# VMware vSphere: Optimize and Scale

Lab Manual

ESXi 6.7 and vCenter Server 6.7

VMware® Education Services
VMware, Inc.
www.vmware.com/education

**VMware vSphere:**
**Optimize and Scale**
Lab Manual
ESXi 6.7 and vCenter Server 6.7
Part Number EDU-EN-VSOS67-LAB (7/2018)



www.vmware.com/education

# CONTENTS

# *Lab 1* Using vSphere Distributed Switches

## Objective: Create, configure, and back up a distributed switch

In this lab, you perform the following tasks:

1. Access Your Lab Environment
2. Verify That the vSphere Licenses Are Valid
3. Assign Valid vSphere Licenses
4. Add ESXi Hosts to the New Distributed Switch
5. Examine Your Distributed Switch Configuration
6. Migrate the Virtual Machines to a Distributed Switch Port Group
7. Enable the Distributed Switch Health Check
8. Back Up the Distributed Switch Configuration

## Task 1: Access Your Lab Environment

You use a View desktop or Remote Desktop Connection to connect to your lab environment and use VMware vSphere® Client™ to connect to VMware vCenter Server®.

1. Use the information that is provided by your instructor to log in to your lab environment.
2. On the student desktop, open Firefox.
3. In the Firefox favorites toolbar, click the **vSphere Client (SA-VCSA-01)** bookmark from the `vSphere Site-A` folder.
4. At the login screen, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.

## Task 2: Verify That the vSphere Licenses Are Valid

You verify that licenses for the vCenter Server systems and the VMware ESXi™ hosts are valid.

1. Verify that the license for the vCenter Server system is valid.
   a. In the left pane, select **sa-vcsa-01.vclass.local**.
   b. In the right pane, click the **Configure** tab and click **Licensing** under System.
   c. Verify that the license expiration date for the vCenter Server instance is valid.
2. Verify that the license for the ESXi hosts are valid.
   a. In the left pane, expand the inventory until you see the ESXi hosts.
   b. Select **sa-esxi-01.vclass.local**.
   c. In the right pane, click the **Configure** tab and click **Licensing** under System.
   d. Verify that sa-esxi-01.vclass.local has a valid license.
   e. Repeat substep d for the remaining hosts in the inventory.
3. If the licenses are valid, go to task 4.

## Task 3: Assign Valid vSphere Licenses

If the vCenter Server system and ESXi hosts licenses are expired, you assign valid licenses to these VMware vSphere® components.

1. Select **Administration** from the **Menu** drop-down menu.
2. Assign a vCenter Server license key to the vCenter Server instance.
   a. In the Navigator pane, select **Licenses**.
   b. In the Content pane, click the **Licenses** tab.
   c. Click the **Add New Licenses** icon.

d. On the Enter license keys page, enter the vCenter Server and VMware vSphere® Enterprise Plus Edition™ license keys provided by your instructor in the **License keys** text box.

   You must enter the license keys on separate lines.

e. Verify that both licenses are listed correctly in the text box and click **Next**.

f. On the Edit license names page, enter `VMware vCenter Server` and `VMware ESXi` in the appropriate **License name** text boxes.

g. Click **Next**.

h. On the Ready to complete page, click **Finish**.

i. In the Licenses pane, click the **Assets** tab.

j. Select the **sa-vcsa-01.vclass.local** check box and click **Assign License**.

k. Select the vCenter Server license and click **OK**.

3. Assign the vSphere Enterprise Plus license key to the ESXi hosts.

   a. In the center pane, click the **Hosts** tab.

   b. Select all hosts by selecting the check box to the left of the Asset column header.

   c. Click **Assign License** and click **Yes** to perform the action on three objects.

   d. In the Assign License dialog box, select the vSphere Enterprise Plus license key and click **OK**.

4. Reconnect the ESXi hosts.

   a. Select **Hosts and Clusters** from the **Menu** drop-down menu.

   b. In the left pane, select **SA-Compute-01**.

   c. In the right pane, click the **Hosts** tab.

      If the ESXi hosts have a status of Disconnected, then perform substeps d through f.

   d. Right-click **sa-esxi-01.vclass.local** and select **Connection** > **Connect**.

   e. Perform step d to reconnect sa-esxi-02.vclass.local and sa-esxi-03.vclass.local.

   f. Verify that all three ESXi hosts have a status of Connected.

## Task 4: Create a Distributed Switch

You create a distributed switch that functions as a single virtual switch across all associated hosts in your vSphere environment.

1. Select **Networking** from the **Menu** drop-down menu.
2. Right-click **SA-Datacenter** and select **Distributed Switch** > **New Distributed Switch**.

   The New Distributed Switch wizard appears.
3. On the Name and location page, enter **`dvs-Lab`** in the **Name** text box and click **Next**.
4. On the Select version page, leave **6.6.0 - ESXi 6.6 and later** selected and click **Next**.
5. On the Configure settings page, enter **`pg-SA-Production`** in the **Port group name** text box, keep all other default values, and click **Next**.
6. On the Ready to complete page, review the configuration settings and click **Finish**.
7. In the left pane, expand **SA-Datacenter** and verify that the dvs-Lab distributed switch appears.
8. Configure the pg-SA-Production port group to use only Uplink 2.
   a. In the left pane, expand dvs-Lab.
   b. Right-click **pg-SA-Production** and select **Edit Settings**.
   c. In the Edit Settings window, select **Teaming and failover** on the left.
   d. Select **Uplink 1** and click the down arrow until the uplink appears under Unused uplinks.
   e. Select **Uplink 3** and click the down arrow to move it to the Unused uplinks section.
   f. Select **Uplink 4** and move it to the Unused uplinks section.


   g. Click **OK**.

## Task 5: Add ESXi Hosts to the New Distributed Switch

You add ESXi hosts and physical adapters to the distributed switch.

1. In the left pane, right-click **dvs-Lab** and select **Add and Manage Hosts**.
2. On the Select task page, leave **Add hosts** clicked and click **Next**.
3. On the Select hosts page, click **New hosts** (the green plus sign).
4. Select the **sa-esxi-01.vclass.local** and **sa-esxi-02.vclass.local** check boxes and click **OK**.

   Do not select the **sa-esxi-03.vclass.local** check box.
5. Click **Next**.
6. On the Manage physical adapters page, assign vmnic2 to Uplink 2 on sa-esxi-01.vclass.local and sa-esxi-02.vclass.local.
   a. Under sa-esxi-01.vclass.local, select **vmnic2** and click **Assign uplink**.
   b. Select **Uplink 2** and click **OK**.
   c. Under sa-esxi-02.vclass.local, select **vmnic2** and click **Assign uplink**.
   d. Select **Uplink 2** and click **OK**.
   e. Click **Next**.
7. On the Manage VMkernel Adapters page, click **Next**.
8. On the Migrate VM Networking page, click **Next**.
9. On the Ready to complete page, review settings and click **Finish**.

## Task 6: Examine Your Distributed Switch Configuration

You examine distributed switch features, including the maximum transmission unit (MTU) value, VLAN capabilities, LACP aggregation groups, NetFlow, and VMware vSphere® Network I/O Control.

1. In the left pane, select **dvs-Lab**.
2. In the right pane, click the **Configure** tab and select **Topology** under Settings.
3. In the distributed switch topology diagram, click the arrow next to Uplink 2 to expand the view.
4. Verify that for both ESXi hosts the vmnic2 is attached and appears under Uplink 2.
5. Select **Properties** under Settings and verify the settings.
   - Network I/O Control is enabled.
   - Number of uplinks is 4.
   - The MTU size is 1500 bytes.
   - The Cisco Discovery Protocol is implemented.

6. Click each additional configuration link on the left and verify settings.
   - LACP LAG is not defined.
   - Private VLAN is not defined.
   - NetFlow collector is not defined.
   - Port mirroring is not configured.
   - Health check is not enabled.
7. In the left pane, select the **pg-SA-Production** port group.
8. In the right pane, click the **Configure** tab and select **Properties** on the left.
9. Verify the distributed port group settings.
   - Port binding is set to static binding.
   - Port allocation is set to elastic.
   - The number of ports is eight.

## Task 7: Migrate the Virtual Machines to a Distributed Switch Port Group

You move the virtual machines from the pg-SA-Management port group on the dvs-SA-Datacenter distributed switch to the pg-SA-Production port group on the dvs-Lab distributed switch.

1. In the left pane, expand the dvs-SA-Datacenter distributed switch.
2. Right-click **pg-SA-Management** and select **Migrate VMs to Another Network**.

   The Migrate VMs to Another Network wizard appears.
3. Migrate the virtual machines from pg-SA-Management on the dvs-SA-Datacenter distributed switch to the pg-SA-Production network on the dvs-Lab distributed switch.
   a. For the Destination network, click **Browse**.
   b. Select **pg-SA-Production** and click **OK**.
   c. Click **Next**.
   d. On the Select VMs to migrate page, select the **All virtual machines** check box.
   e. Click **Next**.
4. On the Ready to complete page, review settings and click **Finish**.

5. Verify your distributed switch configuration.
   a. In the left pane, select **dvs-Lab** and click the **Hosts** tab in the right pane.
   b. Verify that sa-esxi-01.vclass.local and sa-esxi-02.vclass.local are connected to the distributed switch.

      The state of the ESXi hosts should be Connected.
   c. Click the **VMs** tab and verify that your virtual machines are listed.

      If the virtual machines are listed, then they reside on the new distributed switch.
   d. Click the **Ports** tab and verify that pg-SA-Production is listed in the Port Group column and an uplink port group is created for the distributed switch.

      You can expand the Port Group column so that you can view the full name of the uplink port group.
6. Select **Hosts and Clusters** from the **Menu** drop-down menu.
7. Power on Linux01 and log in to its console.
   a. In the left pane, select **Linux01**.
   b. Right-click **Linux01** and select **Power** > **Power On**.
   c. In the right pane, click the **Launch Web Console** link.

      Wait for the virtual machine to finish booting.
   d. Log in as user root and use the password VMware1!.
8. At the command prompt, ping 172.20.10.10 (the domain controller's IP address) to verify that the virtual machine has full network connectivity.

   ```
   ping 172.20.10.10
   ```

   The `ping` command should be successful.
9. If the `ping` command is successful, press Ctrl+C to end the `ping` command.
10. If the `ping` command is not successful, then restart the network.
    a. Enter the **`service network restart`** command to ensure that your virtual machine has a valid DHCP-assigned IP address.
    b. Repeat steps 8 and 9.
11. Close the **Linux01** virtual machine console tab.

