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:
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the Registered Products tab.

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.
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

Introduction xxvi

**PART I: VSPHERE ARCHITECTURE, INTEGRATION, AND REQUIREMENTS**

- **CHAPTER 1** vSphere Overview, Components, and Requirements 3
- **CHAPTER 2** Storage Infrastructure 31
- **CHAPTER 3** Network Infrastructure 91
- **CHAPTER 4** Clusters and High Availability 131
- **CHAPTER 5** vCenter Server Features and Virtual Machines 167
- **CHAPTER 6** VMware Product Integration 205
- **CHAPTER 7** vSphere Security 237

**PART II: VSPHERE INSTALLATION/CONFIGURATION**

- **CHAPTER 8** vSphere Installation 287
- **CHAPTER 9** Configuring and Managing Virtual Networks 331

**PART III: VSPHERE MANAGEMENT AND OPTIMIZATION**

- **CHAPTER 10** Managing and Monitoring Clusters and Resources 365
- **CHAPTER 11** Managing Storage 415
- **CHAPTER 12** Managing vSphere Security 471
- **CHAPTER 13** Managing vSphere and vCenter Server 515
- **CHAPTER 14** Managing Virtual Machines 573
- **CHAPTER 15** Final Preparation 613

**APPENDIX A** Answers to the “Do I Know This Already?” Quizzes and Review Questions 617
- Glossary 637
- Index 645

**ONLINE ELEMENTS:**

- **APPENDIX B** Memory Tables
- **APPENDIX C** Memory Table Answers
- **APPENDIX D** Study Planner
Table of Contents

Introduction   xxvi

Part I: vSphere Architecture, Integration, and Requirements

Chapter 1 vSphere Overview, Components, and Requirements   3

“Do I Know This Already?” Quiz   3

Foundation Topics   6
vSphere Components and Editions   6
vSphere Components   6
Editions and Licenses   8
vCenter Server Topology   10
Single Sign-On (SSO) Domain   11
Enhanced Linked Mode   12
vCenter HA   12

Infrastructure Requirements   13
Compute and System Requirements   14
Storage Requirements   16
Network Requirements   17
Infrastructure Services   21

Other Requirements   23
Additional Requirements   23
vSphere Replication Requirements   24
vCenter High Availability Requirements   24
SDDC Requirements   25

VMware Cloud vs. VMware Virtualization   26
Server Virtualization   26
VMware SDDC   26
cCloud Suite and Private Clouds   27
VCF and Hybrid Clouds   27
VMC on AWS   27
VMware vCloud Director   27
Cloud Automation   27

Exam Preparation Tasks   28
Review All the Key Topics   28
Complete Tables and Lists from Memory   28
Define Key Terms   28
Answer Review Questions   29
Chapter 2  Storage Infrastructure  31

“Do I Know This Already?” Quiz  31

Foundation Topics  34

Storage Models and Datastore Types  34
  How Virtual Machines Access Storage  34
  Storage Virtualization: The Traditional Model  34
  Software-Defined Storage Models  38
  Datastore Types  39
  Storage in vSphere with Kubernetes  43
  VMware NVMe  44

vSAN Concepts  47
  vSAN Characteristics  48
  vSAN Termination  50
  What Is New in vSAN 7.0 and Newer  52
  vSAN Deployment Options  53
  vSAN Limitations  58
  vSAN Space Efficiency  58
  vSAN Encryption  61
  vSAN File Service  61
  vSAN Requirements  63
  Other vSAN Considerations  68

vSphere Storage Integration  69
  VASA  69
  VAAI  70
  Virtual Volumes (vVols)  72

Storage Multipathing and Failover  75
  Multipathing Overview  75
  Pluggable Storage Architecture (PSA)  76

Storage Policies  80
  Storage Policy Based Management (SPBM)  81
  Virtual Disk Types  81
  vSAN-Specific Storage Policies  81

Storage DRS (SDRS)  83
  Initial Placement and Ongoing Balancing  83
  Space Utilization Load Balancing  83
  I/O Latency Load Balancing  83
  SDRS Automation Level  84
  SDRS Thresholds and Behavior  84
  SDRS Recommendations  84
  Anti-affinity Rules  85
  Datastore Cluster Requirements  85
  NIOC, SIOC, and SDRS  86
Exam Preparation Tasks  
Review All Key Topics  87  
Complete Tables and Lists from Memory  87  
Define Key Terms  87  
Review Questions  88

Chapter 3  Network Infrastructure  91

“Do I Know This Already?” Quiz  91

Foundation Topics  94

Networking Terms and Concepts  94
  Traditional Networking Terminology  94
  Virtual NICs  96
  Virtual Switch Concepts  96
  VLANs  97
vSphere Standard Switch (vSS)  98
  MTU  100
  vSS Network Policies  100
  NIC Teaming Policies  101
  Network Security Policies  102
  Traffic Shaping Policy  103
  VLAN Policies  104
vSphere Distributed Switch (vDS)  104
  Distributed Port Groups  105
  Uplink Port Groups  105
  vSS and vDS Comparison  106
  vDS Network Policies  106
  Inbound Traffic Shaping  107
  Port-Blocking Policies  108
  Load-Based NIC Teaming  108
  Resource Allocation Policy  108
  NetFlow and Monitoring Policy  111
  Traffic Filtering and Marking Policy  111
vDS Settings and Features  112
  Private VLANs  113
  Data Center–Level Management  113
  Network Offloads Compatibility  114
  Port State Monitoring  115
  Port State with vMotion  115
  Port Mirroring  116
  Port Binding and Allocation  117
  LACP Support  118
  vDS Health Check  119
Chapter 4 Clusters and High Availability 131

“Do I Know This Already?” Quiz 131

Foundation Topics 134

Cluster Concepts and Overview 134
  vSphere Cluster Services (vCLS) 135
  Enhanced vMotion Compatibility (EVC) 135
  vSAN Services 139
Distributed Resource Scheduler (DRS) 139
  Recent DRS Enhancements 139
  DRS Rules 142
  DRS Migration Sensitivity 143
  Resource Pools 144
vSphere High Availability (HA) 148
  vSphere HA Requirements 149
  vSphere HA Response to Failures 150
  Heartbeats 151
  vSphere HA Admission Control 151
  vSphere HA Advanced Options 153
  Virtual Machine Settings 153
  VM Component Protection (VMCP) 154
  Virtual Machine and Application Monitoring 154
  vSphere HA Best Practices 155
  Proactive HA 155

Other Resource Management and Availability Features 156
  Predictive DRS 156
  Distributed Power Management (DPM) 156
  Fault Tolerance (FT) 157
  vCenter Server High Availability 161
  VMware Service Lifecycle Manager 161
Exam Preparation Tasks  162
Review All Key Topics  162
Complete Tables and Lists from Memory  162
Define Key Terms  162
Review Questions  163

Chapter 5  vCenter Server Features and Virtual Machines  167

“Do I Know This Already?” Quiz  167

Foundation Topics  171
vCenter Server and vSphere  171
  vSphere Managed Inventory Objects  171
Host Profiles  175
Content Libraries  176
Virtual Machine File Structure  178
  Configuration File  179
  Virtual Disk Files  180
  Snapshot Files  180
Virtual Machine Snapshots  180
  Snapshot Use Cases  182
  What a Snapshot Preserves  182
  Parent Snapshots  183
  Snapshot Behavior  183
  Limitations  184
Virtual Machine Settings  185
  VM Hardware/Compatibility  185
  Virtual Disk Provisioning  188
  VMware Tools  188
  Virtual Machine Options  188
  Virtual Machine Advanced Settings  189
Virtual Machine Migration  190
  Migrating Virtual Machines  190
  vMotion Details  194
  Storage vMotion Details  197
Virtual Machine Cloning  199
  Clones  199
  Rapid Provisioning with Templates  200
  Instant Clones  200

Exam Preparation Tasks  202
Review All Key Topics  202
Complete Tables and Lists from Memory  202
Define Key Terms  202
Review Questions  203
Chapter 6  VMware Product Integration  205

“Do I Know This Already?” Quiz  205

Foundation Topics  208

vSphere Add-ons  208
  vSphere with Tanzu  208
  vSphere+  213
  vCenter Converter  214
  VMware vSphere Replication  215
  VMware SkyLine  215

Aria Suite  216
  Aria Operations  216
  Aria for Logs  217
  Aria Automation  218
  Aria Orchestrator  219
  Aria Operations for Networks  220

Desktop and Application Virtualization  222
  VMware Horizon  222
  App Volumes  223

Replication and Disaster Recovery  224
  vSphere Replication  224
  Site Recovery Manager (SRM)  226

Private, Public, and Hybrid Clouds  227
  VMware Cloud Foundation (VCF)  227
  VMware Hybrid Cloud Extension (HCX)  229
  VMware Cloud (VMC) on AWS  231
  Azure VMware Solution  231

Networking and Security  232
  NSX  232

Exam Preparation Tasks  234

Review All Key Topics  234
Complete Tables and Lists from Memory  234
Define Key Terms  234
Review Questions  235

Chapter 7  vSphere Security  237

“Do I Know This Already?” Quiz  237

Foundation Topics  240

vSphere Certificates  240
  vSphere Certificates Overview  240
  Certificate Requirements  242
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Host Certificates</td>
<td>245</td>
</tr>
<tr>
<td>vSphere Permissions</td>
<td>246</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>246</td>
</tr>
<tr>
<td>Inventory Hierarchy and Objects</td>
<td>246</td>
</tr>
<tr>
<td>Privileges and Roles</td>
<td>248</td>
</tr>
<tr>
<td>Permissions</td>
<td>250</td>
</tr>
<tr>
<td>Global Permissions</td>
<td>250</td>
</tr>
<tr>
<td>Best Practices for Roles and Permissions</td>
<td>251</td>
</tr>
<tr>
<td>Required Privileges for Common Tasks</td>
<td>252</td>
</tr>
<tr>
<td>How Permissions Are Applied by vCenter Server</td>
<td>255</td>
</tr>
<tr>
<td>ESXi and vCenter Server Security</td>
<td>257</td>
</tr>
<tr>
<td>Built-in Security Features</td>
<td>257</td>
</tr>
<tr>
<td>Security Profiles</td>
<td>258</td>
</tr>
<tr>
<td>ESXi Password Hardening</td>
<td>260</td>
</tr>
<tr>
<td>Joining an ESXi Host to a Directory Service</td>
<td>260</td>
</tr>
<tr>
<td>vSphere Authentication Proxy</td>
<td>260</td>
</tr>
<tr>
<td>ESXi Host Access</td>
<td>261</td>
</tr>
<tr>
<td>Control MOB Access</td>
<td>261</td>
</tr>
<tr>
<td>ESXi Secure Boot and TPM</td>
<td>261</td>
</tr>
<tr>
<td>vSphere Trust Authority (vTA)</td>
<td>263</td>
</tr>
<tr>
<td>vCenter Server Security</td>
<td>263</td>
</tr>
<tr>
<td>vSphere Network Security</td>
<td>266</td>
</tr>
<tr>
<td>Firewalls</td>
<td>266</td>
</tr>
<tr>
<td>Segmentation and Isolation</td>
<td>266</td>
</tr>
<tr>
<td>Internet Protocol Security</td>
<td>266</td>
</tr>
<tr>
<td>Virtual Machine Security</td>
<td>269</td>
</tr>
<tr>
<td>Virtual Machine Hardening Best Practices</td>
<td>269</td>
</tr>
<tr>
<td>Configuring UEFI Boot</td>
<td>270</td>
</tr>
<tr>
<td>Disabling Unexposed Features</td>
<td>270</td>
</tr>
<tr>
<td>Other Common Settings</td>
<td>270</td>
</tr>
<tr>
<td>Virtual Machine Risk Profiles</td>
<td>272</td>
</tr>
<tr>
<td>Protecting Virtual Machines Against Denial-of-Service Attacks</td>
<td>272</td>
</tr>
<tr>
<td>Controlling VM Device Connections</td>
<td>273</td>
</tr>
<tr>
<td>Virtual Machine Encryption</td>
<td>273</td>
</tr>
<tr>
<td>Encrypted vSphere vMotion</td>
<td>276</td>
</tr>
<tr>
<td>Virtual Trusted Platform Module (vTPM)</td>
<td>277</td>
</tr>
<tr>
<td>Virtual Intel Software Guard Extension (vSGX)</td>
<td>278</td>
</tr>
<tr>
<td>Available Add-on Security</td>
<td>279</td>
</tr>
<tr>
<td>Compliance Using VMware Aria Operations</td>
<td>279</td>
</tr>
<tr>
<td>VMware NSX</td>
<td>280</td>
</tr>
</tbody>
</table>
Exam Preparation Tasks 282
Review All the Key Topics 282
Complete Tables and Lists from Memory 282
Define Key Terms 283
Review Questions 283

Part II: vSphere Installation/Configuration

Chapter 8 vSphere Installation 287
“Do I Know This Already?” Quiz 287

Foundation Topics 290
Installing ESXi Hosts 290
  Installing ESXi Interactively 290
  Scripted ESXi Installation 292
  Using Auto Deploy 296
Deploying vCenter Server Components 301
  vCenter Server Database 301
  Platform Services Controller (PSC) 301
  vCenter Server Appliance 302
Configuring and Managing VMware Certificate Authority (VMCA) 307

Configuring Single Sign-On (SSO) 309
  SSO and Identity Sources Overview 309
  Adding, Editing, and Removing SSO Identity Sources 310
  Adding an Active Directory Identity Source 311
  Adding an LDAP Authentication Source 313
  Enabling and Disabling Single Sign-On (SSO) Users 314
  Configuring SSO Policies 315
  Configuring Identity Federation 316
Initial vSphere Configuration 318
  Implementing vSphere Client 318
  Implementing VMware vSphere Lifecycle Manager 318
  Configuring the vCenter Server Inventory 319
  Using Host Profiles 321
  VMware Tools 324
  ESXi Configuration Settings 324
  Advanced ESXi Host Options 325

Exam Preparation Tasks 327
Review All the Key Topics 327
Complete Tables and Lists from Memory 327
Define Key Terms 327
Review Questions 328
Chapter 9 Configuring and Managing Virtual Networks 331

“Do I Know This Already?” Quiz 331

Foundation Topics 334

vSphere Standard Switches (vSS) 334
  Creating and Configuring vSphere Standard Switches 334
  Creating and Configuring Standard Port Groups 336

vSphere Distributed Switches (vDS) 338
  Creating and Configuring vSphere Distributed Switches 338
  Creating and Configuring Distributed Port Groups 341

VMkernel Networking 342
  Configuring and Managing VMkernel Adapters 342
  Configuring TCP/IP Stacks 343

Configuring and Managing Networking Features 344
  Configuring Network I/O Control (NIoC) 344
  Creating a Network Resource Pool 345
  Using Private VLANs 346
  Using DirectPath I/O 347
  Single Root I/O Virtualization (SR-IOV) 347
  Configuring and Managing Port Mirroring 349
  Configuring and Managing Link Aggregation Groups (LAGs) 350

Managing Host Networking with vDS 354
  Adding Hosts to a vDS 354
  Managing Host Physical Network Adapters on a vDS 355
  Migrating VMkernel Network Adapters to a vDS 356
  Removing Hosts from a vDS 356
  Migrating Virtual Machines to a vDS 357
  Monitoring the State of Ports in a Distributed Port Group 358
  Using the vDS Health Check 358
  Networking Policies and Advanced Features 359

Exam Preparation Tasks 361
  Review All the Key Topics 361
  Complete Tables and Lists from Memory 361
  Define Key Terms 361
  Review Questions 362

Part III: vSphere Management and Optimization

Chapter 10 Managing and Monitoring Clusters and Resources 365

“Do I Know This Already?” Quiz 365

Foundation Topics 368
Creating and Configuring a vSphere Cluster 368
   Creating a Cluster 368
   Configuring a Cluster with Quickstart 369
   EVC Mode 372
Creating and Configuring a vSphere DRS Cluster 372
   Creating a vSphere DRS Cluster 372
   Creating a Resource Pool 372
   Configuring Advanced DRS Options 373
Creating and Configuring a vSphere HA Cluster 374
   Creating a vSphere HA Cluster 374
   Configuring Advanced vSphere HA Options 374
   Configuring vSphere HA Admission Control 375
   Configuring VMCP 375
   Configuring Virtual Machine and Application Monitoring 376
   Configuring Proactive HA 376
   Configuring vSphere Fault Tolerance 377
Monitoring and Managing vSphere Resources 377
   Metrics 378
   vSphere Client Performance Charts 379
   Troubleshooting and Optimizing Performance 383
   Monitoring and Managing Cluster Resources 388
   Monitoring and Managing Resource Pool Resources 389
   Monitoring and Managing Host Resources and Health 390
   Monitoring and Managing Virtual Machine Resources 392
ESXTOP 396
VIMTOP 399
   vCenter Server Management 399
Events, Alarms, and Automated Actions 400
   Events 400
   Viewing Events in the vSphere Client 400
   Viewing the System Event Log 401
   Streaming Events to a Remote Syslog Server 401
   Alarms 402
   Viewing and Acknowledging Triggered Alarms 403
   Creating Alarm Definitions 403
   Alarm Actions 404
   Advanced Use Cases for Alarms 404
Logging in vSphere 405
   ESXi Logs 405
   vCenter Server Logs 407
   Uploading System Logs to VMware 407
   Log Levels 408
Managing PMem 458
Multipathing, Storage Policies, and vVols 459
  Managing Multipathing 460
  Managing Storage Policies 463
  Configuring and Managing vVols 466

Exam Preparation Tasks 468
Review All the Key Topics 468
Complete Tables and Lists from Memory 468
Define Key Terms 468
Review Questions 469

Chapter 12 Managing vSphere Security 471

“Do I Know This Already?” Quiz 471

Foundation Topics 474
Configuring and Managing Authentication and Authorization 474
  Managing SSO 474
  Users and Groups 476
  Privileges and Roles 477
  Permissions 477
  Global Permissions 478
  Editing Permissions 478
Configuring and Managing vSphere Certificates 479
  Managing vSphere Client Certificates 479
  Using Custom Certificates 480
  Managing ESXi Certificates 481
General ESXi Security Recommendations 483
  Hardening Guidelines 484
  Configuring ESXi Using Host Profiles 485
  Using Scripts to Manage Host Configuration Settings 486
  ESXi Passwords and Account Lockout 487
  SSH and ESXi Shell Security 489
  PCI and PCIe Devices and ESXi 491
  Disabling the Managed Object Browser 491
  ESXi Networking Security Recommendations 492
  ESXi Web Proxy Settings 492
  vSphere Auto Deploy Security Considerations 493
  Controlling CIM Access 493
Configuring and Managing ESXi Security 494
  Configuring the ESXi Firewall 494
  Customizing ESXi Services 495
  Using Lockdown Mode 496
  Managing the Acceptance Levels of Hosts and VIBs 497
Assigning Privileges for ESXi Hosts 498
Using Active Directory to Manage ESXi Users 499
Configuring vSphere Authentication Proxy 500
Configuring Smart Card Authentication for ESXi 501
Configuring UEFI Secure Boot for ESXi Hosts 501
Securing ESXi Hosts with Trusted Platform Module 502
Securing ESXi Log Files 503
Additional Security Management 503
Key Management Server 503
Changing Permission Validation Settings 504
Configuring and Managing vSphere Trust Authority (vTA) 504
TLS 1.2 506
FIPS 507
Securing Virtual Machines with Intel Software Guard Extensions (SGX) 507
Encrypting a Virtual Machine 508
Exam Preparation Tasks 510
Review All the Key Topics 510
Complete Tables and Lists from Memory 510
Define Key Terms 510
Review Questions 511

Chapter 13 Managing vSphere and vCenter Server 515
“Do I Know This Already?” Quiz 515
Foundation Topics 518
vCenter Server Backup 518
Back Up and Restoring vSphere with Tanzu 521
Upgrading to vSphere 8.0 523
vCenter Server Data Transfer 524
Upgrading vCenter Server Appliance 525
Migrating vCenter Server for Windows to vCenter Server Appliance 528
Upgrading ESXi and Virtual Machines 530
Using Update Planner 530
Using vSphere Lifecycle Manager 532
About VMware Update Manager 535
VMware Update Manager Download Service (UMDS) 535
Baselines and Images 536
ESXi Quick Boot 542
ESXi Firmware Updates 542
Hardware Compatibility Checks 544
Exporting and Importing Cluster Images 544
Backup and Restore Scenarios 545
Upgrading Virtual Machines 546
Managing ESXi Hosts 547
Monitoring and Managing vCenter Server 549
  Monitoring and Managing vCenter Server with the VAMI 550
  Monitoring and Managing vCenter Server with the vSphere Client 554
  Updating the vCenter Server 561
  Managing a vCenter HA Cluster 564
  Repointing a vCenter Server to Another Domain 565
Exam Preparation Tasks 569
  Review All the Key Topics 569
  Complete Tables and Lists from Memory 569
  Define Key Terms 570
  Review Questions 570

