VDCA550 Exam Preparation

This appendix contains information to prepare the reader for taking and passing the VDCA550 exam, which is a new exam that can be used to qualify a candidate for VCAP5-DCA certification. You should use this appendix after first reading the VCAP5-DCA Cert Guide and applying its advice to gain hands-on experience with the specific administrative tasks it describes. You should use this appendix prior to taking Practice Exam 3, which reflects the VDCA550 exam blueprint.

Introduction

VMware recently announced a new exam that can be used to qualify students for VCAP5-DCA. The new exam, which is based on VMware vSphere 5.5, is identified as exam code VCDA550. The previous exam, which is based on VMware vSphere 5.0 and 5.1, is identified as VDCA-510. Either exam can be used to qualify for VCAP5-DCA. Students have a choice as to which exam to take. For example, you may prefer to take the VCAP510 if you have no actual experience or training on vSphere 5.5. Or, if you recently upgraded to vSphere 5.5 and are just beginning to prepare for the VCAP-5-DCA exam, then you might prefer to take VCDA550. In either case, you should use the *VCAP5-DCA Exam Cert Guide* to prepare for the exam. If you plan to take the VDCA550 exam, then you should also use this appendix.

This appendix can be used to complete your preparation for the recently released VCDA550 exam, whose blueprint was not available while the Cert Guide was being written. It provides information on each exam objective and required skill from the VDCA550 exam blueprint, such as a reference to the corresponding Cert Guide chapter and section. This appendix addresses the new items covered in the VDCA550 exam blueprint that are not covered in the VDCA510 exam blueprint, such as new features in vSphere 5.5. It also addresses the items that are covered in more detail in the new blueprint.

To prepare for the VDCA550 exam, first use the Cert Guide in the normal fashion, and then use this appendix to complete your preparation for the VDCA550 exam. Do not simply rely on this appendix, which is intended to

just focus on the differences between the exams. You should not ignore any items that are listed in the VDCA510 exam blueprint but are not explicitly listed in the VDCA550 exam blueprint. You should first ensure that you understand all the concepts described in the Cert Guide and verify that you can perform the related administrative tasks from memory. Then use this appendix. With this approach, you should already feel comfortable with all the items in this appendix that simply provide *Cert Guide References* because the items are well covered in the Cert Guide. (Feel free to return to the Cert Guide and review the referenced materials, if desired.) You should focus on the items in this appendix that provide a "New Material" section because they contain details on the new vSphere 5.5 features and areas covered in more depth in the new blueprint. For these items, you should spend time using this appendix to learn the concepts and to practice performing the related administrative tasks, prior to taking the practice exams. Practice Exams 1 and 2 contain material that applies to both versions of the exam. Practice Exam 3 does also, but it includes extra exercises that are specific to the VDCA550 exam. It also contains exercises that require the vSphere Web Client.

The authors chose to organize the content of the Cert Guide in a manner based on major areas involving vSphere administration. Its organization is intended to facilitate learning rather than to match the organization of either the VDCA510 blueprint or the VDCA550 blueprint. This appendix is organized identically to the VDCA550 exam blueprint and provides references to the specific, corresponding sections in the Cert Guide.

The Cert Guide states that you should practice performing steps using the vSphere Web Client as well as the vSphere Client (thick client), but it uses the vSphere Client to provide examples. This appendix provides many examples for using the vSphere Web Client, which is required for many new features. To get familiar with using the vSphere Web Client, refer to the online Appendix D, "Using the VMware vSphere Web Client," prior to reading the remainder of this appendix.

If you are strong in vSphere 5.1 but new to version 5.5, briefly read the What's New in VMware vSphere 5.5 Platform guide at http://www.vmware.com/files/pdf/vsphere/VMware-vSphere-Platform-Whats-New.pdf. Then use this appendix to prepare for the VDCA550 exam.

Objective 1.1—Implement Complex Storage Solutions

Determine use cases for and configure VMware DirectPath I/O

Cert Guide References:

- Chapter 3—VMware DirectPath I/O

Determine requirements for and configure NPIV

Cert Guide References:

- Chapter 3—N-Port ID Virtualization

Understand use cases for Raw Device Mapping (RDM)

Cert Guide References:

- Chapter 3—Virtual Disk Format Types

New Material:

The maximum size of a RDM in virtual compatibility mode is increased from 2 TB minus 512 bytes to 62 TB (just as the maximum size for a virtual disk file [VMDK] is increased in vSphere 5.5). The maximum size for a RDM in physical compatibility mode remains at 2 TB minus 512 bytes.

Configure vCenter Server storage filters

Cert Guide References:

- Chapter 3—vCenter Server Storage Filters

Understand and apply VMFS re-signaturing

Cert Guide References:

- Chapter 4—Troubleshoot Storage Snapshot and Resignaturing Issues

Understand and apply LUN masking using PSA-related commands

Cert Guide References:

- Chapter 3—LUN Masking Using PSA-related commands
- Chapter 4—Troubleshoot Storage Performance and Connectivity—Use ESXCLI Commands to Troubleshoot Multipathing and PSA-related Issues
- Chapter 10—Scenario 10-1

Configure Software iSCSI port binding

Cert Guide References:

- Chapter 3—Configure Software iSCSI Port Binding
- Chapter 10—Scenario 10-3

Configure and manage vSphere Flash Read Cache

Cert Guide References: Not covered (new feature in 5.5).

New Material:

A new Flash-based storage solution in vSphere 5.5 is called vSphere Flash Read Cache. It provides performance enhancement of read-intensive applications by providing a write-through cache for virtual disks. It uses the Virtual Flash Resource, which can be built on Flash-based, solid-state drives (SSDs) that are installed locally in the ESXi hosts.

The Virtual Flash Resource (also called the Virtual Flash Cache or simply Virtual Flash) can be used to provide resources for both the Virtual Flash Read Cache and Virtual Flash Host Swap Cache. The Virtual Flash Read Cache is used by the hypervisor to cache data between virtual machines and virtual disks. The Virtual Flash Host Swap Cache is used by the hypervisor to cache data for virtual machine swap (VSWP) files. ESXi hosts use the natively provided, hypervisor-based Virtual Flash Software (also called the Virtual Flash Device) to track which portions of a virtual disk are currently cached.

The Virtual Flash Resource uses a unique file system called the Virtual Flash File System (VFFS), which is new in ESXi 5.5. It is a derivative of VMFS that is optimized for SSDs and is used to group SSDs into a single caching pool. It is a non-persistent file system on which virtual machines cannot be built. VFFS supports up to 8 Flash-based devices per ESXi host and up to 4 TB per device, which means it supports a maximum of 32 TB per ESXi host.

To configure vSphere Flash Resource, use the vSphere Web Client to navigate to **Hosts and Clusters** and perform the following steps:

1. Select the ESXi host.
2. Select **Manage** > **Settings** > **Virtual Flash** > **Virtual Flash Resource Management** as shown in Figure C.1.
3. Click the **Add Capacity** button.
4. In the list of available SSD devices, select an SSD device to add to the ESXi host's Virtual Flash Resource and click **OK**.

5. Examine the contents of the **Device Backing** section and verify that the selected SSD devices appear in the list.

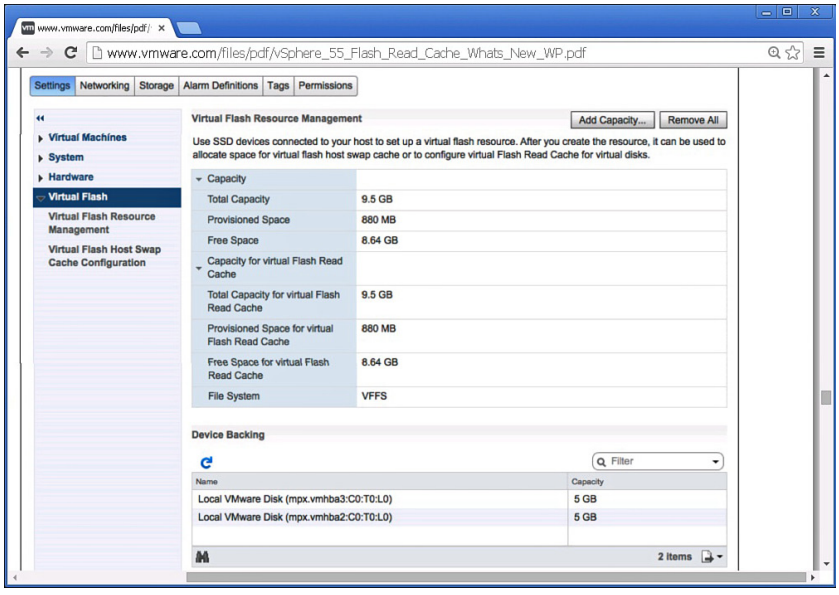

Figure C.1

To configure a virtual machine with a vSphere Flash Read Cache, the following steps can be used:

1. Use the vSphere Web Client to locate the virtual machine.
2. Right-click the virtual machine and select **Edit Settings**.
3. Select and expand the hard disk to which you want to assign the Flash Read Cache—for example, Hard disk 1.
4. Enter the amount of **Flash Read Cache** to assign to the virtual hard disk (vmdk) as shown in Figure C.2.
5. Optionally, select **Virtual Flash Read Cache** > **Advanced** and use the dialog box to set the **Reservation** and **Block Size** for the Virtual Flash Read Cache as shown in Figure C.3.
6. Click **OK**.
7. Optionally, repeat the last couple of steps for other virtual disks used by the virtual machine.

To disable vSphere Flash Read Cache for a virtual machine, use the previous steps, but set the amount of Flash Read Cache to zero for each virtual disk.

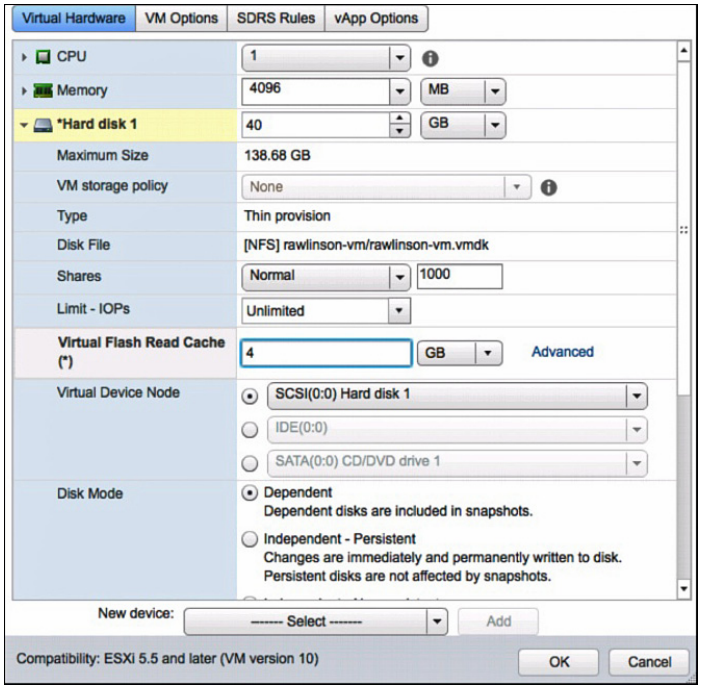

Figure C.2

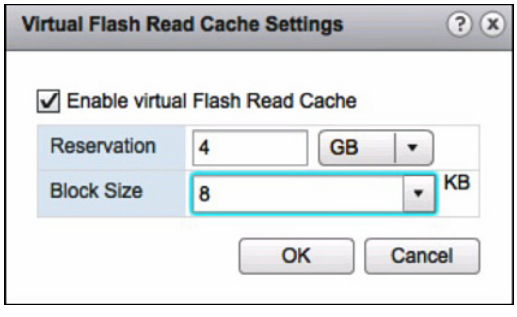

Figure C.3

The virtual flash read cache is created for a VM when it is powered on and destroyed when it is powered off. The virtual flash read cache for a VM is write-through. The size of the cache can be changed on a running VM, but it actually causes the old cache to be dropped and a new cache to be built, requiring a warming period for the new cache. Read-intensive applications should benefit from virtual flash read cache. Write performance in applications could indirectly benefit due to reduced I/O to the datastore where the virtual disk resides.