## Task 8: Enable the Distributed Switch Health Check

You enable the health check service on the dvs-Lab distributed switch.

1. Select **Networking** from the **Menu** drop-down menu.
2. In the left pane, select **dvs-Lab**.
3. In the right pane, click the **Configure** tab and select **Health Check** on the left.
4. Click **Edit**.
5. Under VLAN and MTU, select **Enabled** from the **State** drop-down menu.
6. Under Teaming and failover, select **Enabled** from the **State** drop-down menu.
7. Click **OK**.

## Task 9: Back Up the Distributed Switch Configuration

You back up the dvs-Lab distributed switch configuration.

1. In the left pane, right-click **dvs-Lab** and select **Settings** > **Export Configuration**.
2. In the Export Configuration dialog box, leave **Distributed switch and all port groups** clicked and click **OK**.
3. Save the distributed switch configuration to the desktop of the student desktop machine by using the default `backup.zip` filename.
4. Keep the **vSphere Client** tab open for the next lab.

# *Lab 2* Using Port Mirroring

## Objective: Configure port mirroring and capture network traffic on a distributed switch

In this lab, you perform the following tasks:

1. Prepare to Capture Mirrored Network Traffic
2. Configure Port Mirroring on the Distributed Switch
3. Verify That Port Mirroring Is Capturing Traffic
4. Restore the Distributed Switch Configuration

### Task 1: Prepare to Capture Mirrored Network Traffic

You use the Linux01 virtual machine to capture and monitor mirrored traffic.

1. In Firefox, click the **vSphere Client** tab.
2. If you logged out of vSphere Client, log in as administrator@vsphere.local with the VMware1! password.
3. In vSphere Client, select **Hosts and Clusters** from the **Menu** drop-down menu.
4. In the left pane, expand **SA-Datacenter** and expand the **SA-Compute-01** cluster.
5. Log in to the Linux01 console.
    a. In the left pane, select **Linux01**.
    b. In the right pane, click the **Launch Web Console** link.
    c. If needed, log in as root with the VMware1! password.

6. In the Linux01 console, enter **`tcpdump -nn icmp`** at the command prompt.

   This command line is used to monitor ICMP network traffic.


7. Monitor the command output for a few seconds and verify that ICMP traffic is not being captured.

   `tcpdump` output will not have any information to display until ICMP traffic is detected on the network.

8. Leave the console window open with the `tcpdump` command running uninterrupted.
9. Return to the **vSphere Client** tab.
10. Power on the Linux02 virtual machine and log in to its console.
    a. In the left pane, select **Linux02**.
    b. Right-click **Linux02** and select **Power** > **Power On**.
    c. In the right pane, click the **Launch Web Console** link.

       Wait for the virtual machine to finish booting.

    d. Log in as root with the VMware1! password.

       The Linux02 virtual machine is used as the traffic source to be monitored.

11. At the Linux02 command prompt, enter **`ping 172.20.10.10`**.

    This command pings the default router IP address.

12. If the `ping` command does not work, enter **`service network restart`** and repeat step 11.
13. After the `ping` command begins working, click the **Linux01** console tab.
14. In the Linux01 console window, verify that the running `tcpdump` command output remains silent and has not captured any ICMP traffic.

## Task 2: Configure Port Mirroring on the Distributed Switch

You configure port mirroring so that the port connected to the Linux02 virtual machine is the mirror source and the port connected to the Linux01 virtual machine is the mirror destination. All the traffic present on the Linux02 port is forwarded to the Linux01 port for examination.

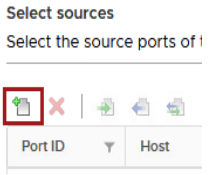
1. Return to the **vSphere Client** tab.
2. Verify that the Linux01 virtual machine is hosted on sa-esxi-01.vclass.local.
   a. In the left pane, select **Linux01**.
   b. On the **Summary** tab, verify that Linux01 resides on the sa-esxi-01.vclass.local host.
3. If Linux01 is not hosted on sa-esxi-01, migrate Linux01 to sa-esxi-01.
   a. Right-click **Linux01** and click **Migrate**.

      The Migrate wizard appears.
   b. On the Select a migration type page, click **Change compute resource only** and click **Next**.
   c. On the Select a compute resource page, click **sa-esxi-01.vclass.local** and click **Next**.
   d. On the Select networks page, keep the default value and click **Next**.
   e. On the Select vMotion priority page, keep the default value and click **Next**.
   f. On the Ready to complete page, click **Finish**.
   g. Expand the Recent Tasks pane and monitor the migration task to completion.
   h. Close the **Linux01** console tab.
   i. Start a new web console to Linux01.
4. Verify that the Linux02 virtual machine is also hosted on sa-esxi-01.vclass.local.
5. If Linux02 is not on sa-esxi-01.vclass.local, then perform step 3 to migrate Linux02 to sa-esxi-01.
6. Add a port mirroring session.
   a. Select **Networking** from the **Menu** drop-down menu.
   b. In the left pane, expand **SA-Datacenter** and select **dvs-Lab**.
   c. In the right pane, click the **Configure** tab and select **Port Mirroring** on the left.
   d. In the Port Mirroring panel, click **New**.

      The Add Port Mirroring Session wizard appears.
   e. On the Select session type page, leave **Distributed Port Mirroring** clicked and click **Next**.

      When you select this session type, distributed ports can only be local. If the source and destination ports are on different hosts, port mirroring does not work between them. The Linux01 and Linux02 virtual machines both reside on sa-esxi-01.vclass.local.

7. On the Edit properties page, configure the port mirroring session.
    a. Select **Enabled** from the **Status** drop-down menu.
    b. Select **Allowed** from the **Normal I/O on destination ports** drop-down menu.
    c. Keep the rest of the default values and click **Next**.
8. On the Select sources page, configure the port mirroring source.
    a. Click the **Select distributed ports to add to this port mirroring session** icon.



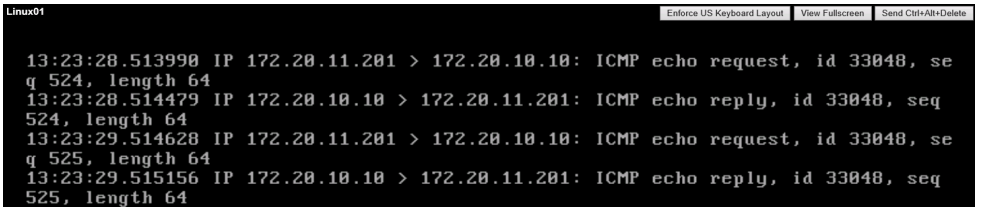

    b. In the Select Ports dialog box, select the check box for the row with a connected entity of Linux02 and click **OK**.
    c. Click **Next**.
9. On the Select destinations page, configure the port mirroring destination.
    a. Click the **Select distributed ports to add to this port mirroring session** icon.
    b. In the Select Ports dialog box, select the check box for the row with a connected entity of Linux01 and click **OK**.
    c. Click **Next**.
10. On the Ready to complete page, review settings and click **Finish**.

## Task 3: Verify That Port Mirroring Is Capturing Traffic

With mirroring between ports configured, you view the `tcpdump` command output and verify that any ICMP traffic appearing on the Linux02 port is duplicated on the Linux01 port.

1. Return to the **Linux02** console tab.
2. Verify that the `ping` command is still reaching the default router IP address.
3. Return to the **Linux01** console tab.
4. In the Linux01 console, examine the `tcpdump` output in the terminal window.

   The output looks similar to the screenshot.




5. Record the local address that appears in the captured traffic. _____

   The local address begins with 172.20.11.
6. In the Linux01 console window, press Ctrl+C to stop the `tcpdump` command.
7. Click the **Linux02** console tab.
8. In the Linux02 console window, press Ctrl+C to stop the `ping` command.
9. At the Linux02 command prompt, enter **`ifconfig`** to examine the IP configuration.
10. Use the command output to verify that the Linux02 IP address matches the address that you recorded in step 5.
11. Close the **Linux01** and **Linux02** console tabs.
12. Shut down Linux01 and Linux02.
    a. Select **Hosts and Clusters** from the **Menu** drop-down menu.
    b. In the left pane, right-click **Linux01** and select **Power** > **Shut Down Guest OS**.
    c. In the pop-up window, click **Yes** to confirm the shutdown operation.
    d. Repeat substeps b and c to shut down Linux02.

## Task 4: Restore the Distributed Switch Configuration

You restore the dvs-Lab distributed switch configuration to reset any configuration change made since the configuration was saved.

1. Select **Networking** from the **Menu** drop-down menu.
2. In the left pane, right-click the **dvs-Lab** distributed switch and select **Settings** > **Restore Configuration**.

   The Restore Configuration wizard appears.
3. On the Restore switch configuration page, click **Browse**, select the **backup.zip** file in the `Desktop` folder, and click **Open**.
4. Leave **Restore distributed switch and all port groups** clicked and click **Next**.
5. On the Ready to complete page, review the settings and click **Finish**.
6. If you lose connection to VMware vSphere® Web Client, restart the Firefox browser.
7. After the switch configuration is restored, verify the configuration.

   **NOTE**

   If the switch configuration did not restore properly, repeat steps 1 through 5.

   a. View the Port Mirroring and verify that the dvs-Lab distributed switch does not have any port mirroring session.
8. Keep the **vSphere Client** tab open for the next lab.

# *Lab 3* Policy-Based Storage

## Objective: Use policy-based storage to create tiered storage

In this lab, you perform the following tasks:

1. Add Datastores for Use by Policy-Based Storage
2. Use vSphere Storage vMotion to Migrate a Virtual Machine to the Gold Datastore
3. Configure Storage Tags
4. Create Virtual Machine Storage Policies
5. Assign Storage Policies to Virtual Machines

### Task 1: Add Datastores for Use by Policy-Based Storage

You create two small datastores for use by your vCenter Server instance as simple tiered storage. One datastore is approximately 7 GB in size and the other is 5 GB.

1. In Firefox, click the **vSphere Client** tab.
2. If you are logged out of vSphere Client, log in as administrator@vsphere.local with the password VMware1!.
3. In vSphere Client, select **Storage** from the **Menu** drop-down menu.