Chapter 14 Managing Virtual Machines 573
“Do I Know This Already?” Quiz 573
Foundation Topics 576
  Creating and Configuring Virtual Machines 576
    Creating a New Virtual Machine 576
    Powering On a VM 577
    Opening a Console to a VM 577
    Installing and Upgrading VMware Tools 578
    Shutting Down a Guest 580
    Cloning a Virtual Machine 580
    Converting Between a VM and a Template 581
    Deploying a Virtual Machine from a Template 582
    Customizing the Guest OS 582
    Deploying OVF/OVA Templates 585
Managing Virtual Machines 586
  Configuring Virtual Machine Hardware 586
  Editing Virtual Machine Options 592
  Configuring Guest User Mappings 594
  Editing OVF Details 594
  Creating and Managing Virtual Machine Snapshots 595
  Migrating Virtual Machines 596
Advanced Virtual Machine Management 598
  Managing OVF Templates 598
  Virtualization-Based Security 598
  Managing VMs by Using PowerCLI 599
  Configuring VMs to Support vGPUs 601
  Managing EVC Mode and CPU Affinity 603
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, MEJEEER, 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/UCYrPi0AqS8fQxChAgZa5Sg.
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>
<thead>
<tr>
<th>Objective</th>
<th>Description</th>
<th>Chapter/Section</th>
<th>Supporting Chapter/Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Architectures and Technologies</td>
<td>1: vSphere Overview, Components, and Requirements</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td>1.1 Identify the prerequisites and components for a VMware vSphere 8.x implementation</td>
<td>▪ Infrastructure Requirements</td>
<td>▪ Installing ESXi Hosts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Other Requirements</td>
<td>▪ Deploying vCenter Server Components</td>
</tr>
<tr>
<td>1.2</td>
<td>Describe the components and topology of a VMware vCenter architecture</td>
<td>1: vSphere Overview, Components, and Requirements</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ vCenter Server Topology</td>
<td>▪ Deploying vCenter Server Components</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>▪ vSphere Managed Inventory Objects</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>1.3</td>
<td>Describe storage concepts</td>
<td>2: Storage Infrastructure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.1</td>
<td>Identify and differentiate storage access protocols for VMware vSphere (NFS, iSCSI, SAN, etc.)</td>
<td>2: Storage Infrastructure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.2</td>
<td>Describe storage datastore types for VMware vSphere</td>
<td>2: Storage Infrastructure</td>
<td>11: Managing Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.3</td>
<td>Explain the importance of advanced storage configurations (vStorage APIs for Array Integration (VAAI), vStorage APIs for Storage Awareness (VASA), multipathing, etc.)</td>
<td>2: Storage Infrastructure</td>
<td>11: Managing Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.4</td>
<td>Describe storage policies</td>
<td>2: Storage Infrastructure</td>
<td>11: Managing Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.5</td>
<td>Describe basic storage concepts in VMware vSAN and VMware Virtual Volumes (vVOLs)</td>
<td>2: Storage Infrastructure</td>
<td>2: Storage Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>1.3.6</td>
<td>Identify use cases for raw device mapping (RDM), Persistent Memory (PMem), Non-Volatile Memory Express (NVMe), NVMe over Fabrics (NVMe-oF), and RDMA (iSER).</td>
<td>2: Storage Infrastructure</td>
<td>11: Managing Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Raw Device Mappings (RDMs)</td>
<td>Managing RDMs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vVols</td>
<td>Managing Storage Policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VMware NVMe</td>
<td>Managing VMware NVMe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>#</td>
<td>Managing PMem</td>
</tr>
<tr>
<td>1.3.7</td>
<td>Describe datastore clusters</td>
<td>2: Storage Infrastructure</td>
<td>11: Managing Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Storage DRS (SDRS)</td>
<td>Configuring and Managing SDRS</td>
</tr>
<tr>
<td>1.3.8</td>
<td>Describe Storage I/O Control (SIOC)</td>
<td>2: Storage Infrastructure</td>
<td>11: Managing Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIOC, SIOC, and SDRS</td>
<td>Configuring and Managing SIOC</td>
</tr>
<tr>
<td>1.4</td>
<td>Describe VMware ESXi cluster concepts</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cluster Concepts and Overview</td>
<td>Creating and Configuring a vSphere Cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distributed Resources Scheduler (DRS)</td>
<td>Creating and Configuring a vSphere DRS Cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Availability (HA)</td>
<td>Creating and Configuring a vSphere HA cluster</td>
</tr>
<tr>
<td>1.4.1</td>
<td>Describe VMware Distributed Resource Scheduler (DRS)</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cluster Concepts and Overview</td>
<td>Creating and Configuring a vSphere Cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distributed Resources Scheduler (DRS)</td>
<td>Creating and Configuring a vSphere DRS Cluster</td>
</tr>
<tr>
<td>1.4.2</td>
<td>Describe vSphere Enhanced vMotion Compatibility (EVC)</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enhanced vMotion Compatibility (EVC)</td>
<td>EVC Mode</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>1.4.3</td>
<td>Describe how DRS scores virtual machines</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ How DRS Scores VMs</td>
<td>■ Creating and Configuring a vSphere DRS Cluster</td>
</tr>
<tr>
<td>1.4.4</td>
<td>Describe VMware vSphere High Availability (HA)</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ vSphere High Availability (HA)</td>
<td>■ Creating and Configuring a vSphere HA cluster</td>
</tr>
<tr>
<td>1.4.4.1</td>
<td>Describe Admission Control</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ vSphere HA Admission Control</td>
<td>■ Creating and Configuring a vSphere HA cluster</td>
</tr>
<tr>
<td>1.4.4.2</td>
<td>Describe vSphere Cluster Services (vCLS)</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ vSphere Cluster Services (vCLS)</td>
<td>■ Creating and Configuring a vSphere HA cluster</td>
</tr>
<tr>
<td>1.4.5</td>
<td>Identify use cases for fault tolerance</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Fault Tolerance (FT)</td>
<td>■ Configuring vSphere Fault Tolerance</td>
</tr>
<tr>
<td>1.5</td>
<td>Explain the difference between VMware standard switches and distributed switches</td>
<td>3: Network Infrastructure</td>
<td>9: Configuring and Managing Virtual Networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ vSphere Standard Switch (vSS)</td>
<td>■ Creating and Configuring vSphere Standard Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ vSphere Distributed Switch (vDS)</td>
<td>■ Creating and Configuring vSphere Distributed Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ vDS Settings and Features</td>
<td></td>
</tr>
<tr>
<td>1.5.1</td>
<td>Describe VMkernel networking</td>
<td>3: Network Infrastructure</td>
<td>9: Configuring and Managing Virtual Networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ VMkernel Networking and TCP/IP Stacks</td>
<td>■ Configuring and Managing VMkernel Adapters</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Configuring TCP/IP Stacks</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>1.5.2</td>
<td>Manage networking on multiple hosts with vSphere Distributed Switch (VDS)</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td>3: Network Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5.3</td>
<td>Describe networking policies</td>
<td>3: Network Infrastructure</td>
<td>9: Configuring and Managing Virtual Networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5.4</td>
<td>Manage Network I/O Control (NIOC) on a vSphere Distributed Switch (VDS)</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td>3: Network Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5.5</td>
<td>Describe Network I/O Control (NIOC)</td>
<td>3: Network Infrastructure</td>
<td>9: Configuring and Managing Virtual Networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.6</td>
<td>Describe VMware vSphere Lifecycle Manager concepts</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.7</td>
<td>Describe the basics of VMware vSAN as primary storage</td>
<td>2: Storage Infrastructure</td>
<td>2: Storage Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.7.1</td>
<td>Identify basic vSAN requirements (networking, disk count, and type)</td>
<td>2: Storage Infrastructure</td>
<td>11: Managing Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.7.2</td>
<td>Identify Express Storage Architecture (ESA) concepts for vSAN 8</td>
<td>2: Storage Infrastructure</td>
<td>2: Storage Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>1.8</td>
<td>Describe the role of Virtual Machine Encryption in a data center</td>
<td>7: vSphere Security</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>1.8.1</td>
<td>Describe vSphere Trust Authority</td>
<td>7: vSphere Security</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>1.8.1.1</td>
<td>Describe the vSphere Trust Authority architecture</td>
<td>7: vSphere Security</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>1.8.1.2</td>
<td>Recognize use cases for vSphere Trust Authority</td>
<td>7: vSphere Security</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>1.8.2</td>
<td>Describe the role of a Key Management Services (KMS) server in vSphere</td>
<td>1: vSphere Overview, Components, and Requirements</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>1.9</td>
<td>Recognize methods of securing virtual machines</td>
<td>7: vSphere Security</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>1.9.1</td>
<td>Recognize use cases for a virtual Trusted Platform Module (vTPM)</td>
<td>7: vSphere Security</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>1.9.2</td>
<td>Differentiate between Basic Input or Output System (BIOS) and Unified Extensible Firmware Interface (UEFI) firmware</td>
<td>7: vSphere Security</td>
<td>12: Managing vSphere Security</td>
</tr>
</tbody>
</table>

- [vSphere Security](#)
- [Configuring and Managing vSphere Trust Authority (vTA)](#)
- [Managing vSphere Security](#)
- [Managing ESXi Secure Boot and TPM](#)
- [Configuring UEFI Secure Boot for ESXi Hosts](#)
<table>
<thead>
<tr>
<th>Objective</th>
<th>Description</th>
<th>Chapter/Section</th>
<th>Supporting Chapter/Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Architectures and Technologies</td>
<td>14: Managing Virtual Machines</td>
<td>14: Managing Virtual Machines</td>
</tr>
<tr>
<td>1.9.3</td>
<td>Recognize use cases for Microsoft virtualization-based security (VBS)</td>
<td>14: Managing Virtual Machines</td>
<td>14: Managing Virtual Machines</td>
</tr>
<tr>
<td>1.10</td>
<td>Describe identity federation</td>
<td>8: vSphere Installation</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td>1.10.1</td>
<td>Describe the architecture of identity federation</td>
<td>8: vSphere Installation</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td>1.10.2</td>
<td>Recognize use cases for identity federation</td>
<td>8: vSphere Installation</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td>1.11</td>
<td>Describe VMware vSphere Distributed Services Engine</td>
<td>3: Network Infrastructure</td>
<td>3: Network Infrastructure</td>
</tr>
<tr>
<td>1.11.1</td>
<td>Describe the role of a data processing unit (DPU) in vSphere</td>
<td>1: vSphere Overview, Components and Requirements</td>
<td>1: vSphere Overview, Components and Requirements</td>
</tr>
<tr>
<td>1.12</td>
<td>Identify use cases for VMware Tools</td>
<td>5: vCenter Server Features and Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td>1.13</td>
<td>Describe the high-level components of VMware vSphere with Tanzu</td>
<td>6: VMware Product Integration</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Architectures and Technologies</td>
<td>1.13.1 Identify the use case for a Supervisor Cluster and Supervisor Namespace</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere with Tanzu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere with Tanzu Use Cases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.13.2 Identify the use case for vSphere Zones</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere with Tanzu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.13.3 Identify the use case for a VMware Tanzu Kubernetes Grid (TKG) cluster</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere with Tanzu</td>
</tr>
<tr>
<td>2</td>
<td>VMware Products and Solutions</td>
<td>2.1 Describe the role of VMware vSphere in the Software-Defined Data Center</td>
<td>1: vSphere Overview, Components, and Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VMware SDDC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.2 Identify use cases for VMware vSphere+</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.3 Identify use cases for VMware vCenter Converter</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vCenter Converter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.4 Identify disaster recovery (DR) use cases</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere Replication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Site Recovery Manager (SRM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.4.1 Identify VMware vCenter replication options</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere Replication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.4.2 Identify use cases for VMware Site Recovery Manager (SRM)</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Site Recovery Manager (SRM)</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>3</td>
<td>Planning and Designing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Installing, Configuring, and Setup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Configure single sign-on (SSO)</td>
<td>1: vSphere Overview, Components and Requirements</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Managing SSO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8: vSphere Installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ vCenter Server Topology</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Configuring Single Sign-On (SSO)</td>
<td></td>
</tr>
<tr>
<td>4.1.1</td>
<td>Configure an SSO domain</td>
<td>8: vSphere Installation</td>
<td>1: vSphere Overview, Components, and Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ vCenter Server Topology</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Configuring Single Sign-On (SSO)</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Join an existing SSO domain</td>
<td>8: vSphere Installation</td>
<td>1: vSphere Overview, Components, and Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ vCenter Server Topology</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Configuring Single Sign-On (SSO)</td>
</tr>
<tr>
<td>4.2</td>
<td>Configure vSphere distributed switches</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td></td>
</tr>
<tr>
<td>4.2.1</td>
<td>Create a distributed switch</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ vSphere Distributed Switches (vDS)</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Add ESXi hosts to the distributed switch</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Adding Hosts to a vDS</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Examine the distributed switch configuration</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td>9: Configuring and Managing Virtual Networks</td>
</tr>
<tr>
<td>4.3</td>
<td>Configure Virtual Standard Switch (VSS) advanced virtual networking options</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td>3: Network Infrastructure</td>
</tr>
<tr>
<td>4.4</td>
<td>Set up identity sources</td>
<td>8: vSphere Installation</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Configure identity federation</td>
<td>8: vSphere Installation</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Configure LDAP integration</td>
<td>8: vSphere Installation</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td>4.5</td>
<td>Deploy and configure VMware vCenter Server Appliance (VCSA)</td>
<td>8: vSphere Installation</td>
<td>1: vSphere Overview, Components, and Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13: Managing vSphere and vCenter Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13: Managing vSphere and vCenter Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13: Managing vSphere and vCenter Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13: Managing vSphere and vCenter Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13: Managing vSphere and vCenter Server</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>4.6</td>
<td>Create and configure VMware HA and DRS advanced options (Admission Control, Proactive HA, etc.)</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>4: Clusters and High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Creating and Configuring a vSphere DRS Cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Creating and Configuring a vSphere HA Cluster</td>
</tr>
<tr>
<td>4.7</td>
<td>Deploy and configure VMware vCenter High Availability</td>
<td>8: vSphere Installation</td>
<td>1: vSphere Overview, Components, and Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Implementing VCSA HA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• vCenter Server Topology</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• vCenter High Availability Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4: Clusters and High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• vCenter Server High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13: Managing vSphere and vCenter Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Managing the vCenter HA Cluster</td>
</tr>
<tr>
<td>4.8</td>
<td>Set up content library</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Content Libraries</td>
</tr>
<tr>
<td>4.8.1</td>
<td>Create a content library</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Content Libraries</td>
</tr>
<tr>
<td>4.8.2</td>
<td>Add content to the content library</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Adding Items to a Content Library</td>
</tr>
<tr>
<td>4.8.3</td>
<td>Publish a local content library</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Publishing a Content Library</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Installing, Configuring, and Setup</td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>4.9</td>
<td>Subscribe to content library</td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>4.9.1</td>
<td>Create a subscribed content library</td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>4.9.2</td>
<td>Subscribe to a published content library</td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>4.9.3</td>
<td>Deploy virtual machines (VMs) from a subscribed content library</td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>4.10</td>
<td>Manage virtual machine (VM) template versions</td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>4.10.1</td>
<td>Update template in content library</td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>4.11</td>
<td>Configure VMware vCenter file-based backup</td>
<td>13: Managing vSphere and vCenter Server</td>
<td></td>
</tr>
<tr>
<td>4.12</td>
<td>Configure vSphere Trust Authority</td>
<td>12: Managing vSphere Security</td>
<td>7: vSphere Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere Trust Authority (vTA)</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Installing, Configuring, and Setup</td>
<td>7: vSphere Security</td>
<td>7: vSphere Security</td>
</tr>
<tr>
<td>4.13</td>
<td>Configure vSphere certificates</td>
<td>12: Managing vSphere Security</td>
<td>vSphere Certificates</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuring and Managing vSphere Certificates</td>
</tr>
<tr>
<td>4.13.1</td>
<td>Describe Enterprise PKIs role for SSL certificates</td>
<td>7: vSphere Security</td>
<td>12: Managing vSphere Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere Certificates Overview</td>
</tr>
<tr>
<td>4.14</td>
<td>Configure vSphere Lifecycle Manager</td>
<td>8: vSphere Installation</td>
<td>13: Managing vSphere and vCenter Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implementing VMware vSphere Lifecycle Manager</td>
</tr>
<tr>
<td>4.15</td>
<td>Configure different network stacks</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td>3: Network Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuring TCP/IP Stacks</td>
</tr>
<tr>
<td>4.16</td>
<td>Configure host profiles</td>
<td>8: vSphere Installation</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuring ESXi Using Host Profiles</td>
</tr>
<tr>
<td>4.17</td>
<td>Identify ESXi boot options</td>
<td>8: vSphere Installation</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ESXi Kernel Options</td>
</tr>
<tr>
<td>4.17.1</td>
<td>Configure Quick Boot</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>13: Managing vSphere and vCenter Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ESXi Quick Boot</td>
</tr>
<tr>
<td>4.17.2</td>
<td>Securely Boot ESXi hosts</td>
<td>12: Managing vSphere Security</td>
<td>7: vSphere Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuring UEFI Secure Boot for ESXi Hosts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere Trusted Authority (vTA)</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>4.18</td>
<td>Deploy and configure clusters using the vSphere Cluster Quickstart workflow</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>Creating a Cluster</td>
</tr>
<tr>
<td>4.18.1</td>
<td>Use Cluster Quickstart workflow to add hosts</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>Configuring a Cluster with Quickstart</td>
</tr>
<tr>
<td>4.18.2</td>
<td>Use Cluster Quickstart workflow to configure a cluster</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>Configuring a Cluster with Quickstart</td>
</tr>
<tr>
<td>4.18.3</td>
<td>Use Quickstart to expand clusters</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>Configuring a Cluster with Quickstart</td>
</tr>
<tr>
<td>4.19</td>
<td>Set up and configure VMware ESXi</td>
<td>8: vSphere Installation 12: Managing vSphere Security</td>
<td>Configuring and Managing ESXi Security 10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td>4.19.1</td>
<td>Configure Time Configuration</td>
<td>12: Managing vSphere Security 8: vSphere Installation</td>
<td>Configuring a Cluster with Quickstart 10: Managing and Monitoring Clusters and Resources</td>
</tr>
</tbody>
</table>

