for Intel

Level	EVC Mode	Description
L0	Intel Merom	Smallest Intel feature set for EVC mode.
L1	Intel Penryn	Includes the Intel Merom feature set and exposes additional CPU features, including SSE4.1.
L2	Intel Nehalem	Includes the Intel Penryn feature set and exposes additional CPU features, including SSE4.2 and POPCOUNT.
L3	Intel Westmere	Includes the Intel Nehalem feature set and exposes additional CPU features, including AES and PCLMULQDQ.
L4	Intel Sandy Bridge	Includes the Intel Westmere feature set and exposes additional CPU features, including AVX and XSAVE.
L5	Intel Ivy Bridge	Includes the Intel Sandy Bridge feature set and exposes additional CPU features, including RDRAND, ENFSTRG, FSGSBASE, SMEP, and F16C.
L6	Intel Haswell	Includes the Intel Ivy Bridge feature set and exposes additional CPU features, including ABMX2, AVX2, MOVBE, FMA, PERMD, RORX/MULX, INVPCID, and VMFUNC.
L7	Intel Broadwell	Includes the Intel Haswell feature set and exposes additional CPU features, including Transactional Synchronization Extensions, Supervisor Mode Access Prevention, Multi-Precision Add-Carry Instruction Extensions, PREFETCHW, and RDSEED.
L8	Intel Skylake	Includes the Intel Broadwell feature set and exposes additional CPU features, including Advanced Vector Extensions 512, Persistent Memory Support Instructions, Protection Key Rights, Save Processor Extended States with Compaction, and Save Processor Extended States Supervisor.
L9	Intel Cascade Lake	Includes the Intel Skylake feature set and exposes additional CPU features, including VNNI and XGETBV with ECX = 1.
L10	Intel Ice Lake	Includes the Intel Cascade Lake feature set and exposes additional CPU features, including HA extensions, Vectorized AES, User Mode Instruction Prevention, Read Processor ID, Fast Short REP MOV, WBNOINVD, Galois Field New Instructions, and AVX512 Integer Fused Multiply Add, Vectorized Bit Manipulation, and Bit Algorithms Instructions.
L11	Intel Sapphire Rapids	Includes the Intel Ice Lake feature set and exposes additional CPU features, including Control-Flow Enforcement Technology, Advanced Matrix Extensions, Supervisor Protection Keys, AVX-VNNI, AVX512 FP16, AVX512 BF16, CLDEMOTE, SERIALIZE, WBNOINVD, and MOVDIRI instructions.

If you choose Enable EVC for AMD Hosts, you can set the EVC Mode setting to one of the options described in Table 4-3.

Table 4-3 EVC Modes for AMD

Level	EVC Mode	Description
A0	AMD Opteron Generation 1	Smallest AMD feature set for EVC mode.
A1	AMD Opteron Generation 2	Includes the AMD Generation 1 feature set and exposes additional CPU features, including CPMXCHG16B and RDTSCP.
A3	AMD Opteron Generation 3	Includes the AMD Generation 2 feature set and exposes additional CPU features, including SSE4A, MisAlignSSE, POPCOUNT, and ABM (LZCNT).
A2, B0	AMD Opteron Generation 3 (without 3DNow!)	Includes the AMD Generation 3 feature set without 3DNow support.
B1	AMD Opteron Generation 4	Includes the AMD Generation 3 no3DNow feature set and exposes additional CPU features, including SSSE3, SSE4.1, AES, AVX, XSAVE, XOP, and FMA4.
B2	AMD Opteron Piledriver	Includes the AMD Generation 4 feature set and exposes additional CPU features, including FMA, TBM, BMI1, and F16C.
B3	AMD Opteron Steamroller	Includes the AMD Piledriver feature set and exposes additional CPU features, including XSAVEOPT RDFSBASE, RDGSBASE, WRFSBASE, WRGSBAS, and FSGSBASE.
B4	AMD Zen	Includes the AMD Steamroller feature set and exposes additional CPU features, including RDRAND, SMEP, AVX2, BMI2, MOVBE, ADX, RDSEED, SMAP, CLFLUSHOPT, XSAVES, XSAVEC, SHA, and CLZERO.
B5	AMD Zen 2	Includes the AMD Zen feature set and exposes additional CPU features, including CLWB, UMIP, RDPID, XGETBV with ECX = 1, WBNOINVD, and GMET.
B6	AMD Zen 3	Includes the AMD Zen 2 feature set and exposes additional CPU features, including always serializing LFENCE, INVPCID, PSFD, SSBD, PCID, PKU, VAES, VPCLMULQDQ, and shadow stacks.
B7	AMD Zen 4	Includes the AMD Zen 3 feature set and exposes additional CPU features, including Fast Short CMPSB and STOSB, Automatic IBRS, AVX512BF16, AVX512BITALG, AVX512BW, AVX512CD, AVX512DQ, AVX512F, AVX512IFMA, AVX512VBMI, AVX512VBMI2, AVX512VL, AVX512VNNI, AVX512VPOPCNTDQ, GFNI, IBRS, and Upper Address Ignore.

Starting with vSphere 7.0 Update 1, EVC provides a feature for Virtual Shared Graphics Acceleration (vSGA), allowing multiple virtual machines to share GPUs and leverage the 3D graphics acceleration capabilities.

vSAN Services

You can enable DRS, vSphere HA, and vSAN at the cluster level. The following sections provide details on DRS and vSphere HA. For details on vSAN, see Chapter 2.

Distributed Resource Scheduler (DRS)

DRS distributes compute workload in a cluster by strategically placing virtual machines during power-on operations and live migrating (vMotion) VMs when necessary. DRS provides many features and settings that enable you to control its behavior.

You can set DRS Automation Mode for a cluster to one of the following:

- **Manual**: DRS does not automatically place or migrate virtual machines. It only makes recommendations.
- **Partially Automated**: DRS automatically places virtual machines as they power on. It makes recommendations for virtual machine migrations.
- **Fully Automated**: DRS automatically places and migrates virtual machines.

You can override Automation Mode at the virtual machine level.