4. Create a datastore named Gold.
    a. In the left pane, right-click **SA-Datacenter** and select **Storage** > **New Datastore**.

       The New Datastore wizard appears.
    b. On the Type page, leave **VMFS** clicked and click **Next**.
    c. On the Name and device selection page, enter `Gold` in the **Datastore name** text box.
    d. Select **sa-esxi-02.vclass.local** from the **Select a host to view its accessible disks/LUNs** list.
    e. In the disk/LUN list, select the entry with 6.94 GB attached as an iSCSI device.

       Local drives are labeled as Local VMware Disk. Do not select these drives.
    f. If iSCSI devices are not present, ask the instructor for instructions to add them.
    g. Click **Next**.
    h. On the VMFS version page, leave **VMFS 6** clicked and click **Next**.
    i. On the Partition configuration page, keep the default values and click **Next**.
    j. On the Ready to complete page, review settings and click **Finish**.
    k. In the left pane, expand **SA-Datacenter** and verify that the Gold datastore appears.
5. Create a datastore named Silver.
    a. In the left pane, right-click **SA-Datacenter** and select **Storage** > **New Datastore**.

       The New Datastore wizard appears.
    b. On the Type page, leave **VMFS** clicked and click **Next**.
    c. On the Name and device selection page, enter `Silver` in the **Datastore name** text box.
    d. Select **sa-esxi-02.vclass.local** from the **Select a host to view its accessible disks/LUNs** list.
    e. In the disk/LUN list, select the entry with 4.94 GB attached as an iSCSI device.

       Local drives are labeled as Local VMware Disk. Do not select these drives.
    f. Click **Next**.
    g. On the VMFS version page, leave **VMFS 6** clicked and click **Next**.
    h. On the Partition configuration page, keep the default values and click **Next**.
    i. On the Ready to complete page, review settings and click **Finish**.
    j. Verify that the Silver datastore appears in the left pane.

## Task 2: Use vSphere Storage vMotion to Migrate a Virtual Machine to the Gold Datastore

Use VMware vSphere® Storage vMotion® to migrate the Photon-01 virtual machine to the Gold datastore.

1. Power on Photon-01.
   a. Select **Hosts and Clusters** from the **Menu** drop-down menu.
   b. Right-click **Photon-01** and select **Power** > **Power On**.
   c. When Photon-01 is powered on, go to step 2.
2. In the left pane, right-click **Photon-01** and select **Migrate**.

   The Migrate wizard appears.
3. On the Select a migration type page, click **Change storage only** and click **Next**.
4. On the Select storage page, select the **Gold** datastore, leave all other settings at their default values, and click **Next**.
5. On the Ready to complete page, click **Finish**.
6. In the Recent Tasks pane, monitor the migration task to completion.
7. Verify that the migration was successful.

   You might have to refresh vSphere Client to see that the migration has completed.
   a. In the left pane, select **Photon-01**.
   b. In the right pane, click the **Datastores** tab and verify that the Gold datastore is listed.

## Task 3: Configure Storage Tags

You create the tags necessary to implement simple tiering. The Storage Tiers tag category contains the Gold and Silver identifier tags associated with individual datastores.

1. Select **Tags & Custom Attributes** from the **Menu** drop-down menu.
2. In the right pane, click the **Tags** tab.
3. Configure a new tag category and the Gold Tier identifier tag.
   a. In the Tags panel, click the **Add Tag** (+) icon.
   b. In the **Name** text box, enter `Gold Tier`.
   c. Click the **Create New Category** link next to the **Category** drop-down menu.

      A dialog box appears that includes tag and category configuration options.

      Categories can be created only as part of the identifier tag creation process.
   d. In the **Category Name** text box, enter `Storage Tiers`.
   e. Keep the default values for the remaining settings and click **OK**.
   f. In the Add Tag dialog box, click **OK**.
4. Create a Silver Tier identifier tag.
   a. In the Tags panel, click the **Add Tag** (+) icon.
   b. In the **Name** text box, enter `Silver Tier`.
   c. Select **Storage Tiers** from the **Category** drop-down menu and click **OK**.
5. Assign the Gold Tier tag to the Gold datastore.
   a. Select **Storage** from the **Menu** drop-down menu.
   b. In the left pane, right-click the **Gold** datastore and select **Tags & Custom Attributes** > **Assign Tag**.
   c. Select the **Gold Tier** tag and click **Assign**.
   d. In the left pane, select the **Gold** datastore.
   e. In the Tags panel on the **Summary** tab, verify that the Gold Tier tag is associated with the Gold datastore.

6. Assign the Silver Tier tag to the Silver datastore.
   a. In the left pane, right-click the **Silver** datastore and select **Tags & Custom Attributes** > **Assign Tag**.
   b. Select the **Silver Tier** tag and click **Assign**.
   c. In the left pane, select the **Silver** datastore.
   d. In the Tags panel on the **Summary** tab, verify that the Silver Tier tag is associated with the Silver datastore.

## Task 4: Create Virtual Machine Storage Policies

You assign storage policies to virtual machines and specify the configuration settings to be enforced.

1. Select **Policies and Profiles** from the **Menu** drop-down menu.
2. In the left pane, click **VM Storage Policies**.
3. Create a Gold Tier storage policy.
   a. In the VM Storage Policies panel, click **Create VM Storage Policy**.

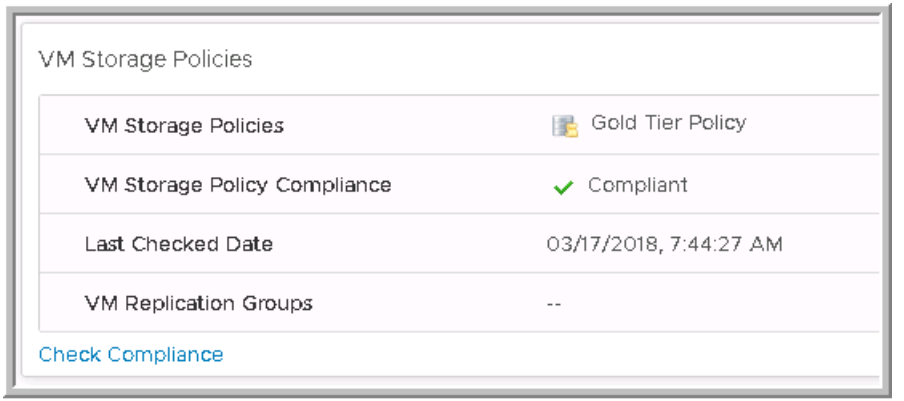
      The Create VM Storage Policy wizard appears.
   b. On the Name and description page, enter `Gold Tier Policy` in the **Name** text box and click **Next**.
   c. On the Policy structure page, select the **Enable tag based placement rules** check box and click **Next**.
   d. On the Tag based placement page, select **Storage Tiers** from the **Tag category** drop-down menu.
   e. Click **Browse Tags**, select the **Gold Tier** check box, and click **OK**.
   f. Click **Next**.
   g. On the Storage compatibility page, verify that the Gold datastore is listed under Compatible storage and click **Next**.
   h. On the Review and finish page, click **Finish**.
4. Repeat step 3 to create Silver Tier Policy by using the Silver Tier tag.

## Task 5: Assign Storage Policies to Virtual Machines

You assign the Gold and Silver storage policies to individual virtual machines and mitigate compliance issues. A storage policy can be assigned to a virtual machine while the virtual machine is either powered on or powered off.

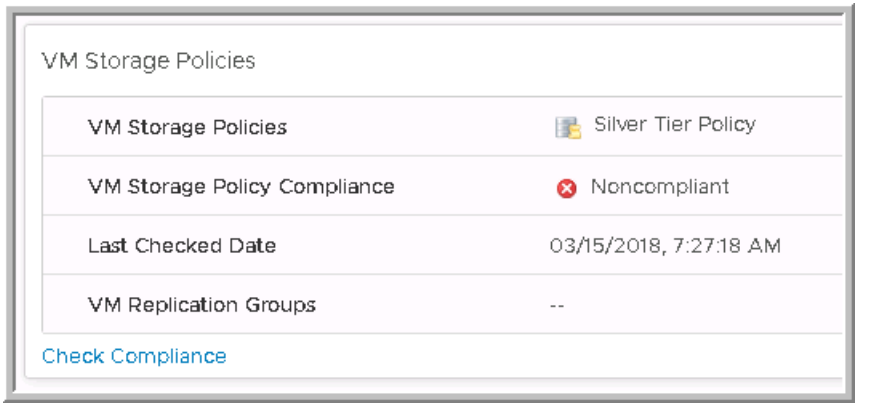
1. Power off Photon-01.
   a. Select **Hosts and Clusters** from the **Menu** drop-down menu.
   b. Right-click **Photon-01** and select **Power** > **Power Off**.
   c. Click **Yes** to confirm the power-off operation.
2. Apply the Gold Tier storage policy to the Photon-01 virtual machine.
   a. Right-click **Photon-01** and select **VM Policies** > **Edit VM Storage Policies**.
   b. In the Edit VM Storage Policies dialog box, select **Gold Tier Policy** from the **VM storage policy** drop-down menu.
   c. Click **OK**.
   d. In the left pane, select **Photon-01**.
   e. In the right pane, click the **Summary** tab.
   f. Scroll down and expand the VM Storage Policies panel.
   g. Verify that Gold Tier Policy appears and that Photon-01 is compliant.

      The Photon-01 virtual machine is compliant because it was already moved to a policy-appropriate datastore.



3. Apply the Silver Tier storage policy to the Photon-02 virtual machine.
   a. In the left pane, right-click **Photon-02** and select **VM Policies** > **Edit VM Storage Policies**.
   b. In the Edit VM Storage Policies dialog box, select **Silver Tier Policy** from the **VM storage policy** drop-down menu.
   c. Click **OK**.
   d. In the left pane, select **Photon-02**.
   e. In the right pane, click the **Summary** tab.
   f. View the VM Storage Policies panel and verify that Silver Tier Policy appears and that Photon-02 is not compliant.

      The Photon-02 virtual machine is noncompliant because its virtual disk is stored on a datastore that is not tagged as a part of the assigned policy.




4. Remediate the compliance issue for Photon-02.
   a. In the left pane, right-click **Photon-02** and select **Migrate**.

      The Migrate wizard appears.
   b. On the Select a migration type page, click **Change storage only** and click **Next**.
   c. On the Select storage page, select the **Silver** datastore in the datastore list.