- Installing ESXi Hosts
- Initial vSphere Configuration
- ESXi Configuration Settings
<table>
<thead>
<tr>
<th>Objective</th>
<th>Description</th>
<th>Chapter/Section</th>
<th>Supporting Chapter/Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.19.2</td>
<td>Configure ESXi services</td>
<td>12: Managing vSphere Security</td>
<td>Customizing ESXi Services</td>
</tr>
<tr>
<td>4.19.2.1</td>
<td>Configure ESXi Shell</td>
<td>12: Managing vSphere Security</td>
<td>SSH and ESXi Shell Security</td>
</tr>
<tr>
<td>4.19.2.2</td>
<td>Configure SSH</td>
<td>12: Managing vSphere Security</td>
<td>SSH and ESXi Shell Security</td>
</tr>
<tr>
<td>4.19.3</td>
<td>Configure Product Locker</td>
<td>8: vSphere Installation</td>
<td>Configuring ESXi Using Host Profiles</td>
</tr>
<tr>
<td>4.19.4</td>
<td>Configure Lockdown Mode</td>
<td>12: Managing vSphere Security</td>
<td>Using Lockdown Mode</td>
</tr>
<tr>
<td>4.19.5</td>
<td>Configure ESXi firewall</td>
<td>12: Managing vSphere Security</td>
<td>Configuring the ESXi Firewall</td>
</tr>
<tr>
<td>4.20</td>
<td>Configure VMware vSphere with Tanzu</td>
<td>6: VMware Product Integration</td>
<td>vSphere with Tanzu Integration</td>
</tr>
<tr>
<td>4.20.1</td>
<td>Configure a Supervisor Cluster &amp; Supervisor Namespace</td>
<td>6: VMware Product Integration</td>
<td>vSphere with Tanzu</td>
</tr>
<tr>
<td>4.20.2</td>
<td>Configure a Tanzu Kubernetes Grid Cluster</td>
<td>6: VMware Product Integration</td>
<td>vSphere with Tanzu</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Installing, Configuring, and Setup</td>
<td>6: VMware Product Integration</td>
<td>vSphere with Tanzu</td>
</tr>
<tr>
<td>4.20.3</td>
<td>Configure vSphere Zones</td>
<td>6: VMware Product Integration</td>
<td>vSphere with Tanzu</td>
</tr>
<tr>
<td>4.20.4</td>
<td>Configure Namespace permissions</td>
<td>6: VMware Product Integration</td>
<td>vSphere with Tanzu</td>
</tr>
<tr>
<td>5</td>
<td>Performance-tuning, Optimization, Upgrades</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td>5.1</td>
<td>Identify resource pools use cases</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Explain shares, limits, and reservations (resource management)</td>
<td>4: Clusters and High Availability</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
</tr>
<tr>
<td>5.2</td>
<td>Monitor resources of a VMware vCenter Server Appliance (VCSA) and vSphere 8.x environment</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>4: Clusters and High Availability</td>
</tr>
<tr>
<td>5.3</td>
<td>Identify and use resource monitoring tools</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>4: Clusters and High Availability</td>
</tr>
<tr>
<td>5.4</td>
<td>Configure Network I/O Control (NIOC)</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td>3: Network Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network I/O Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuring Network I/O Control (NIOC)</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>5.5</td>
<td>Configure Storage I/O Control (SIOC)</td>
<td>11: Managing Storage</td>
<td>2: Storage Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Configuring and Managing SIOC</td>
<td>- NIOC, SIOC, and SDRS</td>
</tr>
<tr>
<td>5.6</td>
<td>Configure a virtual machine port group to be offloaded to a data processing unit (DPU)</td>
<td>9: Configuring and Managing Virtual Networks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- vSphere Distributed Switches (vDS)</td>
<td></td>
</tr>
<tr>
<td>5.7</td>
<td>Explain the performance impact of maintaining virtual machine snapshots</td>
<td>5: vCenter Server Features and Virtual Machines</td>
<td>14: Managing Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Virtual Machine Snapshots</td>
<td>- Creating and Managing Virtual Machine Snapshots</td>
</tr>
<tr>
<td>5.8</td>
<td>Use Update Planner to identify opportunities to update VMware vCenter</td>
<td>13: Managing vSphere and vCenter Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Using Update Planner</td>
<td></td>
</tr>
<tr>
<td>5.9</td>
<td>Use vSphere Lifecycle Manager to determine the need for upgrades and updates</td>
<td>13: Managing vSphere and vCenter Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Using Lifecycle Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Upgrading to vSphere 7.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Using Update Planner</td>
<td></td>
</tr>
<tr>
<td>5.9.1</td>
<td>Update virtual machines</td>
<td>4: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Installing and Upgrading VMware Tools</td>
<td></td>
</tr>
<tr>
<td>5.9.2</td>
<td>Update VMware ESXi</td>
<td>13: Managing vSphere and vCenter Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Using vSphere Lifecycle Manager</td>
<td></td>
</tr>
<tr>
<td>5.10</td>
<td>Use performance charts to monitor performance</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Monitoring and Managing vSphere Resources</td>
<td></td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>5</td>
<td>Performance-tuning, Optimization, Upgrades</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>6: VMware Product Integration</td>
</tr>
<tr>
<td>5.11</td>
<td>Perform proactive management with VMware Skyline</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>VMware Skyline</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Monitoring and Managing Host Resources and Health</td>
</tr>
<tr>
<td>5.12</td>
<td>Use VMware vCenter management interface to update VMware vCenter</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>Patching with VAMI</td>
</tr>
<tr>
<td>5.13</td>
<td>Complete lifecycle activities for VMware vSphere with Tanzu</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>Using vSphere Lifecycle Manager</td>
</tr>
<tr>
<td>5.13.1</td>
<td>Update Supervisor cluster</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>Using vSphere Lifecycle Manager</td>
</tr>
<tr>
<td>5.13.2</td>
<td>Back up and restore VMware vSphere with Tanzu</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>vCenter Server</td>
</tr>
<tr>
<td>6</td>
<td>Troubleshooting and Repairing</td>
<td>4: Clusters and High Availability</td>
<td>vSphere Cluster Services (vCLS)</td>
</tr>
<tr>
<td>6.1</td>
<td>Identify use cases for enabling vSphere Cluster Services (vCLS) retreat mode</td>
<td>4: Clusters and High Availability</td>
<td>vSphere Cluster Services (vCLS)</td>
</tr>
<tr>
<td>6.2</td>
<td>Differentiate between the main management services in VMware ESXi and vCenter and their corresponding log files</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>ESXi Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vCenter Server Logs</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>6 Troubleshooting andRepairing</td>
<td>Generate a log bundle</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ ESXi Logs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ vCenter Server Logs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Uploading System Logs to VMware</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>13: Managing vSphere and vCenter Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Monitoring and Managing vCenter Server with the VAMI</td>
<td></td>
</tr>
<tr>
<td>7 Administrative and Operational Tasks</td>
<td>Create and manage virtual machine snapshots</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Creating and Managing Virtual Machine Snapshots</td>
<td>■ Virtual Machine Snapshots</td>
</tr>
<tr>
<td></td>
<td>Create virtual machines using different methods (Open Virtualization Format (OVF) templates, content library, etc.)</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Managing VMs by Using PowerCLI</td>
<td>■ Virtual Machine Cloning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Deploying OVF/OVA Templates</td>
<td>14: Managing Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Deploying VMs by Using a Content Library</td>
<td>■ Managing OVF Templates</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Content Libraries</td>
</tr>
<tr>
<td></td>
<td>Manage virtual machines (modifying virtual machine settings, VMware per-VM EVC, latency sensitivity, CPU affinity, etc.)</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Managing EVC Mode and CPU Affinity</td>
<td>■ Virtual Machine Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Latency Sensitivity</td>
<td></td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Administrative and Operational Tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.4</td>
<td>Manage storage</td>
<td>11: Managing Storage</td>
<td>2: Storage Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managing Datastores</td>
<td>Datastore Types</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managing Storage Policies</td>
<td>Storage Policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managing Multipathing</td>
<td>Storage Multipathing and Failover</td>
</tr>
<tr>
<td>7.4.1</td>
<td>Configure and modify datastores</td>
<td>11: Managing Storage</td>
<td>2: Storage Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managing Datastores</td>
<td>Datastore Types</td>
</tr>
<tr>
<td>7.4.2</td>
<td>Create virtual machine storage policies</td>
<td>11: Managing Storage</td>
<td>2: Storage Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managing Storage Policies</td>
<td>Storage Policies</td>
</tr>
<tr>
<td>7.4.3</td>
<td>Configure storage cluster options</td>
<td>11: Managing Storage</td>
<td>2: Storage Infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuring and Managing Storage DRS</td>
<td>SDRS</td>
</tr>
<tr>
<td>7.5</td>
<td>Create DRS affinity and anti-affinity rules for common use cases</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td>4: Clusters and High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creating Affinity/Anti-Affinity Rules</td>
<td>DRS Rules</td>
</tr>
<tr>
<td>7.6</td>
<td>Migrate virtual machines</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Migrating Virtual Machines</td>
<td>Virtual Machine Migration</td>
</tr>
<tr>
<td>7.6.1</td>
<td>Identify requirements for Storage vMotion, Cold Migration, vMotion, and Cross vCenter Export</td>
<td>14: Managing Virtual Machines</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Migrating Virtual Machines</td>
<td>Virtual Machine Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vMotion Details</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Storage vMotion Details</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Administrative and Operational Tasks</td>
<td>12: Managing vSphere Security</td>
<td>7: vSphere Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere Permissions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8: vSphere Installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Applying Permissions to ESXi Hosts Using Host Profiles</td>
</tr>
<tr>
<td>7.7</td>
<td>Configure role-based access control</td>
<td>12: Managing vSphere Security</td>
<td>7: vSphere Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vSphere Permissions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8: vSphere Installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Applying Permissions to ESXi Hosts Using Host Profiles</td>
</tr>
<tr>
<td>7.8</td>
<td>Manage host profiles</td>
<td>8: vSphere Installation</td>
<td>5: vCenter Server Features and Virtual Machines</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuring ESXi by Using Host Profiles</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host Profiles</td>
</tr>
<tr>
<td>7.9</td>
<td>Utilize VMware vSphere Lifecycle Manager</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implementing VMware vSphere Lifecycle Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Installing and Upgrading VMware Tools</td>
</tr>
<tr>
<td>7.9.1</td>
<td>Describe firmware upgrades for VMware ESXi</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implementing VMware vSphere Lifecycle Manager</td>
</tr>
<tr>
<td>7.9.2</td>
<td>Describe ESXi updates</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implementing VMware vSphere Lifecycle Manager</td>
</tr>
<tr>
<td>7.9.3</td>
<td>Describe component and driver updates for ESXi</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implementing VMware vSphere Lifecycle Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implementing VMware vSphere Lifecycle Manager Implementation</td>
</tr>
<tr>
<td>7.9.4</td>
<td>Describe hardware compatibility check</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implementing VMware vSphere Lifecycle Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5: vCenter Server Features and Virtual Machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VM Hardware/Compatibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14: Managing Virtual Machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuring Virtual Machine Hardware</td>
</tr>
<tr>
<td>Objective</td>
<td>Description</td>
<td>Chapter/Section</td>
<td>Supporting Chapter/Section</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>7.9.5</td>
<td>Describe ESXi cluster image export functionality</td>
<td>13: Managing vSphere and vCenter Server</td>
<td>8: vSphere Installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implementing VMware vSphere Lifecycle Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4: Clusters and High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cluster Concepts and Overview</td>
</tr>
<tr>
<td>7.9.6</td>
<td>Create ESXi cluster image</td>
<td>13: Managing vSphere and vCenter Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Using vSphere Lifecycle Manager</td>
</tr>
<tr>
<td>7.10</td>
<td>Use predefined alarms in VMware vCenter</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Alarms</td>
</tr>
<tr>
<td>7.11</td>
<td>Create custom alarms</td>
<td>10: Managing and Monitoring Clusters and Resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Advanced Use Cases for Alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Creating Alarm Definitions</td>
</tr>
<tr>
<td>7.12</td>
<td>Deploy an encrypted virtual machine</td>
<td>12: Managing vSphere Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Encrypting a Virtual Machine</td>
</tr>
<tr>
<td>7.12.1</td>
<td>Convert a non-encrypted virtual machine to an encrypted virtual machine</td>
<td>12: Managing vSphere Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Encrypting a Virtual Machine</td>
</tr>
<tr>
<td>7.12.2</td>
<td>Migrate an encrypted virtual machine</td>
<td>7: vSphere Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Encrypted vSphere vMotion</td>
</tr>
<tr>
<td>7.12.3</td>
<td>Configure virtual machine vMotion encryption properties</td>
<td>7: vSphere Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Encrypted vSphere vMotion</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Concepts and Overview</td>
<td>1</td>
</tr>
<tr>
<td>Distributed Resource Scheduler (DRS)</td>
<td>2–4</td>
</tr>
<tr>
<td>vSphere High Availability (HA)</td>
<td>5–7</td>
</tr>
<tr>
<td>Other Resource Management and Availability Features</td>
<td>8–10</td>
</tr>
</tbody>
</table>

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.
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

<table>
<thead>
<tr>
<th>Level</th>
<th>EVC Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L0</td>
<td>Intel Merom</td>
<td>Smallest Intel feature set for EVC mode.</td>
</tr>
<tr>
<td>L1</td>
<td>Intel Penryn</td>
<td>Includes the Intel Merom feature set and exposes additional CPU features,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>including SSE4.1.</td>
</tr>
<tr>
<td>L2</td>
<td>Intel Nehalem</td>
<td>Includes the Intel Penryn feature set and exposes additional CPU features,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>including SSE4.2 and POPCOUNT.</td>
</tr>
<tr>
<td>L3</td>
<td>Intel Westmere</td>
<td>Includes the Intel Nehalem feature set and exposes additional CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features, including AES and PCLMULQDQ.</td>
</tr>
<tr>
<td>L4</td>
<td>Intel Sandy Bridge</td>
<td>Includes the Intel Westmere feature set and exposes additional CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features, including AVX and XSAVE.</td>
</tr>
<tr>
<td>L5</td>
<td>Intel Ivy Bridge</td>
<td>Includes the Intel Sandy Bridge feature set and exposes additional CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features, including RDRAND, ENFSTRG, FSGSBASE, SMEP, and F16C.</td>
</tr>
<tr>
<td>L6</td>
<td>Intel Haswell</td>
<td>Includes the Intel Ivy Bridge feature set and exposes additional CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features, including ABMX2, AVX2, MOVBE, FMA, PERMD, RORX/MULX, INVPCID,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and VMFUNC.</td>
</tr>
<tr>
<td>L7</td>
<td>Intel Broadwell</td>
<td>Includes the Intel Haswell feature set and exposes additional CPU features,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>including Transactional Synchronization Extensions, Supervisor Mode Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prevention, Multi-Precision Add-Carry Instruction Extensions, PREFETCHW,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and RDSEED.</td>
</tr>
<tr>
<td>L8</td>
<td>Intel Skylake</td>
<td>Includes the Intel Broadwell feature set and exposes additional CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features, including Advanced Vector Extensions 512, Persistent Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Support Instructions, Protection Key Rights, Save Processor Extended States</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with Compaction, and Save Processor Extended States Supervisor.</td>
</tr>
<tr>
<td>L9</td>
<td>Intel Cascade Lake</td>
<td>Includes the Intel Skylake feature set and exposes additional CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features, including VNNI and XGETBV with ECX = 1.</td>
</tr>
<tr>
<td>L10</td>
<td>Intel Ice Lake</td>
<td>Includes the Intel Cascade Lake feature set and exposes additional CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features, including HA extensions, Vectorized AES, User Mode Instruction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prevention, Read Processor ID, Fast Short REP MOV, WBNMOINVD, Galois Field</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New Instructions, and AVX512 Integer Fused Multiply Add, Vectorized Bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manipulation, and Bit Algorithms Instructions.</td>
</tr>
<tr>
<td>L11</td>
<td>Intel Sapphire Rapids</td>
<td>Includes the Intel Ice Lake feature set and exposes additional CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features, including Control-Flow Enforcement Technology, Advanced Matrix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extensions, Supervisor Protection Keys, AVX-VNNI, AVX512 FP16, AVX512 BF16,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLDEMOTE, SERIALIZE, WBNMOINVD, and MOVDIRI instructions.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Level</th>
<th>EVC Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>AMD Opteron Generation 1</td>
<td>Smallest AMD feature set for EVC mode.</td>
</tr>
<tr>
<td>A1</td>
<td>AMD Opteron Generation 2</td>
<td>Includes the AMD Generation 1 feature set and exposes additional CPU features, including CPMXCHG16B and RDTSCP.</td>
</tr>
<tr>
<td>A3</td>
<td>AMD Opteron Generation 3</td>
<td>Includes the AMD Generation 2 feature set and exposes additional CPU features, including SSE4A, MisAlignSSE, POPCOUNT, and ABM (LZCNT).</td>
</tr>
<tr>
<td>A2, B0</td>
<td>AMD Opteron Generation 3 (without 3DNow!)</td>
<td>Includes the AMD Generation 3 feature set without 3DNow support.</td>
</tr>
<tr>
<td>B1</td>
<td>AMD Opteron Generation 4</td>
<td>Includes the AMD Generation 3 no3DNow feature set and exposes additional CPU features, including SSSE3, SSE4.1, AES, AVX, XSAVE, XOP, and FMA4.</td>
</tr>
<tr>
<td>B2</td>
<td>AMD Opteron Piledriver</td>
<td>Includes the AMD Generation 4 feature set and exposes additional CPU features, including FMA, TBM, BMI1, and F16C.</td>
</tr>
<tr>
<td>B3</td>
<td>AMD Opteron Steamroller</td>
<td>Includes the AMD Piledriver feature set and exposes additional CPU features, including XSAVEOPT RDFSBASE, RDGSBASE, WRFSBASE, WRGSBAS, and FSGBASE.</td>
</tr>
<tr>
<td>B4</td>
<td>AMD Zen</td>
<td>Includes the AMD Steamroller feature set and exposes additional CPU features, including RDRAND, SMEM, AVX2, BM2, MOVBE, ADX, RDSEED, SMAP, CLFLUSHOPT, XSAVES, XSAVEC, SHA, and CLZERO.</td>
</tr>
<tr>
<td>B5</td>
<td>AMD Zen 2</td>
<td>Includes the AMD Zen feature set and exposes additional CPU features, including CLWB, UMIIP, RDPID, XGETBV with ECX = 1, WBN0INVTD, and GMET.</td>
</tr>
<tr>
<td>B6</td>
<td>AMD Zen 3</td>
<td>Includes the AMD Zen 2 feature set and exposes additional CPU features, including always serializing LFENCE, INVPID, PSFD, SSBD, PCID, PKU, VAES, VPCLMULQDQ, and shadow stacks.</td>
</tr>
<tr>
<td>B7</td>
<td>AMD Zen 4</td>
<td>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, AVX512VBM12, AVX512VL, AVX512VNNI, AVX512VPOPCNTDQ, GFNI, IBRS, and Upper Address Ignore.</td>
</tr>
</tbody>
</table>
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**

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

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:

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shares</td>
<td>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%.</td>
</tr>
<tr>
<td>Reservations</td>
<td>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.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Setting</th>
<th>CPU Share Value</th>
<th>Memory Share Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>2000 per vCPU</td>
<td>20 per MB</td>
</tr>
<tr>
<td>Normal</td>
<td>1000 per vCPU</td>
<td>10 per MB</td>
</tr>
<tr>
<td>Low</td>
<td>500 per vCPU</td>
<td>5 per MB</td>
</tr>
</tbody>
</table>

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

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.
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](image-url)
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Failure Response &gt; Failure Response</td>
<td>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.</td>
</tr>
<tr>
<td>Host Failure Response &gt; Default VM Restart Priority</td>
<td>You can indicate the order in which virtual machines are restarted when the host fails (higher-priority machines first).</td>
</tr>
<tr>
<td>Host Failure Response &gt; VM Restart Priority Condition</td>
<td>The restart priority condition must be met before HA restarts the next priority group.</td>
</tr>
<tr>
<td>Response for Host Isolation</td>
<td>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.</td>
</tr>
<tr>
<td>VM Monitoring</td>
<td>You can indicate the sensitivity (Low, High, or Custom) with which vSphere HA responds to lost VMware Tools heartbeats.</td>
</tr>
<tr>
<td>Application Monitoring</td>
<td>You can indicate the sensitivity (Low, High, or Custom) with which vSphere HA responds to lost application heartbeats.</td>
</tr>
</tbody>
</table>

**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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>das.isolationaddressX</td>
<td>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.isolationaddressX, where X is a number between 0 and 9.</td>
</tr>
<tr>
<td>das.usedefaultisolationaddress</td>
<td>Specifies whether to use the default gateway IP address for isolation tests.</td>
</tr>
<tr>
<td>das.isolationshutdowntimeout</td>
<td>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.</td>
</tr>
<tr>
<td>das.slotmeminmb</td>
<td>Defines the maximum bound on the memory slot size.</td>
</tr>
<tr>
<td>das.slotcpuminhz</td>
<td>Defines the maximum bound on the CPU slot size.</td>
</tr>
<tr>
<td>das.vmmemoryminmb</td>
<td>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.</td>
</tr>
<tr>
<td>das.vmcpuminhz</td>
<td>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.</td>
</tr>
<tr>
<td>das.heartbeatsperhost</td>
<td>Specifies the number of heartbeat datastores required per host. The default is 2. The acceptable values are 2 to 5.</td>
</tr>
<tr>
<td>das.config.fdm.</td>
<td>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.</td>
</tr>
<tr>
<td>isolationPolicyDelaySec</td>
<td></td>
</tr>
<tr>
<td>das.respectvmmantiaffinityrules</td>
<td>Determines whether vSphere HA should enforce VM–VM anti-affinity rules even when DRS is not enabled.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Setting</th>
<th>Failure Interval</th>
<th>Reset Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>30 seconds</td>
<td>1 hour</td>
</tr>
<tr>
<td>Medium</td>
<td>60 seconds</td>
<td>24 hours</td>
</tr>
<tr>
<td>Low</td>
<td>120 seconds</td>
<td>7 days</td>
</tr>
</tbody>
</table>
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 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 Lifecycle 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 Lifecycle 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.