Virtual Flash Read Cache can only be built on the Virtual Flash Resource, which can only be built on locally attached SSD. It can be used to cache virtual disks that are stored on any VMFS datastore, regardless of the underlying storage type. It can also be used to cache virtual disks provided by NFS and raw device mappings (RDMs) in virtual compatibility mode, but it cannot be used to cache RDMs in physical compatibility mode. No SSD can be used for both Virtual Flash Resource and VSAN. The allocation of Virtual Flash Read Cache resources is handled by reservations only, not by shares. Reservations can be set per virtual disk.

The Host Swap Caches is not equivalent to placing VM swap (VSWP) files on SSD. Instead, the Host Swap Cache provides an SSD-backed cache for all VM swap files running on the host. It is a write back cache that enables some of the active VM swapping to be served by the cache rather than the swap file. It does not remove the requirement to utilize swap files for the VMs, but it makes VM swapping more efficient. It may provide similar performance to placing VM swap files on SSDs whenever swapping is light. It requires much less SSD storage than placing all VM swap files on SSDs.

The Host Swap Cache for an ESXi host can be configured on specific SSD-backed datastores or on the Virtual Flash Read Cache. To configure the Host Swap Cache for an ESXi host to use a Virtual Flash Read Cache, use these steps:

1. In the vSphere Web Client, open the **Hosts and Clusters** view and navigate to the ESXi host.
2. Click the **Manage** tab and click **Settings**.
3. Under Virtual Flash, select **Virtual Flash Host Swap Cache Configuration** and click **Edit**.
4. Select the **Enable virtual flash host swap cache** option.
5. Specify the amount of space to use for **Virtual Flash Host Swap Cache**, as shown in Figure C.4.
6. Click **OK** to apply the changes.

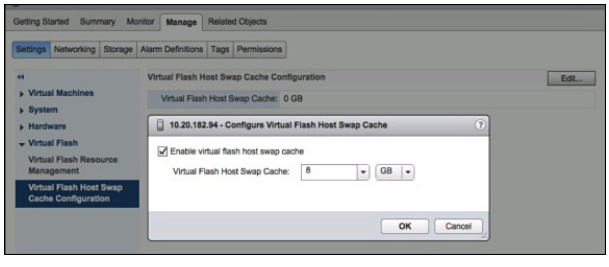

Figure C.4

To configure the Host Cache for an ESXi host to use an SSD-backed datastore, use these steps:

1. Ensure that at least one SSD-backed datastore is available for the ESXi host.
2. Select the ESXi host in the **Host and Clusters** view.
3. Select **Manage** > **Storage** > **Host Cache Configuration**.
4. Select the datastore in the list and click the **Allocate space for host cache** icon.
5. Select a size for the host cache allocation on the drive.
6. Click **OK**.

When using the vSphere Web Client to migrate VMs that are utilizing Virtual Flash Read Cache, you can choose from two options for handling the cache as shown in Figure C.5:

- **Always migrate the cache contents**—This option guarantees that the migration proceeds only if the contents of the cache can be migrated to the target ESXi host with the VM
- **Do not migrate the cache contents**—This option drops the contents of the cache, requiring it to rewarm on the target ESXi host.

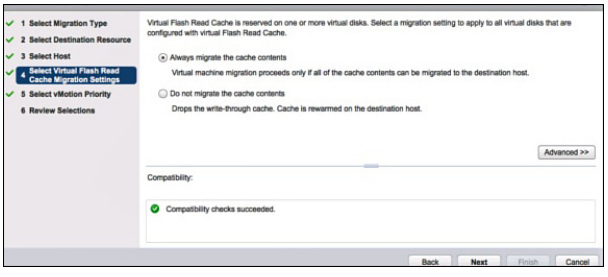

Figure C.5

Configure Datastore Cluster

Cert Guide References:

- Chapter 3—VMware Storage DRS—Storage DRS Configuration
- Chapter 10—Scenario 10-2

Upgrade VMware storage infrastructure

Cert Guide References:

- Chapter 3—Upgrading VMware Storage Infrastructure

New Material:

A known issue involving ESXi hosts that accessed more than 30 TB of open files was addressed in vSphere 5.0 and 5.1 by using a larger VMFS heap size. In vSphere 5.5, the heap eviction process is improved, which eliminates the need for the larger heap size. This allows the heap to use less memory in vSphere 5.5, which can access the entire 64 TB address space of a 64 TB VMFS datastore using a 256 MB heap.

Objective 1.2—Manage Complex Storage Solutions

Analyze I/O workloads to determine storage performance requirements

Cert Guide References:

- Chapter 4—Tune and Optimize vSphere Performance—Tune ESXi Host Storage Configuration
- Chapter 3—Optimize Virtual Machine Resources—Tune Virtual Machine Storage Configurations

Identify and tag SSD and local devices

Cert Guide References:

- Chapter 3—Identifying and Tagging SSD Devices

Administer hardware acceleration for VAAI

Cert Guide References:

- Chapter 3—VAAI Hardware Acceleration

Configure and administer profile-based storage

Cert Guide References:

- Chapter 3—Configuring and Administering Profile-based Storage

New Material:

A new feature in VMware vSphere 5.5 is VM Storage Policies. Actually, the VM Storage Profile feature in vSphere 5.1 has been renamed and extended to provide the VM Storage Policies feature in vSphere 5.5. VM storage policies can be used during VM provisioning to ensure that the virtual disks are placed on proper storage. VM storage policies can be used to facilitate the management of the VM, such as during migrations, to ensure that the VM remains on compliant storage. A VM storage profile is a set of storage capabilities (tags) that can be associated with a set of virtual machines. Storage capabilities are used to define the performance and other characteristics of the storage on which a datastore resides. Storage capabilities can be automatically assigned by a storage provider (vendor-specific storage capabilities) or manually assigned using abstract tags (user-defined storage capabilities).

You can use VM storage policies to define the storage requirements for a VM. Multiple policies can be applied to a single VM to define unique requirements for the VM's home files (such as the VMX file) and virtual disk files. You can check virtual machines for compliance with their storage policies. If some of its files are stored in datastores that do not meet the requirements of the associated policy, then the virtual machine is not storage compliant.

If you are familiar with VM Storage Profiles in vSphere 5.1, you will likely find that VM Storage Policies in vSphere 5.5 is similar but provides more flexibility. Basically, the term *policy* replaces the term *profile* and the term *storage tag* is used interchangeably with the term *user-defined storage capability*. The main reason for the changes appears to be to accommodate the new Virtual SAN feature, which provides VM storage policies for capacity, availability, and performance.

Storage capabilities, which are well defined in the Cert Guide *(Chapter 3*—section *Configuring and Administering Profile-based Storage)*, can be used to identify capacity-, availability-, and performance-related characteristics of the storage. For example, a specific storage provide may automatically identify the speed or bandwidth of each storage device.

To enable VM Storage Policies for hosts or clusters, use the vSphere Web Client and follow theses steps:

1. Select the **VM Storage Policies icon** in the Home page as shown in Figure C.6.
2. Select the button to **Enable VM storage policies** as shown in Figure C.7.