      With a virtual machine storage policy assigned to the Photon-02 virtual machine, datastores are listed as either Compatible or Incompatible.
   d. Click **Next**.
   e. On the Ready to complete page, review the migration details and click **Finish**.
   f. In the Recent Tasks pane, monitor the migration task to completion.

      The migration must complete successfully.

5. Verify that Photon-02 is reported as compliant.
   a. In the right pane, verify that the status in the VM Storage Policies panel is Compliant.
   b. If the status is not Compliant, click the **Check Compliance** link in the VM Storage Policies panel.
   c. Verify that the status changes to Compliant.
6. Keep the **vSphere Client** tab open for the next lab.

# *Lab 4* Creating vSAN Storage Policies

## Objective: Create and review vSAN storage policies

In this lab, you perform the following tasks:

1. Examine the Default Storage Policy
2. Create a Custom Policy with No Failure Tolerance
3. Assign the Custom Policy to a Virtual Machine
4. Make the Virtual Machine Compliant
5. Create an Invalid Storage Policy

### Task 1: Examine the Default Storage Policy

You examine the VMware vSAN™ default storage policy.

**NOTE**

A vSAN datastore has been preconfigured for you.

1. In Firefox, click the **vSphere Client** tab.
2. If you are logged out of vSphere Client, log back in.
3. Select **Policies and Profiles** from the **Menu** drop-down menu.
4. In the left pane, select **VM Storage Policies**.
5. In the right pane, select **vSAN Default Storage Policy** and click **Edit Settings**.

6. On the Name and description page, click **Next**.
7. On the Policy structure page, click **Next**.
8. Examine the rules under the **Availability**, **Advanced Policy Rules**, and **Tags** tabs.

   **Q1. How many failures can be tolerated?**

9. Click **Cancel**.

## Task 2: Create a Custom Policy with No Failure Tolerance

You create a custom vSAN storage policy that does not provide failure tolerance.

1. In the right pane, click **Create VM Storage Policy**.
2. On the Name and description page, enter `Custom01` in the **Name** text box and click **Next**.
3. On the Policy structure page, select the **Enable rules for "vSAN" storage** check box and click **Next**.
4. On the **Availability** tab, select **No data redundancy** from the **Failures to tolerate** drop-down menu.
5. View the consumed storage space information below the drop-down menu.

   **Q1. Why is the storage space size equal to the virtual machine size?**

6. Click **Next**.

   Only the vSAN datastore is listed under Compatible storage.
7. Select **Incompatible** from the drop-down menu in the upper-right corner.

   Several datastores are listed under Incompatible storage.
8. Click **Next**.
9. On the Review and finish page, click **Finish**.
10. Verify that the custom storage policy is created and appears in the list.

## Task 3: Assign the Custom Policy to a Virtual Machine

You create a second virtual machine and apply your new vSAN storage policy.

1. Select **Hosts and Clusters** from the **Menu** drop-down menu.
2. Clone a virtual machine from Photon-01.
   a. In the left pane, right-click **Photon-01** and select **Clone** > **Clone to Virtual Machine**.
   b. On the Select a name and folder page, enter `Payload-02` in the **Virtual machine name** text box and click **Next.**
   c. On the Select a compute resource page, expand **SA-Compute-01**, select **sa-esxi-02.vclass.local**, and click **Next**.
   d. On the Select storage page, select **Datastore Default** from the **VM Storage Policy** drop-down menu.
   e. Select **OPSCALE-Datastore** from the datastore list and click **Next**.
   f. On the Select clone options page, select the **Power on virtual machine after creation** check box and click **Next**.
   g. On the Ready to complete page, click **Finish**.
   h. Monitor the Recent Tasks pane to verify that the Clone virtual machine task completes successfully.
3. Verify that your new virtual machine is listed in the left pane and is powered on.

   If you do not see the virtual machine listed and powered on, click the **Refresh** icon in vSphere Client.
4. Assign the Custom01 storage policy to Payload-02.
   a. In the left pane, right-click **Payload-02** and select **VM Policies** > **Edit VM Storage Policies**.
   b. Select **Custom01** from the **VM storage policy** drop-down menu.

      **Q1. Why do the VM home and Hard disk 1 objects have warning icons?**

   c. Click **OK**.
   d. Monitor the Recent Tasks pane to verify that the Reconfigure virtual machine task completes successfully.
5. In the left pane, select **Payload-02**.

6. In the **Summary** tab, review the Related Objects panel and the VM Storage Policies panel.

   You might need to scroll down in the right pane to see these panels.

   **Q2. On which datastore is the virtual machine located?**

   **Q3. Which storage policy is the virtual machine using?**

   **Q4. Is the virtual machine compliant with its storage policy?**

## Task 4: Make the Virtual Machine Compliant

You migrate the Payload-02 virtual machine from the shared VMware vSphere® VMFS datastore to the vSAN datastore to make it compliant with its storage policy.

1. Migrate the Payload-02 virtual machine to the vSAN datastore to bring it into compliance.
   a. In the left pane, right-click **Payload-02** and select **Migrate**.
   b. On the Select a migration type page, click **Change storage only** and click **Next**.
   c. Leave **Keep existing VM storage policies** selected in the **VM Storage Policy** drop-down menu.
   d. In the datastore list, select **vsanDatastore** and click **Next**.
   e. On the Ready to complete page, click **Finish**.
   f. Monitor the Recent Tasks pane until the task completes successfully.
2. In the right pane, view the VM Storage Policies panel and click the **Check Compliance** link.
3. Verify that the compliance status of Payload-02 changes to Compliant.

## Task 5: Create an Invalid Storage Policy

You create a storage policy that is invalid for the vSAN datastore and apply it to a virtual machine. The purpose of this task is to provide another example of the warning messages that appear when an invalid storage policy is created.

1. Select **Policies and Profiles** from the **Menu** drop-down menu.
2. In the left pane, click **VM Storage Policies**.
3. Use RAID 5/6 erasure coding to create a storage policy that tolerates one failure.
   a. In the right pane, click **Create VM Storage Policy**.
   b. On the Name and description page, enter `RAID5` in the **Name** text box and click **Next**.
   c. On the Policy structure page, select the **Enable rules for "vSAN" storage** check box and click **Next**.
   d. On the **Availability** tab, select **1 failure - RAID-5 (Erasure Coding)** from the **Failures to tolerate** drop-down menu.
   e. Click **Next**.
   f. On the Storage compatibility page, click **Next**.

      Compatible datastores do not exist.

   g. On the Review and finish page, click **Finish**.
4. Assign the RAID5 storage policy to Payload-02.
   a. Select **Hosts and Clusters** from the **Menu** drop-down menu.
   b. In the left pane, right-click **Payload-02** and select **VM Policies** > **Edit VM Storage Policies**.
   c. Select **RAID5** from the **VM storage policy** drop-down menu.

      **Q1. Why do the VM home and Hard disk 1 objects have warning icons?**

5. Click **Cancel**.
6. Select **Policies and Profiles** from the **Menu** drop-down menu.
7. In the left pane, click **VM Storage Policies**.
8. In the right pane, select **RAID5** and click **Delete**.
9. Click **OK**.
10. Leave the **vSphere Client** tab open for the next lab.

# *Lab 5* Managing Datastore Clusters

## Objective: Create a datastore cluster and work with vSphere Storage DRS

In this lab, you perform the following tasks:

1. Create a Datastore Cluster That Is Enabled for vSphere Storage DRS
2. Use Datastore Maintenance Mode to Evacuate a Datastore
3. Run vSphere Storage DRS and Apply Migration Recommendations
4. Clean Up for the Next Lab

### Task 1: Create a Datastore Cluster That Is Enabled for vSphere Storage DRS

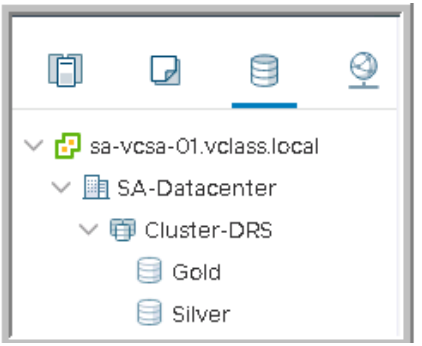
You create a datastore cluster that is enabled for VMware vSphere® Storage DRS™. The Gold and Silver datastores are reused as members of the cluster.

1. In Firefox, click the **vSphere Client** tab.
2. If you are logged out of vSphere Client, log back in.
3. In vSphere Client, select **Storage** from the **Menu** drop-down menu.
4. In the left pane, right-click **SA-Datacenter** and select **Storage > New Datastore Cluster**.

   The New Datastore Cluster wizard appears.
5. On the Name and Location page, name the datastore cluster and enable vSphere Storage DRS.
   a. In the **Datastore cluster name** text box, enter `Cluster-DRS`.
   b. Leave the **Turn ON Storage DRS** check box selected and click **Next**.

6. On the Storage DRS Automation page, view the automation settings.
   a. Click **No Automation (Manual Mode)**.
   b. Keep the rest of the default values and click **Next**.
7. On the Storage DRS Runtime Settings page, keep the default values and click **Next**.
8. On the Select Clusters and Hosts page, select the **SA-Compute-01** check box and click **Next**.
9. On the Select Datastores page, select the datastores for the datastore cluster.
   a. Select **Show all datastores** from the drop-down menu at the top.
   b. Select the **Gold** and **Silver** check boxes and click **Next**.
10. On the Ready to Complete page, review the configuration summary and click **Finish**.

    In a production environment, the best practice is to select datastores that are connected to all hosts in the cluster and to group them by storage capabilities.
11. In the left pane, expand **Cluster-DRS** and verify that the Gold and Silver datastores appear.




12. View information about the Gold datastore.
    a. In the left pane, select the **Gold** datastore.
    b. In the right pane, click the **VMs** tab.
    c. Verify that the datastore contains only one virtual machine.
13. View information about the Silver datastore.
    a. In the left pane, select the **Silver** datastore.
    b. In the right pane, click the **VMs** tab.
    c. Verify that the datastore contains only one virtual machine.

14. View information about the datastore cluster.
    a. In the left pane, select **Cluster-DRS**.
    b. In the right pane, click the **Configure** tab and click **Storage DRS** on the left.
    c. In the vSphere Storage DRS panel, expand each item and verify settings.
        - Cluster automation level is set to No Automation (Manual Mode).
        - Space threshold is 80 percent.
        - I/O metrics for vSphere Storage DRS recommendations are enabled.
        - Imbalances are checked every 8 hours.
        - Minimum space utilization difference is 5 percent.