Table 4-11 Key Topics for Chapter 4

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

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

Numbers
802.1ax, 95
802.1q, 97, 99, 106
802.3ad, 95, 101, 108

A
absent component state, vSAN, 51
acceptance levels
  ESXi hosts, 497–498
  VIB (vSphere Installation Bundle),
    497–498
account lockout, ESXi, 487–489
accounts
  Pearson Vue, 614
  VMware Certification, 614
actions, alarm, 404
Active Directory (AD), 21, 258
  ESXi host management with, 499–500
  identity sources, 311–313
Active Directory Federation Services (AD
FS), 246
Active node, vCenter HA clusters, 12–13
AD, See Active Directory (AD)
adapters
  host physical network
    managing on vDS, 355–356
    migration to vDS, 356
  VMkernel, 342–343
Add-DelayRule, 299
add-ons
  Dell, 543
  HPE, 543
  overview of, 208, 540
vCenter Converter, 214–215
VMware Skyline, 215–216
vSphere Replication, 215
vSphere requirements, 7, 23–24
vSphere with Tanzu, 208–213, 521–523
vSphere+ 213–214
Address Resolution Protocol (ARP), 336
addresses
  IP (Internet Protocol), 94, 553
  MAC (media access control), 94,
    102–103
Administration server, 10
Administrator privileges, 249, 265, 498
Administrators group, 315
admission control
  virtual machine resources, 394
  vSphere HA, 151–152, 375
Advisor (Skyline), 215
affinity/anti-affinity rules
  Predictive DRS, 156, 374
  vSphere DRS clusters, 373–374
Agent, vCenter Server, 11
AI (artificial intelligence), 601
alarms, 402–405
  actions, 404
  creating, 403–404
  elements of, 402
  use cases, 404–405
  viewing/acknowledging, 403
all paths down (APD), 154
Amazon Web Services, VMC (VMware
Cloud) on, 27, 231
AMD
  AMD-V Extended Migration, 136
EVC (Enhanced vMotion Compatibility) modes for, 138–139
anti-affinity rules, 85
Predictive DRS, 156, 374
vSphere DRS clusters, 373–374
anything as a service (XaaS), 219
APD (all paths down), 154
App Volumes, 223
Appliance, vCenter Server compatibility, 524
migrating vCenter Server for Windows to, 528–530
patching vCenter Server with, 563–564
storage sizes, 16–17
upgrading, 525–527
Appliance Management Interface, vCenter Server, 225
monitoring/managing vCenter Server with, 550–554
patching vCenter Server with, 561–563
vCenter Server backup with, 518–521
application monitoring, in vSphere HA clusters, 376
Application Path Resiliency service, 230
application virtualization
App Volumes, 223
VMware Horizon, 222–223
Apply-ESXiImageProfile, 300
Aria Suite, 7
Aria Automation, 27, 218–219
Aria for Logs, 217–218
Aria Operations, 27, 216–217, 279–280
Aria Operations for Networks, 220–221
Aria Orchestrator, 219–220
ARP (Address Resolution Protocol), 336
array-based failover with iSCSI, 76
artificial intelligence (AI), 601
ATS (Atomic Test and Set), 71
ATS Only Flag primitive, 71
Attested, 258
authentication and authorization, 474–479
content libraries, 605
permissions, 245–246
applying to ESXi hosts, 323
authentication and authorization, 245–246
best practices, 251–252
content libraries, 606–607
editing, 478–479
ESXi hosts, 323
global, 250–251, 478
inventory hierarchy and objects, 246–248
management, 504
permission validation settings, 504
permissions diagram, 250
privileges and roles, 248–250, 477, 498–499
required permissions for common tasks, 252–254
setting, 477–478
validation settings, 504
vCenter Server application of, 255–257
privileges
configuration, 477
ESXi hosts, 498–499
management, 477, 498–499
types of, 248–250
vCenter Server, 265
privileges and roles
best practices, 251–252
creating, 477
required permissions for common tasks, 252–254
types of, 248–250
vCenter Server application of, 255–257
smart card, 501
SSO (single sign-on). See SSO (single sign-on)
users and groups, 476–477
VMware Enhanced Authentication Plug-in, 307
dvSphere Authentication Proxy, 260, 500
Authentication Proxy, 500
authorization. See authentication and authorization
Auto Deploy
  cmdlets, 299–300
  compatibility, 524
  ESXi host installation with, 296–301
  security considerations, 493
Automated Lifecycle Management (LCM), 228
automation
  Aria Automation, 218–219
  Aria Orchestrator, 219–220
  cloud computing, 27
  DRS (Distributed Resource Scheduler), 139
  SDRS (Storage DRS), 84
Average Bandwidth option, traffic shaping policy, 103
AWS (Amazon Web Services), VMC (VMware Cloud) on, 27, 231
Azure VMware Solution, 231
B
backup and recovery
  snapshots, 182
  vCenter Server, 23, 518–521
  vCenter Server file-based backup and restore, 23
  vLCM (vSphere Lifecycle Manager), 544–545
  vSphere with Tanzu, 208–213, 521–523
bar charts, 379
base image, ESXi, 540
baselines, 536–542
block primitives, 71
blueprints, Cloud Assembly, 218
boot
  ESXi Quick Boot, 542
  ESXi scripted installation, 294
  ESXi Secure Boot, 261–262
  UEFI Secure Boot, 501–502
  VMs (virtual machines), 189
  vSAN and, 68
  boot.cfg file, 293
brute-force attacks, 100
built-in storage providers, 69
Bulk Migration service, VMware Hybrid Cloud Extension, 229
Burst Size option, traffic shaping policy, 104
C
CAAdmins group, 314
caching
  stateless, 296
cvSAN requirements, 65
capacity reservation, vSphere HA, 423
CAs (certificate authorities)
  overview of, 240
  VMCA (VMware Certificate Authority), 240–241, 298, 307–309
  CAT I-CAT III (DISA), 484
  CBT (Change Block Tracking), 225
  CDP (Cisco Discovery Protocol), 121
  CD-ROM drives, 186
  CEIP (Customer Improvement Program), 530
certificate authorities. See CAs (certificate authorities)
Certificate Manager, 479, 480–481
certificate signing requests (CSRs), 309
certificates
  core identity services, 241
  CSR (certificate signing request), 309
  ESXi host, 245
  overview of, 240–241
  recommended modes for, 241
  requirements for, 242–245
  solution user certificate stores, 244
types of, 243–244
  vCenter Server, 265
Change Block Tracking (CBT), 225
change rollbacks, 182
chipsets, 186
Chrome, VMware support for, 23
CIM (Common Information Model) access, 493–494
CIM Server, 259
Cisco Discovery Protocol (CDP), 121
Citrix Virtual Apps and Desktops, VMware App Volumes integration, 223
claim rules, 462
citizen, vSphere. See vSphere Client
client performance charts
advanced performance charts, 381–383
definition of, 377
types of, 379
views, 379–380
cloning VMs (virtual machines), 199–201
cold clones, 199
hot clones, 199
instant clones, 200–201
linked clones, 182, 200
privileges required for, 580–581
Cloud Assembly, 27, 218
Cloud Builder, 228
cloud computing
Aria Automation, 218–219
automation, 27
Azure VMware Solution, 231
Cloud Assembly, 27, 218
Cloud Builder, 228
CNS (Cloud Native Storage), 53
HCX (Hybrid Cloud Extension), 229–231
hybrid cloud, 27
VMC (VMware Cloud), 27, 226–227, 231
vSphere+, 213–214
Cloud Native Storage (CNS), 53
clusters
cluster images, importing/exporting, 544–545
configuring with Quickstart, 369–371
creating, 368
datastore, 85, 135
definition of, 172–173
DPM (Distributed Power Management), 156–157
DRS (Distributed Resource Scheduler)
automation modes, 139
evacuation workflow, 141
memory metric for load balancing, 140
migration sensitivity, 143–144
network-aware DRS, 140
NVM (non-volatile memory) support, 141
Predictive DRS, 156
recent enhancements, 139–142
resource pools, 144–148
rules, 142–143
virtual machine distribution, 140
virtual machine initial placement, 140–141
virtual machine scores, 142
EVC (Enhanced vMotion Compatibility)
configuration, 136–139
overview of, 135–136, 372
requirements for, 136
Kubernetes, vSphere with Tanzu and,
208–211
moving hosts into, 254
overview of, 134
resource monitoring and management, 388–389
vCenter HA, 12–13, 161, 564–565
vCLS (vSphere Cluster Services), 135
vSAN
creating with Quickstart, 419
encryption in, 61, 434–437
expanding, 424–426
extending across two sites, 428–430
managing devices in, 430–432
requirements for, 67
space efficiency in, 58–60, 433
standard, 53
stretched, 55–58
two-host, 54
vSphere DRS, 372–374
vSphere HA, 148–155
admission control, 151–152
advanced options, 153
benefits of, 148–149
best practices, 155
creating and configuring, 374–378
heartbeats, 151
configuration

Proactive HA, 155
Proactive HA (High Availability), 7, 155, 376
requirements for, 149–150
response to failures, 150
virtual machine settings, 153–154
VM monitoring settings, 154–155
VMCP (Virtual Machine Component Protection), 154

CNS (Cloud Native Storage), 53
Code Stream (Aria Automation), 218
cold clones, 199
Collector (Skyline), 215
Common Information Model (CIM) access, 493–494
community secondary PVLANs, 113
Community-Supported VIBs, 498
compatibility
  EVC (Enhanced vMotion Compatibility), 135–139
    configuration, 136–139
    overview of, 135–136
    requirements for, 136
    hardware compatibility checks, 544
    vCenter Server 7.0, 524
    VMs (virtual machines), 586
compliance
  Aria Operations, 279–280
  VMs (virtual machines), 51
Compliant clusters, 541
component state, vSAN, 51
components, vSphere, 6–8
compression, vSAN, 58, 59
compute and system requirements, 14–16
configuration. See also installation;
  management; VMware product integration
authentication and authorization, 474–479
permissions, 477–479
privileges and roles, 477

SSO (single sign-on). See SSO (single sign-on)
users and groups, 476–477
certificates, 479–483
custom, 480–481
ESXi, 481–483
vSphere Client, 479–480
clusters, 134
  cluster creation, 368
  EVC mode, 372
  Quickstart, 369–371
  vSphere DRS, 372–374
  vSphere HA, 374–378
content libraries, 603
  adding items to, 608
  authentication, 605
  creating, 604–605
  definition of, 604
  deploying VMs with, 608–609
  managing VM templates in, 609
  overview of, 176–178
  permissions, 606–607
  publishing, 605
  subscribing to, 606
  synchronization options, 607
  versioning, 177

ESXi hosts
  configuration scripts, 485–487
  profiles, 484–485

ESXi security, 493–494
  Active Directory, 499–500
  ESXi firewall, 494–495
  ESXi services, 495–496
  general security recommendations, 483–492
  host acceptance levels, 497–498
  Lockdown Mode, 496–497
  log files, 503
  networking security recommendations, 492–494
  privileges, 498–499
  smart card authentication, 501
TPM (Trusted Platform Module), 502–503
UEFI Secure Boot, 501–502
VIB acceptance levels, 497–498
vSphere Authentication Proxy, 500
EVC (Enhanced vMotion Compatibility)
EVC modes for AMD hosts, 138–139
EVC modes for Intel hosts, 136–137
EVC modes for VMs (virtual machines), 603
EVC modes for vSphere clusters, 372
Identity Federation, 316–318
LACP (Link Aggregation Control Protocol), 118–119
NetFlow on vDS (vSphere Distributed Switches), 340–341
SSO (single sign-on)
Active Directory identity sources, 311–313
LDAP identity sources, 313
overview of, 309–310
policies, 315–316
SSO identity sources, 310
users, enabling/disabling, 314–315
storage infrastructure
NFS datastores, 447–449
RDMs (raw device mappings), 446–447
VMFS datastores, 441–449
vSAN, 418–440
vVols (virtual volumes), 466–468
syslog, 409–410
vCenter Server
common management tasks, 555–557
repointing to another domain, 565–569
SSL certificate verification for legacy hosts, 561
statistics collection settings, 558–560
updates, 561–564
vCenter HA clusters, 564–565
VMCA (VMware Certificate Authority), 307–309
virtual network infrastructure
DirectPath I/O, 122, 347
distributed port groups, 341–342, 357
network resource pools, 109–111, 345–346
NIOC (Network I/O Control), 108–109, 344–345
PVLANs (private VLANs), 346
SR-IOV (single root I/O virtualization), 347–349
standard port groups, 341–342
vDS (vSphere Distributed Switches), 338–342
VMkernel networking, 342–344
vSS (vSphere Standard Switches), 334–338
VMs (virtual machines)
advanced options, 189
cloning, 199–201, 580–581
compatibility options, 185–187, 586
configuration files, 179
content libraries, 176–178, 604–609
converting to templates, 581
CPU affinity, 603
creating, 252, 576–577
deploying from templates, 253, 582
disk mode settings, 590
encrypting, 589
EVC mode, 603
guest OS, 253, 582
guest user mapping, 594
hardware devices, 185–187
migration, 190–194, 254, 596–598
moving to resource pools, 253
Open VM Tools, 578
opening consoles to, 577–578
options, 188–189, 592–593
OVF/OVA templates, 178, 585, 594, 598, 608
performance impact of, 396
powering on, 577
provisioning, 188, 200, 589
shutting down guests, 580
snapshots, 180–185, 253, 595
VBS (virtualization-based security), 598–599
versions, 587–588
vGPU (virtual GPU) support, 601–603
VM hardware configuration, 586–592
VMware PowerCLI, 599–601
VMware Tools, 153, 188, 189, 221, 272, 324, 395, 524, 578–580
vSAN, 86
   cluster creation, 419
custom TCP/IP stack, 125
custom certificates, 480–481
customization. See configuration; management
D
das.config.fdm.isolationPolicyDelaySec, 153
das.heartbeatdsperhost, 153
das.isolationaddressX, 153, 155

config.vpxd.filter.vmfsFilter, 446
Config-vVol, 74
Connect-VIServer, 487, 600
consumed capacity, 50
content libraries, 603
description of, 7
disk/device management, 430–432
downloading, 445
encryption, 434–437
default policy, 428
File Service, 439–440
discarding space, 433
disabling, 423
driver freeze, 419
encryption, 434–437
event service, 419
File Service, 439–440
controller
   NVDIMM, 187
   NVMe, 187
   SATA, 187
   SCSI, 187, 591
   SIO, 187
   USB, 187
Converter Standalone, 214–215
Coordinated Universal Time (UTC), 24
custom certificates, 480–481
custom TCP/IP stack, 125
Customer Improvement Program (CEIP), 530
customization. See configuration; management
D
das.config.fdm.isolationPolicyDelaySec, 153
das.heartbeatdsperhost, 153
das.isolationaddressX, 153, 155
default TCP/IP stack, 125, 194–197
Defense Information Systems Agency (DISA), 484
degraded component state, vSAN, 51
DEKs (data encryption keys), 61, 274
Dell OpenManage Integration for VMware vCenter Server (OMIVV), 543
delta disk files, 184
denial-of-service (DoS) attacks, 272
dependent hardware iSCSI adapter, 454
deployment
OVF/OVA templates, 585–586
VCSA (vCenter Server Appliance)
  CLI (command-line interface), 305–306
  GUI installer, 303–305
  post-installation, 306–307
  requirements for, 302–303
VMs (virtual machines)
  with content libraries, 608–609
  from templates, 253, 582
vSAN, 53–58, 424
depot, 539, 540
desktop and application virtualization
  App Volumes, 223
  VMware Horizon, 222–223
device connections, disabling, 271
DFW (Distributed Firewall), 280
DHCP server, 297
Direct Console User Interface (DCUI), 258, 547
direct memory access (DMA), 349
directory services, joining hosts to, 260
DirectPath I/O, 122, 347
DISA (Defense Information Systems Agency), 484
Disable Object Checksum policy, 83
disabling
  copying and pasting, 271
  device connections, 271
  disk shrinking, 270–271
  MOB (managed object browser), 491–492
SSO (single sign-on) users, 314–315
vSAN, 423
disaster recovery
SRM (Site Recovery Manager), 226–227
VMware Hybrid Cloud Extension, 229
vSphere Replication, 224–226
Discovery Protocol, 121
disk groups, 50
disk mode settings, VMs (virtual machines), 590
disk shrinking, 270–271
disks, virtual, 35, 81
Distributed Firewall (DFW), 280
distributed port groups, 105
configuration, 341–342
port monitoring in, 357
Distributed Power Management (DPM), 7, 24, 156–157
Distributed Resource Scheduler. See DRS (Distributed Resource Scheduler)
DMA (direct memory access), 349
DNS (Domain Name System), 21–22
domains
DNS (Domain Name System), 21–22
repointing vCenter Server to, 565–569
DoS (denial-of-service) attacks, 272
double-encapsulation attacks, 100
DPM (Distributed Power Management), 7, 24, 156–157
DPUs (data processing units), 15–16, 95
DRS (Distributed Resource Scheduler)
automation modes, 139
cluster creation, 372–374
affinity/anti-affinity rules, 373–374
Predictive DRS, 156, 374
resource pools, 372–373
description of, 7
evacuation workflow, 141
memory metric for load balancing, 140
migration sensitivity, 143–144
network-aware DRS, 140
NVM (non-volatile memory) support, 141
Predictive DRS, 156, 374
recent enhancements, 139–142
resource pools
enhanced resource pool reservation, 147
scalable shares, 147–148
shares, limits, and reservations, 145–146
use cases, 144
rules, 142–143
SDRS (Storage DRS)
anti-affinity rules, 85
automation levels, 84
datasyncore cluster requirements, 85
initial placement and ongoing balancing, 83
load balancing, 83
management of, 449–452
NIOC (Network I/O Control) versus, 86
recommendations, 84–85
SIOC (Storage I/O Control) versus, 86, 452–454
thresholds and behavior, 84
virtual machine distribution, 140
virtual machine initial placement, 140–141
virtual machine scores, 142, 389
DVD/CD-ROM drives, 186
dynamic link aggregation, 118–119, 350–354
E
eager zeroed thick virtual disks, 81
Edge, VMware support for, 23
editing. See also configuration
host profiles, 322–323
OVF (Open Virtual Format) templates, 594
permissions, 478–479
SSO identity sources, 310
Egress Traffic Shaping, 359
EKs (endorsement keys), 277
elastic port allocation, 117
Embedded Harbor Registry, 212
embedded_vCSA_on_ESXi.json, 306
embedded_vCSA_on_VC.json, 306
embedded_vCSA_replication_on_ESXi.json, 306
embedded_vCSA_replication_on_VC.json, 306
EMC RecoverPoint, 227
Encrypted vSphere vMotion, 276–277
encryption
  Encrypted vSphere vMotion, 276–277
  VMs (virtual machines), 189, 273–276, 508–510, 589
vSAN, 61, 434–437
endorsement keys (EKs), 277
Enhanced Linked Mode, 12, 476
enhanced resource pool reservation, 147
Enhanced vMotion Compatibility. See EVC
  (Enhanced vMotion Compatibility)
ephemeral binding, 117
erasure coding, 58, 59–60
ESA (Express Storage Architecture), 47, 63
esxcli commands, 460–462, 486–487
  esxcli network ip ipsec sa add, 267
  esxcli rdma iser add, 455
  esxcli storage core claimrule add, 457–458
  esxcli storage hpp device set, 458
esxcli network namespace, 486
esxcli storage namespace, 486
ESXi, 243, 357
  base image, 540
  CBT (Change Block Tracking), 225
certificates, 243, 481–483
  clusters. See clusters
compute and system requirements, 14–16
directPath I/O, 122, 347
ESXi Shell, 258
firmware updates, 542–544
genl security recommendations
  hardening guidelines, 484–485
host configuration scripts, 485–487
host profiles. See host profiles
MOB (managed object browser), 491–492
overview of, 483–484
passwords and account lockout, 487–489
PCI and PCIe devices, 491
shell security, 489–491
SSH (Secure Shell), 489–491
host networking management with vDS
  host addition to vDS, 354–355
  host removal, 356–357
  network adapter management, 355–356
  network adapter migration to vDS, 356
  networking policies and advanced features, 359–361
  port monitoring in distributed port groups, 357
  virtual machine migration to vDS, 357
hosts
  acceptance levels, 497–498
  advanced system settings, 325–327
  certificates, 245
  configuration, 324–325
definition of, 173–174
  DNS resolution, 21–22
  dynamic link aggregation, 118–119, 350–354
  firewalls, 494–495, 548–549
  health checks, 390–391
  host access, 261
  host configuration scripts, 485–487
  host networking with vDS, 354–361
  installation, 290–301
  joining to directory services, 260
  kernel options, 325–327
  lifecycle management with vLCM, 532–546
  Maintenance Mode, 301
  management, 499–500, 547–549
moving into clusters, 254
overview of, 21–22
permissions, 323
privileges, 498–499
profiles, 7, 175–176, 321–323, 484–485, 524
resource management and monitoring, 390–391
syslog data collection with Aria for Logs, 217–218
time synchronization with NTP (network time protocol), 22
TPM (Trusted Platform Module), 502–503
UEFI Secure Boot, 501–502
vSAN hardware requirements, 25–26
vSphere+, 213–214
log files, 405–407
namespaces, 486
network requirements, 20–21
networking security recommendations, 492–494
Auto Deploy, 493
CIM (Common Information Model) access, 493–494
web proxy settings, 492
Quick Boot, 542
security
Active Directory, 499–500
built-in features, 257–258
ESXi firewall, 494–495
ESXi services, 495–496
firewall ports, 259–260
general security recommendations, 483–492
host acceptance levels, 497–498
host access, 261
hosts, joining to directory services, 260
Lockdown Mode, 496–497
log files, 503
MOB (managed object browser), 261
networking security recommendations, 492–494
password hardening, 260
privileges, 498–499
Secure Boot, 261–262
security profiles, 258–260
smart card authentication, 501
TPM (Trusted Platform Module), 261–262, 502–503
UEFI Secure Boot, 501–502
VIB acceptance levels, 497–498
vSphere Authentication Proxy, 260, 500
vTA (vSphere Trust Authority), 263
storage requirements, 17
upgrading, 530
VLAN support, 97
ESXTOP, 396–399
EtherChannels (LAGs), 95, 350–354
evacuation workflow, DRS (Distributed Resource Scheduler), 141
EVC (Enhanced vMotion Compatibility), 135–139
configuration
EVC modes for AMD hosts, 138–139
EVC modes for Intel hosts, 136–137
EVC modes for VMs (virtual machines), 603
EVC modes for vSphere clusters, 372
overview of, 135–136
requirements for, 136
events
monitoring and management, 400–402
streaming to remote syslog server, 401–402
system event log, 401
viewing, 400
exam preparation
exam-day tips, 614–616
pre-exam activities, 613–614
expanding vSAN clusters, 424–426
expiration, certificates, 483
exporting cluster images, 544–545
Express Storage Architecture (ESA), 47, 63
Extended Copy (XCOPY), 71
Extended Statistics option, VAAI NAS primitives, 72
failback, 359
failover. See multipathing and failover
failure
  definition of, 149
  Failure Tolerance Method policy, 82
  FTT (failures to tolerate), 143
  vsphere HA response to, 150
Fast File Clone/Native Snapshot Support
  option, VAAI NAS primitives, 71
fault domains, vSAN, 64–65, 428
Fault Tolerance. See FT (Fault Tolerance)
FC (Fibre Channel), 35, 44–45, 76, 189
FCD (First Class Disk), 44
FC-NVMe (NVMe over Fibre Channel),
  455
FCoE (Fibre Channel over Ethernet), 36
fdm.cfg file, 153
Federal Information Processing Standards
  (FIPS), 507
Fibre Channel (FC), 35, 44–45, 76, 189
Fibre Channel over Ethernet (FCoE), 36
file service virtual machines (FSVMs),
  61–62
File Service, vSAN
  management and configuration, 439–440
  overview of, 61–62
file-based backup and restore, 23
file-based persistent volumes, 53
files. See also log files
  boot.cfg, 293
  fdm.cfg, 153
  kickstart, 293
  snapshot, 184–185
VM (virtual machine)
  configuration files, 179
  file structure, 178–179
  snapshot files, 180
  virtual disk files, 180
filters
  I/O, 39
  multicast, 120–121
  storage protection, 446
FIPS (Federal Information Processing
  Standards), 507
Firefox, VMware support for, 23
firewalls, 266
  DFW (Distributed Firewall), 280
  ESXi, 494–495, 548–549
  ports, 259–260
  VMware NSX, 280–281
firmware updates, ESXi, 542–544
First Class Disk (FCD), 44
fixed port allocation, 117
Flash Read Cache Reservation policy, 82
flat files, 183
Flexible Launch Control (FLC) mode, 508
folders, definition of, 172
Force Provisioning policy, 82
Forged Transmits option, network security
  policies, 103
FQDNs (fully qualified domain names),
  21–22, 521, 553
FSVMs (file service virtual machine), 61–62
FT (Fault Tolerance), 157–161
description of, 7
  legacy, 524
  vsphere HA clusters, 377
FTT (failures to tolerate), 143
Full File Clone option, VAAI NAS
  primitives, 71
fully qualified domain names (FQDNs),
  21–22, 521, 553