Recent DRS Enhancements

VMware added many improvements to DRS beginning with vSphere 6.5. For example, in vSphere 7.0, DRS runs once every minute rather than every 5 minutes, as in older DRS versions. The newer DRS versions tend to recommend smaller (in terms of memory) virtual machines for migration to facilitate faster vMotion migrations, whereas older versions tend to recommend large virtual machines to minimize the number of migrations. Older DRS versions use an imbalance metric that is derived from the standard deviation of load across the hosts in the cluster. Newer DRS versions focus on virtual machine happiness. Newer DRS versions are much lighter and faster than the older versions.

Newer DRS versions recognize that vMotion is an expensive operation and account for it in their recommendations. In a cluster where virtual machines are frequently powered on and the workload is volatile, it is not necessary to continuously migrate virtual machines. DRS calculates the gain duration for live migrating a virtual machine and considers the gain duration when making recommendations.

In vSphere 8.0, when PMEM is present, DRS performance can be improved by leveraging memory statistics to optimize VM placement.

The following sections provide details on other recent DRS enhancements.

Network-Aware DRS

Key Topic

In vSphere 6.5, DRS considers the utilization of host network adapters during initial placement and load balancing, but it does not balance the network load. Instead, its goal is to ensure that the target host has sufficient available network resources. It works by eliminating hosts with saturated networks from the list of possible migration hosts. The threshold used by DRS for network saturation is 80% by default. When DRS cannot migrate VMs due to network saturation, the result may be an imbalanced cluster.

Beginning with vSphere 7.0, DRS uses a new cost modeling algorithm that is flexible and balances network bandwidth along with CPU and memory usage.

Virtual Machine Distribution

Starting with vSphere 6.5, you can enable an option to distribute a more even number of virtual machines across hosts. The main use case for this is to improve availability. The primary goals of DRS—to ensure that all VMs are getting the resources they need and that the load is balanced in the cluster—remain unchanged. But with this new option enabled, DRS also tries to ensure that the number of virtual machines per host is balanced in the cluster.

Memory Metric for Load Balancing

Historically, vSphere has used the Active Memory metric for load-balancing decisions. In vSphere 6.5 and 6.7, you have the option to set DRS to balance the load based on the Consumed Memory metric. vSphere 7.0 and later do not support the option to change this behavior.

Virtual Machine Initial Placement

Starting with vSphere 6.5, DRS began to use a new initial placement algorithm that is faster, lighter, and more effective than the previous algorithm. In earlier versions, DRS takes a snapshot of the cluster state when making virtual machine placement recommendations. With the new algorithm, DRS does not snapshot the cluster state, which allows for more accurate recommendations and faster virtual machine

power on. In vSphere 6.5, the new placement feature is not supported for the following configurations:

- Clusters where DPM, Proactive HA, or HA Admission Control is enabled
- Clusters with DRS configured in Manual Mode
- Virtual machines with the Manual DRS Override setting enabled
- Virtual machines that are FT enabled
- Virtual machines that are part of a vApp

In vSphere 6.7 and later, the new placement is available for all configurations.

Enhancements to the Evacuation Workflow

Prior to vSphere 6.5, when evacuating a host entering Maintenance Mode, DRS waited to migrate templates and power off virtual machines until after the completion of vMotion migrations, leaving those objects unavailable for use for a long time. Starting with vSphere 6.5, DRS prioritizes the migration of virtual machine templates and powered-off virtual machines over powered-on virtual machines, making those objects available for use without the need to wait on vMotion migrations.

Prior to vSphere 6.5, the evacuation of powered-off virtual machines was inefficient. In versions since vSphere 6.5, these evacuations occur in parallel, making use of up to 100 re-register threads per vCenter Server. This means that you may see only a small difference when evacuating up to 100 virtual machines.

In versions since vSphere 6.7, DRS is more efficient at evacuating powered-on virtual machines from a host that is entering Maintenance Mode. Instead of simultaneously initiating vMotion for all the powered-on VMs on the host, as in previous versions, DRS initiates vMotion migrations in batches of eight at a time. Each vMotion batch is issued after the previous batch completes. The vMotion batching makes the entire workflow more controlled and predictable.

DRS Support for NVM

In versions since vSphere 6.7, DRS supports virtual machines running on next-generation persistent memory devices, known as non-volatile memory (NVM) devices. NVM is exposed as a datastore that is local to the host. Virtual machines can use the datastore as an NVM device exposed to the guest (Virtual Persistent Memory [vPMem]) or as a location for a virtual machine disk (Virtual Persistent Memory Disk [vPMemDisk]). DRS is aware of the NVM devices used by virtual machines and guarantees that the destination ESXi host has enough free persistent memory to accommodate placements and migrations.

How DRS Scores VMs

Key Topic

Historically, DRS balanced the workload in a cluster based on host compute resource usage. In versions since vSphere 7.0, DRS balances the workload based on virtual machine happiness. A virtual machine's DRS score is a measure of its happiness, which, in turn, is a measure of the resources available for consumption by the virtual machine. The higher the DRS score for a VM, the better its resource availability. DRS moves virtual machines to improve their DRS scores. DRS also calculates a DRS score for a cluster, which is a weighted sum of the DRS scores of all the virtual machines in the cluster.

In versions since Sphere 7.0, DRS calculates the core for each virtual machine on each ESXi host in the cluster every minute. Simply put, DRS logic computes an ideal throughput (demand) and an actual throughput (goodness) for each resource (CPU, memory, and network) for each virtual machine. The virtual machine's efficiency for a particular resource is a ratio of the goodness over the demand. A virtual machine's DRS score (total efficiency) is the product of its CPU, memory, and network efficiencies.

When calculating the efficiency, DRS applies resource costs. For CPU resources, DRS includes costs for CPU cache, CPU ready, and CPU tax. For memory resources, DRS includes costs for memory burstiness, memory reclamation, and memory tax. For network resources, DRS includes a network utilization cost.

DRS compares a virtual machine's DRS score for the host on which it currently runs. DRS determines whether another host can provide a better DRS score for the virtual machine. If so, DRS calculates the cost for migrating the virtual machine to the host and factors that score into its load-balancing decision.

DRS Rules

You can configure rules to control the behavior of DRS.

A VM–host affinity rule specifies whether the members of a selected virtual machine DRS group can run on the members of a specific host DRS group. Unlike a virtual machine–to–virtual machine (VM–VM) affinity rule, which specifies affinity (or anti-affinity) between individual virtual machines, a VM–host affinity rule specifies an affinity relationship between a group of virtual machines and a group of hosts. There are *required* rules (designated by "must") and *preferential* rules (designated by "should").