## Task 2: Use Datastore Maintenance Mode to Evacuate a Datastore

You place a datastore in maintenance mode to demonstrate the capabilities of vSphere Storage DRS.

1. Put the Gold datastore in maintenance mode.
    a. In the left pane, right-click the **Gold** datastore.
    b. Select **Maintenance Mode** > **Enter Maintenance Mode**.
    c. In the Enter Maintenance Mode Warning dialog box, read the provided recommendations.
    d. Click **Continue**.
    e. If prompted to apply recommendations despite warnings, click **Yes**.

       The virtual machine is migrated to the Silver datastore.
    f. In the Recent Tasks pane, monitor the migration task to completion.
2. In the left pane, verify that the Gold datastore is in maintenance mode.
3. Click the **Refresh** icon in the vSphere Client interface.

4. View information about the Silver and Gold datastores.
   a. Select the **Gold** datastore and click the **VMs** tab.
   b. Verify that zero virtual machines are stored on the Gold datastore.
   c. Select the **Silver** datastore and click the **VMs** tab.
   d. Verify that two virtual machines are stored on the Silver datastore.
5. Take the Gold datastore out of maintenance mode.
   a. Right-click the **Gold** datastore and select **Maintenance Mode**> **Exit Maintenance Mode**.
   b. Verify that the Gold datastore icon no longer indicates maintenance mode.
6. Select **Hosts and Clusters** from the **Menu** drop-down menu.
7. Power on the Photon-01 and Photon-02 virtual machines.

## Task 3: Run vSphere Storage DRS and Apply Migration Recommendations

You configure vSphere Storage DRS to maintain a balance in usage across all datastores in a cluster. The cluster imbalance is mitigated by using vSphere Storage DRS recommendations.

1. Select **Storage** from the **Menu** drop-down menu.
2. In the left pane, select **Cluster-DRS**.
3. In the right pane, click the **Configure** tab and select **Storage DRS** on the left.
4. Configure vSphere Storage DRS so that recommendations are reported.
   a. In the vSphere Storage DRS panel, click **Edit**.
   b. Click the **Runtime Settings** tab.
   c. Next to Space threshold, drag the **Utilized space** slider to the left to set the threshold to 60 percent.

      The imbalance between the Gold and Silver datastore utilization is detected at a 60 percent space threshold trigger.
   d. Click **OK**.
5. Refresh the Gold datastore usage report
   a. In the left pane, select **Gold**.
   b. In the right pane, click the **Summary** tab.
   c. In the right pane, click the **Refresh** link to the far right.
6. Repeat step 5 for the Silver datastore.

7. Run vSphere Storage DRS and review recommendations.
   a. In the left pane, select **Cluster-DRS**.
   b. In the right pane, click the **Monitor** tab.
   c. Under Storage DRS, select **Recommendations** on the left.

      A vSphere Storage DRS recommendation appears in the recommendation list.

      If the recommendation does not appear, then click **Run Storage DRS Now**.

      It might take a few minutes before the recommendation appears.
   d. Review the recommendation and reason.

      vSphere Storage DRS recommends the migration of a virtual machine.
8. Examine the vSphere Storage DRS recommendation alarm.
   a. In the right pane, click the **Summary** tab and find the yellow vSphere Storage DRS recommendation alarm.

      The administrator can reset the recommendation alarm manually. The vSphere Storage DRS recommendation alarm is reset when the recommendation is applied.
9. Apply the vSphere Storage DRS recommendation.
   a. In the right pane, click the **Monitor** tab.
   b. Select **Recommendations** on the left.
   c. In the bottom-right corner of the Storage DRS recommendations panel, click **Apply Recommendations**.
   d. In the Recent Tasks pane, monitor the migration task to completion.
10. In the right pane, click the **Summary** tab and verify that no alarms appear.
11. Review vSphere Storage DRS history.
   a. In the right pane, click the **Monitor** tab.
   b. Under Storage DRS, select **History**.
   c. Verify in the vSphere Storage DRS history that a virtual machine was recently migrated from Silver to Gold.
   d. Verify in the vSphere Storage DRS history that a virtual machine was migrated earlier from Gold to Silver.

      This migration occurred when the Gold datastore was placed in maintenance mode.

## Task 4: Clean Up for the Next Lab

You remove the vSphere Storage DRS cluster to prepare for the next lab.

1. Select **Hosts and Clusters** from the **Menu** drop-down menu.
2. Power off the Photon-01 and Photon-02 virtual machines.
3. Delete the vSphere Storage DRS cluster.
   a. Select **Storage** from the **Menu** drop-down menu.
   b. In the left pane, right-click **Cluster-DRS** and select **Delete**.
   c. When prompted, click **Yes** to delete the datastore cluster.
   d. After the cluster is deleted, verify that the Gold and Silver datastores appear in the left pane, directly under the data center.
4. Keep the **vSphere Client** tab open for the next lab.

# *Lab 6* Creating a Content Library

## Objective: Create a multisite content library

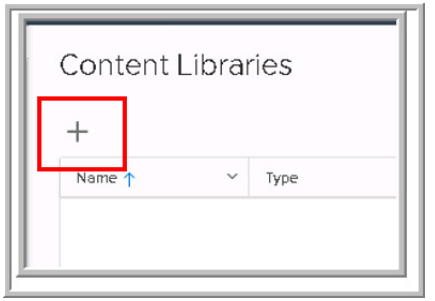
In this lab, you perform the following tasks:

1. Create a Content Library
2. Upload Data to the New Content Library
3. Create a Subscriber Content Library
4. Clone a Template to the Source Library
5. Synchronize the Content Libraries
6. Deploy a Virtual Machine from the Library

## Task 1: Create a Content Library

You configure a local content library that you publish externally for other content libraries to subscribe to.

1. In Firefox, click the **vSphere Client** tab.
2. If you are logged out of vSphere Client, log back in.
3. In vSphere Client, select **Content Libraries** from the **Menu** drop-down menu.
4. In the right pane, click the **Create a new content library** (+) icon.




5. On the Name and location page, name the content library and verify the vCenter Server location.
   a. In the **Name** text box, enter **`SA-Source`**.
   b. In the **vCenter Server** drop-down menu, verify that **sa-vcsa-01.vclass.local** is selected and click **Next**.
6. On the Configure content library page, configure a local content library.
   a. Leave **Local content library** selected.
   b. Select the **Publish externally** check box.
   c. Select the **Enable authentication** check box.
   d. In the **Password** and **Confirm password** text boxes, enter **`VMware1!`**.
   e. Click **Next**.
7. On the Add storage page, click **OPSCALE-Datastore** and click **Next**.
8. On the Ready to complete page, click **Finish**.
9. Verify that the SA-Source content library appears in the list.

   Refresh vSphere Client if you do not see the new content library in the list.

## Task 2: Upload Data to the New Content Library

You upload an Open Virtualization Format (OVF) file from your student desktop to the new content library.

1. In the right pane, right-click the **SA-Source** library and select **Import item**.
2. In the Import Library Item window, click **Local file** and click **Upload File**.
3. In the File Upload window, click the **Desktop** icon on the left bar.
4. Double-click the **Class Materials and Licenses** folder in the right pane and double-click the **Downloads** folder.
5. In the `Downloads` folder, double-click the **SampleVM** folder.
6. Double-click **SampleVM.ovf**.

   `SampleVM.ovf` is added to the Import Library Item dialog box. However, you must also upload `SampleVM-1.vmdk`, `SampleVM-2.iso`, and `SampleVM-3.nvram`.
7. Click the **Upload** link on the right of `SampleVM-1.vmdk`.
8. In the File Upload window, select **SampleVM-1.vmdk**, press Ctrl, and select **SampleVM-2.iso** and **SampleVM-3.nvram**.

   You can use Ctrl to select multiple files in this window.

   Ensure that all three files are selected.
9. Click **Open**.

   You should see four files ready to import.
10. Click **Import**.
11. View the Recent Tasks pane to monitor the task to completion.

    The task might take a few minutes to complete.
12. After the task is complete, click the **SA-Source** link in the right pane.
13. Click the **Templates** tab.
14. Verify that the uploaded SampleVM template is listed.

## Task 3: Create a Subscriber Content Library

You configure a content library that is subscribed to the first library.

1. Copy the link to the local content library to the clipboard.
   a. In the SA-Source pane, click the **Summary** tab and scroll down until the Publication panel appears.
   b. In the Publication panel, click **Copy Link**.
2. Select **Content Libraries** from the **Menu** drop-down menu.
3. In the right pane, click **Create a new content library** (+) icon.

   The New Content Library wizard appears.
4. On the Name and location page, name the content library and verify the vCenter Server location.
   a. In the **Name** text box, enter **`SA-Subscriber`**.
   b. In the **vCenter Server** drop-down menu, verify that **sa-vcsa-01.vclass.local** is selected.
   c. Click **Next**.
5. On the Configure content library page, configure a subscribed content library.
   a. Click **Subscribed content library**.
   b. Click the **Subscription URL** text box and press Ctrl+V.

      The subscription URL is pasted into the text box. If Ctrl+V does not work, you must enter the URL manually.
   c. Select the **Enable authentication** check box.
   d. In the **Password** text box, enter **`VMware1!`**.
   e. In the Download content line, click **when needed**.
   f. Click **Next**.
6. On the Add storage page, select **OPSCALE-Datastore** and click **Next**.
7. On the Ready to complete page, click **Finish**.
8. View the Recent Tasks pane to monitor the task to completion.
9. View the contents of the content library subscriber.
   a. In the left pane, select the **SA-Subscriber** library.
   b. In the right pane, click the **Templates** tab.
   c. On the **Templates** tab, verify that the `SampleVM.ovf` template is present.

      This virtual machine template is the same template that is in the source content library.

d. Verify that the Stored Locally column indicates No and the Size column indicates 0 bytes.

   The SA-Subscriber library is configured to download library content only when needed. As a result, only the template's metadata has been synchronized. The actual template has not been synchronized with the SA-Subscriber library, because it is not needed yet.

10. Turn off automatic synchronization.
    a. In the right pane, click the **Summary** tab.
    b. In the Subscription panel, click the **Edit Settings** link.
    c. Deselect the **Enable automatic synchronization with the external content library** check box.
    d. Reenter the standard lab password in the **Password** text box.