G
Get-DeployCommand, 299
Get-DeployMachineIdentity, 300
Get-DeployOption, 300
Get-DeployRule, 299
Get-DeployRuleSet, 299
Get-VM cmdlet, 600
Get-VMHost, 487
Get-VMHostAttributes, 300
Get-VMHostImageProfile, 300
Get-VMHostMatchingRules, 299
global permissions
host networking management with vDS

- definition of, 250–251
- management of, 478
- Google Chrome, VMware support for, 23
- GPUs (graphics processing units), VM configuration for, 601–603
- graphical user interface (GUI), 297, 302–305
- graphics processing units (GPUs), VM configuration for, 601–603
- GRID model, 601–603
- groups
  - authentication and authorization, 476–477
  - LAGs (link aggregation groups), 95, 350–354
- port groups
  - distributed, 341–342
  - standard, 336–338
- SSO (single sign-on), 314–315
- guest OS
  - customizing, 582
  - upgrade rollbacks, 182
- guest user mapping, 594
- GUI (graphical user interface), 297, 302–305

H
- hard disks, 186
- hardening
  - ESXi passwords, 260
  - guidelines for, 484–485
  - VMs (virtual machines), 269
- hardware
  - compatibility checks, 544
  - health checks, 390–391
  - VM hardware configuration, 586–592
  - vSAN requirements, 65–66
- HCI (hyperconverged infrastructure)
  - technology, 227–229
- HCX (Hybrid Cloud Extension), 229–231
- health checks
  - Skyline Health, 390–391
- vDS (vSphere Distributed Switches), 119–120
- health states, 51, 553
- heartbeats, vSphere HA, 151
- Hewlett-Packard Integrated Lights-Out (iLO), 156–157
- high availability, 24
- vCenter HA
  - clusters, 12–13, 564–565
  - overview of, 161
- vSphere HA
  - admission control, 151–152
  - advanced options, 153
  - benefits of, 148–149
  - best practices, 155
  - capacity reservation, 423
  - cluster configuration, 374–378
  - description of, 7
  - heartbeats, 151
  - Proactive HA, 155
  - Proactive HA (High Availability), 7, 155, 376
  - requirements for, 149–150
  - response to failures, 150
  - virtual machine settings, 153–154
  - VM monitoring settings, 154–155
  - VMCP (Virtual Machine Component Protection), 154
  - vSAN and vSphere HA configuration, 422–423
  - vSphere requirements, 6, 24–25
- High-Performance Plug-in (HPP), 45–46
- Horizon, 201, 222–223
- Host Agent, 11
- Host Isolation Response Shutdown setting, vSphere HA, 153
- host limits, virtual machine migration, 193
- host networking management with vDS, 354–361
- host addition to vDS, 354–355
- host removal, 356–357
- network adapter management, 355–356
- network adapter migration to vDS, 356
networking policies and advanced features, 359–361
port monitoring in distributed port groups, 357
virtual machine migration to vDS, 357
host profiles, 175–176
configuration, 321–323
applying, 321–322
applying ESXi host permissions with, 323
editing, 322–323
ESXi configuration with, 321, 484–485
description of, 7
host_wipe_vsan_disks command, 431
host-based failover with iSCSI, 76
hostd, 547
hosts, 21–22
acceptance levels, 497–498
certificates, 245
configuration
advanced system settings, 325–327
common ESXi host settings, 324–325
core options, 325–327
definition of, 173–174
DNS resolution, 21–22
dynamic link aggregation, 118–119, 350–354
firewalls, 494–495, 548–549
health checks, 390–391
host access, 261
host configuration scripts, 485–487
host networking management with vDS, 354–361
host addition to vDS, 354–355
host removal, 356–357
network adapter management, 355–356
network adapter migration to vDS, 356
networking policies and advanced features, 359–361
port monitoring in distributed port groups, 357
virtual machine migration to vDS, 357
installation, 290–301
Auto Deploy, 296–301, 493
interactive installation, 290–292
scripted installation, 292–296
joining to directory services, 260
cycle management with vLCM, 532–546
backup and restore scenarios, 544–545
baselines and images, 536–542
cluster images, importing/exporting, 544–545
ESXi firmware updates, 542–544
ESXi Quick Boot, 542
hardware compatibility checks, 544
overview of, 532–535
remediation settings, 534
terminology for, 539
UMDS (Update Manager Download Service), 535–536
virtual machine upgrades, 546
Maintenance Mode, 301
management, 547–549
managing with Active Directory, 499–500
moving into clusters, 254
permissions, 323
privileges, 498–499
profiles, 175–176, 484–485, 524
applying, 321–322
applying ESXi host permissions with, 323
compatibility, 524
configuration, 321–323, 484–485
definition of, 175–176
description of, 7
editing, 322–323
ESXi configuration with, 321
resource monitoring and management, 390–391
syslog data collection with Aria for Logs, 217–218
time synchronization with NTP (network time protocol), 22
TPM (Trusted Platform Module), 502–503
UEFI Secure Boot, 501–502
vSAN hardware requirements, 25–26
vSphere+213–214
hot clones, 199
HPE iLO Amplifier, 543
HPP (High-Performance Plug-in), 45–46
HTML5, 23
hybrid cloud, 27
Azure VMware Solution, 231
HCX (Hybrid Cloud Extension), 229–231
VCF (VMware Cloud Foundation), 227–229
Hybrid Cloud Extension (HCX), 229–231
hyperconverged infrastructure (HCI) technology, 227–229
hypervisor-based replication, 224–226

IDE (Integrated Drive Electronics) interfaces, 186
Identity Federation, 316–318
identity sources
Active Directory, 311–313
LDAP, 313
SSO (single sign-on), 310
IEEE (Institute of Electrical and Electronics Engineers)
802.1ax, 95
802.1q, 97, 106
802.3ad, 95, 101, 108
IEEE 802.1ax, 95
IEEE 802.1Q, 97
IEEE 802.3ad, 95
IETF (Internet Engineering Task Force) Requests for Comments, 94
IGMP (Internet Group Management Protocol), 121
iLO Amplifier, 543
Image Builder PowerCLI, 297
image profiles, 297
images
cluster images, importing/exporting, 544–545
vLCM (vSphere Lifecycle Manager), 536–542
importing cluster images, 544–545
Incompatible clusters, 542
independent hardware iSCSI adapter, 454
infrastructure requirements, vSphere compute and system, 14–16
high availability, 6, 24–25
network, 17–21
for optional components and add-ons, 23–24
SDDC (software-defined data center), 25–26
storage, 16–17
Supporting infrastructure services, 21–23
vSphere replication, 6, 24
Ingress Traffic Shaping, 359
installable core vSphere components, 6
installation. See also configuration; management; VMware product integration
ESXi
compute and system requirements, 14–16
network requirements, 20–21
storage requirements, 17
ESXi hosts
Auto Deploy, 296–301, 493
interactive installation, 290–292
scripted installation, 292–296
SSO (single sign-on)
Active Directory identity sources, 311–313
LDAP identity sources, 313
overview of, 309–310
policies, 315–316
SSO identity sources, 310
users, enabling/disabling, 314–315
vCenter Server components
PSC (Platform Services Controller), 301–302
SSO (single sign-on), 309–316
vCenter Server database, 301
VCSA (vCenter Server Appliance), 302–307
VMCA (VMware Certificate Authority), 307–309
VMware Tools, 189, 578–580
vSphere
ESXi hosts, 290–301
Identity Federation, 316–318
initial configuration, 318–327
vCenter Server components, 301–307
instant clones, 200–201
Institute of Electrical and Electronics Engineers. See IEEE (Institute of Electrical and Electronics Engineers)
Integrated Drive Electronics (IDE) interfaces, 186
Integrated Lights-Out (iLO), 156–157
integration
Aria Suite
Aria Automation, 218–219
Aria for Logs, 217–218
Aria Operations, 216–217
Aria Operations for Networks, 220–221
Aria Orchestrator, 219–220
cloud computing
HCX (Hybrid Cloud Extension), 229–231
VCF (VMware Cloud Foundation), 227–229
VMC (VMware Cloud) on AWS, 231
desktop and application virtualization
App Volumes, 223
Horizon, 222–223
networking and security, 232–233
replication and disaster recovery
SRM (Site Recovery Manager), 226–227
vSphere Replication, 224–226
storage, 69–75
VAAI (vSphere APIs for Array Integration), 70–72
VASA (vSphere APIs for Storage Awareness), 69–70
vVols (virtual volumes), 72–75
VMware NSX Data Center (NSX), 232–233
VMware NSX-T Data Center (NSX-T), 232–233
vSphere add-ons
overview of, 208
vCenter Converter (Converter Standalone), 214–215
VMware Skyline, 215–216
text of, 215
vSphere with Tänzü, 208–213, 521–523
text of, 521
vSphere+ 213–214
Intel FlexMigration, 136
Intel hosts, EVC (Enhanced vMotion Compatibility) modes for, 136–137
Intel Software Guard Extensions (SGX), 278–279, 507–508
Intelligent Platform Management Interface (IPMI), 156–157
interactive ESXi installation, 290–292
Interconnect service, VMware Hybrid Cloud Extension, 229
Internet Group Management Protocol (IGMP), 121
Internet Protocol Flow Information Export (IPFIX), Aria Operations support for, 221
Internet Protocol Security (IPsec), 266–267
Internet SCSI (iSCSI)
management of, 454–455
overview of, 35–36
inventory
definition of, 171
hierarchy and objects, 171–173, 246–248
vCenter Server, 319–321
I/O (input/output)
DirectPath I/O, 122, 347
I/O filters, 39
IOMMU (I/O memory management unit), 122, 349
IOVP (VMware-I/O Vendor Program), 75
NIOC (Network I/O Control), 86, 108–109, 344–345, 524
SIOC (Storage I/O Control), 86, 452–454
SR-IOV (single root I/O virtualization), 123–125, 347–349
VAIO (vSphere APIs for I/O Filtering), 70, 275
IOFilter, 275
IOMMU (I/O memory management unit), 349
IOPS Limit for Object policy, 83
IOVP (VMware-I/O Vendor Program), 75
IP (Internet Protocol), 125–126
addresses, 94, 553
IP hash NIC teaming, 101–102
IPFIX (Internet Protocol Flow Information Export), Aria Operations support for, 221
IPMI (Intelligent Platform Management Interface), 156–157
IPsec (Internet Protocol Security), 266–267
iSCSI (Internet SCSI)
iSCSI Extensions for RDMA, 36
iSCSI over RDMA. See iSER (iSCSI Extensions for RDMA)
iSER (iSCSI Extensions for RDMA), 36, 455
management of, 454–455
overview of, 35–36
iSER (iSCSI Extensions for RDMA), 36, 455
isolated secondary PVLANs, 113
isolation, 149, 266

J
JSON (Javascript Object Notation) templates, 306
jumbo frames, 100
just-in-time (JIT) delivery, 222–223

K
KEK (Key Exchange Key), 270
KEKs (key encryption keys), 61, 274
kernel, ESXi, 325–327
Key Management Interoperability Protocol (KMIP), 23, 274, 434–436
key management server (KMS), 61, 263, 434–436, 503–504
Key Management Services (KMS), 23
keyboards, 186
keys
DEKs (data encryption keys), 61, 274
KEK (Key Exchange Key), 270
KEKs (key encryption keys), 61, 274
KMIP (Key Management Interoperability Protocol), 23, 274, 434–436
KMS (key management server), 23, 61, 263, 434–436, 503–504
PKI (public key infrastructure), 240
SSH (Secure Shell), 491
kickstart file, 293
KMIP (Key Management Interoperability Protocol), 23, 274, 434–436
KMS (key management server), 23, 61, 263, 434–436, 503–504
Kmxd, 258
Kubernetes, 53
Aria Automation and, 219
clusters, 208–211
storage, 43–44