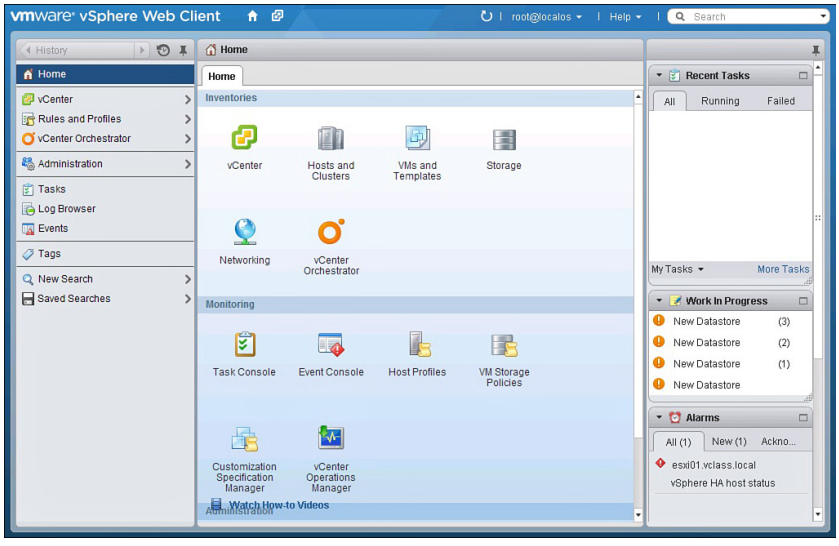

Figure C.6

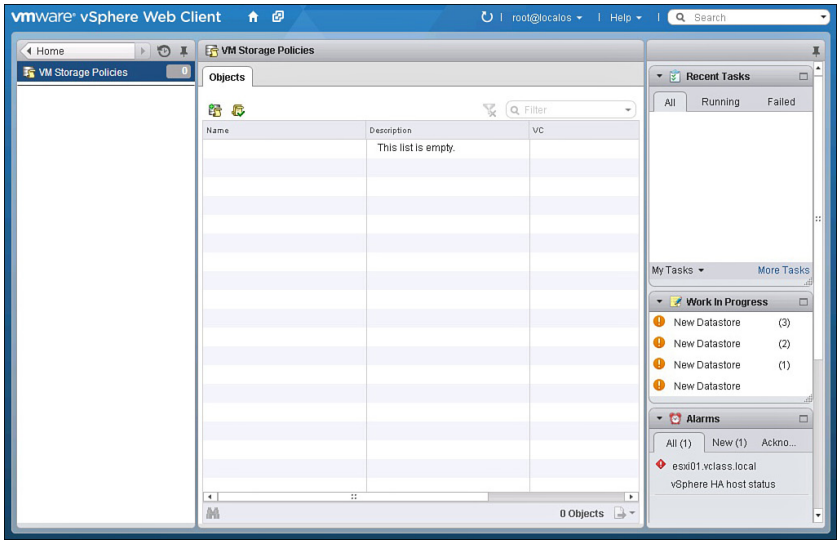

Figure C.7

3. Select the desired hosts or clusters and click the **Enable** button as shown in Figure C.8.

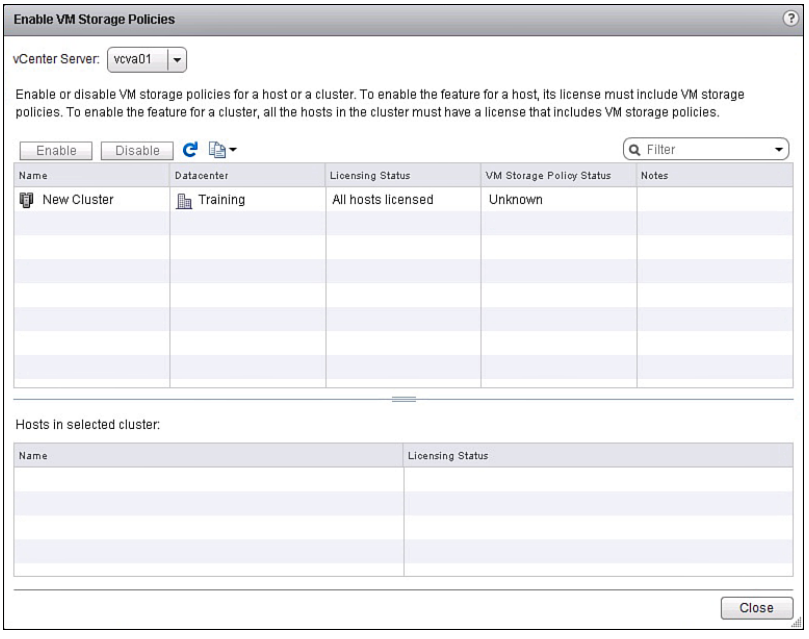

Figure C.8

Verify that the **VM Storage Policy Status** now indicates *Enabled* for the selected hosts and clusters.

To create user-defined storage capabilities, which are also called storage tags, you can use the following steps:

1. Use the vSphere Web Client to select **Home** > **Storage**.
2. Select a datastore in the inventory and select **Manage** > **Tags**.
3. Select a datastore in the inventory and select **Manage** > **Tags** as shown in Figure C-9.
4. For **Category**, select *New Category* in the drop-down menu.
5. Provide a **Name**, such as *15K*.
6. Provide a **Category Name**, such as *Storage Capabilities*.
7. Click **OK**.

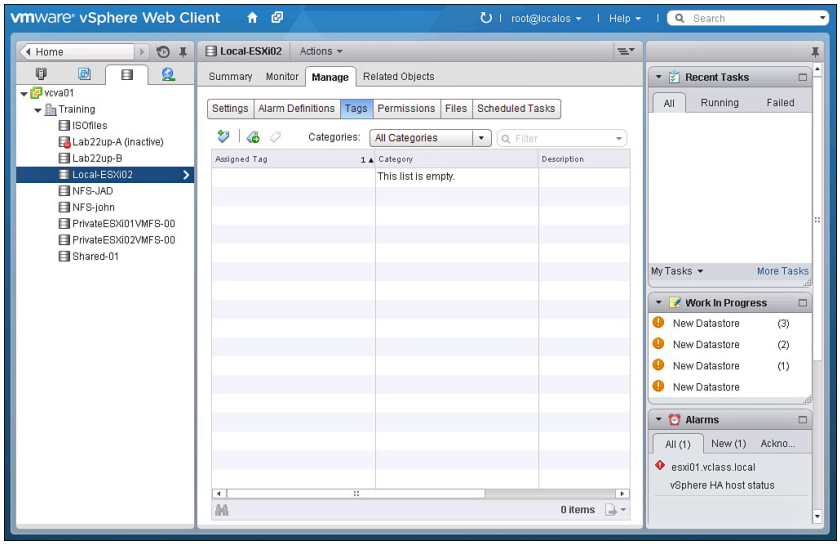

Figure C.9

When creating additional storage tags, you can use the same procedure, except simply select the *Storage Capabilities* category rather than New Category.

To create a VM Storage Policy, you can use the following steps:

1. Use the vSphere Web Client to navigate to **VM Storage Policies**.
2. Click the **Create a new VM storage policy** icon as shown in Figure C.10.

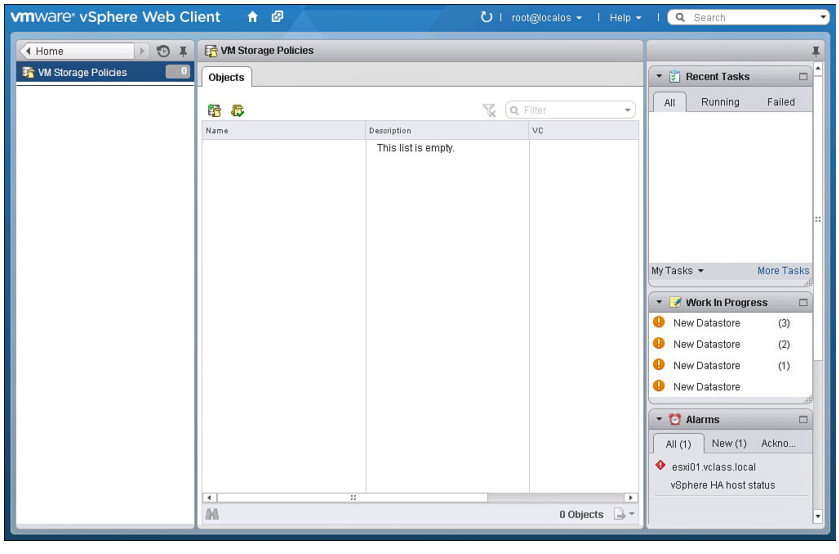

Figure C.10

3. Provide a name for the policy, such as *Tier-1*. Click **Next**.
4. Click **Add tag-based rule**.
5. Select the proper category from the **Categories** drop-down menu, such as 15K, as shown in Figure C.11.

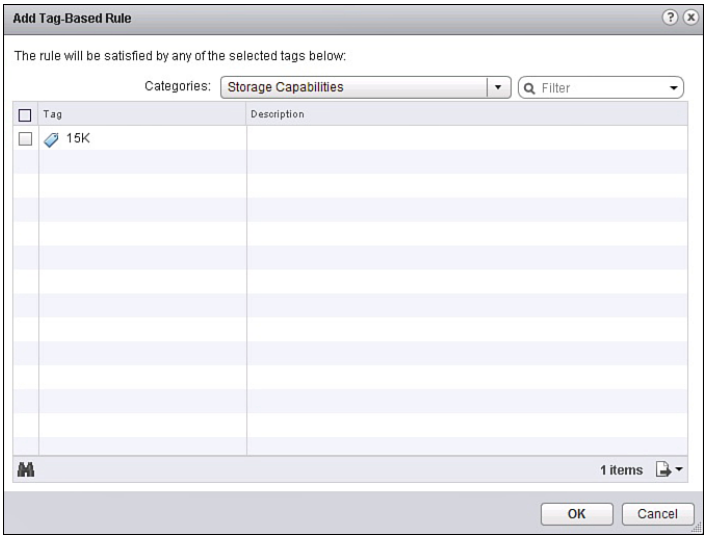

Figure C.11

6. Click **OK** and click **Next**.
7. Verify that the appropriate datastores are listed and click **Finish**.

To assign a storage policy to a VM during provisioning, on the **Select Storage** page of the **New Virtual Machine** wizard, set the **VM Storage Policy** to the desired policy and select one of the datastores in the **Compatible** section.

To check for compliance for a VM Storage Policy, the following steps can be used:

1. Use the vSphere Web Client to select **Home** > **VM Storage Policies**.
2. Select a policy and select **Summary** > **Check Compliance**.

Prepare storage for maintenance

Cert Guide References:

- Chapter 3—Preparing Storage for Maintenance

Apply space utilization data to manage storage resources

Cert Guide References:

- Chapter 4—Troubleshoot Storage Performance and Connectivity
- Chapter 5—VMware Storage DRS
- Chapter 10—Scenario 10-2

Provision and manage storage resources according to virtual machine requirements

Cert Guide References:

- Chapter 3—Virtual Disk Format Types
- Chapter 3—DirectPath I/O
- Chapter 4—Troubleshoot Storage Performance and Connectivity
- Chapter 5—VMware Storage DRS

Understand interactions between virtual storage provisioning and physical storage provisioning

Cert Guide References:

- Chapter 3—Virtual Disk Format Types
- Chapter 4—Troubleshoot Storage Performance and Connectivity

Configure datastore alarms

Cert Guide References:

- Chapter 3—Configuring Datastore Alarms
- Chapter 10—Scenario 10-2

Create and analyze datastore alarms and errors to determine space availability

Cert Guide References:

- Chapter 3—Configuring Datastore Alarms
- Chapter 4—Troubleshooting Storage Performance and Connectivity—Analyze Log Files to Identify Storage and Multipathing Problems.
- Chapter 10—Scenario 10-2

Objective 1.3—Troubleshoot complex storage solutions

Perform command-line configuration of multipathing options

Cert Guide References:

- Chapter 4—Troubleshoot Storage Performance and Connectivity—Use ESX-CLI Commands to Troubleshoot Multipathing and PSA related Issues

Change a multipath policy

Cert Guide References:

- Chapter 3—Installing and Configuring PSA Plugins
- Chapter 3—Multipathing Policies

Troubleshoot common storage issues

Cert Guide References:

- Chapter 4—Troubleshooting Storage Performance and Connectivity
- Chapter 10—Scenario 10-19

New Material:

A new tool was introduced in vSphere 5.1 but is not mentioned in the Cert Guide or either blueprint—the Sphere On-disk Metadata Analyzer (VOMA), which can be used to check VMFS metadata consistency. When used, VOMA should be run against a partition containing a VMFS datastore. Prior to running VOMA against a partition, ensure that you stop all running VMs in the datastore and unmount the datastore from all ESXi hosts. Then run VOMA tool using a command that identifies the partition to be analyzed and the name of a text file to export the results. For example, the following command can be use to analyze the first partition on a storage device whose NAA ID is *naa.6000d771000020f30f1ac91fb1053941* and to store its results in a file named analysis.txt

```
voma -m vmfs -d /vmfs/devices/disksnaa.6000d771000020f30f1ac91
fb1053941:1 -s /tmp/analysis.txt
```

Objective 2.1—Implement and manage virtual standard switch (vSS) networks

Create and manage vSS components

Cert Guide References:

- Chapter 2—Implement and Manage Complex Networks—Overview

Create and manage vmkernel ports on standard switches

Cert Guide References:

- Chapter 2—Implement and Manage Complex Networks—Overview
- Chapter 10—Scenario 10-4

Configure advanced vSS settings

- Chapter 2—Implement and Manage Complex Networks—Configure Virtual vSwitches Using CLI Commands
- Chapter 2—Identify NIC Teaming Policies