A VM–host affinity rule includes the following components:

- One virtual machine DRS group
- One host DRS group
- A designation of whether the rule is a requirement ("must") or a preference ("should") and whether it is affinity ("run on") or anti-affinity ("not run on")

A VM–VM affinity rule specifies whether selected individual virtual machines should run on the same host or whether they should be kept on separate hosts. This type of rule is used to create affinity or anti-affinity between individual virtual machines. When an affinity rule is created, DRS tries to keep the specified virtual machines together on the same host. You might want to do this, for example, for performance reasons.

With an anti-affinity rule, DRS tries to keep the specified virtual machines apart. You can use such a rule if you want to guarantee that certain virtual machines are always on different physical hosts. In that case, if a problem occurs with one host, not all virtual machines are at risk. You can create VM–VM affinity rules to specify whether selected individual virtual machines should run on the same host or be kept on separate hosts.

VM–VM affinity rule conflicts can occur when you use multiple VM–VM affinity and VM–VM anti-affinity rules. If two VM–VM affinity rules are in conflict, you cannot enable both of them. For example, if one rule keeps two virtual machines together and another rule keeps the same two virtual machines apart, you cannot enable both rules. Select one of the rules to apply and disable or remove the conflicting rule. When two VM–VM affinity rules conflict, the older one takes precedence, and the newer rule is disabled. DRS tries to satisfy only enabled rules and ignores disabled rules. DRS gives higher precedence to preventing violations of anti-affinity rules than violations of affinity rules.

NOTE A VM–VM rule does not allow the "should" qualifier. You should consider these as "must" rules.

DRS Migration Sensitivity

Prior to vSphere 7.0, DRS used a migration threshold to determine when virtual machines should be migrated to balance the cluster workload. In vSphere 7.0 and newer, DRS is designed to be more virtual machine centric and workload centric rather than cluster centric. You can set the DRS Migration Sensitivity parameter to one of the following values:

Key Topic

- **Level 1**: DRS only makes recommendations to fix rule violations or to facilitate a host entering Maintenance Mode.
- **Level 2**: DRS expands on Level 1 by making recommendations in situations that are at or close to resource contention. It does not make recommendations just to improve virtual machine happiness or cluster load distribution.
- **Level 3**: DRS expands on Level 2 by making recommendations to improve VM happiness and cluster load distribution. This is the default level.

- **Level 4**: DRS expands on Level 3 by making recommendations for occasional bursts in the workload and reacts to sudden load changes.
- **Level 5**: DRS expands on Level 4 by making recommendations dynamic and greatly varying workloads. DRS reacts to the workload changes every time.

Resource Pools

Resource pools are container objects in the vSphere inventory that are used to compartmentalize the CPU and memory resources of a host, a cluster, or a parent resource pool. Virtual machines run in and draw resources from resource pools. You can create multiple resource pools as direct children of a standalone host or a DRS cluster. You cannot create child resource pools on a host that has been added to a cluster or on a cluster that is not enabled for DRS.

You can use resource pools to organize VMs. You can delegate control over each resource pool to specific individuals and groups. You can monitor resources and set alarms on resource pools. If you need a container just for organization and permission purposes, consider using a folder. If you also need resource management, then consider using a resource pool. You can assign resource settings such as shares, reservations, and limits to resource pools.

Use Cases

You can use resource pools to compartmentalize a cluster's resources and then use the resource pools to delegate control to individuals or organizations. Table 4-4 provides some use cases for resource pools.

Table 4-4 Resource Pool Use Cases

Use Case	Details
Flexible hierarchical organization	Add, remove, modify, and reorganize resource pools, as needed.
Resource isolation	Use resource pools to allocate resources to separate departments, in such a manner that changes in a pool do not unfairly impact other departments.
Access control and delegation	Use permissions to delegate activities, such as virtual machine creation and management, to other administrators.
Separation of resources from hardware	In a DRS cluster, perform resource management independently of the actual hosts.
Managing multitier applications	Manage the resources for a group of virtual machines (in a specific resource pool), which is easier than managing resources per virtual machine.

Shares, Limits, and Reservations

You can configure CPU and memory shares, reservations, and limits on resource pools, as described in Table 4-5.

Table 4-5 Shares, Limits, and Reservations

Option	Description
Shares	Shares specify the relative importance of a virtual machine or a resource pool. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources. Shares can be thought of as priority under contention. Shares are typically set to High, Normal, or Low, and these values specify share values with a 4:2:1 ratio. You can also select Custom and assign a specific number of shares (to express a proportional weight). A resource pool uses its shares to compete for the parent's resources and is allocated a portion based on the ratio of the pool's shares compared with its siblings. Siblings share the parent's resources according to their relative share values, bounded by the reservation and limit. For example, consider a scenario where a cluster has two child resource pools with normal CPU shares, another child resource pool with high CPU shares, and no other child objects. During periods of contention, each of the pools with normal shares would get access to 25% of the cluster's CPU resources, and the pool with high shares would get access to 50%.
Reservations	A reservation specifies the guaranteed minimum allocation for a virtual machine or a resource pool. A CPU reservation is expressed in megahertz, and a memory reservation is expressed in megabytes. You can power on a virtual machine only if there are enough unreserved resources to satisfy the reservation of the virtual machine. If the virtual machine starts, then it is guaranteed that amount, even when the physical server is heavily loaded. For example, if you configure the CPU reservation for each virtual machine as 1 GHz, you can start eight VMs in a resource pool where the CPU reservation is set for 8 GHz and expandable reservations are disabled. But you cannot start additional virtual machines in the pool. You can use reservations to guarantee a specific amount of resources for a resource pool. The default value for a resource pool's CPU or memory reservation is 0. If you change this value, it is subtracted from the unreserved resources of the parent. The resources are considered reserved, regardless of whether virtual machines are associated with the resource pool.