       If you do not reenter the password, the process fails.

    e. Click **OK**.
    f. In the Subscription panel, verify that automatic synchronization is off.

## Task 4: Clone a Template to the Source Library

You clone a virtual machine template into the published content library.

1. Select **Hosts and Clusters** from the **Menu** drop-down menu.
2. Power off the Photon-01 virtual machine if it is powered on.
3. In the left pane, right-click the **Photon-01** virtual machine and select **Clone** > **Clone to Template in Library**.

   The Clone to Template in Library window appears.
4. Click **SA-Source**.
5. Append **`-Library`** to the virtual machine name in the **Template name** text box and click **OK**.
6. In the Recent Tasks pane, view the tasks that start up and monitor the tasks to completion.

   All tasks might take a few minutes to complete.
7. View the template list in both libraries.
   a. Select **Content Libraries** from the **Menu** drop-down menu.
   b. In the left pane, select the **SA-Source** library.
   c. In the right pane, click the **Templates** tab and verify that both templates are listed.
   d. In the left pane, select the **SA-Subscriber** library.
   e. In the right pane, view the **Templates** tab and verify that only the original template is listed.

## Task 5: Synchronize the Content Libraries

You use vSphere Client to synchronize the content libraries.

1. In the right pane at the top, select **Synchronize** from the **Actions** drop-down menu.
2. In the Recent Tasks pane, monitor the task to completion.
3. Verify that both the virtual machine templates appear in the SA-Subscriber library.

   You might need to refresh the screen to see both templates.

## Task 6: Deploy a Virtual Machine from the Library

You use vSphere Client to deploy a new virtual machine from the Photon-01-Library template available in the SA-Subscriber library.

1. In the SA-Subscriber pane, right-click **Photon-01-Library** on the **Templates** tab and select **New VM from This Template**.

   The New Virtual Machine from Content Library wizard appears.
2. On the Select a name and folder page, name the virtual machine and select the inventory tree location.
   a. In the **Virtual machine name** text box, enter `Photon-03`.
   b. For the virtual machine location, select **SA-Datacenter** and click **Next**.
3. On the Select a compute resource page, expand **SA-Compute-01**, select **sa-esxi-01.vclass.local**, and click **Next**.
4. On the Review details page, click **Next**.
5. On the Select storage page, configure the virtual disk format and select a datastore.
   a. Select **OPSCALE-Datastore**.
   b. Select **Thin Provision** from the **Select virtual disk format** list.
   c. Select **Datastore Default** from the **VM Storage Policy** list.
   d. Click **Next**.
6. On the Select networks page, keep the default value and click **Next**.
7. On the Ready to complete page, click **Finish**.

8. In the Recent Tasks pane, view the tasks that are started and monitor the tasks to completion.

   All tasks might take a few minutes to complete.

9. For the Photon-01-Library template, view the Stored Locally column.

   The column value changes to Yes.

   You might need to refresh the screen to see the change.

   The Size column has a nonzero value.

10. Verify that the virtual machine is deployed.
    a. Select **Hosts and Clusters** from the **Menu** drop-down menu.
    b. In the left pane, verify that the Photon-03 virtual machine appears in the inventory.
11. In preparation for the next lab, ensure that all virtual machines in the SA-Compute-01 cluster are shut down.
12. Log out of vSphere Client and close the tab.

# *Lab 7* Using vSphere Auto Deploy

## Objective: Configure vSphere Auto Deploy on vCenter Server Appliance to boot stateless hosts

In this lab, you perform the following tasks:

1. Create a Folder for Autodeployed Hosts
2. Start the vSphere Auto Deploy Service
3. Start the vSphere ESXi Image Builder Service
4. Import a Software Depot and Create a Custom Depot
5. Create a Custom Image Profile and Export the Image Profile
6. Create and Activate a Deployment Rule
7. Configure DHCP
8. Start the TFTP Service on vCenter Server Appliance
9. Review the Autodeployment Preparation Steps
10. Prepare to Monitor ESXi Bootup During the Autodeploy Process
11. Power On the ESXi Host and Monitor the Bootup Process
12. Verify Host Profile Compliance of the Autodeployed Host
13. Review the Noncompliant Items

You use vSphere Web Client to perform the tasks in this lab.

## Task 1: Create a Folder for Autodeployed Hosts

You create a folder in the vCenter Server inventory into which autodeployed hosts are placed. A deploy rule assigns hosts to this folder.

1. On the student desktop, open Firefox.
2. In the Firefox favorites toolbar, click the **vSphere Web Client (SA-VCSA-01)** bookmark from the `vSphere Site-A` folder.
3. At the login screen, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
4. In vSphere Web Client, point to the **Home** icon and select **Hosts and Clusters**.
5. In the Hosts and Clusters inventory tree, right-click **SA-Datacenter** and select **New Folder** > **New Host and Cluster Folder** from the drop-down menu.
6. Enter **`Auto-Deployed-Hosts`** in the **folder name** text box and click **OK**.

   At this stage, you can create clusters, folders, or other vSphere configurations to apply to autodeployed hosts. Deploy rules enable selective application of host profiles and destination containers to hosts that are booting up.

## Task 2: Start the vSphere Auto Deploy Service

The VMware vSphere® Auto Deploy™ capability is already installed on VMware vCenter® Server Appliance™, but the service is not started by default. You start the service and set the startup type to automatic.

1. Point to the **Home** icon and select **Home**.
2. Select the vSphere Auto Deploy service.
   a. In the center pane, click the **System Configuration** icon under Administration.
   b. In the left pane, select **Services**.
   c. Under Services, select **Auto Deploy**.
3. Start the vSphere Auto Deploy service.
   a. Select **Start** from the **Actions** drop-down menu.
   b. In the center pane, view the **Summary** tab and verify the state of the service.
4. Configure the vSphere Auto Deploy service to automatically start when vCenter Server starts.
   a. Select **Edit Startup Type** from the **Actions** drop-down menu.
   b. In the Edit Startup Type window, click **Automatic** and click **OK**.
   c. In the **Summary** tab, verify that the startup type is Automatic.

## Task 3: Start the vSphere ESXi Image Builder Service

On vCenter Server Appliance, the VMware vSphere® ESXi™ Image Builder CLI capability is already installed, but the service is not started by default.

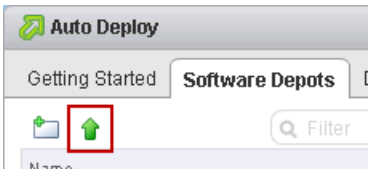
1. In the left pane under Services, select **ImageBuilder Service**.
2. Start the vSphere ESXi Image Builder service.
   a. Select **Start** from the **Actions** drop-down menu.
   b. In the center pane, view the **Summary** tab and verify that the service state is Running.
3. Configure the vSphere ESXi ImageBuilder service to automatically start when vCenter Server starts.
   a. Select **Edit Startup Type** from the **Actions** drop-down menu.
   b. In the Edit Startup Type window, select **Automatic** and click **OK**.
   c. In the **Summary** tab, verify that the startup type is Automatic.
4. Make the **Auto Deploy** icon visible in vSphere Web Client.

   The **Auto Deploy** icon is not visible until you log out and log in to vSphere Web Client.
   a. Log out of vSphere Web Client.
   b. Log in to vSphere Web Client as administrator@vsphere.local with the password VMware1!.

## Task 4: Import a Software Depot and Create a Custom Depot

You use vSphere Web Client to import an ESXi software depot into vCenter Server and to create a custom software depot.

1. Point to the **Home** icon and select **Home**.
2. In the center pane, click the **Auto Deploy** icon under Operations and Policies.
3. Import an ESXi software depot into vCenter Server.
   a. In the center pane, click the **Software Depots** tab.
   b. Click the **Import software depot** icon.




   c. In the **Name** text box, enter `SA Depot`.

d. Click **Browse** next to the **File** text box.

e. In the File Upload window, navigate to `C:\Materials\Downloads`.

f. Select **VMware-ESXi-6.7.0-depot.zip** and click **Open**.

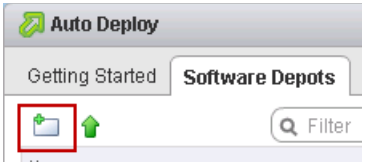
g. Click **Upload** and wait for the file to upload.

h. When the file is successfully uploaded, click **Close**.

i. Verify that the software depot appears in the list.

4. Create a custom software depot.

a. Click the **Add Software Depot** icon.




b. In the Add Software Depot dialog box, click **Custom depot**.

c. In the **Name** text box, enter **`My Depot`**.

d. Click **OK**.

## Task 5: Create a Custom Image Profile and Export the Image Profile

You use vSphere Web Client to clone an image profile and export the profile to a ZIP archive.

1. Clone an image profile.

a. In the center pane, select **SA Depot** on the **Software Depots** tab.

b. Under Image Profiles, select the image profile whose name ends in `-no-tools`.

c. Click the **Clone image profile** icon.


The Clone Image Profile wizard appears.

d. On the Name and details page, keep the default name in the **Name** text box.

e. In the **Vendor** text box, enter **`VMware`**.

f. From the **Software depot** list, select **My Depot** and click **Next**.

g. On the Select software packages page, view the various software packages and click **Next**.

h. On the Ready to complete page, click **Finish**.

2. Verify that the clone is created.

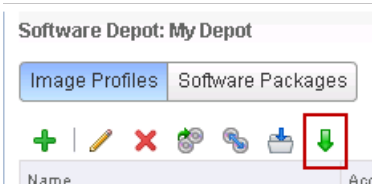
   a. Select **My Depot**.

   b. Under Image Profiles, verify that the cloned image profile appears.

3. Export the image profile to a ZIP archive.

   a. Under Image Profiles, select the cloned image profile.

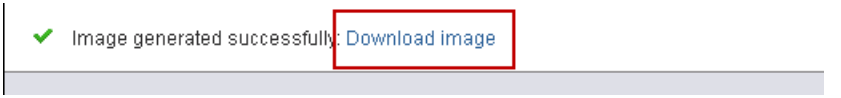
   b. Click the **Export the selected image profile as ISO or ZIP** icon.




   c. In the Export Image Profile dialog box, click **ZIP**.

   d. Click **Generate image**.

   e. When the image generation completes, click the **Download image** link.




   f. Use the default name and save the ZIP file to the desktop on the student machine.

   g. In the Export Image Profile dialog box, click **Close**.