Objective 2.2—Implement and manage virtual distributed switch (vDS) networks

Determine use cases for and apply VMware DirectPath I/O

Cert Guide References:

- Chapter 3—VMware DirectPath I/O

Migrate a vSS network to a hybrid or full vDS solution

Cert Guide References:

- Chapter 2—Migrate from Standard to Distributed Virtual Switches

Configure vSS and vDS settings using command-line tools

Cert Guide References:

- Chapter 2—Implement and Manage Complex Networks—Configure Virtual Switches Using CLI Commands
- Chapter 10—Scenario 10-4

Analyze command-line output to identify vSS and vDS configuration details

Cert Guide References:

- Chapter 2—Implement and Manage Complex Networks—Configure Virtual Switches Using CLI Commands
- Chapter 4—Use net-dvs to Troubleshoot vSphere Distributed Switch Configurations

Configure NetFlow

Cert Guide References:

- Chapter 2—Implement and Manage Complex Networks—Configure NetFlow

Determine appropriate discovery protocol

Cert Guide References:

- Chapter 2—Implement and Manage Complex Networks—Discovery Protocols

Determine use cases for and configure PVLANs

Cert Guide References:

- Chapter 2—Configure and Maintain VLANS and PVLANs—Types of VLANS and PVLANs
- Chapter 2—Configure and Maintain VLANS and PVLANs—Determine Use Cases for PVLAN Trunking
- Chapter 10—Scenario 10-5

Use command-line tools to troubleshoot and identify VLAN configurations

Cert Guide References:

- Chapter 2—Configure and Maintain VLANS and PVLANs—Command Tools to Troubleshoot and Identify VLAN configurations

Objective 2.3—Troubleshoot virtual switch solutions

Understand the NIC Teaming failover types and related physical network settings

Cert Guide References:

- Chapter 2—Deploy and Maintain Scalable Virtual Networking—Identify NIC Teaming Policies

New Material:

VMware vSphere 5.5 provides Link Aggregation Control Protocol (LACP) enhancements. It allows up to 64 link aggregation groups (LAGs) per ESXi host and per distributed virtual switch. LACP can be configured on the uplinks on distributed virtual switches. VMware support for dynamic LACP begins with vSphere 5.1 on distributed virtual switches. It can be configured only using the vSphere Web Client.

To configure LACP on uplink port groups using the vSphere Web Client, you can use the following steps as explained in VMware KB Article 2034277:

1. Use the **Networking** view to select the distributed virtual switch.
2. Select **Related Objects** > **Uplink Port Groups**.
3. Select the Uplink port group.
4. Select **Manage** > **Settings**.
5. Click the **Edit** button and use the interface to enable LACP and set the **LCAP Mode** to either *Active* or *Passive*.
6. Click **OK**.

Another new LACP feature in vSphere 5.5 is support for all LACP load-balancing types. In vSphere 5.1, only IP Hash-based load balancing is supported, but in vSphere 5.5 the following load-balancing types are supported:

- Destination IP address
- Destination IP address and TCP/UDP port
- Destination IP address and VLAN
- Destination IP address, TCP/UDP port, and VLAN
- Destination MAC address
- Destination TCP/UDP port
- Source IP address
- Source IP address and TCP/UDP port
- Source IP address and VLAN
- Source IP address, TCP/UDP port, and VLAN
- Source MAC address
- Source TCP/UDP port
- Source and destination IP address
- Source and destination IP address and TCP/UDP port
- Source and destination IP address and VLAN
- Source and destination IP address, TCP/UDP port, and VLAN
- Source and destination MAC address
- Source and destination TCP/UDP port
- Source port ID
- VLAN

These policies, which are configured for LAG, always override any settings made on the distributed port group.

First, verify the distributed virtual switch is version 5.5; it indicates that LACP has Enhanced Support as shown in Figure C.12.

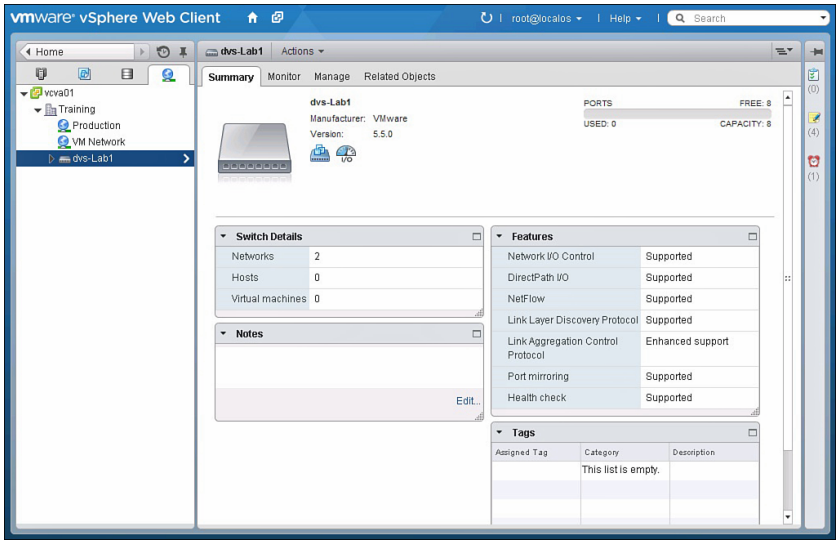

Figure C.12

Then use **Manage** > **LACP** > **New Link Aggregation Group** and select a load balancing mode (one of the 20 options listed previously) as shown in Figure C.13.

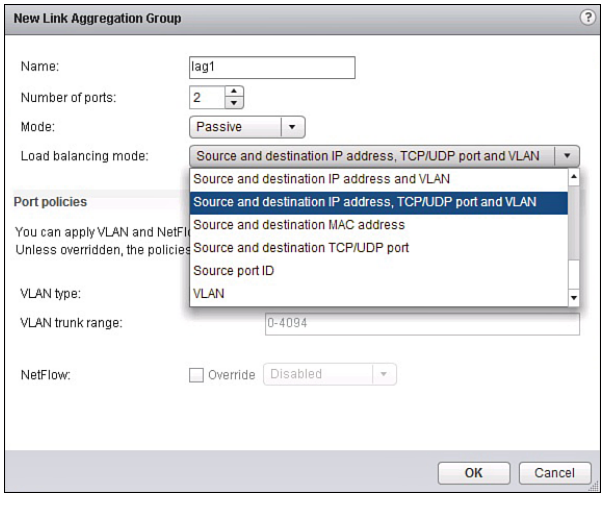

Figure C.13

By default, Passive Mode is used with Normal Interval (30 seconds), but this can be changed to Active. Active Mode is where the port initiates negotiations with remote ports by sending LACP packets. Passive Mode is where the port responds to LACP packets it receives but does not initiate LACP negotiation.

The LAG is represented as an uplink on the NIC Teaming and Failover settings as shown in Figure C.14.

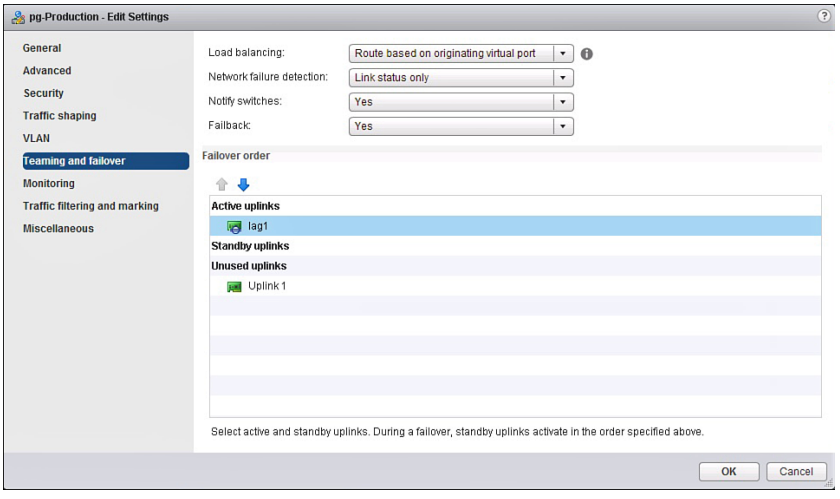

Figure C.14

Determine and apply failover settings

Cert Guide References:

- Chapter 2—Deploy and Maintain Scalable Virtual Networking—Determine and Apply Failover Settings

Configure explicit failover to conform with VMware best practices

Cert Guide References:

- Chapter 2—Deploy and Maintain Scalable Virtual Networking—Determine and Apply Failover Settings
- Chapter 10—Scenario 10-6

Configure port groups to properly isolate network traffic

Cert Guide References:

- Chapter 2—Deploy and Maintain Scalable Virtual Networking—Configure Port Groups to Properly Isolate Network Traffic
- Chapter 10—Scenario 10-18

Given a set of network requirements, identify the appropriate distributed switch technology to use

Cert Guide References:

- Chapter 2—Administer vSphere Distributed Switches—Identify Distributed Virtual Switch Technologies to Satisfy Network Requirements

Configure and administer vSphere Network I/O Control

Cert Guide References:

- Chapter 2—Administer vSphere Distributed Switches—Configure and Administer vSphere Network I/O Control
- Chapter 10—Scenario 10-7

Use command-line tools to troubleshoot and identify configuration items from an existing vDS

Cert Guide References:

- Chapter 2—Implement and Manage Complex Networks—Configure Virtual Switches Using CLI Commands
- Chapter 4—Use net-dvs to Troubleshoot vSphere Distributed Switch Configurations

Objective 3.1—Implement and Maintain Complex VMware HA Solutions

Calculate host failure requirements

Cert Guide References:

- Chapter 5—VMware High Availability—Calculate Host Failure Requirements

New Material:

vSphere App HA is a new feature in vSphere 5.5 that works with vSphere HA to improve application uptime. It can be configured to restart several commonly used commercial applications, such as SQL Server and SharePoint, when issues are detected. The VDCA550 blueprint does not mention vSphere App HA, so you should not need to learn how to fully implement or to gain hands-on experience with App HA. But, you should have an understanding of what it is and the basic approach for implementation.

To deploy vSphere App HA, provision one vSphere App HA virtual appliance and one vFabric Hyperic virtual appliance per vCenter Server. The vSphere App HA virtual appliance stores and manages vSphere App HA policies. The vFabric Hyperic virtual appliance monitors your VM-based applications and enforces vSphere App HA policies. Use the Administration section in the vSphere Web Client to configure policies that specify at least the application type and the remediation action (restart the application service or reset the VM). Optionally, create vCenter Server alarms for the policy and specify email addresses for notification.