Option	Description
Expandable reservations	You can enable expandable reservations to effectively allow a child resource pool to borrow from its parent. Expandable reservations, which are enabled by default, are considered during admission control. When powering on a virtual machine, if the resource pool does not have sufficient unreserved resources, the resource pool can use resources from its parent or ancestors. For example, say that in a resource pool where 8 GHz is reserved and expandable reservations are disabled, you try to start nine virtual machines each with 1 GHz, but the last virtual machine does not start. If you enable expandable reservations in the resource pool, and its parent pool (or cluster) has sufficient unreserved CPU resources, you can start the ninth virtual machine.
Limits	A limit specifies an upper bound for CPU or memory resources that can be allocated to a virtual machine or a resource pool. You can set a limit on the amount of CPU and memory allocated to a resource pool. The default is unlimited. For example, if you power on multiple CPU-intensive virtual machines in a resource pool, where the CPU limit is 10 GHz, then, collectively, the virtual machines cannot use more than 10 GHz CPU resources, regardless of the pool's reservation settings, the pool's share settings, or the amount of available resources in the parent.

Table 4-6 provides the CPU and memory share values for virtual machines when using the High, Normal, and Low settings. For resource pools, the share values are equivalent to those of a virtual machine with four vCPUs and 16 GB memory.

Table 4-6 Virtual Machine Shares

Setting	CPU Share Value	Memory Share Value
High	2000 per vCPU	20 per MB
Normal	1000 per vCPU	10 per MB
Low	500 per vCPU	5 per MB

For example, the share values for a resource pool configured with normal CPU shares and high memory shares are 4000 (that is, 4×1000) CPU shares and 327,680 (that is, $16 \times 1024 \times 20$) memory shares.

NOTE The relative priority represented by each share changes with the addition and removal of virtual machines in a resource pool or cluster. It also changes as you increase or decrease the shares on a specific virtual machine or resource pool.

Enhanced Resource Pool Reservation

In versions since vSphere 6.7, DRS uses a two-pass algorithm to allocate resource reservations to children. The old allocation model does not reserve more resources than the current demand, even when the resource pool is configured with a higher reservation. When a spike in virtual machine demand occurs after resource allocation is complete, DRS does not make the remaining pool reservation available to the virtual machine until the next allocation operation occurs. As a result, a virtual machine's performance may be temporarily impacted. In the new allocation model, each allocation operation uses two passes. In the first pass, the resource pool reservation is allocated based on virtual machine demand. In the second pass, excess pool reservation is allocated proportionally, limited by the virtual machine's configured size, which reduces the performance impact due to virtual machine spikes.

Scalable Shares

Key Topic

In versions since vSphere 7.0, DRS provides scalable shares. The main use case for scalable shares is a scenario in which you want to use shares to give high-priority resource access to a set of virtual machines in a resource pool, without concern for the relative number of objects in the pool compared to other pools. With standard shares, each pool in a cluster competes for resource allocation with its siblings, based on the share ratio. With scalable shares, the allocation for each pool factors in the number of objects in the pool.

For example, consider a scenario in which a cluster with 100 GHz CPU capacity has a high-priority resource pool with CPU Shares set to High and a low-priority resource pool with CPU Shares set to Normal, as shown in Figure 4-1. This means that the share ratio between the pools is 2:1, so the high-priority pool is effectively allocated twice the CPU resources as the low-priority pool whenever CPU contention exists in the cluster. The high-priority pool is allocated 66.7 GHz, and the low-priority pool is effectively allocated 33.3 GHz. In this cluster, 40 virtual machines of equal size are running, with 32 in the high-priority pool and 8 in the low-priority pool. The virtual machines are all demanding CPU resources, causing CPU contention in the cluster. In the high-priority pool, each virtual machine is allocated 2.1 GHz. In the low-priority pool, each virtual machine is allocated 4.2 GHz.

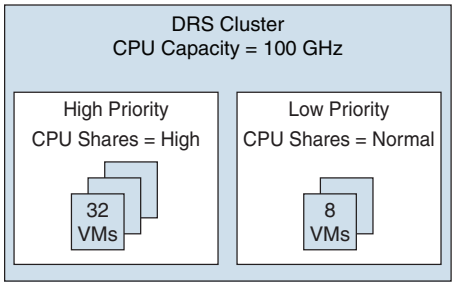

Figure 4-1 Scalable Shares Example

If you want to change the resource allocation such that each virtual machine in the high-priority pool is effectively allocated more resources than the virtual machines in the low-priority pool, you can use scalable shares. If you enable scalable shares in the cluster, DRS effectively allocates resources to the pools based on the Shares settings and the number of virtual machines in the pool. In this example, the CPU shares for the pools provide a 2:1 ratio. Factoring this with the number of virtual machines in each pool, the allocation ratio between the high-priority pool and the low-priority pool is 2 times 32 to 1 times 8, or simply 8:1. The high-priority pool is allocated 88.9 GHz, and the low-priority pool is allocated 11.1 GHz. Each virtual machine in the high-priority pool is allocated 2.8 GHz. Each virtual machine in the low-priority pool is allocated 1.4 GHz.

vSphere High Availability (HA)

vSphere HA is a cluster service that provides high availability for the virtual machines running in the cluster. You can enable vSphere High Availability (HA) on a vSphere cluster to provide rapid recovery from outages and cost-effective high availability for applications running in virtual machines. vSphere HA provides application availability in the following ways:

- It protects against server failure by restarting the virtual machines on other hosts in the cluster when a host failure is detected, as illustrated in Figure 4-2.
- It protects against application failure by continuously monitoring a virtual machine and resetting it if a failure is detected.
- It protects against datastore accessibility failures by restarting affected virtual machines on other hosts that still have access to their datastores.
- It protects virtual machines against network isolation by restarting them if their host becomes isolated on the management or vSAN network. This protection is provided even if the network has become partitioned.

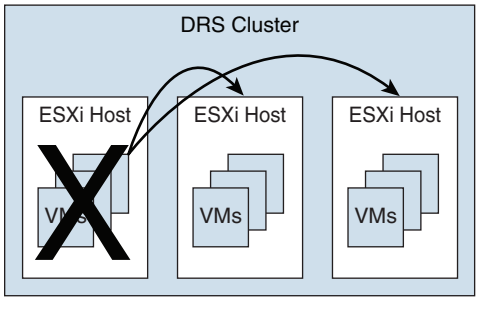

Figure 4-2 vSphere HA Host Failover

Benefits of vSphere HA over traditional failover solutions include the following:

- Minimal configuration
- Reduced hardware cost
- Increased application availability
- DRS and vMotion integration

vSphere HA can detect the following types of host issues:

- **Failure**: A host stops functioning.
- **Isolation**: A host cannot communicate with any other hosts in the cluster.
- **Partition**: A host loses network connectivity with the primary host.