## Task 6: Create and Activate a Deployment Rule

You create and activate a deployment rule. Deployment rules associate host profiles, image profiles, destination containers, and many other capabilities to hosts engaged in the autodeploy process. Different sets of rules can associate different characteristics to hosts, based on several conditions and qualifiers, such as the network on which the host boots.

1. Create a deployment rule.
   a. In the center pane, click the **Deploy Rules** tab.
   b. Click the **New Deploy Rule** icon.

      The New Deploy Rule wizard appears.
   c. On the Name and hosts page, enter `SA Deploy Rule` in the **Name** text box.
   d. Verify that **Hosts that match the following pattern** is selected.
   e. From the <Add pattern> list, select **IPv4**.
   f. In the **IPv4** text box, enter `172.20.10.219` and click **Next**.

      172.20.10.219 is the IP address that the DHCP will assign to the host after it is PXE-booted.
   g. On the Select image profile page, select **My Depot** from the **Software depot** drop-down menu.
   h. Verify that the clone of the image profile is selected and click **Next**.
   i. On the Select host profile page, click **Autodeployed-Host-Profile** and click **Next**.

      Autodeployed-Host-Profile is preconfigured for use in this lab.
   j. On the Select host location page, expand **SA-Datacenter** and select **Auto-Deployed-Hosts**.
   k. Click **Next**.
   l. On the Ready to complete page, click **Finish**.
   m. In the Recent Tasks pane, monitor the task to completion.

      This task takes several minutes.
   n. Verify that the deploy rule is successfully created.

2. Activate the deployment rule.
   a. In the center pane, select **SA Deploy Rule**.
   b. Click **Activate/Deactivate rules**.

      The Activate and Reorder wizard appears.
   c. On the Activate and reorder page, select the rule at the bottom and click **Activate**.
   d. Click **Next**.
   e. On the Ready to complete page, click **Finish**.
   f. Verify that the rule status changes to Active.

## Task 7: Configure DHCP

You configure a single DHCP reservation in the Management network scope to focus vSphere Auto Deploy on a single ESXi host based on the host MAC address. Individual reservations are used instead of configuring options for a full scope. You can use the same DHCP scope with different options set for each reservation to simultaneously autodeploy hosts.

Use the following information from the class configuration handout:

- MAC address of ESXi host to autodeploy

1. Open a console to dc.vclass.local.
   a. Click the **Remote Desktop Connection Manager** icon in the Windows desktop toolbar.

      The Remote Desktop Connection Manager window appears.
   b. In the left pane, double-click **DC (vclass.local)**.

   The desktop for dc.vclass.local appears in the right pane and you are automatically logged in as a domain administrator.
2. In the RDP session to the DC, click the **DHCP** icon in the taskbar.

3. In the left pane, expand **DHCP** and expand **dc.vclass.local**.
4. Expand **IPv4**.

   The IPv4 scopes are visible.
5. Resize the left pane by dragging the pane separator to the right.
6. Expand the **Scope [172.20.10.0] SA-Management** scope and select **Reservations**.
7. Configure a new reservation that uses the MAC address of your ESXi host.
   a. Right-click **Reservations** and select **New Reservation**.
   b. In the **Reservation name** text box, enter `SA_reservation`.
   c. In the **IP address** text box, enter `172.20.10.219`.

      172.20.10.219 is the IP address of the ESXi host to autodeploy.
   d. In the **MAC address** text box, enter the MAC address of the ESXi host to autodeploy.

      The MAC address is in the class configuration handout.

      You must use hyphens, not colons, between hexadecimal values, for example, 00-50-56-01-9e-35
   e. Leave the rest of the settings at their defaults and click **Add**.
   f. Click **Close**.

      The new reservation appears in the right pane of the DHCP console window.
8. In the left pane, expand **Reservations** so that your new reservation appears.

   The reservation name is in the form [172.20.10.219] SA_reservation.
9. Double-click your reservation and verify that options inherited from the parent scope appear in the right pane.

   The scope-inherited options should include the following items:

   - 003 Router
   - 006 DNS Servers
   - 015 DNS Domain Name
10. In the left pane, right-click your reservation and select **Configure Options**.
11. On the **General** tab of the Reservation Options dialog box, scroll down to the **066 Boot Server Host Name** option.

12. Select the **066 Boot Server Host Name** check box and enter **`172.20.10.94`** in the **String value** text box.

    172.20.10.94 is the IP address of the vCenter Server Appliance instance.

13. In the options list, select the **067 Bootfile Name** check box and enter **`undionly.kpxe.vmw-hardwired`** in the **String value** text box.

14. Click **OK**.

15. Verify that your new options appear in the right pane.

    The inherited options and reservation-specific options have different icons to identify them.

16. Minimize the DHCP console window.

17. Minimize the Remote Desktop Connection Manager.

## Task 8: Start the TFTP Service on vCenter Server Appliance

vCenter Server Appliance is already configured to serve as a TFTP server for vSphere Auto Deploy. The service must be started.

1. Start an SSH session to vCenter Server Appliance.
   a. On the student desktop taskbar, click the **MTPuTTY** shortcut.
   b. In the Servers pane on the left, double-click **SA-VCSA-01**.
   c. If the PuTTY security alert appears, click **Yes**.

      You are automatically logged in to vCenter Server Appliance as user root.

2. At the command prompt, enter **`shell`** to start the Bash shell.

3. At the Bash prompt, view the TFTP service configuration.

   ```
   cat /etc/sysconfig/atftpd
   ```

   **Q1. What is the TFTP directory set to?**

4. View the contents of the TFTP directory.

   ```
   ls /var/lib/tftpboot
   ```

   **Q2. In the /var/lib/tftpboot file list, do you see the TFTP boot image filename that you entered when configuring DHCP options for your reservation?**

5. Start the TFTP service.

   ```
   service atftpd start
   ```

6. Verify that the TFTP service has started.

   ```
   service atftpd status
   ```

   The TFTP service does not start automatically when the vSphere Auto Deploy service is started from vSphere Web Client.

7. Open the TFTP firewall port on the vCenter Server Appliance instance.

   ```
   iptables -A port_filter -p udp -m udp --dport 69 -j ACCEPT
   ```

8. Enter **`exit`** and enter **`exit`** again to close the MTPuTTY window.

## Task 9: Review the Autodeployment Preparation Steps

You review your work and prepare for autodeployment.

1. Review the configuration and autodeployment steps.
   - Containers and host profiles for use by autodeployed hosts are configured.

     The use of containers can be beneficial when designing prestaging and poststaging scenarios for host deployments.
   - The vSphere Auto Deploy service is started in vSphere Web Client.
   - A custom host image profile is created.

     Custom image profiles enable you to customize deployments for different sets of hosts and can be updated and customized with additional VMware or third-party software packages.
   - A deployment rule is created to associate an image profile, a host profile, and a container to specific autodeployed hosts.

     Using rules with different patterns enables different image, host profile, and other configurations to be assigned to groups of hosts.
   - DHCP options are configured to identify a TFTP server and a boot image filename.
   - The TFTP service is started on vCenter Server Appliance.

     For expediency, the lab environment uses vCenter Server Appliance as the TFTP server. In the production environment, you can use a compatible TFTP service that is not colocated with vCenter Server Appliance.

## Task 10: Prepare to Monitor ESXi Bootup During the Autodeploy Process

You move out of your student desktop and use the VMware OneCloud web interface to open a console to the ESXi host to autodeploy.

1. Verify that you have your student login credentials.

   Your login credentials are sent to you in a class welcome email. Your instructor can help you if you do not have your login information.

2. Record the VMware OneCloud URL provided by your instructor. _____

   The URL should be similar to wdc-vclass-a.vmeduc.com/cloud/org/classroom-101.

3. Minimize the Remote Desktop Protocol (RDP) session to the student desktop machine in your lab sandbox.

   You can access the desktop of the server that you first logged in to at the start of the class. If you have questions about which RDP session to minimize, ask your instructor.

4. On the login server desktop, double-click the **Firefox** shortcut.

5. In the Firefox window, browse to the VMware OneCloud URL that you recorded in step 2.

6. When prompted, log in with the student credentials.

   The user name and password are the same as those that you used to access the login server at the start of the class.

7. In the VMware vCloud Director® OneCloud interface, one vApp appears on the **Home** tab.

   The name and time on your vApp will be different from that displayed in the screenshot.

8. In the vApp panel, click the **Open** link above the **Stop** icon.

   The vCloud Director OneCloud interface changes to the **My Cloud** tab with the vApp details in the right pane.

9. In the right pane, click the **Virtual Machines** tab.

10. In the virtual machines list, find SA-ESXi-04.

    SA-ESXi-04 is the name of the ESXi host to autodeploy.

## Task 11: Power On the ESXi Host and Monitor the Bootup Process

You power on the ESXi host to autodeploy (SA-ESXi-04), and you monitor the ESXi host console to observe the autodeploy process.

1. Power off and power on the ESXi host to autodeploy.
   a. Right-click **SA-ESXi-04** and select **Power Off**.
   b. Click **Yes** to confirm the power-off operation.
   c. Right-click **SA-ESXi-04** and select **Power On**.
2. When the ESXi host status changes to Powered On, right-click **SA-ESXi-04** and select **Popout Console**.

   A new window shows the console view of the selected ESXi host.
3. If the Firefox pop-up blocker blocks the console from opening, select the **Always allow pop-ups** option and repeat step 2.
4. If a window appears asking if you want to upgrade to a newer version of the Client Integration Plug-In, click **No**.
5. Monitor the ESXi host bootup process.

   The host performs a network preboot execution environment (PXE) boot. The host contacts the TFTP server identified in the DHCP scope options.

   If you see a message about PXE boot attempts timing out, contact the instructor for assistance.