Configure customized isolation response settings

Cert Guide References:

- Chapter 5—VMware High Availability—Customize Isolation Response Settings

Configure HA redundancy (Management Network, Datastore Heartbeat, Network Partitions)

Cert Guide References:

- Chapter 5—VMware High Availability—Configure HA Redundancy

Configure HA-related alarms and monitor an HA cluster

Cert Guide References:

- Chapter 5—VMware High Availability—Configure HA-related Alarms and Monitor HA Clusters

Create a custom slot size configuration

Cert Guide References:

- Chapter 5—VMware High Availability—Create a Custom Slot Size Configuration

Understand interactions between DRS and HA

Cert Guide References:

- Chapter 5—VMware High Availability—Interactions between DRS and HA

New Material:

vSphere HA in vSphere 5.5 has been enhanced to conform to VM-to-VM anti-affinity rules. In earlier versions, HA did not comply with VM-to-VM anti-affinity rules. Instead, HA could start two VMs in an anti-affinity rule on the same ESXi host and DRS could be used to detect and correct the violation of the rule. In vSphere 5.5, an advanced option can be configured to enable HA to comply directly with the anti-affinity rule. To configure vSphere HA to comply with VM-to-VM affinity rules, the following steps can be used:

1. Use the vSphere Web Client to navigate to **Host and Clusters**.
2. Select the cluster and select **Manage** > **Settings**.
3. Select **vSphere HA** and click **Edit**.
4. Expand **Advanced Options** and click **Add**.
5. Enter the option name as *parameter das.respectVmVmAntiAffinityRules* and set its value to *TRUE*.

Analyze vSphere environment to determine appropriate HA admission control policy

Cert Guide References:

- Chapter 5—VMware High Availability—Admission Control Policies and Determining the Best Policy
- Chapter 10—Scenario 10-12

Analyze performance metrics to calculate host failure requirements

Cert Guide References:

- Chapter 5—VMware High Availability—Calculate Host Failure Requirements

Analyze virtual machine workload to determine optimum slot size

Cert Guide References:

- Chapter 5—VMware High Availability—Create a Custom Slot Size Configuration

Analyze HA cluster capacity to determine optimum cluster size

Cert Guide References:

- Chapter 5—VMware High Availability—Create a Custom Slot Size Configuration
- Chapter 10—Scenario 10-12

New Material:

The vSphere Web Client now offers a direct means to configure the HA slot size. To set the slot size, you can edit the cluster and select VMware HA. Set the Admission Control policy to **Reserved failover capacity** for at least one host and choose **Fixed slot size** for the **Slot Size Policy**. Provide appropriate values CPU slot size and Memory slot size as shown in Figure C.15. If advanced settings are used to configure the minimum and maximum slot sizes, then be sure to assign compliant values on this web page.

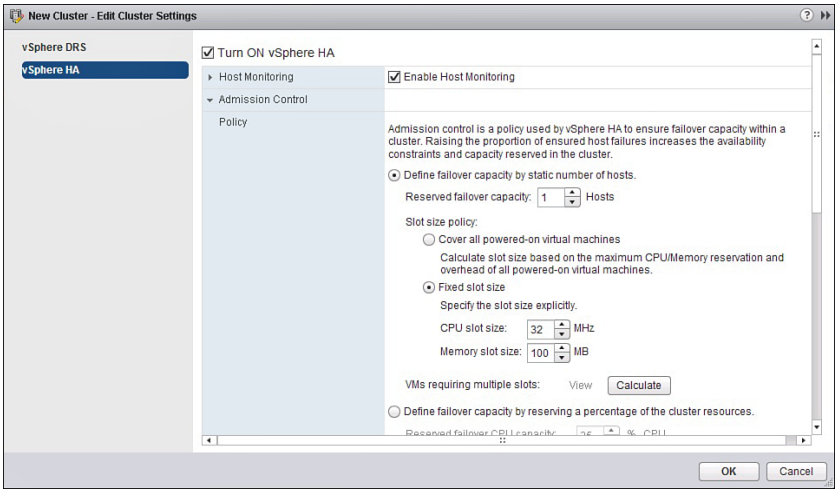

Figure C.15

Objective 3.2—Implement and manage complex DRS solutions

Explain DRS/storage DRS affinity and anti-affinity rules

Cert Guide References:

- Chapter 5—VMware Distributed Resource Scheduler—DRS Affinity and Anti-affinity rules

New Material:

In vSphere 5.5, vSphere HA can now be configured to comply with VM to VM anti-affinity rules. Refer to the *Objective 3.1—Implement and Maintain Complex VMware HA Solutions—Understand interactions between DRS and HAs* in this appendix for details.

Identify required hardware components to support Distributed Power Management (DPM)

Cert Guide References:

- Chapter 5—VMware Distributed Power Management—DPM Configuration

Identify EVC requirements, baselines, and components

Cert Guide References:

- Chapter 5—VMware Enhanced vMotion Compatibility—EVC Configuration
- Chapter 10—Scenario 10-10

Understand the DRS/storage DRS migration algorithms, the Load Imbalance Metrics, and their impact on migration recommendations

Cert Guide References:

- Chapter 5—VMware Distributed Resource Scheduler—DRS Configuration

Properly configure BIOS and management settings to support DPM

Cert Guide References:

- Chapter 5—VMware Distributed Power Management—DPM Configuration

Test DPM to verify proper configuration

Cert Guide References:

- Chapter 5—VMware Distributed Power Management—DPM Configuration

Configure appropriate DPM threshold to meet business requirements

Cert Guide References:

- Chapter 5—VMware Distributed Power Management—DPM Configuration

Configure EVC using appropriate baseline

Cert Guide References:

- Chapter 5—VMware Enhanced vMotion Compatibility—EVC Configuration
- Chapter 10—Scenario 10-10

Change the EVC mode on an existing DRS cluster

Cert Guide References:

- Chapter 5—VMware Enhanced vMotion Compatibility—EVC Configuration

Create DRS and DPM alarms

Cert Guide References:

- Chapter 5—VMware Distributed Resource Scheduler—DRS Alarms
- Chapter 5—VMware Distributed Power Management—DPM Alarms

Configure applicable power management settings for ESXi hosts

Cert Guide References:

- Chapter 5—VMware Distributed Power Management—DPM Configuration

New Material:

Enhancements to CPU C.States—In earlier vSphere versions, the *balanced* policy for host power management leveraged only the performance state (P-state), which kept

the processor running at a lower frequency and voltage. In vSphere 5.5, the deep processor power state (C-state) is also used to provide additional power savings.

To set the power policy to *Balanced* on an ESXi host using the vSphere Web Client, follow these steps:

1. Use the **Host and Clusters** view to select the ESXi host.
2. Select **Manage** > **Settings**.
3. Select **Hardware** > **Power Management**.
4. Click **Edit**.
5. In the **Edit Power Policy Settings** dialog box select **Balanced**.
6. Click **OK**.

Properly size virtual machines and clusters for optimal DRS efficiency

Cert Guide References:

- Chapter 5—VMware Distributed Resource Scheduler—DRS Configuration

Properly apply virtual machine automation levels based upon application requirements

Cert Guide References:

- Chapter 5—VMware Distributed Resource Scheduler—DRS Configuration

Create and administer ESXi host and datastore clusters

Cert Guide References:

- Chapter 5—VMware Distributed Resource Scheduler—DRS Configuration

Administer DRS/Storage DRS

Cert Guide References:

- Chapter 5—VMware Distributed Resource Scheduler—DRS Configuration
- Chapter 5—VMware Distributed Resource Scheduler—User PowerCLI to Configure DRS

Objective 3.3—Troubleshoot vSphere clusters

NOTE All four of these objectives are already stated in Objective 3.2.

Configure EVC using appropriate baseline

(See Objective 3.2—Configure EVC using appropriate baseline)

Create and manage DRS and DPM alarms

(See Objective 3.2—Create and manage DRS and DPM alarms)

Properly size virtual machines and clusters for optimal DRS efficiency

(See Objective 3.2—Properly size virtual machines and clusters for optimal DRS efficiency)

Properly apply virtual machine automation levels based upon application requirement

(See Objective 3.2—Properly apply virtual machine automation levels based upon application requirement)

Objective 4.1—Utilize Advanced vSphere Performance Monitoring Tools

Configure esxtop/resxtop custom profiles

Cert Guide References:

- Chapter 4—Utilize Advanced vSphere Performance Monitoring Tools—Configure ESXTOP / RESXTOP Custom Profiles

Determine use cases for and apply esxtop/resxtop Interactive, Batch, and Replay modes

Cert Guide References:

- Chapter 4—Utilize Advanced vSphere Performance Monitoring Tools—ESXTOP Interactive, Batch and Replay Modes
- Chapter 10—Scenario 10-11

Use vscsiStats to gather storage performance data

Cert Guide References:

- Chapter 4—Utilize Advanced vSphere Performance Monitoring Tools—Use vscsiStats to Gather Storage Performance Data

Use esxtop/resxtop to collect performance data

Cert Guide References:

- Chapter 1—ESXTOP and RESXTOP commands—Usage

Given esxtop/resxtop output, identify relative performance data for capacity planning purposes

Cert Guide References:

- Chapter 4—Tune and Optimize vSphere Performance

Objective 4.2—Optimize virtual machine resources

Compare and contrast virtual and physical hardware resources

Cert Guide References:

- Chapter 4—Tune and Optimize vSphere Performance—Tune Capacity Planning and Peak Workload
- Chapter 4—Tune and Optimize vSphere Performance—Tune ESXi Host Memory Configuration
- Chapter 4—Optimize Virtual Machine Resources—Modify Large Memory Page Settings
- Chapter 4—Optimize Virtual Machine Resources—Tune Virtual Machine Memory Configurations
- Chapter 10—Scenario 10-17

Identify VMware memory management techniques

Cert Guide References:

- Chapter 4—Troubleshooting Memory Performance

- Chapter 4—Optimize Virtual Machine Resources—Tune Virtual Machine Memory Configurations
- Chapter 4—Troubleshoot CPU and Memory Performance—Troubleshoot Memory Performance Issues

New Material:

The new vSphere Flash Cache is a new feature in vSphere 5.5. See "Objective 1.1—Configure and manage vSphere Flash Read Cache" in this appendix for details.

Identify VMware CPU load-balancing techniques

Cert Guide References:

- Chapter 4—Tune and Optimize vSphere Performance—Tune ESXi Host CPU Configuration
- Chapter 4—Optimize Virtual Machine Resources—Tune Virtual Machine CPU Configurations
- Chapter 4—Troubleshoot CPU and Memory Performance—Troubleshoot CPU Performance Issues

Identify prerequisites for Hot Add features

Cert Guide References:

- Chapter 4—Troubleshoot CPU and Memory Performance—Use Hot-Add Functionality to Address CPU and Memory Performance Issues

Tune virtual machine memory configurations

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Tune Virtual Machine Memory Configurations

New Material:

An important skill that is not mentioned directly in the blueprints or the Cert Guide is the ability to enable or disable the memory compression cache on ESXi hosts. The steps to enable or disable memory compression cache on an ESXi host are:

1. Use the vSphere Client to select the ESXi host.
2. Navigate to **Configuration** tab > **Software** and select **Advanced Settings**.
3. In the left pane, select *Mem* and locate *Mem.MemZipEnable*.
4. Set its value to 1 (enable) or 0 (disable).
5. Click **OK**.