When you enable vSphere HA on a cluster, the cluster elects one of the hosts to act as the primary host. The primary host communicates with vCenter Server to report cluster health. It monitors the state of all protected virtual machines and secondary hosts. It uses network and datastore heartbeating to detect failed hosts, isolation, and network partitions. vSphere HA takes appropriate actions to respond to host failures, host isolation, and network partitions. For host failures, the typical reaction is to restart the failed virtual machines on surviving hosts in the cluster. If a network partition occurs, a primary host is elected in each partition. If a specific host is isolated, vSphere HA takes the predefined host isolation action, which may be to shut down or power down the host's virtual machines. If the primary host fails, the surviving hosts elect a new primary host. You can configure vSphere to monitor and respond to virtual machine failures, such as guest OS failures, by monitoring heartbeats from VMware Tools.

NOTE Although vCenter Server is required to implement vSphere HA, the health of an HA cluster is not dependent on vCenter Server. If vCenter Server fails, vSphere HA still functions. If vCenter Server is offline when a host fails, vSphere HA can fail over the affected virtual machines.

vSphere HA Requirements

Key Topic

When planning a vSphere HA cluster, you need to address the following requirements:

- The cluster must have at least two hosts, licensed for vSphere HA.
- Hosts must use static IP addresses or guarantee that IP addresses assigned by DHCP persist across host reboots.

- Each host must have at least one—and preferably two—management networks in common.
- To ensure that virtual machines can run any host in the cluster, the hosts must access the same networks and datastores.
- To use VM Monitoring, you need to install VMware Tools in each virtual machine.
- IPv4 or IPv6 can be used.

NOTE The Virtual Machine Startup and Shutdown (automatic startup) feature is disabled and unsupported for all virtual machines residing in a vSphere HA cluster.

vSphere HA Response to Failures

You can configure how a vSphere HA cluster should respond to different types of failures, as described in Table 4-7.

Key Topic

Table 4-7 vSphere HA Response to Failure Settings

Option	Description
Host Failure Response > Failure Response	If Enabled, the cluster responds to host failures by restarting virtual machines. If Disabled, host monitoring is turned off, and the cluster does not respond to host failures.
Host Failure Response > Default VM Restart Priority	You can indicate the order in which virtual machines are restarted when the host fails (higher-priority machines first).
Host Failure Response > VM Restart Priority Condition	The restart priority condition must be met before HA restarts the next priority group.
Response for Host Isolation	You can indicate the action that you want to occur if a host becomes isolated. You can choose Disabled, Shutdown and Restart VMs, or Power Off and Restart VMs.
VM Monitoring	You can indicate the sensitivity (Low, High, or Custom) with which vSphere HA responds to lost VMware Tools heartbeats.
Application Monitoring	You can indicate the sensitivity (Low, High, or Custom) with which vSphere HA responds to lost application heartbeats.

NOTE If multiple hosts fail, the virtual machines on the failed host migrate first in order of priority, and then the virtual machines from the next host migrate.

Heartbeats

The primary host and secondary hosts exchange network heartbeats every second. When the primary host stops receiving these heartbeats from a secondary host, it checks for ping responses or the presence of datastore heartbeats from the secondary host. If the primary host does not receive a response after checking for a secondary host's network heartbeat, ping, or datastore heartbeats, it declares that the secondary host has failed. If the primary host detects datastore heartbeats for a secondary host but no network heartbeats or ping responses, it assumes that the secondary host is isolated or in a network partition.

If any host is running but no longer observes network heartbeats, it attempts to ping the set of cluster isolation addresses. If those pings also fail, the host declares itself to be isolated from the network.

vSphere HA Admission Control

vSphere uses admission control when you power on a virtual machine. It checks the amount of unreserved compute resources and determines whether it can guarantee that any reservation configured for the virtual machine is configured. If so, it allows the virtual machine to power on. Otherwise, it generates an "Insufficient Resources" warning.

vSphere HA Admission Control is a setting that you can use to specify whether virtual machines can be started if they violate availability constraints. The cluster reserves resources so that failover can occur for all running virtual machines on the specified number of hosts. When you configure vSphere HA admission control, you can set the options described in Table 4-8.

Table 4-8 vSphere HA Admission Control Options

Option	Description
Host Failures Cluster Tolerates	Specifies the maximum number of host failures for which the cluster guarantees failover
Define Host Failover Capacity By set to Cluster Resource Percentage	Specifies the percentage of the cluster's compute resources to reserve as spare capacity to support failovers
Define Host Failover Capacity By set to Slot Policy (for powered-on VMs)	Specifies a slot size policy that covers all powered-on VMs
Define Host Failover Capacity By set to Dedicated Failover Hosts	Specifies the designated hosts to use for failover actions
Define Host Failover Capacity By set to Disabled	Disables admission control
Performance Degradation VMs Tolerate	Specifies the percentage of performance degradation the VMs in a cluster are allowed to tolerate during a failure

If you disable vSphere HA admission control, then you enable the cluster to allow virtual machines to power on regardless of whether they violate availability constraints. In the event of a host failover, you may discover that vSphere HA cannot start some virtual machines.

In vSphere 8.0, the default admission control setting is Cluster Resource Percentage, which reserves a percentage of the total available CPU and memory resources in the cluster. For simplicity, the percentage is calculated automatically by defining the number of host failures to tolerate (FTT). The percentage is dynamically changed as hosts are added to the cluster or removed from it. Another new enhancement is the Performance Degradation VMs Tolerate setting, which controls the amount of performance reduction that is tolerated after a failure. A value of 0% indicates that no performance degradation is tolerated.

With the Slot Policy option, vSphere HA admission control ensures that a specified number of hosts can fail, leaving sufficient resources in the cluster to accommodate the failover of the impacted virtual machines. Using the Slot Policy option, when you perform certain operations, such as powering on a virtual machine, vSphere HA applies admission control in the following manner:

Step 1. HA calculates the slot size, which is a logical representation of memory and CPU resources. By default, it is sized to satisfy the requirements for any powered-on virtual machine in the cluster. For example, it may be sized to accommodate the virtual machine with the greatest CPU reservation and the virtual machine with the greatest memory reservation.