L
labs, VMware Hands-on Labs, 613
LACP (Link Aggregation Control Protocol), 95, 118–119
LAGs (link aggregation groups), 95, 350–354
LANs, virtual. See VLANs (virtual LANs)
l latency sensitivity, VMs (virtual machines), 395
lazy zeroed thick virtual disks, 81
LCM (Lifecycle Manager), 52, 219, 228, 318–319. See also vLCM (vSphere Lifecycle Manager)
LDAP (Lightweight Directory Access Protocol), 11, 309, 313
least significant bit (LSB), 101
legacy fault tolerance, 524
legacy hosts, SSL certificate verification for, 561
libraries, content, 603
adding items to, 608
authentication, 605
creating, 604–605
definition of, 604
deploying VMs with, 608–609
managing VM templates in, 609
overview of, 176–178
permissions, 606–607
publishing, 605
subscribing to, 606
synchronization options, 607
versioning, 177
License Service, 11
licenses
vSAN, 67–68, 421–422
vSphere, 8–9
LicenseService.Administrators group, 315
Lifecycle Manager (LCM), 52, 219, 228, 318–319. See also vLCM (vSphere Lifecycle Manager)
Lightweight Directory Access Protocol (LDAP), 11, 309, 313
line charts, 379
Link Aggregation Control Protocol (LACP), 95, 118–119
link aggregation groups, 350–354
link aggregation groups (LAGs), 95, 350–354
linked clones, 182, 200
load balancing, 359
DRS (Distributed Resource Scheduler), 140
SDRS (Storage DRS), 83
load-based NIC teaming, 108
Load-Based Teaming Daemon, 258
local storage, 35
Lockdown Mode, ESXi, 496–497
lockout policy, 316
Log Assist (Skyline), 215
log files
Aria for Logs, 217–218
ESXi, 405–407, 503
limiting number of, 271
log levels, 408–409
monitoring and management, 405–412
system event log
configuration, 409–410
streaming events to, 401–402
viewing, 401
vRLI (vRealize Log Insight), 411–412
vCenter Server, 407–408
VMware Skyline, 215
vSAN, 68
logical unit numbers (LUNs), 35
LSB (least significant bit), 101
LZ4, 58
MAC (media access control) addresses, 102–103
definition of, 94
network security policies and, 102–103
MAC Address Changes option, network security policies, 103
Machine certificate store, 244
machine learning (ML), 601
machine SSL certificates, 243
Machine SSL store (MACHINE_SSL_CERT), 307
Maintenance Mode
ESXi hosts, 301
vSAN, 426–428
managed object browser (MOB), 261, 491–492
management. See also configuration; installation
certificates
custom, 480–481
ESXi, 481–483
vSphere Client, 479–480
clusters
configuring with Quickstart, 369–371
creating, 368
EVC mode, 372
vCenter HA, 564–565
vSphere DRS, 372–374
vSphere HA, 374–378
content libraries
adding items to, 608
authentication, 605
creating, 604–605
definition of, 604
deploying VMs with, 608–609
managing VM templates in, 609
overview of, 176–178
permissions, 606–607
publishing, 605
subscribing to, 606
synchronization options, 607
versioning, 177
data center-level, 113–114
ESXi host lifecycle management
backup and restore scenarios, 544–545
baselines and images, 536–542
cluster images, importing/exporting, 544–545
ESXi firmware updates, 542–544
ESXi Quick Boot, 542
hardware compatibility checks, 544
overview of, 532–535
remediation settings, 534
terminology for, 539
UMDS (Update Manager Download Service), 535–536
virtual machine upgrades, 546
ESXi host networking with vDS
host addition to vDS, 354–355
host removal, 356–357
network adapter management, 355–356
network adapter migration to vDS, 356
networking policies and advanced features, 359–361
port monitoring in distributed port groups, 357
virtual machine migration to vDS, 357
ESXi security
Active Directory, 499–500
ESXi firewall, 494–495
ESXi services, 495–496
general security recommendations, 483–492
host acceptance levels, 497–498
Lockdown Mode, 496–497
log files, 503
networking security recommendations, 492–494
overview of, 493–494
privileges, 498–499
smart card authentication, 501
TPM (Trusted Platform Module), 502–503
UEFI Secure Boot, 501–502
VIB acceptance levels, 497–498
vSphere Authentication Proxy, 500
OVA (Open Virtual Appliance) templates
adding to content libraries, 608
reverting to previous version, 609
OVF (Open Virtual Format) templates
adding to content libraries, 608
managing, 178, 598
reverting to previous version, 609
SSO (single sign-on), 474–479
storage infrastructure
iSCSI (Internet SCSI), 454–455
multipathing and failover, 460–462
NFS datastores, 447–449
PMem devices, 458–459
RDMs (raw device mappings), 446–447
SDRS (Storage DRS), 449–452
SIOC (Storage I/O Control), 452–454
storage policies, 463–466
VMFS datastores, 441–449
VMware NVMe (Non-Volatile Memory Express), 455–458
vSAN, 418–440
vVols (virtual volumes), 466–468
vCenter Server
overview of, 549–550
repointing to another domain, 565–569
with VAMI, 550–554
vCenter HA clusters, 564–565
VMCA (VMware Certificate Authority), 307–309
with vSphere Client, 554–564
virtual networks
DirectPath I/O, 347
host networking with vDS, 354–361
LAGs (link aggregation groups), 95, 350–354
network resource pools, 109–111, 345–346
NIOC (Network I/O Control), 108–109, 344–345
port mirroring, 116, 349–350
private VLANs (PVLANs), 346
SR-IOV (single root I/O virtualization), 347–349
VMkernel adapters, 342–343
VMs (virtual machines)
advanced options, 189
cloning, 199–201, 580–581
compatibility options, 185–187, 586
content libraries, 176–178, 604–609
creating to templates, 581
CPU affinity, 603
deploying from templates, 253, 582
disk mode settings, 590
equalization, 589
EVC mode, 603
guest OS customization, 582–585
guest user mapping, 594
hardware devices, 185–187
migration, 190–194, 596–598
Open VM Tools, 578
opening consoles to, 577–578
options, 188–189, 592–593
OVF/OVA templates, 178, 585–586, 594, 598, 608
powering on, 577
provisioning, 188, 200, 589
shutting down guests, 580
snapshots, 180–185, 595–596
upgrading, 546
VBS (virtualization-based security), 598–599
versions, 587–588
vGPU (virtual GPU) support, 601–603
VM hardware configuration, 586–592
VMware PowerCLI, 599–601
VMware Tools, 153, 188, 189, 221, 272, 324, 395, 524, 578–580
vSAN, 86
cluster creation, 419
cluster expansion, 424–426
datastores, 422
deployment with vCenter Server, 424
disabling, 423
disk/device management, 430–432
encryption, 434–437
fault domains, 428
File Service, 439–440
licensing, 421–422
Maintenance Mode, 426–428
manually enabling, 420–421
policies, 437–438
preparation, 418
settings, 421
shutdown and restart, 424
space efficiency, 433
storage providers, viewing, 439
stretched clusters, 428–430
vSAN and vSphere HA, 422–423
vSphere
backup and recovery with vSphere with Tanzu, 208–213, 521–523
ESXi hosts, 547–549
upgrading to vSphere 8.0, 523–531
vCenter Server backup, 518–521
vLCM (vSphere Lifecycle Manager), 532–546
vSphere resources
alarms, 402–405
client performance charts, 377, 379–383
cluster resources, 388–389
events, 400–402
host resources and health, 390–391
logging, 405–412
metrics, 378
pool resources, 389–390
troubleshooting and optimization, 383–387
vCenter Server resources, 399
virtual machine resources, 392–399
Managing Host and Cluster Lifecycle documentation, 371
man-in-the-middle (MITM) attacks, 265
mapping VM guest users, 594
Maximum per-VM Resets setting, vSphere HA, 155
maximum round-trip time (RTT), 26
maximum transmission units. See MTUs (maximum transmission units)
media access control. See MAC (media access control) addresses
memory, 186
files, 184
NVDIMMs (non-volatile dual in-line memory modules), 458
NVM (non-volatile memory), 141
objects, 51
PMem devices, 458–459
RDMA (Remote Direct Memory Access), 457
NVMe over RDMA, 44–45, 455
RDMA over Converged Ethernet, 457
vPMeM (Virtual Persistent Memory), 141, 458–459
vSAN, 66
Mem-vVol, 74
metadata
VIB (vSphere Installation Bundle), 539
VMDK file, 183
metrics
virtual machine resources, 392
vSphere resources, 378
microsegmentation, 280–281
Microsoft Active Directory. See Active Directory (AD)
Microsoft Azure VMware Solution, 231
Microsoft Edge, VMware support for, 23
Microsoft Key Exchange Key (KEK), 270
Microsoft virtualization-based security (VBS), 598–599
Microsoft Windows Perfmon, 395
migration
DRS (Distributed Resource Scheduler) migration sensitivity, 143–144
host physical network adapters to vDS, 356
Storage vMotion, 197–199
vCenter Server for Windows to vCenter Server Appliance, 528–530
virtual machines to vDS, 357
vMotion, 194–197
VMs (virtual machines), 190–194, 254, 596–598
mirroring, port, 116, 349–350
MITM (man-in-the-middle) attacks, 265
ML (machine learning), 601
MLD (Multicast Listener Discovery), 121
MOB (managed object browser), 261, 491–492
Mobility Groups service, VMware Hybrid Cloud Extension, 229
Mobility Optimized Networking (MON), 230
models, storage
  software-defined storage, 38–39
  storage virtualization, 34–38
  virtual machine storage, 34
MON (Mobility Optimized Networking), 230
monitoring
  applications in vSphere HA clusters, 376
  ports, 115–117, 357
vCenter Server
  overview of, 549–550
  repointing to another domain, 565–569
  with VAMI, 550–554
  with vSphere Client, 554–564
vDS (vSphere Distributed Switches), 111
VMs (virtual machines), 376
vSphere HA, 154–155
vSphere resources
  alarms, 402–405
  client performance charts, 377, 379–383
  cluster resources, 388–389
  events, 400–402
  host resources and health, 390–391
  logging, 405–412
  metrics, 378
  pool resources, 389–390
  troubleshooting and optimization, 383–387
  vCenter Server resources, 399
  virtual machine resources, 392–399
Monterey project, 114
mounting datastores, 444
Mozilla Firefox, VMware support for, 23
MPPs (multipathing plug-ins), 76
MTUs (maximum transmission units)
  overview of, 100
  vSS (vSphere Standard Switches), 335
  multicast brute-force attacks, 100
  multicast filtering mode, 120–121
  Multicast Listener Discovery (MLD), 121
  multipathing and failover, 76
  esxcli commands for, 460–462
  failover types, 76
  management of, 460–462
  MPPs (multipathing plug-ins), 76
NMP (Native Multipathing Plug-in)
  PSPs (Path Selection Plug-ins), 78–79
  SATPs (Storage Array Type Plug-ins), 77–78
  VMware NMP, 76–77
  overview of, 75–76, 359
  PSA (Pluggable Storage Architecture), 76–80
multipathing plug-ins (MPPs), 76
N
names, inventory objects, 171
namespaces, 50, 486
NAS (network-attached storage), 36, 71–72
Native Multipathing Plug-in (NMP), 76–77
  PSPs (Path Selection Plug-ins), 78–79
  SATPs (Storage Array Type Plug-ins), 77–78
  VMware NMP, 76–77
NetFlow
  configuration, 340–341
  policies, 111
network adapters, 186
Network Extension service, VMware
  Hybrid Cloud Extension, 229
network failure detection, 359
Network File System. See NFS (Network File System)
network interface cards. See NICs (network interface cards)
Network I/O Control (NIOC), 86, 108–109, 344–345, 524
network limits, virtual machine migration, 192–193
network offloads compatibility, 114–115, 338
network policies
vDS (vSphere Distributed Switches), 106–112
load-based NIC teaming, 108
NetFlow and monitoring, 111
port-blocking, 108
resource allocation, 108–111
traffic filtering and marking, 111–112
traffic shaping, 107
vSS (vSphere Standard Switches), 100–104
network resource pools. See resource pools
network time protocol. See NTP (network time protocol)
network-attached storage (NAS), 36, 71–72
network-aware DRS (Distributed Resource Scheduler), 140
networks, 350–354
Aria Operations for Networks, 220–221
CDP (Cisco Discovery Protocol), 121
definition of, 174
DirectPath I/O, 122, 347
host networking management with vDS
host addition to vDS, 354–355
host removal, 356–357
network adapter management, 355–356
network adapter migration to vDS, 356
networking policies and advanced features, 359–361
port monitoring in distributed port groups, 357
virtual machine migration to vDS, 357
multicast filtering mode, 120–121
opaque, 18, 95
physical, 18, 94
policies
vDS (vSphere Distributed Switches), 106–112
vSS (vSphere Standard Switches), 100–104
resource pools. See resource pools
security
Auto Deploy, 493
CIM (Common Information Model) access, 493–494
firewalls, 266
general recommendations, 267–268
IPsec (Internet Protocol Security), 266–267
network security policies, 268
segmentation and isolation, 266
web proxy settings, 492
SR-IOV (single root I/O virtualization), 123–125
TCP/IP stacks, 125–126
terminology for, 94–95
TSO (TCP Segmentation Offload), 122
vDS (vSphere Distributed Switches)
data center-level management, 113–114
distributed port groups, 105
health checks, 119–120
LACP (Link Aggregation Control Protocol), 118–119
network offloads compatibility, 114–115
network policies, 106–112
overview of, 104
port binding and allocation, 117
port mirroring, 116, 349–350
port state monitoring, 115–117
PVLANs (private VLANs), 113
uplink port groups, 105–106
vSS compared to, 106
virtual, 18
DirectPath I/O, 122, 347
host networking management with vDS, 354–361
LAGs (link aggregation groups), 95, 330–354
network resource pools, 109–111, 345–346
NIOC (Network I/O Control), 108–109, 344–345
port mirroring, 116, 349–350
PVLANs (private VLANs), 113, 346
SR-IOV (single root I/O virtualization), 123–125, 347–349
vDS (vSphere Distributed Switches), 104–120, 338–342
VLANs (virtual LANs), 97–98, 104, 113, 346
VMkernel networking, 125–126, 342–344
VMware NSX Data Center (NSX), 232–233
VMware product integration, 232–233
vSS (vSphere Standard Switches), 98–104, 334–336
vNICs (virtual NICs), 96
vSAN support, 67
vSphere requirements, 17–21
vSS (vSphere Standard Switches) configuration, 334–336
MTUs (maximum transmission units), 100
network policies, 100–104
overview of, 98–100
standard port groups, 336–338
vDS compared to, 106
New Virtual Machine wizard, 577
New-DeployRule, 299
NFS (Network File System) datastores management of, 447–449
overview of, 41–43
overview of, 36
NICs (network interface cards) hardware accelerators, 95

No Access privileges, 249, 498
Non-Compliant clusters, 541
Non-offloading mode before NSX is enabled (vDS), 115
non-volatile dual in-line memory modules (NVDIMMs), 187, 458
Non-Volatile Memory Express. See NVMe (Non-Volatile Memory Express)
non-volatile memory (NVM), DRS support for, 141
Normal Lockdown Mode, 496
notify switches, 359
NPIV (N-Port ID Virtualization), 189
N-Port ID Virtualization (NPIV), 189
NSX, 7, 18, 26, 232–233, 280–281
NSX-T, 232
NTP (network time protocol), 22, 258
ntpd, 547
Number of Disk Stripes per Object policy, 82
NVDIMMs (non-volatile dual in-line memory modules), 187, 458
NVIDIA BlueField, 15, 338–339
NVIDIA vGPU (GRID), 601–603
NVM (non-volatile memory), DRS support for, 141
NVMe (Non-Volatile Memory Express), 44–46
controllers, 187
Hot-Plug, 52
management of, 455–458
NVMe over Fabrics, 455, 456
NVMe over Fibre Channel, 455
NVMe over PCIe, 455
NVMe over Remote Direct Memory Access, 455, 457

O
Object Space Reservation policy, 82
object state, 51
object-based storage, 50
objects, inventory, 171–173
Observer, vSAN, 51–52
OEMs (original equipment manufacturers), 539, 540
offline bundle/offline depot, 539
Offloading mode after NSX is enabled (vDS), 115
OIDC (OpenID Connect), 209
OMIVV (OpenManage Integration for VMware vCenter Server), 543
opaque networks, 18, 95
Open Virtual Appliance templates. See OVA (Open Virtual Appliance) templates
Open Virtual Format templates. See OVF (Open Virtual Format) templates
Open VM Tools, 578
OpenID Connect (OIDC), 209
OpenLDAP, 11, 246, 309, 313
OpenManage Integration for VMware vCenter Server (OMIVV), 543
OpenWSMAN daemon, 260
Operations Manager, Aria, 216–217
optimization, vSphere resource performance, 383–387
Orchestrator, Aria, 219–220
original equipment manufacturers (OEMs), 539, 540
Original Storage Architecture (OSA), 47
OS Assisted Migration service, 230
OSA (Original Storage Architecture), 47
OSs (operating systems), guest, 253, 582
Other-vVol, 74
OVA (Open Virtual Appliance) templates, 585–586
adding to content libraries, 608
reverting to previous version, 609
OVF (Open Virtual Format) templates, 178
adding to content libraries, 608
deploying, 585–586
editing, 594
managing, 598
reverting to previous version, 609

P
parallel ports, 186
parent snapshots, 183
partitions, 149
PartnerSupported VIBs, 498
Passive node, vCenter HA clusters, 12–13
passwords
ESXi, 260, 487–489
policy, 264, 315
patching
definition of, 539
vCenter Server with VAMI, 561–563
with vCenter Server Appliance shell, 563–564
path failover. See multipathing and failover
Path Selection Plug-ins (PSPs), 78–79
PCE devices, 187
PCI (Peripheral Component Interconnect) devices, 186, 491
PCIe (Peripheral Component Interconnect Express) devices
ESXi security recommendations, 491
NVMe (Non-Volatile Memory Express) over PCIe, 44
SR-IOV (single root I/O virtualization), 123–125, 347–349
PC/SC Smart Card Daemon, 258
PDL (permanent device loss), 154
Peak Bandwidth option, traffic shaping policy, 104
Pearson Vue, 614
Pensando Distributed Services Card (Pensando DSC), 15
Pensando network offloads compatibility, 338–339
Perfmon, 395
performance charts, client
   advanced performance charts, 381–383
definition of, 377
types of, 379
views, 379–380
performance counters, 272
Peripheral Component Interconnect Express. See PCIe (Peripheral Component Interconnect Express) devices
Peripheral Component Interconnect (PCI) devices, 186, 491
permanent device loss (PDL), 154
permissions
   applying to ESXi hosts, 323
   authentication and authorization, 245–246
   best practices, 251–252
   content libraries, 606–607
   editing, 478–479
ESXi hosts, 323
   global
   definition of, 250–251
   management, 478
   inventory hierarchy and objects, 246–248
   management, 504
   permission validation settings, 504
   permissions diagram, 250
   privileges and roles
   best practices, 251–252
   configuration, 477
   creating, 477
   ESXi hosts, 498–499
   management, 477, 498–499
   required permissions for common tasks, 252–254
   types of, 248–250
vCenter Server, 265
vCenter Server application of, 255–257
   required permissions for common tasks, 252–254
   setting, 477–478
   validation settings, 504
vCenter Server application of, 255–257
persistent logging, 68
persistent storage providers, 69
PEs (protocol endpoints), 73
PFTT (Primary Level of Failures to Tolerate), 430
PFTT (Primary Level of Failures to Tolerate) policy, 82
physical networks, 18, 94
PID (primary network identifier), 553
pie charts, 379
PKI (public key infrastructure), 240
Planned Migration Mode, SRM (Site Recovery Manager), 226
Platform Services Controller Administration, 10
Platform Services Controller (PSC), 301–302
Pluggable Storage Architecture (PSA), 76–80, 460
plug-ins
   HPP (High-Performance Plug-in), 45–46
   MPPs (multipathing plug-ins), 76
   NMP (Native Multipathing Plug-in)
      PSPs (Path Selection Plug-ins), 78–79
      SATPs (Storage Array Type Plug-ins), 77–78
   VMware NMP, 76–77
   PSPs (Path Selection Plug-ins), 78–79
   SATPs (Storage Array Type Plug-ins), 77–78
   vCenter Server plug-ins, 10
   VMware Enhanced Authentication Plug-in, 307
PMem devices, 458–459, 577
pointing devices, 188
policies
   network

host networking management with vDS, 359–361
security, 268
vDS (vSphere Distributed Switches), 106–112
vSS (vSphere Standard Switches), 100–104
SSO (single sign-on), 315–316
storage, 80–83
management of, 463–466
SPBM (Storage Policy Based Management), 81
virtual disk types, 81
vSAN-specific, 81–83
vCenter Server, 264
vDS (vSphere Distributed Switches), 106–112
VMs (virtual machines), 589
vSAN, 69, 437–438
vSS (vSphere Standard Switches), 100–104
pools, network resource, 345–346
ports
binding and allocation, 117
distributed, 105
ESXi, 20–21
firewall, 259–260
mirroring, 115–117, 349–350
parallel, 186
port-blocking policies, 108
serial, 187
state monitoring, 115–117
vCenter Server, 19–20
virtual machine port groups
distributed, 105, 341–342, 357
standard, 336–338
uplink, 105–106
VLAN ID range, 97–98
for vSphere Replication deployment, 225
power management
DPM (Distributed Power Management), 156–157
VMs (virtual machines), 189
PowerCLI, 51, 297
host management with, 487
VM management with, 599–601
powering on VMs (virtual machines), 577
practice exams, 614
Predictive DRS, 156, 374
preparation, exam
test-day tips, 614–616
pre-exam preparation, 613–614
Primary Level of Failures to Tolerate (PFTT), 82, 430
primary network identifier (PID), 553
primitives, storage, 70–72
private cloud
Azure VMware Solution, 231
VMware Hybrid Cloud Extension (HCX), 229–231
private VLANs (PVLANs), 113, 346
privileges
configuration, 477
ESXi hosts, 498–499
management, 477, 498–499
types of, 248–250
vCenter Server, 265
Proactive HA (High Availability), 155
description of, 7
product integration. See VMware product integration
profiles
ESXi security, 258–260
host, 484–485, 524
applying, 321–322
applying ESXi host permissions with, 323
definition of, 175–176
description of, 7
editing, 322–323
ESXi configuration with, 321
image, 297
VM risk, 272
Promiscuous Mode, network security policies, 103
promiscuous secondary PVLANs, 113
protocol endpoints (PEs), 73
provisioning, 188
policies, 589
rapid, 200
TCP/IP stack, 125
thin, 58
PSA (Pluggable Storage Architecture), 76–80, 460
PSC (Platform Services Controller), 301–302
PSPs (Path Selection Plug-ins), 78–79
public cloud
Azure VMware Solution, 231
VMware Hybrid Cloud Extension (HCX), 229–231
public key infrastructure (PKI), 240
publishing content libraries, 605
PVLANs (private VLANs), 113, 346
PXE server, 297

Q
questions, exam, 614–616
Quick Boot, 542
Quickstart, cluster configuration with, 369–371, 419

R
RAID 5/RAID 6 erasure coding, 59–60
rapid provisioning with templates, 200
RAV (Replication Assisted vMotion), 230
raw device mappings (RDMs), 36–38, 446–447, 576, 591
RDMA (Remote Direct Memory Access), 457
NVMe over RDMA, 44–45, 455
RDMA over Converged Ethernet, 457
RDMs (raw device mappings), 36–38, 446–447, 576, 591
RDSH (Remote Desktop Services Host), 223
Read Only privileges, 249, 498
Ready Node, vSAN, 52
RecoverPoint, 227
recovery. See backup and recovery
registering storage providers, 465
regulatory standards, compliance with, 279–280
remediation settings, vLCM (vSphere Lifecycle Manager), 534
Remote Desktop Services Host (RDSH), 223
Remote Direct Memory Access. See RDMA (Remote Direct Memory Access)
Remove-DeployRule, 299
removing
hosts from vDS, 356–357
SSO identity sources, 310
Repair-DeployImageCache, 300
Repair-DeployRulesetCompliance, 300
replication. See also backup and recovery
RAV (Replication Assisted vMotion), 230
Replication objects, 53
SRM (Site Recovery Manager), 226–227
VRMS (vSphere Replication Management Service), 24, 225
VRS (vSphere Replication Service), 24, 225
vSphere Replication, 215, 224–226
vSphere requirements, 6, 24
repointing vCenter Server to another domain, 565–569
Requests for Comments, 94
requirements
EVC (Enhanced vMotion Compatibility), 136
FT (Fault Tolerance), 158
vCenter Server
compute and system requirements, 14
network requirements, 19–20
VCSA (vCenter Server Appliance), 302–303
vSAN, 25–26, 63–68
vSphere
compute and system, 14–16
high availability, 6, 24–25
infrastructure services support, 21–23
network, 17–21
for optional components and add-ons, 23–24
SDDC (software-defined data center), 25–26
storage, 16–17
vSphere replication, 6, 24
vSphere HA, 149–150
reservations
DRS (Distributed Resource Scheduler)
migration sensitivity, 145–146
virtual machine resources, 392–394
Reserve Space option, VAAI NAS
primitives, 72
resignaturing, 442–443
resource management. See also resource pools
alarms
actions, 404
creating, 403–404
elements of, 402
use cases, 404–405
viewing/acknowledging, 403
client performance charts
advanced performance charts, 381–383
definition of, 377
types of, 379
views, 379–380
clusters. See clusters
DPM (Distributed Power Management), 156–157
events, 400–402
streaming to remote syslog server, 401–402
system event log, 401
viewing, 400
FT (Fault Tolerance), 157–161
host resources and health, 390–391
log files
ESXi, 405–407
log levels, 408–409
syslog configuration, 409–410
system logs, uploading to VMware, 407–408
vCenter Server, 407
vRLI (vRealize Log Insight), 411–412
metrics, 378
Predictive DRS, 156, 374
troubleshooting and optimization, 383–387
vCenter HA, 161
vCenter Server resources, 399
vDS (vSphere Distributed Switches)
policies, 108–111
virtual machine resources
admission control, 394
ESXTOP, 396–399
latency sensitivity, 395
metrics, 392
Microsoft Windows Perfmon, 395
shares, limits, and reservations, 392–394
vCenter Server Management, 399
VIMTOP, 399
virtual machine configurations, 396
VMware Tools, 153, 188, 189, 221, 272, 324, 395, 524, 578–580
VMware Service Lifecycle Manager, 161–162
creating, 372–373
definition of, 173
drives, storage, 16–17
shares, limits, and reservations, 145–146
use cases, 144
moving VMs to, 253
Restart VMs setting, vSphere HA, 153
restarting vSAN, 424
restore. See backup and recovery
RFB protocol, 260
RFCs (Requests for Comments), 94
Risk Management Framework (RMF), 484
risk profiles, VM (virtual machine), 272
RMF (Risk Management Framework), 484
RoCE (RDMA over Converged Ethernet), 457

roles
best practices, 251–252
creating, 477
required permissions for common tasks, 252–254
types of, 248–250
vCenter Server application of, 255–257
root users, 499
round trip time (RTT), 67
Route Based on IP Hash policy, 101–102
Route Based on Originating Virtual Port policy, 101
Route Based on Source MAC Hash policy, 101
RTT (round-trip time), 26, 67
Ruby vSphere Console (RVC), 51
runweasel command, 293
RVC (Ruby vSphere Console), 51