Tune virtual machine networking configurations

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Tune Virtual Machine Networking Configurations

Tune virtual machine CPU configurations

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Tune Virtual Machine CPU Configurations

Tune virtual machine storage configurations

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Tune Virtual Machine Storage Configurations

Calculate available resources

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Calculate Available Resources

Properly size a virtual machine based on application workload

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Properly Size a Virtual Machine Based on Application Workload

Modify large memory page settings

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Modify Large Memory Page Settings

Understand appropriate use cases for CPU affinity

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Understand Appropriate Cases for CPU Affinity

Configure alternative virtual machine swap locations

Cert Guide References:

- Chapter 4—Optimize Virtual Machine Resources—Configure Alternate Virtual Machine Swap Locations
- Chapter 10—Scenario 10-9

Objective 4.3—Manage advanced virtual machine configurations

NOTE Some of these objectives are already stated in Objective 4.2.

Compare and contrast virtual and physical hardware resources

(See Objective 4.2—Compare and contrast virtual and physical hardware resources)

Identify VMware memory management techniques

(See Objective 4.2—Identify VMware memory management techniques)

Identify VMware CPU load-balancing techniques

(See Objective 4.2—Identify VMware CPU load balancing techniques)

Identify prerequisites for Hot Add features

(See Objective 4.2—Identify pre-requisites for Hot Add features)

Configure VMware fault tolerance

Cert Guide References:

- Chapter 5—VMware Fault Tolerance—Configuration and Best Practices
- Chapter 10—Scenario 10-13

Upgrade virtual machine hardware and VMware Tools

Cert Guide References:

- Chapter 6—Install and Configure VMware Update Manager—Overview
- Chapter 6—Install and Configure VMware Update Manager—Orchestrated vSphere Upgrades

New Material:

VM hardware version 10 provides virtual SATA controller for virtual disks and virtual CD-ROM devices, which allows up to 30 devices per virtual controller. Four virtual storage controllers per VM is still the limit, so the maximum virtual SATA disks per VM is now 120. In ESXi 5.1, the maximum number of virtual disks per VM is 60 (15 devices per virtual controller). The vSphere client cannot be used to edit the settings of virtual machines of version 10 or higher. The vSphere Web Client must be used to edit the settings of these VMs.

Objective 4.4—Configure and manage vSphere Replication

The VDCA510 blueprint does not mention vSphere Replication. So no references to the Cert Guide are provided for this objective.

VMware vSphere Replication is a feature that provides hypervisor-based replication and recovery for VMs. It can be used as an alternative to storage-based replication for disaster recovery (DR) and other purposes. It supports replication between sites, between clusters within a single site, and from multiple sites to a shared site. It provides VM protection at a lower cost with more flexibility than storage-based replication.

Configure and manage a vSphere Replication infrastructure

The key step in implementing vSphere Replication is to deploy the vSphere Replication appliance, which provides all the required components, including a vSphere Web Client plug-in, an embedded database, a Sphere Replication Management server, and a vSphere Replication server. The vSphere Replication Management server provides the necessary management services, such as configuration, monitoring, and authentication. The vSphere Replication (VR) server provides the core functionality involved in protecting VMs.

VMware vSphere Replication is a feature of several editions of vSphere, including Essentials Plus, Standard Enterprise, and Enterprise Plus. It requires several network ports. Some of the major ports are

- **80**—For management of traffic between a VR appliance and the remote vCenter Server
- **5480**—For the VR Management server's web-based administrator portal
- **31031**—Initial replication traffic from an ESXi host to a remote VR server
- **44046**—Ongoing replication traffic from an ESXi host to a remote VR server

To configure VR, begin by deploying the VR appliance, typically one appliance at the protected site and one appliance at the recovery site. The main steps are:

1. Use the vSphere Web Client to select **Deploy OVF template**.
2. Provide the necessary parameters when prompted, such as the name of the OVF file, VM name, datastore, and virtual switch port group.
3. Provide VR-specific parameters when prompted, such as root account password and IP configuration.
4. Use the previous steps to deploy a VR appliance at each site.
5. Navigate to the Home page and select **vSphere Replication**.
6. Select the **Summary** tab and examine the **Local sites** pane.
7. Right-click the name of the protected site and select **All vSphere Replication Actions** > **Connect to target site**.
8. Enter the IP address or hostname of the remote vCenter Server site.
9. Provide the user credentials to connect to the remote vCenter Server.

VR utilizes an embedded database by default, but it can be configured to use a remote database. You can use the VR Management web portal https://<VR-appliance-hostname>:5480 to change the database and other VR settings.

Configure and manage vSphere Replication of virtual machines

To configure replication for a single VM, the following steps can be used:

1. Right-click the VM and select **All vSphere Replication Actions** > **Configure replication**.
2. Select the protected site.
3. Accept the automatic assignment of a target vSphere Replication server.
4. Select the target datastore.
5. Optionally, select **Advanced disk configuration** and configure replication separately for individual virtual disks.
6. Optionally, select **Microsoft Volume Shadow Copy Service (VSS)** for Guest OS Quiescing.
7. Set the **Recover Point Objective (RPO)**. The acceptable range is 15 minutes to 24 hours.
8. Click **Finish**.

In vSphere 5.5, the VMs that are protected with vSphere Replication can be migrated with SDRS and Storage vMotion at the protected site. This was not supported in earlier vSphere versions. Storage vMotion is still not supported at the recovery site for VMs that are protected with vSphere Replication. Multi-Point-in-Time (MPIT) Snapshot Retention is provided for vSphere Replication in vSphere version 5.5, where multiple snapshots are maintained at the recovery site for each VM. This allows the VM to be recovered to various points in time. To implement MPIT, use the vSphere Web Client to configure vSphere Replication for the VM, select **Enable** for **Points in time instances** and specify the number of instances to **Keep** per day and the number of **days**.

Troubleshoot vSphere Replication

One reason for potential problems with vSphere Replication is that it is not compatible with some other vSphere features. For example, if you cannot successfully protect a VM with vSphere Replication, it could be that the VMs are protected with vSphere Fault Tolerance, which is not supported with vSphere Replication.

Another potential problem is that one or more of the required network ports cannot be used between required components. For example, if VR successfully performs the initial copy for a protected VM but fails to perform the ongoing replication, the issue could be that port 44046 is not functional between the ESXi hosts at the protected site and the VR appliance at the recovery site.

If the vSphere Replication service fails unexpectedly shortly after a restart, you should examine its logs. If it contains an entry "unable to resolve host", the following steps can be used to correct the issue:

1. In the vSphere Web Client, select the vCenter Server.
2. Select **Manage** > **Settings** > **Advanced Settings**.
3. Set the value of the VirtualCenter.FQDN parameter to the fully qualified name of the vCenter Server.
4. Use a web browser to connect to https://<VR-appliance-hostname>:5480.
5. Ensure the same value for fully qualified name of the vCenter Server is provided for the VR appliance to use to connect to vCenter Server.

Objective 5.1—Implement and maintain host profiles

Use Profile Editor to edit and/or disable policies

Cert Guide References:

- Chapter 9—Using a Host Profile from a Reference Host—Use Profile Editor to Edit Policies
- Chapter 10—Scenario 10-14

Create sub-profiles

Cert Guide References:

- Chapter 9—Using a Host Profile from a Reference Host—Use Profile Editor to Edit Policies

Use host profiles to deploy vDS

Cert Guide References:

- Chapter 9—Using a Host Profile form a Reference Host with Auto Deploy

Use host profiles to deploy vStorage policies

Cert Guide References:

- Chapter 9—Using a Host Profile form a Reference Host with Auto Deploy

Objective 5.2—Utilize Update Manager for patches and upgrades

Install and configure Update Manager Download Service

Cert Guide References:

- Chapter 6—Install and Configure VMware Update Manager—VUM Installation

Configure a shared repository

Cert Guide References:

- Chapter 6—Install and Configure VMware Update Manager—Shared Repository and Download to Repository
- Chapter 10—Scenario 10-15

Configure smart rebooting

Cert Guide References:

- Chapter 6—Upgrade vApps and Appliances—Smart Rebooting

Manually download updates to a repository

Cert Guide References:

- Chapter 6—Install and Configure VMware Update Manager— Shared Repository and Download to Repository
- Chapter 10—Scenario 10-15

Perform orchestrated vSphere upgrades

Cert Guide References:

- Chapter 6—Orchestrated vSphere Upgrades

Create and modify baseline groups

Cert Guide References:

- Chapter 6—Create and Modify Baselines

Troubleshoot Update Manager problem areas and issues

Cert Guide References:

- Chapter 6—Troubleshooting and Reporting—Troubleshooting

Generate database reports using MS Excel or MS SQL

Cert Guide References:

- Chapter 6—Troubleshooting and Reporting—VUM Reporting Using Excel
- Chapter 6—Troubleshooting and Reporting—VUM Reporting Using SQL Server Query

Upgrade vApps using Update Manager

Cert Guide References:

- Chapter 6—Upgrade vApps and Appliances—Upgrade vApps
- Chapter 6—Upgrade vApps and Appliances—Virtual Appliances

Utilize Update Manager PowerCLI to export baselines for testing

Cert Guide References:

- Chapter 6—PowerCLI and Update Manager Utility—VUM PowerCLI Installation and Usage

Objective 5.3—Manage vCenter inventory

Apply vSphere tags

The vSphere Web Client can be use to assign tags to the objects managed by vCenter Server, such as datacenters, datastores ESXi hosts, VMs, and networks. A tag is a mechanism that allows you to assign metadata to objects. The first step for creating tags is to create one or more categories. When creating a category, you need to specify whether its cardinality will permit only one tag per object or many tags per object. You also need to specify the types of objects, where the tags can be assigned.

For example, you might want to use tags to identify a point of contact (POC) and a tier level for each VM. To accomplish this, you could define two new categories using these steps:

1. Use the vSphere Web Client to navigate to the Home page and click **Tags**.
2. Select **Items** > **Categories**.

3. Click **New Category** icon, as shown in Figure C.16.

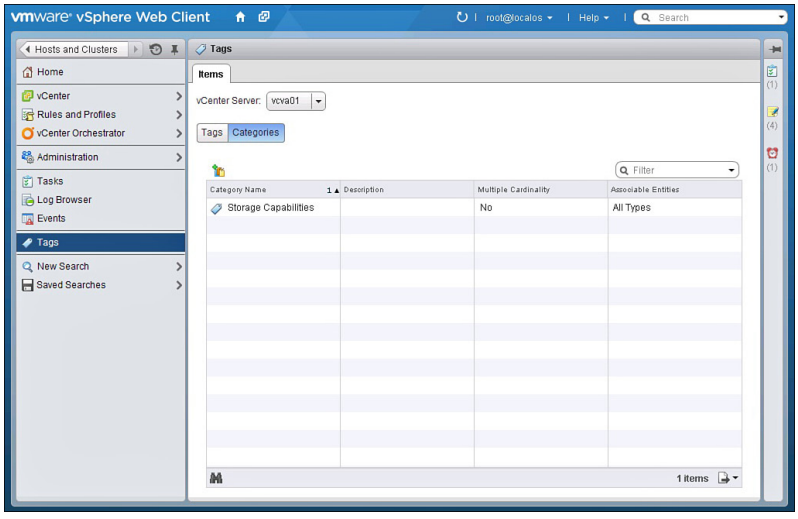

Figure C.16

4. Set the **Category Name** to *POC*.
5. Set the **Cardinality** to **One** tag per object.
6. Set the **Object Type** to **Virtual Machine**.
7. Click **OK** as shown in Figure C.17.
8. Repeat these steps exactly to create another category, but set its name to *Tier*.