Step 2. HA determines how many slots each host in the cluster can hold.

Step 3. HA determines the current failover capacity of the cluster, which is the number of hosts that can fail while still leaving enough slots to satisfy all the powered-on virtual machines.

Step 4. HA determines whether the current failover capacity is less than the configured failover capacity (provided by the user).

Step 5. If the current failover capacity is less than the configured failover capacity, admission control disallows the operation.

If a cluster has a few virtual machines that have much larger reservations than the others, they will distort slot size calculation. To remediate this, you can specify an upper bound for the CPU or memory component of the slot size by using advanced options. You can also set a specific slot size (CPU size and memory size). The next section describes the advanced options that affect the slot size.

vSphere HA Advanced Options

You can set vSphere HA advanced options by using the vSphere Client or in the fdm.cfg file on the hosts. Table 4-9 provides some of the advanced vSphere HA options.

Table 4-9 Advanced vSphere HA Options

Option	Description
das.isolationaddress*X*	Provides the addresses to use to test for host isolation when no heartbeats are received from other hosts in the cluster. If this option is not specified (which is the default setting), the management network default gateway is used to test for isolation. To specify multiple addresses, you can set das.isolationaddress*X*, where *X* is a number between 0 and 9.
das.usedefaultisolationaddress	Specifies whether to use the default gateway IP address for isolation tests.
das.isolationshutdowntimeout	For scenarios where the host's isolation response is to shut down, specifies the period of time that the virtual machine is permitted to shut down before the system powers it off.
das.slotmeminmb	Defines the maximum bound on the memory slot size.
das.slotcpuinmhz	Defines the maximum bound on the CPU slot size.
das.vmmemoryminmb	Defines the default memory resource value assigned to a virtual machine whose memory reservation is not specified or is zero. This is used for the Host Failures Cluster Tolerates admission control policy.
das.vmcpuminmhz	Defines the default CPU resource value assigned to a virtual machine whose CPU reservation is not specified or is zero. This is used for the Host Failures Cluster Tolerates admission control policy. If no value is specified, the default of 32 MHz is used.
das.heartbeatdsperhost	Specifies the number of heartbeat datastores required per host. The default is 2. The acceptable values are 2 to 5.
das.config.fdm. isolationPolicyDelaySec	Specifies the number of seconds the system delays before executing the isolation policy after determining that a host is isolated. The minimum is 30. A lower value results in a 30-second delay.
das.respectvmvmantiaffinityrules	Determines whether vSphere HA should enforce VM–VM anti-affinity rules even when DRS is not enabled.

Virtual Machine Settings

To use the Host Isolation Response Shutdown and Restart VMs setting, you must install VMware Tools on the virtual machine. If a guest OS fails to shut down in 300 seconds (or a value specified by das.isolationshutdowntimeout), the virtual machine is powered off.

You can override the cluster's settings for Restart Priority and Isolation Response for each virtual machine. For example, you might want to prioritize virtual machines providing infrastructure services such as DNS or DHCP.

At the cluster level, you can create dependencies between groups of virtual machines. You can create VM groups, host groups, and dependency rules between the groups. In the rules, you can specify that one VM group cannot be restarted if another specific VM group is started.

VM Component Protection (VMCP)

Virtual Machine Component Protection (VMCP) is a vSphere HA feature that can detect datastore accessibility issues and provide remediation for affected virtual machines. When a failure occurs such that a host can no longer access the storage path for a specific datastore, vSphere HA can respond by taking actions such as creating event alarms or restarting a virtual machine on other hosts. The main requirements are that vSphere HA is enabled in the cluster and that ESX 6.0 or later is used on all hosts in the cluster.

The failures VMCP detects are permanent device loss (PDL) and all paths down (APD). PDL is an unrecoverable loss of accessibility to the storage device that cannot be fixed without powering down the virtual machines. APD is a transient accessibility loss or other issue that is recoverable.

For PDL and APD failures, you can set VMCP to either issue event alerts or to power off and restart virtual machines. For APD failures only, you can additionally control the restart policy for virtual machines by setting it to Conservative or Aggressive. With the Conservative setting, the virtual machine is powered off only if HA determines that it can be restarted on another host. With the Aggressive setting, HA powers off the virtual machine regardless of the state of other hosts.

Virtual Machine and Application Monitoring

VM Monitoring restarts specific virtual machines if their VMware Tools heartbeats are not received within a specified time. Likewise, Application Monitoring can restart a virtual machine if the heartbeats from a specific application in the virtual machine are not received. If you enable these features, you can configure the monitoring settings to control the failure interval and reset period. Table 4-10 lists these settings.

Table 4-10 VM Monitoring Settings

Setting	Failure Interval	Reset Period
High	30 seconds	1 hour
Medium	60 seconds	24 hours
Low	120 seconds	7 days

The Maximum per-VM Resets setting can be used to configure the maximum number of times vSphere HA attempts to restart a specific failing virtual machine within the reset period.

vSphere HA Best Practices

You should provide network path redundancy between cluster nodes. To do so, you can use NIC teaming for the virtual switch. You can also create a second management network connection, using a separate virtual switch.

When performing disruptive network maintenance operations on the network used by clustered ESXi hosts, you should suspend the Host Monitoring feature to ensure that vSphere HA does not falsely detect network isolation or host failures. You can reenable host monitoring after completing the work.

To keep vSphere HA agent traffic on the specified network, you should ensure that the VMkernel virtual network adapters used for HA heartbeats (enabled for management traffic) do not share the same subnet as VMkernel adapters used for vMotion and other purposes.

You use the das.isolationaddress*X* advanced option to add an isolation address for each management network.