S
SATA (Serial ATA), 15, 187
SATPs (Storage Array Type Plug-ins), 77–78
scalable shares, DRS (Distributed Resource Scheduler) migration sensitivity, 147–148
scripted ESXi host configuration, 485–487
scripted ESXi installation, 292–296
SCSI controllers, 187, 591
SCSI UNMAP commands, 58
SDDC (software-defined data center), 25–27, 231
SDRS (Storage DRS), 83–86
anti-affinity rules, 85
automation levels, 84
datastore cluster requirements, 85
initial placement and ongoing balancing, 83
load balancing, 83
management of, 449–452
NIOC (Network I/O Control) versus, 86
recommendations, 84–85
SIOC (Storage I/O Control) versus, 86, 452–454
thresholds and behavior, 84
Secondary Level of Failures to Tolerate (SFTT) policy, 82
Secure Boot, 261–262, 270
Secure Shell (SSH), 258, 489–491
security, 474–483. See also authentication and authorization; permissions; privileges
certificates
core identity services, 241
CSR (certificate signing request), 309
ESXi host, 245
overview of, 240–241
recommended modes for, 241
requirements for, 242–245
solution user certificate stores, 244
types of, 243–244
vCenter Server, 265
ESXi
Active Directory, 499–500
built-in features, 257–258
ESXi firewall, 494–495
ESXi services, 495–496
firewall ports, 259–260
general security recommendations, 483–492
host acceptance levels, 497–498
host access, 261
hosts, joining to directory services, 260
Lockdown Mode, 496–497
log files, 503
MOB (managed object browser), 261
networking security recommendations, 492–494
password hardening, 260
privileges, 498–499
Secure Boot, 261–262
security profiles, 258–260
smart card authentication, 501
TPM (Trusted Platform Module), 261–262, 502–503
UEFI Secure Boot, 501–502
VIB acceptance levels, 497–498
vSphere Authentication Proxy, 260, 500
vTA (vSphere Trust Authority), 263
FIPS (Federal Information Processing Standards), 507
firewalls, 266
  DFW (Distributed Firewall), 280
ESXi, 494–495, 548–549
  ports, 259–260
VMware NSX, 280–281
KMS (key management server), 503–504
network
  Auto Deploy, 493
  CIM (Common Information Model) access, 493–494
firewalls, 266
general recommendations, 267–268
IPsec (Internet Protocol Security), 266–267
network security policies, 268
  security policies, 102–103
  segmentation and isolation, 266
  web proxy settings, 492
NSX Data Center, 232–233
  shell, 489–491, 563–564
STIGs (Security Technical Implementation Guides), 484
Service Broker, 27, 218
Service Composer (VMware NSX), 281
Service Lifecycle Manager, 161–162
SEsparse, 184
Set-DeployMachineIdentity, 300
Set-DeployOption, 300
Set-DeployRule, 299
Set-DeployRuleSet, 299
setup.exe command, 579–580
Set-VMHost, 487
sfcbd, 547
SFTT (Secondary Level of Failures to Tolerate) policy, 82
SGX (Software Guard Extensions), 278–279, 507–508
shares
  DRS (Distributed Resource Scheduler) migration sensitivity, 145–148
  DoS (denial-of-service) attacks, 272
  Encrypted vSphere vMotion, 276–277
  encryption, 273–276, 508–510, 589
  hardening, 269
  Intel Software Guard Extensions (SGX), 278–279
  management of, 508–510
  risk profiles, 272
  UEFI Secure Boot, 270
  unexposed features, disabling, 270
  vTPM (virtual Trusted Platform Module), 277–278
  VMware Aria Operations, 279–280
  VMware NSX, 280–281
  VMware NSX-T, 232–233
  VMware NSX-T Data Center (NSX-T), 232–233
  vTA (vSphere Trust Authority), 504–506
  Security Technical Implementation Guides (STIGs), 484
  Security Token Service (STS), 10, 475
  segmentation, 266, 280–281
  Serial ATA (SATA), 15, 187
  serial ports, 187
  Service Composer (VMware NSX), 281
  Service Lifecycle Manager, 161–162
  SEsparse, 184
  Set-DeployMachineIdentity, 300
  Set-DeployOption, 300
  Set-DeployRule, 299
  Set-DeployRuleSet, 299
  setup.exe command, 579–580
  Set-VMHost, 487
  sfcbd, 547
  SFTT (Secondary Level of Failures to Tolerate) policy, 82
  SGX (Software Guard Extensions), 278–279, 507–508
  shares
    DRS (Distributed Resource Scheduler) migration sensitivity, 145–148
virtual machine resources, 392–394
shell security, 489–491, 563–564
shutdown reboot -r "patch reboot"
command, 564
shutting down
VMs (virtual machines), 580
vSAN, 424
single root I/O virtualization (SR-IOV),
123–125, 347–349
single sign-on. See SSO (single sign-on)
single-level cell (SLC) devices, 66, 68
SIO controllers, 187
SIOC (Storage I/O Control), 86, 452–454
Skyline, 215–216
Skyline Advisor, 392
Skyline Health, 390–391
SLC (single-level cell) devices, 66, 68
slpd, 547
smart card authentication, 501
smart network card (SmartNIC), 339
SmartNICs, 15–16
SMP (symmetric multiprocessor) virtual
machines, 158
SMP-FT (Symmetric Multiprocessing Fault
Tolerance) virtual machines, 430
Snapshot delta VMDKs, 51
snapshots, virtual machine
behavior of, 183–184
benefits of, 182–183
creating/managing, 595–596
limitations of, 184–185
overview of, 180–182
parent, 183
required permissions, 253
snapshot files, 180
use cases, 182
SNMP Server, 259
software depot, 297
Software Guard Extensions (SGX),
278–279, 507–508
software iSCSI adapter, 454
software-defined data center (SDDC),
25–27, 231
software-defined storage, 38–39
software-packages install --iso command,
563
software-packages install -staged command,
563
software-packages install --url command,
564
software-packages list --history command,
563
software-packages list --patch command,
563
software-packages stage --iso command,
563
software-packages stage --url command,
563
solution user certificate, 244
solution user stores, 308
SolutionUsers group, 314
space efficiency, vSAN, 58–60
spanning tree attacks, 100
SPBM (Storage Policy Based Management),
39, 51, 59, 81, 463
SR-IOV (single root I/O virtualization),
123–125, 347–349
SRM (Site Recovery Manager), 226–227
SSH (Secure Shell), 258, 489–491
SSL certificate verification for legacy hosts,
561
SSO (single sign-on), 246, 474–479
configuration
Active Directory identity sources,
311–313
LDAP identity sources, 313
overview of, 309–310
policies, 315–316
SSO identity sources, 310
users, enabling/disabling, 314–315
enabling with Windows session authenti-
cation, 474–479
Enhanced Linked Mode, 476
STS (Security Token Service), 475
tCenter Server, 11
tCenter Single Sign-On, 6, 10, 11
stacked charts, 379
stacks, TCP/IP
  definition of, 94
  for VMkernel networking, 125–126, 343–344
standalone VIB (vSphere Installation Bundle), 539
standard port groups, 336–338
standard switch, 18
standard vSAN clusters, 53
stateless caching, 296
static binding, 117
statistics collection, 558–560
statistics levels, 560
STIGs (Security Technical Implementation Guides), 484
Storage Array Type Plug-ins (SATPs), 77–78
storage devices (LUNs), 35
Storage DRS. See SDRS (Storage DRS)
storage infrastructure, 69
datastores
  clusters, 85, 135
  definition of, 174
  management and configuration, 441–449
  NFS (Network File System), 41–43, 447–449
types of, 39–43, 50
virtual machine migration, 193
VMFS (Virtual Machine File System), 39–41, 441–449
vSAN, 43, 50, 422
vVols (virtual volumes), 43
FC (Fibre Channel), 35
FCoE (Fibre Channel over Ethernet), 36
I/O filters, 39
iSCSI (Internet SCSI)
  management of, 454–455
  overview of, 35–36
iSER (iSCSI Extensions for RDMA), 36, 455
Kubernetes, 43–44
local storage, 35
management and configuration, 446–447
iSCSI (Internet SCSI), 454–455
multipathing and failover, 460–462
NFS datastores, 447–449
PMem devices, 458–459
RDMs (raw device mappings), 446–447
storage policies, 463–466
VMFS datastores, 441–449
VMware NVMe (Non-Volatile Memory Express), 455–458
vSAN, 418–440
vVols (virtual volumes), 466–468
multipathing and failover
esxcli commands for, 460–462
failover types, 76
management of, 460–462
MPPs (multipathing plug-ins), 76
NMP (Native Multipathing Plug-in), 76–80
overview of, 75–76
PSA (Pluggable Storage Architecture), 76–80
NFS (Network File System)
datastores, 41–43, 447–449
overview of, 36
NVMe (Non-Volatile Memory Express), 43, 44–46
PMem devices, 458–459, 577
RDMs (raw device mappings), 36–38, 446–447, 576, 591
SDRS (Storage DRS)
  anti-affinity rules, 85
  automation levels, 84
datastore cluster requirements, 85
initial placement and ongoing balancing, 83
load balancing, 83
management and configuration, 449–452
management of, 449–452
NIOC (Network I/O Control) versus, 86
recommendations, 84–85
SIOC (Storage I/O Control) versus, 86, 452–454
thresholds and behavior, 84
SIOC (Storage I/O Control), 86, 452–454
SPBM (Storage Policy Based Management), 39, 51, 59, 81, 463
storage devices (LUNs), 35
storage integration
VAAI (vSphere APIs for Array Integration), 70–72
VASA (vSphere APIs for Storage Awareness), 69–70
vVols (virtual volumes), 72–75
storage models
software-defined storage, 38–39
storage virtualization, 34–38
virtual machine storage, 34
storage policies
management of, 463–466
SPBM (Storage Policy Based Management), 81
virtual disk types, 81
vSAN-specific, 81–83
storage virtualization, 34–38
Storage vMotion, 7, 41, 197–199
virtual disks, 35
virtual machine storage, 34
VMFS (Virtual Machine File System)
datastores, 39–41, 441–446
definition of, 36
VMware NVMe (Non-Volatile Memory Express), 455–458
vSAN. See vSAN
vSphere requirements, 16–17
vVols (virtual volumes)
datastores, 43
definition of, 39
management and configuration, 466–468
storage integration
VAAI (vSphere APIs for Array Integration), 70–72
VASA (vSphere APIs for Storage Awareness), 69–70
vVols (virtual volumes), 72–75
Storage I/O Control (SIOC), 86, 452–454
Storage Policy Based Management (SPBM), 39, 51, 59, 81, 463
storage primitives, 70–72
storage protection filters, 446
storage providers
managing, 465
registering, 465
vSAN, 439
storage virtualization, 34–38
Storage vMotion, 7, 41, 197–199
stpres, 307
streaming events to remote syslog server, 401–402
stretched vSAN clusters, 54, 428–430
Strict Lockdown Mode, 496
STS (Security Token Service), 10, 475
subscribing to content libraries, 606
supervisor clusters, vSphere with Tanzu, 208–211
supervisors, vSphere with Tanzu, 208–211
Swap-vVol, 74
Switch-ActiveDeployRuleSet, 299
switches
notify, 359
overview of, 96–97
vDS (vSphere Distributed Switches)
configuration, 338–341
data center-level management, 113–114
distributed port groups, 105, 341–342, 357
health checks, 119–120
host networking management with, 354–361
LACP (Link Aggregation Control Protocol), 118–119
modifying, 340
network offloads compatibility, 114–115
network policies, 106–112
overview of, 104
port binding and allocation, 117
port mirroring, 116, 349–350
port state monitoring, 115–117
PVLANs (private VLANs), 113
upgrading, 339–340
uplink port groups, 105–106
vSS compared to, 106
vSS (vSphere Standard Switches)
configuration, 334–336
MTUs (maximum transmission units), 100
network policies, 100–104
overview of, 98–100
standard port groups, 336–338
vDS compared to, 106
Symmetric Multiprocessing Fault Tolerance (SMP-FT) virtual machines, 430
symmetric multiprocessor (SMP) virtual machines, 158
synchronization, content libraries, 607
Syslog Server, 259
system event log
configuration, 409–410
data collection, 217–218
streaming events to, 401–402
uploading to VMware, 407–408
viewing, 401
vRLI (vRealize Log Insight), 411–412
system requirements, vSphere, 14–16
system settings, ESXi hosts, 325–327
SystemConfiguration.Administrators group, 315
SystemConfiguration.BashShellAdministrators group, 315
T
tables, ARP (Address Resolution Protocol), 336
Tanzu, vSphere with, 208–213, 521–523
TBW (terabytes written), 17
TCP (Transmission Control Protocol)
ports, 19–21, 225
TCP Flow Conditioning service, 230
TSO (TCP Segmentation Offload), 122
TCP/IP (Transmission Control Protocol/Internet Protocol)
definition of, 94
for VMkernel networking, 125–126, 343–344
vMotion, 125, 194–197
tcServer, 11
templates
converting VMs to, 581
definition of, 174
deploying VMs from, 253, 582
JSON vCenter Server templates, 306
managing in content libraries, 609
OVA (Open Virtual Appliance), 585–586
adding to content libraries, 608
reverting to previous version, 609
OVF (Open Virtual Format)
adding to content libraries, 608
deploying, 585–586
editing, 594
managing, 178, 598
reverting to previous version, 609
rapid provisioning with, 200
terabytes written (TBW), 17
Test Mode, SRM (Site Recovery Manager), 227
Test-DeployRulesetCompliance, 300
test-taking tips, 614–616
TFTP server, 297
thick eager zeroed provisioning, 188
thick lazy zeroed provisioning, 188
thin provisioning, 58, 72, 81, 188
third-party software providers, 539, 540
third-party storage providers, 69
thresholds, SDRS (Storage DRS), 84
Thumbprint Mode, ESXi, 244, 245, 481–482
time synchronization
  ESXi hosts, 22
  vCenter Server, 265
TLS (Transport Layer Security), 227, 506
tokens
  STS (Security Token Service), 475
token policy, 316
TPM (Trusted Platform Module), 187, 261–262, 502–503. See also vTPM (virtual Trusted Platform Module)
traffic filtering and marking policy, 111–112, 360–361
traffic shaping, 359
  vDS (vSphere Distributed Switches), 107
  vSS (vSphere Standard Switches), 103–104
training and development labs, 182
Transmission Control Protocol. See TCP (Transmission Control Protocol)
Transport Layer Security (TLS), 227, 506
  triage, 182
troubleshooting
  snapshots, 182
  vSphere resource performance, 383–387
trust
  TPM (Trusted Platform Module), 187, 261–262. See also vTPM (virtual Trusted Platform Module)
  vTA (vSphere Trust Authority), 263, 504–506
  vTPM (virtual Trusted Platform Module), 23, 277–278
  Trusted Platform Module (TPM), 187, 261–262. See also vTPM (virtual Trusted Platform Module)
  Trusted root store (TRUSTED_ROOTS), 307
TSO (TCP Segmentation Offload), 122
two-host vSAN clusters, 54