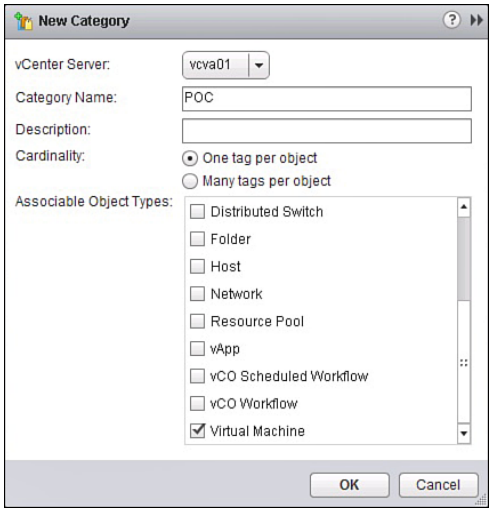

Figure C.17

In this example, you can now assign tags for the POC and Tier categories to the VMs. For example, to create a tag named *Tier-1* in the *Tier* category and assign the tag a VM, follow these steps:

1. Right-click a VM and select **Assign Tag**.
2. Click the **New Tag** icon.
3. Set the **Name** to *Tier-1* as shown in Figure C.18.
4. Set **Category** to *Tier*.
5. Click OK.

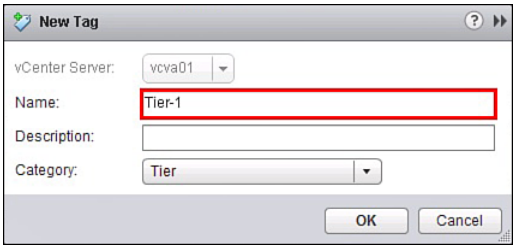

Figure C.18

Search vSphere inventory

Using the vSphere Web Client 5.5, you can perform an advanced search for objects that meet multiple criteria. For example, the following steps can be used to search for a VM that has a name that contains the string "Win" and resides on an ESXi host named "esxi01":

1. From the Home page in the vSphere Web Client, click **New Search** > **Advanced Search**.
2. In the **Search for** menu, select **Virtual Machines**.
3. Specify that the results must match all of the specified criteria by selecting **all**.
4. Select the **Name** property and select the **contains** option.
5. Enter *Win* in the search box.
6. Select **Add new criteria**.

7. Select the **Host** property and select the **is** option.
8. Enter *esxi01*.
9. Click **Search**.

The vSphere Web Client can be used to save and reuse searches. To save a search after performing a search, click **Save** and enter a name. To use a search that was previously saved, navigate to the Home page, click **Saved Searches**, and select the search.

Troubleshoot the vSphere inventory infrastructure

Cert Guide References:

- Chapter 4—Troubleshoot vCenter Server and ESXi Host Management
- Chapter 10—Scenario 10-20

Objective 5.4—Configure, manage, and analyze vSphere and SSO log files

Generate vCenter Server and ESXi log bundles

Cert Guide References:

- Chapter 7—Generate vCenter Server and ESXi Log Bundles

Use esxcli system syslog to configure centralized logging on ESXi hosts

Cert Guide References:

- Chapter 7—Use ESXCLI System Syslog to Configure Centralized Logging on ESXi Hosts

Test centralized logging configuration

Cert Guide References:

- Chapter 7—Analyze and Test Logging Configuration Information

Analyze log entries to obtain configuration information

Cert Guide References:

- Chapter 7—Analyze and Test Logging Configuration Information

Analyze log entries to identify and resolve issues

Cert Guide References:

- Chapter 7—Analyze Log Files to Resolve Issues

Install and configure VMware syslog Collector and ESXi Dump Collector

Cert Guide References:

- Chapter 7—Install and Configure VMware Syslog Collector
- Chapter 7—Install and Configure vSphere ESXi Dump Collector
- Chapter 10—Scenario 10-16

Objective 6.1—Manage authentication and end-user security

Add/Edit/Remove users/groups on an ESXi host

Cert Guide References:

- Chapter 8—Users and Groups on an ESXi Host

Customize SSH settings for increased security

Cert Guide References:

- Chapter 8—Customize SSH Settings for Increased Security

Enable/Disable certificate checking

Cert Guide References:

- Chapter 8—Enable / Disable Certificate Checking

Generate ESXi host certificates

Cert Guide References:

- Chapter 8—Generate Host Certificates
- Chapter 10—Scenario 10-21

Enable ESXi lockdown mode

Cert Guide References:

- Chapter 8—Enable ESXi Lockdown Mode

Objective 6.2—Manage SSL certificates

NOTE Some of these objectives are already stated in Objective 6.1.

Add/Edit/Remove users/groups on an ESXi host

(See Objective 6.1—Add/Edit Remove users/groups on an ESXi host)

Customize SSH settings for increased security

(See Objective 6.1—Customize SSH settings for increased security)

Enable/Disable certificate checking

(See Objective 6.1—Enable/Disable certificate checking)

Generate ESXi host certificates

(See Objective 6.1—Generate ESXi host certificates)

Enable ESXi lockdown mode

(See Objective 6.1—Enable ESXi lockdown mode)

Replace default certificate with CA-signed certificate

Cert Guide References:

- Chapter 8—Replace Default Certificate with CA-Signed Certificate

Configure SSL timeouts

Cert Guide References:

- Chapter 8—Configure SSL Timeouts

Configure vSphere Authentication Proxy

Cert Guide References:

- Chapter 8—Configure vSphere Authentication Proxy

Enable strong passwords and configure password policies

Cert Guide References:

- Chapter 8—Enable Strong Passwords and Configure Password Policies

Identify methods for hardening virtual machines

Cert Guide References:

- Chapter 8—Identify Methods for Hardening Virtual Machines

Analyze logs for security-related messages

Cert Guide References:

- Chapter 4—Troubleshoot vCenter Server and ESXi Host Management—Troubleshoot ESXi Firewall Issues

Manage Active Directory integration

Cert Guide References:

- Chapter 8—Manage Active Directory Integration

Objective 7.1—Execute VMware Cmdlets and Customize Scripts Using PowerCLI

Identify vSphere PowerCLI requirements

Cert Guide References:

- Chapter 1—PowerCLI—Installation

Identify Cmdlet concepts

Cert Guide References:

- Chapter 1—PowerCLI—Usage

Identify environment variables usage

Cert Guide References:

- Chapter 1—PowerCLI—Running Scripts in a VM

Install and configure vSphere PowerCLI

Cert Guide References:

- Chapter 1—PowerCLI—Installation

Install and configure Update Manager PowerShell Library

Cert Guide References:

- Chapter 6—PowerCLI and Update Manager Utility—VUM PowerCLI Installation and Usage

Use basic and advanced Cmdlets to manage VMs and ESXi Hosts

Cert Guide References:

- Chapter 1—PowerCLI—Usage
- Chapter 7—Generate a Diagnostic Log Bundle on the ESXi Host or vCenter Server using PowerCLI
- Chapter 10—Scenario 10-23

- Chapter 8—Enable ESXi Lockdown Mode—Enable or Disable Lockdown Mode with PowerCLI
- Chapter 8—Manage Active Directory Integration—Configure Active Directory Using PowerCLI
- Chapter 8—Configure the ESXi Firewall Using PowerCLI

NOTE Many other chapters provide PowerCLI examples for managing items other than VMs and ESXi hosts, such as DRS, SDRS, and HA.

Use web service access cmdlets

Web service cmdlets enable access to the vSphere.NET SDK. PowerCLI provides two web service access cmdlets called **get-view** and **get-viobjectview**. These cmdlets access underlying .NET objects or PowerCLI objects. **get-view** converts PowerShell VIObjects and to vSphere .NET View Objects. **get-viobjectByView** converts vSphere .NET View Objects to PowerShell VIObjects.

For example, the following set of commands retrieves the set of vSphere .NET objects of all virtual machines, assigns the results to an object variable named *$view*, and converts the results back to the standard PowerShell object:

```
$view=Get-View -viewtype "VirtualMachine"
Get-VIObjectByVIView $view
```

Use datastore and inventory providers

PowerCLI includes an inventory provider (VimInventory) that can be used to traverse the vCenter Server inventory in a manner that is similar to navigating a directory tree. In other words, VimInventory is recognized as a file system type by the **New-PSDrive** command. To use this provider, use the **New_PSDrive** cmdlet and provide the value *VimInventory* for the **-PSprovider** parameter. For example, the following set of commands can be used to connect to a vCenter server named *vc01*, retrieve the root object in the vCenter Server inventory, effectively map a drive letter(s) *vi* to the root object in the inventory, and change the default directory to the root object:

```
Connect-VIServer -Server vc01 -user Administrator -password vmware
$root = Get-Folder -Norecursion
New-PSDrive -Location $root -Name V -PSprovider VimInventory -Root
'\'
cd V:
```

After executing these commands, standard commands such as **cd**, **ls**, **dir**, and **del** can be used to navigate through the nodes of the vCenter Server hierarchy much like they are typically used to navigate and manipulate folders and files in a file system. (Alternatively, you can replace the cmdlet New-PSDrive with *New-VIInventory Drive*.) For example, the following commands can be used to navigate to an ESXi host named *esxi01.vclass.local* and list all the VMs (and other objects) on the host. In this example, the ESXi host is in a cluster named *New Cluster* that is attached to a datacenter named *Training*:

```
cd  '\Training\host\New Cluster\esxi01.vclass.local'
ls
```

Likewise, PowerCLI provides a datastore provider (VimDatastore) that can be used with the New-PSDrive cmdlet. For example, to list the contents of the folder used to store a VM named vm01 that resides on a datastore named *Shared-01*, the following commands can be used:

```
$datastore = Get-Datastore Shared-01
New-PSDrive -Location $datastore -Name X -PSProvider VimDatastore
-Root '\'
cd X:
cd vm01
ls
```

Given a sample script, modify the script to perform a given action

Cert Guide References:

- Chapter 10—Scenario 10-23

Objective 7.2—Utilize basic workflows using Orchestrator

The VDCA510 blueprint does not mention VMware vCenter Orchestrator. So no references to the Cert Guide are provided for this objective.

VMware vCenter Orchestrator is a platform for development automation and process automation. It provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage the VMware vSphere infrastructure and other solutions. Orchestrator allows you to integrate all the operations exposed in the vCenter Server API into your automated processes. It utilizes a library of workflows and accepts third-party plug-ins. The workflow library and the plug-ins can be extended and integrated into large architectures. It provides per-

sistence, central management, check-pointing, security, and versioning. It utilizes a scripting engine, a workflow engine, a policy engine, and a Web 2.0 front end.