Proactive HA

Proactive High Availability (Proactive HA) integrates with select hardware partners to detect degraded components and evacuate VMs from affected vSphere hosts before an incident causes a service interruption. Hardware partners offer a vCenter Server plug-in to provide the health status of the system memory, local storage, power supplies, cooling fans, and network adapters. As hardware components become degraded, Proactive HA determines which hosts are at risk and places them into either Quarantine Mode or Maintenance Mode. When a host enters Maintenance Mode, DRS evacuates its virtual machines to healthy hosts, and the host is not used to run virtual machines. When a host enters Quarantine Mode, DRS leaves the current virtual machines running on the host but avoids placing or migrating virtual machines to the host. If you prefer that Proactive HA simply make evacuation recommendations rather than automatic migrations, you can set Automation Level to Manual.

The vendor-provided health providers read sensor data in the server and provide the health state to vCenter Server. The health states are Healthy, Moderate Degradation, Severe Degradation, and Unknown.

Other Resource Management and Availability Features

This section describes other vSphere features related to resource management and availability.

Predictive DRS

Predictive DRS is a feature in vSphere 6.5 and later that leverages the predictive analytics of VMware Aria Operations, formerly known as vRealize Operations (vROps), and vSphere DRS. Together, these two products can provide workload balancing prior to the occurrence of resource utilization spikes and resource contention. Every night, Aria Operations calculates dynamic thresholds, which are used to create forecasted metrics for the future utilization of virtual machines. Aria Operations passes the predictive metrics to vSphere DRS to determine the best placement and balance of virtual machines before resource utilization spikes occur. Predictive DRS helps prevent resource contention on hosts that run virtual machines with predictable utilization patterns.

The following prerequisites are needed to run Predictive DRS:

- vCenter Server 6.5 or later is required.
- Predictive DRS must be configured and enabled in both vCenter Server and Aria Operations.
- The vCenter Server and Aria Operations clocks must be synchronized.

Distributed Power Management (DPM)

The vSphere Distributed Power Management (DPM) feature enables a DRS cluster to reduce its power consumption by powering hosts on and off, as needed, based on cluster resource utilization. DPM monitors the cumulative virtual machine demand for memory and CPU resources in the cluster and compares this to the available resources in the cluster. If sufficient excess capacity is found, vSphere DPM directs the host to enter Standby Mode. When DRS detects that a host is entering Standby Mode, it evacuates the virtual machines. Once the host is evacuated, DPM powers it off, and the host is in Standby Mode. When DPM determines that capacity is inadequate to meet the resource demand, DPM brings a host out of Standby Mode by powering it on. Once the host exits Standby Mode, DRS migrates virtual machines to it.

To power on a host, DPM can use one of three power management protocols: Intelligent Platform Management Interface (IPMI), Hewlett-Packard Integrated Lights-Out (iLO), or Wake-on-LAN (WoL). If a host supports multiple protocols, they

are used in the following order: IPMI, iLO, WOL. If a host does not support one of these protocols, DPM cannot automatically bring a host out of Standby Mode.

DPM is very configurable. As with DRS, you can set DPM's automation to be manual or automatic.

NOTE Do not disconnect a host that is in Standby Mode or remove it from a DRS cluster without first powering it on. Otherwise, vCenter Server is not able to power the host back on.

To configure IPMI or iLO settings for a host, you can edit the host's Power Management settings. You should provide credentials for the Baseboard Management Controller (BMC) account, the IP address of the appropriate NIC, and the MAC address of the NIC.

Using WOL with DPM requires that the following prerequisites be met:

- ESXi 3.5 or later is required.
- vMotion must be configured.
- The vMotion NIC must support WOL.
- The physical switch port must be set to automatically negotiate the link speed.

Before enabling DPM, use the vSphere Client to request the host to enter Standby Mode. After the host powers down, right-click the host and attempt to power on. If this is successful, you can allow the host to participate in DPM. Otherwise, you should disable power management for the host.

You can enable DPM in a DRS cluster's settings. You can set Automation Level to Off, Manual, or Automatic. When this option is set to Off, DPM is disabled. When it is set to Manual, DPM makes recommendations only. When it is set to Automatic, DPM automatically performs host power operations as needed.

Much as with DRS, with DPM you can control the aggressiveness of DPM (that is, the DPM threshold) with a slider bar in the vSphere Client. The DRS threshold and the DPM threshold are independent of one another. You can override automation settings per host. For example, for a 16-host cluster, you might want to set DPM Automation to Automatic on only 8 of the hosts.

Fault Tolerance (FT)

If you have virtual machines that require continuous availability as opposed to high availability, you can consider protecting the virtual machines with ***vSphere Fault***

Tolerance (FT). vSphere FT provides continuous availability for a virtual machine (the primary VM) by ensuring that the state of a secondary VM is identical at any point in the instruction execution of the virtual machine.

If the host running the primary VM fails, an immediate and transparent failover occurs. The secondary VM becomes the primary VM host without losing network connection or in-progress transactions. With transparent failover, there is no data loss, and network connections are maintained. The failover is fully automated and occurs even if vCenter Server is unavailable. Following the failover, FT spawns a new secondary VM and reestablishes redundancy and protection, assuming that a host with sufficient resources is available in the cluster. Likewise, if the host running the secondary VM fails, a new secondary VM is deployed. vSphere Fault Tolerance can accommodate symmetric multiprocessor (SMP) virtual machines with up to eight vCPUs.

Use cases for FT include the following:

- Applications that require continuous availability, especially those with long-lasting client connections that need to be maintained during hardware failure
- Custom applications that have no other way of being clustered
- Cases in which other clustering solutions are available but are too complicated or expensive to configure and maintain

Before implementing FT, consider the following requirements:

- CPUs must be vMotion compatible.
- CPUs must support hardware MMU virtualization.
- A low-latency 10 Gbps network is required for FT Logging.
- Virtual machine files other than VMDK files must be stored on shared storage.
- A vSphere Standard License is required for FT protection of virtual machines with up to two virtual CPUs.
- A vSphere Enterprise Plus License is required for FT protection of virtual machines with up to eight virtual CPUs.
- Hardware Virtualization (HV) must be enabled in the host BIOS.
- Hosts must be certified for FT.
- The virtual memory reservation should be set to match the memory size.
- vSphere HA must be enabled on the cluster.
- SSL certificate checking must be enabled in the vCenter Server settings.
- The hosts must use ESXi 6.x or later.

You should also consider the following VMware recommendations concerning vSphere FT:

- VMware recommends a minimum of two physical NICs.
- VMware recommends that the host BIOS power management settings be set to Maximum Performance or OS-Managed Performance.
- You should have at least three hosts in the cluster to accommodate a new secondary VM following a failover.