U
UDP (User Datagram Protocol)
  ESXi ports, 20–21
  vCenter Server ports, 19–20
UEFI (Unified Extensible Firmware Interface), 15, 261–262, 270, 501–502
UMDS (Update Manager Download Service), 318–319, 535–536
unhealthy component state, vSAN, 51
universally unique ID (UUID), 442–443
Unknown clusters, 542
UNMAP command, 58, 72
Update Manager Download Service (UMDS), 318–319, 535–536
Update Planner, 530–531
updates
  ARP (Address Resolution Protocol) tables, 336
definition of, 539
  ESXi firmware, 542–544
update.set --CheckUpdates enabled command, 563
update.set --currentURL command, 563
update.set --currentURL default command, 563
upgrades
  definition of, 539
  vCenter Server Appliance, 525–527
  vDS (vSphere Distributed Switches), 339–340
  VMs (virtual machines), 546
  VMware Tools, 578–580
to vSphere 8.0, 523–531
  ESXi, 530
  Update Planner, 530–531
  vCenter Server 7.0 compatibility, 524
  vCenter Server Appliance, upgrading, 525–527
  vCenter Server data transfer, 524–525
vCenter Server for Windows, migrating to vCenter Server Appliance, 528–530
VMs (virtual machines), 530
U.S. Department of Defense (DoD), 484
USB controllers, 187
USB devices, 187
Use Explicit Failover Order policy, 102
User Datagram Protocol. See UDP (User Datagram Protocol)
user-defined vSAN clusters, 52
users
   authentication and authorization, 476–477
   ESXi, 499–500
   SSO (single sign-on)
      enabling/disabling, 314–315
      policies, 315–316
   vCenter Server user access, 263–264, 265
Users group, 314
UTC (Coordinated Universal Time), 24
UUID (universally unique ID), 442–443
V
VAAI (vSphere APIs for Array Integration), 70–72
VAIO (vSphere APIs for I/O Filtering), 70, 275
VAMI (vCenter Server Appliance Management Interface), 225
monitoring/managing vCenter Server with, 550–554
patching vCenter Server with, 561–563
vCenter Server backup with, 518–521
vApps, 175, 189
VASA (vSphere APIs for Storage Awareness), 69–70, 463–465
VBS (virtualization-based security), 189, 598–599
vCenter Appliance File-Based Backup and Restore, 7
vCenter Converter (Converter Standalone), 214–215
vCenter HA
   clusters, 12–13
   management, 564–565
   requirements for, 24–25
   overview of, 161
vCenter Lookup Service, 10
vCenter Server, 71, 297
   backup and recovery, 518–521
   compatibility, 524
   compute and system requirements, 14
   configuration
      common management tasks, 555–557
      repointing to another domain, 565–569
   SSL certificate verification for legacy hosts, 561
   statistics collection settings, 558–560
   updates, 561–564
   vCenter HA clusters, 564–565
content libraries, 603
   creating, 604–605
   definition of, 604
   overview of, 176–178
   publishing, 605
   subscribing to, 605
data transfer, 524–525
database
   compatibility, 524
   description of, 10
description of, 6
Enhanced Linked Mode, 12
host profiles, 175–176
installation
   PSC (Platform Services Controller), 301–302
   vCenter Server database, 301
   VCSA (vCenter Server Appliance), 302–307
   VMCA (VMware Certificate Authority), 307–309
inventory, 171–173, 319–321
log files, 407
management, 399
overview of, 549–550
repointing to another domain, 565–569
with VAMI, 550–554
vCenter HA clusters, 564–565
with vSphere Client, 554–564
network requirements, 19–20
patching
with VAMI, 561–563
with vCenter Server Appliance shell, 563–564
permissions
  authentication and authorization, 245–246
  best practices, 251–252
  global, 250–251, 478
  inventory hierarchy and objects, 246–248
  management, 504
  permissions diagram, 250
  privileges and roles, 248–250, 477, 498–499
  required permissions for common tasks, 252–254
vCenter Server application of, 255–257
plug-ins, 10
rapid provisioning with templates, 200
resource monitoring and management, 399
security, 263–265
services, 8–11
Storage vMotion, 197–199
system logs, uploading to VMware, 407–408
topology, 8–9
updating, 561–564
vCenter HA
  clusters, 12–13, 24–25, 564–565
  overview of, 161
vCenter Server Agent, 11
vCenter Server Appliance
  compatibility, 524
  migrating vCenter Server for Windows to, 528–530
  patching vCenter Server with, 563–564
  storage sizes, 16–17
  upgrading, 525–527
vCenter Server Appliance Management Interface (VAMI), 225
monitoring/managing vCenter Server with, 550–554
patching vCenter Server with, 561–563
vCenter Server backup with, 518–521
vCenter Single Sign-On, 6, 10, 11
virtual machine cloning, 199–200
virtual machine files
  configuration files, 179
  file structure, 178–179
  snapshot files, 180
  virtual disk files, 180
virtual machine migration, 190–194
virtual machine settings
  advanced options, 189
  compatibility options, 185–187
  hardware devices, 185–187
  options, 188–189
  provisioning type, 188
  VMware Tools, 188
virtual machine snapshots
  behavior of, 183–184
  benefits of, 182–183
  creating/managing, 595–596
  limitations of, 184–185
  overview of, 180–182
  parent, 183
  snapshot files, 180
  use cases, 182
vCenter Server for Windows compatibility, 524
  migrating to vCenter Server Appliance, 528–530
vCenter Single Sign-On, 6, 10, 11, 244
VCF (VMware Cloud Foundation), 27, 226–227
vCloud Director, 27
Virtual Machine Communication Interface (VMCI)
Virtual Machine Component Protection (VMCP), 154, 375
virtual machine disks (VMDKs), 50, 180, 444
Virtual Machine File System. See VMFS (Virtual Machine File System)
virtual machine port groups
distributed, 105
uplink, 105–106
virtual machines. See VMs (virtual machines)
virtual networks, 18
DirectPath I/O, 122, 347
host networking management with vDS
host addition to vDS, 354–355
host removal, 356–357
network adapter management,
355–356
network adapter migration to vDS, 356
networking policies and advanced features, 359–361
port monitoring in distributed port groups, 357
virtual machine migration to vDS, 357
LAGs (link aggregation groups), 350–354
network resource pools, 109–111, 345–346
NIOC (Network I/O Control), 108–109, 344–345
port mirroring, 116, 349–350
PVLANs (private VLANs), 113, 346
SR-IOV (single root I/O virtualization), 123–125, 347–349
vDS (vSphere Distributed Switches)
configuration, 338–341
data center-level management,
113–114
distributed port groups, 105, 341–342, 357
health checks, 119–120
host networking management with,
354–361
LACP (Link Aggregation Control Protocol), 118–119
modifying, 340
network offloads compatibility,
114–115
network policies, 106–112
overview of, 104
port binding and allocation, 117
port mirroring, 116, 349–350
port state monitoring, 115–117
PVLANs (private VLANs), 113
upgrading, 339–340
uplink port groups, 105–106
vSS compared to, 106
VLANs (virtual LANs)
overview of, 97–98
policies, 104
PVLANs (private VLANs), 113, 346
VMkernel networking, 125–126, 342–344
VMware product integration, 232–233
vSS (vSphere Standard Switches)
configuration, 334–336
MTUs (maximum transmission units), 100
network policies, 100–104
overview of, 98–100
standard port groups, 336–338
virtual NICs (vNICs), 96
virtual non-volatile dual in-line memory module (NVDIMM), 187
Virtual Persistent Memory Disk (vPMemDisk), 141, 459
Virtual Persistent Memory (vPMem), 141, 458–459
Virtual Shared Graphics Acceleration (vSGA), 601–603
virtual switches. See vDS (vSphere Distributed Switches); vSS (vSphere Standard Switches)
virtual Trusted Platform Module (vTPM), 23, 277–278
virtual volumes. See vVols (virtual volumes)
virtualization-based security (VBS), 189, 598–599
VLANS (virtual LANs)
overview of, 97–98
policies, 104
PVLANs (private VLANs), 113, 346
vLCM (vSphere Lifecycle Manager), 52
backup and restore scenarios, 545
baselines and images, 536–542
cluster images, importing/exporting, 544–545
configuration, 318–319
ESXi firmware updates, 542–544
ESXi Quick Boot, 542
hardware compatibility checks, 544
overview of, 532–535
remediation settings, 534
terminology for, 539
UMDS (Update Manager Download Service), 535–536
virtual machine upgrades, 546
VMAFD (VMware Authentication Framework Daemon), 241
VMC (VMware Cloud), 27, 231
VMCA (VMware Certificate Authority), 240–241, 298, 307–309
VMCA Mode, ESXi certificates, 245, 481–482
VMCI (Virtual Machine Communication Interface), 187, 272–273
VMCP (Virtual Machine Component Protection), 154
VMDKs (virtual machine disks), 50, 180, 444
vmFork, 201
VMFS (Virtual Machine File System), 17, 524
compatibility, 524
datastores
management of, 441–446
overview of, 39–41
definition of, 36
VM-host affinity rules (DRS), 142
VMkernel networking
configuration, 342–344
overview of, 125–126
TCP/IP networking layer, 18
vmkfstools, 71
vMotion, 7. See also Storage vMotion
EVC (Enhanced vMotion Compatibility), 135–139
Migration service, 229
port state monitoring, 115–116
TCP/IP stack, 125, 194–197
VMRC (VMware Remote Console), 577–578
VMs (virtual machines). See also vSphere
HA
advanced options, 189
cloning, 199–201
cold clones, 199
hot clones, 199
instant clones, 200–201
linked clones, 182, 200
privileges required for, 580–581
compatibility, 185–187, 524, 586
compliance status, 51
configuration, 396
content libraries, 603
adding items to, 608
creating, 604–605
definition of, 604
deploying VMs with, 608–609
managing VM templates in, 609
overview of, 176–178
permissions, 606–607
publishing, 605
subscribing to, 606
synchronization options, 607
converting to templates, 581
CPU affinity, 603
creating, 252, 576–577
definition of, 174
deploying from templates, 253, 582
disk mode settings, 590
distribution of, 140
DRS (Distributed Resource Scheduler)  
- scores, 142
- EVC mode, 603
- files
  - configuration files, 179
  - file structure, 178–179
  - snapshot files, 180
  - virtual disk files, 180
- guest OS, 253, 582
- guest user mapping, 594
- hardware configuration, 586–592
- hardware devices, 185–187
- home namespace, 50
- initial placement of, 140–141
- migration, 190–194, 254, 596–598
- monitoring in vSphere HA clusters, 376
- moving to resource pools, 253
- Open VM Tools, 578
- options, 188–189, 592–593
- OVF/OVA templates, 178
  - adding to content libraries, 608
  - deploying, 585–586
  - editing, 594
  - managing, 598
  - rapid provisioning with, 200–201
  - reverting to previous version, 609
- path failover. See multipathing and failover
- port groups
  - distributed, 105, 341–342
  - standard, 336–338
  - uplink, 105–106
- powering on, 576–577
- provisioning, 188, 589
- resource monitoring and management
  - admission control, 394
  - ESXTOP, 396–399
  - latency sensitivity, 395
  - metrics, 392
  - Microsoft Windows Perfmon, 395
  - shares, limits, and reservations, 392–394
  - vCenter Server Management, 399
- VIMTOP, 399
- VMware Tools, 395
- security
  - common settings, 270–272
  - device connections, 271, 273
  - DoS (denial-of-service) attacks, 272
  - Encrypted vSphere vMotion, 276–277
  - encryption, 273–276, 508–510, 589
  - hardening, 269
  - Intel Software Guard Extensions (SGX), 278–279
  - risk profiles, 272
  - UEFI Secure Boot, 270
  - unexposed features, disabling, 270
  - vTPM (virtual Trusted Platform Module), 277–278
- shutting down guests, 580
- SMP (symmetric multiprocessor), 158
- snapshots
  - behavior of, 183–184
  - benefits of, 182–183
  - creating/managing, 595–596
  - limitations of, 184–185
  - overview of, 180–182
  - parent, 183
  - required permissions, 253
  - snapshot files, 180
  - use cases, 182
- storage, 34, 466
- swap objects, 51
- upgrading, 530, 546
- VBS (virtualization-based security), 598–599
- versions, 587–588
- vGPU (virtual GPU) support, 601–603
- Virtual Intel SGX (vSGX), 507–508
- VMware PowerCLI, 599–601
- VMware Tools, 188
  - installation, 578–580
  - upgrading, 578–580
  - virtual machine options, 189
- vSphere with Tanzu and, 210
.vmsd extension, 184
.vmsn extension, 184
vmtoolsd, 188
VM-VM affinity rules (DRS), 143
VMW_PSP_FIXED, 79
VMW_PSP_MRU, 79
VMW_PSP_RR, 79
VMW_SATP_ALUA, 78
VMW_SATP_DEFAULT_AA, 78
VMW_SATP_DEFAULT_AP, 78
VMW_SATP_LOCAL, 78
VMware App Volumes, 223
VMware Aria. See Aria Suite
VMware Aria Suite. See Aria Suite
VMware Authentication Framework
Daemon (VMAFD), 241
VMware Certificate Authority (VMCA),
VMware Certification, 614
VMware Cloud Assembly, 27
VMware Cloud Foundation (VCF), 27,
226–227
VMware Cloud (VMC), 27, 231
VMware Customer Experience
Improvement Program (CEIP), 530
VMware Directory Service (vmdir), 10, 11,
241, 244
VMware Endpoint Certificate Store
(VECS), 240–241, 298, 307–308
VMware Enhanced Authentication Plug-in,
307
VMware Global Services, 213–214
VMware Hands-on Labs, 613
VMware High-Performance Plug-in (HPP),
45–46
VMware Horizon, 171, 201, 222–223
VMware Hybrid Cloud Extension (HCX),
229–231
VMware Identity Manager (vIDM), 219
VMware iSER adapter, 454
VMware NMP (Native Multipathing Plug-in),
76–77
PSPs (Path Selection Plug-ins), 78–79
SATPs (Storage Array Type Plug-ins),
77–78
VMware NMP, 76–77
VMware NSX, 18, 26, 280–281
VMware NSX-T, 232
VMware NVMe. See NVMe (Non-Volatile
Memory Express)
VMware PowerCLI, 51, 599–601
VMware product integration
Aria Suite
Aria Automation, 218–219
Aria for Logs, 217–218
Aria Operations, 216–217
Aria Operations for Networks,
220–221
Aria Orchestrator, 219–220
cloud computing
Azure VMware Solution, 231
HCX (Hybrid Cloud Extension),
229–231
VCF (VMware Cloud Foundation),
227–229
VMC (VMware Cloud) on AWS, 231
desktop and application virtualization
App Volumes, 223
Horizon, 222–223
networking and security, 232–233
opening consoles to, 577–578
replication and disaster recovery
SRM (Site Recovery Manager),
226–227
vSphere Replication, 224–226
VMware NSX Data Center (NSX),
232–233
VMware NSX-T Data Center (NSX-T),
232–233
vSphere add-ons
overview of, 208
vCenter Converter (Converter
Standalone), 214–215
VMware SkyLine, 215–216
vSphere Replication, 215
vSphere with Tanzu, 208–213, 521–523
vSphere+213–214
VMware Remote Console (VMRC), 577–578
VMware Service Broker, 27
VMware Service Lifecycle Manager, 161–162
VMware Skyline, 215–216
Skyline Advisor, 392
Skyline Health, 390–391
VMware Tools, 153, 188, 189, 221
compatibility, 524
configuration, 324
installation, 578–580
lifecycle management, 579
performance counters, 272
upgrading, 578–580
virtual machine monitoring and management, 189, 395
VMware vCenter Agent (vpxa), 259
VMware vCloud Director, 27
VMware vCloud Suite, 27
VMware vSphere 8 STIG Readiness Guide, 484
VMware Workspace ONE Access, 222
VMWARE_HTTPSPROXY environment variable, 578
VMwareAccepted VIBs, 498
VMwareCertified VIBs, 498
VMware-I/O Vendor Program (IOVP), 75
VMX files, 179, 271
vmx.log.guest.level option, 579
vNICs (virtual NICs), 96
vobd, 547
vPMem (Virtual Persistent Memory), 141, 458–459
vPMem (Virtual PMem), 458–459
vPMemDisk (Virtual Persistent Memory Disk), 141, 459
vpxd certificate store, 244
vpxd-extension certificate store, 244
vpxuser, 499
vRealize Suite. See Aria Suite
vRLI (vRealize Log Insight), 411–412
VRMS (vSphere Replication Management Service), 24, 225
VRS (vSphere Replication Service), 24, 225
vSAN. See also vSphere HA
benefits of, 47–48
best practices, 68
boot devices and, 68
characteristics of, 48–50
clusters
creating with Quickstart, 419
encryption in, 61, 434–437
expanding, 424–426
extending across two sites, 428–430
managing devices in, 430–432
requirements for, 67
space efficiency in, 58–60, 433
standard, 53
stretched, 55–58
two-host, 54
compatibility, 524
datastores
overview of, 43
types of, 50
viewing, 422
deployment, 53–58
disabling, 423
disk version, 524
DRS (Distributed Resource Scheduler)
automation modes, 139
description of, 7
evacuation workflow, 141
memory metric for load balancing, 140
migration sensitivity, 143–144
network-aware DRS, 140
NVM (non-volatile memory) support, 141
Predictive DRS, 156, 374
recent enhancements, 139–142
resource pools, 144–148
rules, 142–143
virtual machine distribution, 140
vSphere

virtual machine initial placement, 140–141
virtual machine scores, 142
ESA (Express Storage Architecture), 63
Health, 52
licenses, 67–68, 421–422
limitations of, 58
logging, 68
Maintenance Mode, 426–428
management and configuration, 86
cluster creation, 419
cluster expansion, 424–426
datastores, 422
deployment with vCenter Server, 424
disabling of vSAN, 423
disk/device management, 430–432
encryption, 434–437
fault domains, 428
File Service, 439–440
licensing, 421–422
Maintenance Mode, 426–428
manually enabling vSAN, 420–421
policies, 437–438
preparation, 418
settings, 421
shutdown and restart, 424
space efficiency, 433
storage providers, viewing, 439
stretched clusters, 428–430
vSAN and vSphere HA, 422–423
manually enabling, 420–421
memory consumption, 66
new features in, 52–53
objects and components, 50
Observer, 51–52
OSA (Original Storage Architecture), 47
overview of, 7, 47–48
planning and size, 63–64
policies, 69
configuration, 437–438
storage, 81–83
preparing for, 418
Ready Node, 52
requirements for, 25–26, 63–68
shutting down/restarting, 424
storage providers, viewing, 439
terminology for, 50–52
vDFS (vSAN Distributed File System), 61–62
vsan.unmap_support –enable command, 433
vSGA (Virtual Shared Graphics Acceleration), 601–603
vSGX (virtual Intel SGX), 278
vSphere. See also individual components
add-ons
overview of, 208
vCenter Converter (Converter Standalone), 214–215
VMware Skyline, 215–216
vSphere Replication, 215
vSphere with Tanzu, 208–213, 521–523
vSphere+213–214
components overview, 6–8
editions and licenses, 8–9
infrastructure requirements
compute and system, 14–16
high availability, 6, 24–25
network, 17–21
for optional components and add-ons, 23–24
SDDC (software-defined data center), 25–26
storage, 16–17
supporting infrastructure services, 21–23
vSphere replication, 6, 24
installation of. See vSphere installation inventory, 171–173
management of. See vSphere manage-
ment resources. See resource management security. See security
upgrading to vSphere 8.0, 523–531
ESXi, 530
Update Planner, 530–531
vCenter Server 7.0 compatibility, 524
vCenter Server Appliance, upgrading, 525–527
vCenter Server data transfer, 524–525
vCenter Server for Windows, migrating to vCenter Server Appliance, 528–530
VMs (virtual machines), 530
virtualization, 26–27
vSphere APIs for Array Integration (VAAI), 70–72
vSphere APIs for I/O Filtering (VAIO), 70, 275
vSphere APIs for Storage Awareness (VASA), 69–70, 463–465
vSphere Authentication Proxy, 260, 500
vSphere Certificate Manager utility backup store (BACKUP_STORE), 308
vSphere Client. See also clusters; vDS (vSphere Distributed Switches); vSS (vSphere Standard Switches)
certificates, 479–480
configuration, 318
data center-level management, 113–114
monitoring/managing vCenter Server with
common management tasks, 555–557
SSL certificate verification for legacy hosts, 561
statistics collection settings, 558–560
vCenter Server, repointing to another domain, 565–569
vCenter Server updates, 561–564
path management with, 461–462
physical switch information, viewing, 121
port state monitoring, 115–117
vSphere Cluster Services (vCLS), 135
vSphere clusters. See clusters
vSphere Distributed Services Engine (vDSE), 114
vSphere Distributed Switches. See vDS (vSphere Distributed Switches)
vSphere DRS. See DRS (Distributed Resource Scheduler)
vSphere Fault Tolerance. See FT (Fault Tolerance)
vSphere HA, 148–155
admission control, 151–152
advanced options, 153
benefits of, 148–149
capacity reservation, 423
cluster configuration
admission control, 375
advanced options, 374
cluster creation, 374
FT (Fault Tolerance), 377
Proactive HA, 376
Proactive HA (High Availability), 7, 155, 376
VCMP (Virtual Machine Component Protection), 375
virtual machine and application monitoring, 376
description of, 7
heartbeats, 151
requirements for, 149–150
response to failures, 150
vSAN and, 422–423
vSphere Health, 52
vSphere installation
ESXi hosts, 290–301
Auto Deploy, 296–301, 493
interactive installation, 290–292
scripted installation, 292–296
Identity Federation, 316–318
initial configuration
advanced ESXi host options, 325–327
common ESXi host settings, 324–325
host profiles, 321–323
vCenter Server inventory, 319–321
vLCM (vSphere Lifecycle Manager), 318–319
VMware Tools, 324
vSphere Client, 318
SSO (single sign-on)
Active Directory identity sources, 311–313
LDAP identity sources, 313
overview of, 309–310
policies, 315–316
SSO identity sources, 310
users, enabling/disabling, 314–315
vCenter Server components
PSC (Platform Services Controller), 301–302
center Server database, 301
VCSA (vCenter Server Appliance), 302–307
VMCA (VMware Certificate Authority), 307–309
VIB (vSphere Installation Bundle), 298
acceptance levels, 497–498
definition of, 539
metadata, 539
standalone, 539
vSphere Installation Bundle (VIB), 298
acceptance levels, 497–498
definition of, 539
metadata, 539
standalone, 539
vSphere Lifecycle Manager. See vLCM (vSphere Lifecycle Manager)
vSphere management. See also vCenter Server
backup and recovery with vSphere with Tanzu, 208–213, 521–523
ESXi hosts, 547–549
resource management
alarms, 402–405
client performance charts, 377, 379–383
cluster resources, 388–389
events, 400–402
host resources and health, 390–391
logging, 405–412
metrics, 378
pool resources, 389–390
troubleshooting and optimization, 383–387
vCenter Server resources, 399
virtual machine resources, 392–399
upgrading to vSphere 8.0, 523–531
ESXi, 530
Update Planner, 530–531
vCenter Server 7.0 compatibility, 524
vCenter Server Appliance, 525–527
vCenter Server data transfer, 524–525
vCenter Server for Windows, migrating to vCenter Server Appliance, 528–530
VMs (virtual machines), 530
vCenter Server backup, 518–521
vLCM (vSphere Lifecycle Manager), 532–546
vSphere Pods, 212
vSphere Replication Management Service (VRMS), 24, 225
vSphere Replication objects, 53
vSphere Replication Service (VRS), 24, 225
vSphere Standard Switches. See vSS (vSphere Standard Switches)
vSphere Trust Authority (vTA), 263, 504–506
vSphere Virtual Machine Encryption Certificates, 244
vSphere with Tanzu, 208–213, 521–523
vSphere+213–214
tphere-webclient certificate store, 244
vSS (vSphere Standard Switches)
configuration, 334–336
MTUs (maximum transmission units), 100
network policies, 100–104
overview of, 98–100
standard port groups, 336–338
vDS compared to, 106
vTA (vSphere Trust Authority), 263, 504–506
vTPM (virtual Trusted Platform Module), 23, 277–278
vVols (virtual volumes), 53, 72–75
datastores, 43
definition of, 39
management and configuration, 466–468

W
Wake-on-LAN (WoL), 156–157
WAN Optimization service, VMware
   Hybrid Cloud Extension, 229
wcp certificate store, 244
web proxies, ESXi web proxy settings, 492
Windows Server failover clusters (WSFCs), 49, 444
Windows session authentication, 474–479
Witness node, vCenter HA clusters, 12–13
witnesses, 51
WoL (Wake-on-LAN), 156–157
worldwide names (WWNs), 189
Write Same (Zero), 71
WSFCs (Windows Server failover clusters), 49, 444
wsman, 547
WWNs (worldwide names), 189

X-Y-Z
XaaS (anything as a service), 219
XCOPY (Extended Copy), 71
X.Org Server, 259
zeroing out files, 81