Here are some of the standard workflows provided in the workflow library:

- Create cluster
- Enable DRS on cluster
- Add custom attributes to a virtual machine
- Rename datacenter
- Find all unused files in datastores
- Move host into cluster
- Add port group to distributed virtual switch
- Connect virtual machine NIC number to distributed virtual port group
- Add datastore on iSCSI/FC/local SCSI
- Add iSCSI target
- Configure datastore cluster
- Upgrade virtual machine

Configure and manage vCenter Orchestrator

VMware vCenter Orchestrator (Orchestrator) can be implemented in several manners, such as installing its components on separate Windows servers or by deploying the Orchestrator Appliance. A common method is to perform a simple installation of vCenter Server 5.5, which silently installs Orchestrator 5.5 on the vCenter Server.

To install Orchestrator independently, you can run the Orchestrator installer (vCenterOrchestrator.exe) directly. During the installation, the only prompt that is unique to Orchestrator is the *Type of Installation*. The choices are *Client*, *Server*, and *Client-Server*. Typically, the Client-Server type is preferred over just Server; however, you can use the Client type to install the Orchestrator Client on desktops to enable several administrators and developers to use the same Orchestrator Server.

Orchestrator requires a database. When Orchestrator standalone is installed or deployed as the Orchestrator appliance, it is preconfigured to use an embedded database. When Orchestrator is installed with vCenter Server, it is preconfigured to use the vCenter Server database. The embedded databases are suitable only for small environments and are not compatible with cluster mode. VMware recommends us-

ing a database provided by a separate server, such as SQL Server or Oracle, for large environments. To use an external Orchestrator database, use the Orchestrator configuration interface to configure the database, with these steps:

1. Click **Database**.
2. Set the **Select the database type** to the correct type, such as *SQL Server* or *Oracle*.
3. Set the values for the connection parameters, such as User name, Password, Database server IP address, or DNS name.
4. Click **Apply Changes**.
5. Select **Create the database tables**.
6. Click **Apply Changes**.

The Orchestrator Configuration service does not start automatically by default. Instead the following steps should be applied:

1. Use **Administrative Tools** > **Services** to right-click the VMware vCenter Orchestrator Configuration.
2. Select **Start**.
3. Use **Start** > **Programs** >**VMware** > **vCenter Orchestrator Configuration**.
4. Click **Orchestrator Configuration**.
5. Use a web browser to connect to https://<orchestrator-server-hostname>:8283.
6. Logon with username vmware and password vmware.
7. Click **Network**.
8. Use the drop-down menu to select an IP address (from the list of IP addresses that are assigned in Windows on the server running Orchestrator) to assign to Orchestrator server.
9. Typically, the default ports are acceptable and no further network changes are needed. If this is the case, select **Apply Changes**.

To import the SSL Certificate, the following steps can be used:

1. Click the **SSL Trust Manager** tab and select **Import from URL**.
2. Specify the URL of the vCenter Server.
3. Click **Import**.

4. Repeat these steps to register Orchestrator as a vCenter Single Sign-On solution, but specify the URL of vCenter Single Sign-on with port 7444 (https://<SSO-hostname>:7444*)*.

To register Orchestrator with SSO, first import the SSL Certificate from SSO (as described in the previous paragraph); then perform these steps:

1. Click **Startup Options**.
2. Click **Restart the vCO configuration server**.
3. Reconnect to the Orchestrator configuration service and click **Authentication**.
4. In the **Authentication Mode** drop-down, select *SSO Authentication*.
5. In the **Host** text box, enter https://<SSO-hostname>:7444.
6. Provide the credentials for the SSO server.
7. Click **Register Orchestrator**.

Add Orchestrator to vCenter

You can register Orchestrator as a vCenter Server extension using the following steps:

1. In the Orchestrator configuration interface, select **vCenter Server** > **New vCenter Server Host**.
2. From the **Available** drop-down menu, select **Enabled**.
3. In the **Host** text box, enter the DNS name of the vCenter Server.
4. In the **Port** text box, retain the default value, *443*.
5. (Optional) Select the **Secure channel** check box to establish a secure connection to your vCenter Server system.
6. In the **Path** text box, retain the default value, */sdk*.
7. Select the method for managing user access on the vCenter Server system—either **Share a unique session** or **Session per user.**
8. Click **Apply Changes**.

Create basic vCenter management workflows

The steps to simply create a workflow in vCenter Orchestrator are as follows:

1. From the drop-down menu in the Orchestrator client, select **Design**.
2. Click the **Workflows** view.
3. Right-click a folder and select **New workflow**.
4. Name the new workflow.
5. Click **OK**.

Alternatively, you can produce new workflows by duplicating and modifying an existing workflow using these steps:

1. From the drop-down menu in the Orchestrator client, select **Design**. Click the **Workflows** view.
2. (Optional) Right-click the root of the hierarchical list of workflow folders and select **New folder** to create a folder to contain the workflow to edit.
3. Expand the Library hierarchical list of standard workflows to navigate to the workflow to edit. Right-click the workflow to edit. The Edit option is dimmed. The workflow is read-only. Right-click the workflow and select **Duplicate workflow**.
4. Provide a name for the duplicate workflow. By default, Orchestrator names the duplicate workflow Copy of workflow_name. Click the Workflow folder value to search for a folder in which to save the duplicate workflow.
5. Click **Yes** or **No** to copy the workflow version history to the duplicate.
6. Click **Duplicate** to duplicate the workflow.
7. Right-click the duplicate workflow and select **Edit**.
8. Use each of the provided tabs to make appropriate settings. Some of the main tabs are
    - **General**—To set the workflow name, descriptions, and so on
    - **Inputs**—To define required input parameters
    - **Outputs**—To define values to be generated by the workflow
    - **Schema**—To drag and drop schema elements from a palette to include in the workflow
    - **Presentation**—To define the user input dialog box layout

Troubleshoot existing workflows

VMware provides a client for vCenter Orchestrator. The vCenter Orchestrator Client allows you to launch workflows manually on a local or remote vCenter Orchestrator server. The main purpose for launching workflows manually with the client is to troubleshoot workflows. The client can be installed independently on a 32-bit or 64-bit Windows system.

To use the Orchestrator client, the following steps can be used:

1. Select **Start** > **Programs** > **VMware** > **vCenter Orchestrator Client**.
2. In the **Host** name field, provide the IP address of the Orchestrator Server.
3. Provide proper credentials to log on to Orchestrator.
4. In the Security Warning window, click **Ignore**.

VMware Orchestrator 5.5 has a new workflow debugger that allows you to troubleshoot more quickly and easily than you could with previous versions of Orchestrator. For example, you can rerun a workflow in debug mode without entering the last known values for the workflow input parameters. The inputs are automatically stored and populated for the consequent workflow execution. Also, with debug mode you can set breakpoints on specific items in the workflow and examine variable values at various steps of the debugging process. You can also resume a workflow from a failed state.

Import/export packages

The standard workflow library contains a folder named *Troubleshooting* that contains workflows that can be used to export application settings and log files to Zip files that can be used by VMware Support for troubleshooting.

Other New Features in VMware vCenter 5.5

Here is a list of other new features and changes in vSphere 5.5 that do not appear to be directly mentioned in the VDCA550 blueprint. A brief description is provided for each item.

- **VMware vSphere Web Client—**This has been improved to support new features in vSphere 5.5 that cannot be done via the vSphere Client. It offers an increased platform support, including full client support for Mac OS X and full browser support for both Firefox and Chrome. It now provides drag and drop for objects from the center panel onto the vSphere inventory, enabling bulk actions. It now provides filters that can be used to limit the contents of

a list of displayed objects based on specific search criteria. For example, two check box filters can allow an administrator to see all virtual machines on a host that are powered on and running Windows Server 2008. It now provides a view for recent items that allows administrators to easily navigate to their most commonly used objects.

- **VMware vCenter Single Sign-On (SSO)—**This is the authentication services of VMware vCloud Suite, and it has been greatly enhanced in vSphere 5.5 to provide a better experience that allows users to log in to vCloud Suite products in a true single sign-on manner. The enhancements include
- **Simplified deployment—**A single installation model for customers of all sizes is now offered. For example, a single server running vCenter Server, the Inventory Service, the Web Client, and the SSO Server could support 1000 ESXi hosts and 10,000 VMs.
- **Enhanced Microsoft Active Directory integration—**The addition of native Active Directory support enables cross-domain authentication with one- and two-way trusts common in multidomain environments.
- **Architecture—**Built from the ground up, the new architecture removes the requirement of a database and delivers a multimaster authentication solution with built-in replication and support for multiple tenants.

Although the new VCAP5-DCA blueprint does not directly state much about Single Sign-on (SSO), it still makes sense to prepare as if you need to have a good understanding of how to implement SSO. You should be able to identify the main SSO requirements and describe the main installation and upgrade steps. Here are a few details:

- The requirements for vCenter Server and SSO depend on many factors, such as the deployment mode. For example, a simple installation of vCenter Server (where all components are installed on a single Windows server) requires at least two 64-bit CPUs cores and 12 GB memory. The minimum compute requirements to run SSO on a standalone server are at least two 64-bit CPUs cores and 3 GB memory.
- SSO 5.5 supports several types of identity sources: AD versions 2003 and later, AD over LDAP, OpenLDAP versions 2.4 and later, local operating system users, and SSO system users.
- SSO 5.5 creates a new domain named *vsphere.local*. SSO 5.5 provides a user account named administrator@vsphere.local that replaces the functionality of the admin@System-Domain account in vSphere 5.1.

- The proper installation and upgrade order for vCenter Server components is SSO, vSphere Web Client, Inventory Service, and vCenter Server.
- When upgrading a simple installation of vCenter Server (where all components are installed on a single Windows server) to version 5.5, SSO will recognize local user accounts. If the original version of vCenter Server did not include SSO, then SSO must be installed to upgrade vCenter Server and the Active Directory (AD) domain must be added as an identity source, if you need to support AD users. If the original version of vCenter Server did include SSO and SSO already used an AD domain as an identify source, then the AD users continue to have access after the upgrade, but users might need to fully qualify their usernames during login.
- Custom installations and upgrades can be used to place vCenter Server components on separate Windows servers. If you upgrade vCenter Server from a version that did not include SSO and you install SSO on a separate server, SSO does not recognize local user accounts.
- During an upgrade of SSO 5.1 to 5.5, the database is not automatically removed. Because is the database is not used by SS0 5.5, you can manually remove it.
- **VMware vCenter Server Appliance—**This can now support 100 hosts and 3000 VMs when using its embedded Postgres database. The Windows-based vCenter Server still supports only 5 ESXi hosts and 50 VMs when using its embedded SQL Server Express database. Each model of vCenter Server can still support additional ESXi hosts and VMs when using a remote database.
- **ESXi 5.5 support for SSD devices—**It now provides the ability to hot-add and hot-remove PCIe SSD devices.