The following vSphere features are not supported for FT-protected virtual machines:

- Snapshots (An exception is that disk-only snapshots created for vStorage APIs for Data Protection [VADP] backups are supported for FT but not for legacy FT.)
- Storage vMotion
- Linked clones
- Virtual Volumes datastores
- Storage-based policy management (However, vSAN storage policies are supported.)
- I/O filters
- Disk encryption
- Trusted Platform Module (TPM)
- Virtual Based Security (VBS)–enabled VMs
- Universal Point in Time snapshots (a next-generation vSAN feature)
- Physical raw device mappings (RDMs) (However, virtual RDMs are supported for legacy FT.)
- Virtual CD-ROMs for floppy drives backed by physical devices
- USB devices, sound devices, serial ports, and parallel ports
    - N-Port ID Virtualization (NPIV)
- Network adapter passthrough
- Hot plugging devices (Note that the hot plug feature is automatically disabled when you enable FT on a virtual machine.)
- Changing the network where a virtual NIC is connected

- Virtual Machine Communication Interface (VMCI)
- Virtual disk files larger than 2 TB
- Video devices with 3D enabled

You should apply the following best practices for FT:

- Use similar CPU frequencies in the hosts.
- Use active/standby NIC teaming settings.
- Ensure that the FT Logging network is secure (that is, FT data is not encrypted).
- Enable jumbo frames and 10 Gbps for the FT network. Optionally, configure multiple NICs for FT Logging.
- Place ISO files on shared storage.
- If vSAN is used for primary or secondary VMs, do not also connect those virtual machines to other storage types. Also, place the primary and secondary VMs in separate vSAN fault domains.
- Keep vSAN and FT Logging on separate networks.

In vSphere 6.5, FT is supported with DRS only when EVC is enabled. You can assign a DRS automation to the primary VM and let the secondary VM assume the same setting. If you enable FT for a virtual machine in a cluster where EVC is disabled, the virtual machine DRS automation level is automatically disabled. In versions since vSphere 6.7, EVC is not required for FT to support DRS.

To enable FT, you first create a VMkernel virtual network adapter on each host and connect to the FT Logging network. You should enable vMotion on a separate VMkernel adapter and network.

When you enable FT protection for a virtual machine, the following events occur:

- If the primary VM is powered on, validation tests occur. If validation is passed, then the entire state of the primary VM is copied and used to create the secondary VM on a separate host. The secondary VM is powered on. The virtual machine's FT status is Protected.
- If the primary VM is powered off, the secondary VM is created and registered to a host in the cluster but not powered on. The virtual machine FT Status setting is Not Protected, VM not Running. When you power on the primary VM, the validation checks occur, and the secondary VM is powered on. Then FT Status changes to Protected.

Legacy FT VMs can exist only on ESXi hosts running on vSphere versions earlier than 6.5. If you require legacy FT, you should configure a separate vSphere 6.0 cluster.

vCenter Server High Availability

vCenter Server High Availability (vCenter HA) is described in Chapter 1, "vSphere Overview, Components, and Requirements." vCenter HA implementation is covered in Chapter 8, "vSphere Installation." vCenter HA management is covered in Chapter 13, "Managing vSphere and vCenter Server."

VMware Service Lifecyle Manager

If a vCenter service fails, ***VMware Service Lifecycle Manager*** (vmon) restarts it. VMware Service Lifecycle Manager is a service that runs in a vCenter server that monitors the health of services and takes preconfigured remediation action when it detects a failure. If multiple attempts to restart a service fail, the service is considered failed.

NOTE Do not confuse VMware Service Lifecyle Manager with VMware vSphere Lifecycle Manager, which provides simple, centralized lifecycle management for ESXi hosts through the use of images and baselines.

Exam Preparation Tasks

As mentioned in the section "Book Features and Exam Preparation Methods" in the Introduction, you have some choices for exam preparation: the exercises here, Chapter 15, "Final Preparation," and the exam simulation questions on the companion website.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 4-11 lists these key topics and the page number on which each is found.

Key Topic

Table 4-11 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
Section	Network-aware DRS	140
Section	How DRS scores VMs	142
List	DRS migration sensitivity	143
Section	Scalable shares	147
List	vSphere HA requirements	149
Table 4-7	vSphere HA response to failure settings	150
List	vSphere FT requirements	158

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables" (found on the companion website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Table Answers" (also on the companion website), includes completed tables and lists to check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Virtual Machine Component Protection (VMCP), Proactive High Availability (Proactive HA), Predictive DRS, vSphere Fault Tolerance (FT), VMware Service Lifecycle Manager

Review Questions

1. You are configuring EVC. Which of the following is not a requirement?
   a. A vSphere cluster
   b. A DRS cluster
   c. CPUs in the same family
   d. CPUs with the same base instruction set

2. In vSphere 8.0, you want to configure the DRS migration threshold such that it is at the maximum level at which resource contention is considered but virtual machine happiness is not. Which of the following values should you choose?
   a. Level 1
   b. Level 2
   c. Level 3
   d. Level 4
   e. Level 5

3. In a vSphere cluster, which of the following statements is true if the primary host detects datastore heartbeats for a secondary host but no network heartbeats or ping responses?
   a. The primary host declares that the secondary host is isolated.
   b. The primary host assumes that the secondary host is isolated or in a network partition.
   c. The primary host takes the host isolation response action.
   d. The primary host restarts the virtual machines on the failed secondary host.

4. You want to configure vSphere HA. Which of the following is a requirement?
   a. IPv4 must be used for all host management interfaces.
   b. vMotion must be enabled on each host.
   c. The Virtual Machine Startup and Shutdown (automatic startup) feature must be enabled on each virtual machine.
   d. Host IP addresses must persist across reboots.

5. You are configuring vSphere Distributed Power Management (DPM) in your vSphere 8.0 environment. Which of the following is not a requirement for using Wake-on-LAN (WoL) in DPM?
   a. The management NIC must support WOL.
   b. vMotion is configured.
   c. The vMotion NIC must support WOL.
   d. The physical switch port must be set to auto negotiate the link speed.

This page intentionally left blank

Index

B

C

D

E

F

G

H

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z