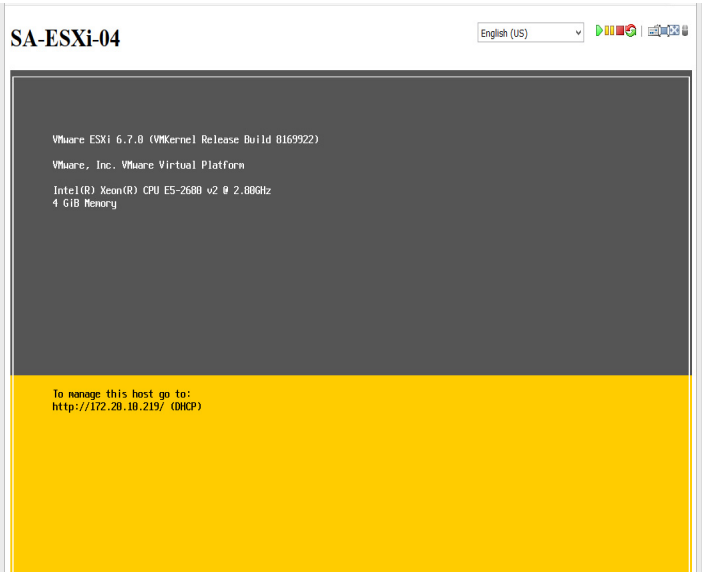
   The image binaries are transferred to the host and installed. This process can take up to 20 minutes to complete.

   ESXi modules are loaded and the associated host profile tasks are performed.

   Services are started.

6. Wait for the autodeploy process to complete.

   The autodeploy process is complete when the main Direct Console User Interface screen appears.



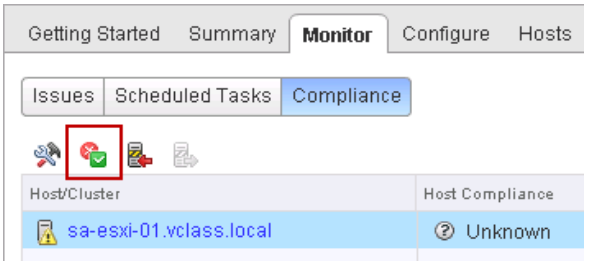

7. Restore the minimized RDP session to the student desktop machine.

## Task 12: Verify Host Profile Compliance of the Autodeployed Host

Each autodeployed host must be minimally configured so that the host can handle workloads as a member of a cluster. You perform the minimal configuration of the host networking.

1. Restore the minimized Firefox window and click the **vSphere Web Client** tab.
2. If you are logged out of vSphere Web Client, log back in.
3. Point to the **Home** icon and select **Hosts and Clusters**.
4. In the left pane, expand the **Auto-Deployed-Hosts** folder.

   The autodeployed host appears in the folder, with the reservation IP as the host name. This host has been placed into maintenance mode.
5. Right-click the autodeployed host and select **Maintenance Mode** > **Exit Maintenance Mode**.
6. Point to the **Home** icon and select **Policies and Profiles**.
7. In the left pane, click **Host Profiles**.
8. In the left pane, select **Autodeployed-Host-Profile**.
9. In the center pane, click the **Monitor** tab and click **Compliance**.
10. In the host list, select the autodeployed ESXi host.
11. Click the **Check Host Profile Compliance** icon.



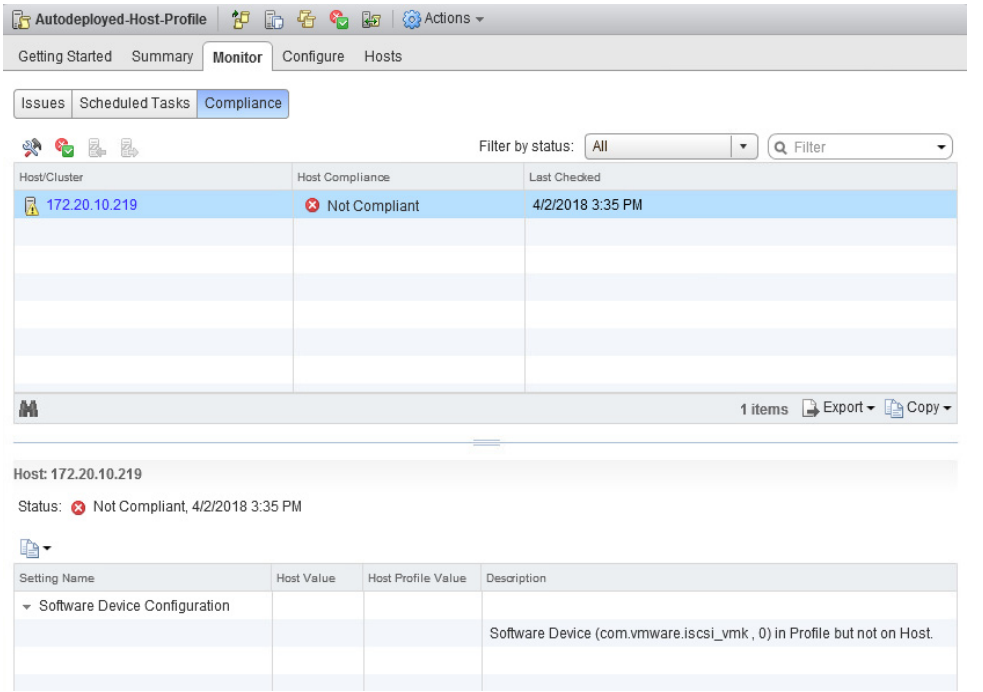

12. In the Recent Tasks pane, monitor the task and wait for the compliance check to complete.
13. Verify whether the ESXi host is in compliance with the host profile.
14. If the ESXi host is not compliant, then go to task 13.
15. If the ESXi host is compliant, you have completed this lab.
16. Log out of vSphere Web Client and close the tab.

    You use vSphere Client to perform the remaining labs.

## Task 13: Review the Noncompliant Items

You review and resolve any items that are not compliant with the host profile.

1. Review any noncompliant settings in the panel at the bottom of the screen and understand the reasons for these noncompliant items.




   In the screenshot, the noncompliant message shows that the iSCSI adapter is configured in the host profile, but not on the host.

2. (Optional) Resolve the noncompliant item by adding an iSCSI adapter to sa-esxi-04.vclass.local.

   a. Point to the **Home** icon and select **Hosts and Clusters**.

   b. In the left pane, select **172.20.10.219** (your autodeployed host).

   c. In the center pane, click the **Configure** tab.

   d. Select **Storage Adapters** on the left.

   e. Click the **Add new storage adapter** icon (green plus sign) and click **Software iSCSI adapter**.

f. Click **OK** to add the adapter.

g. In the Adapter list, select **vmhba65**.

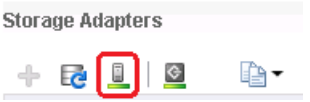
h. In the Adapter Details pane, click the **Targets** tab.

   The **Dynamic Discovery** tab is selected.

i. Click **Add**.

j. Enter `dc.vclass.local` in the **iSCSI Server** text box and click **OK**.

k. Click the **Rescans all storage adapters on the host** icon and click **OK** to start the scan.




l. Point to the **Home** icon and select **Policies and Profiles**.

m. In the left pane, click **Host Profiles**.

n. In the left pane, click **Autodeployed-Host-Profile**.

o. In the right pane, click the **Monitor** tab and click **Compliance**.

p. Select **172.20.10.219**.

q. Click the **Check Host Profile Compliance** icon.

r. In the Recent Tasks pane, monitor the task to completion.

s. Verify that the configuration change makes the setting compliant.

If you have additional noncompliant items in the list, you can consult your instructor. Your instructor can discuss the reasons for noncompliance with you.

3. Log out of vSphere Web Client and close the tab.

   You use vSphere Client to perform the remaining labs.

# *Lab 8* Monitoring CPU Performance

## Objective: Use the esxtop command to monitor CPU performance

In this lab, you perform the following tasks:

1. Run a Single-Threaded Program in a Single-vCPU Virtual Machine
2. Start esxtop and View Statistics
3. Record Statistics for Case 1: Single Thread and Single vCPU
4. Run a Single-Threaded Program in a Dual-vCPU Virtual Machine
5. Record Statistics for Case 2: One Thread and Two vCPUs
6. Run a Dual-Threaded Program in a Dual-vCPU Virtual Machine
7. Record Statistics for Case 3: Two Threads and Two vCPUs
8. Analyze the Test Results

## Task 1: Run a Single-Threaded Program in a Single-vCPU Virtual Machine

You run a test program to generate continuous database activity on the test virtual machine for statistical analysis. The test virtual machine is configured with one vCPU.

1. If needed, open Firefox and log in to the sa-vcsa-01 vSphere Client as administrator@vsphere.local with the password VMware1!.
2. Verify that the Linux01 virtual machine is hosted on sa-esxi-01.vclass.local.
   a. In the left pane, expand the inventory and select **Linux01**.
   b. In the right pane, view the **Summary** tab and verify that the host on which Linux01 resides is sa-esxi-01.vclass.local.
3. If Linux01 is not hosted on sa-esxi-01, migrate Linux01 to sa-esxi-01.
   a. Right-click **Linux01** and click **Migrate**.

      The Migrate wizard appears.
   b. On the Select a migration type page, click **Change compute resource only** and click **Next**.
   c. On the Select a compute resource page, select **sa-esxi-01.vclass.local** and click **Next**.
   d. On the Select networks page, keep the default and click **Next**.
   e. On the Ready to complete page, click **Finish**.
   f. Wait for the migration to complete.
4. Power on the Linux01 virtual machine.
5. Log in to the Linux01 virtual machine console.
   a. On the **Summary** tab, click the **Launch Web Console** link.
   b. Wait for the virtual machine to complete its bootup process.
   c. Log in as user root with the password VMware1!.
6. Verify that you are in the `/root` directory.

   ```
   pwd
   ```
7. If you are not in the `/root` directory, enter **`cd /root`**.
8. Start the test program on Linux01.

   ```
   ./starttest1
   ```

   The test program generates database operations to a medium-size database and writes output to the screen. The program must run uninterrupted.

## Task 2: Start esxtop and View Statistics

You use the `esxtop` command to observe performance statistics for supported objects.

1. Start an SSH session to sa-esxi-01.vclass.local.
   a. On the student desktop taskbar, click the **MTPuTTY** shortcut.
   b. In the Servers pane on the left, double-click **SA-ESXi-01**.
   c. If the PuTTY security alert appears, click **Yes**.

      You are automatically logged in to the appliance as user root.
2. Start `esxtop`.

   By default, `esxtop` starts with the CPU screen.
3. Change the update delay from the default (5 seconds) to 10 seconds.
   a. Enter **`s`**.
   b. Enter **`10`**.
4. To filter the CPU screen output only to the virtual machines, enter uppercase **`V`**.

   By default, the CPU screen shows statistics for virtual machine processes and active ESXi host processes.
5. In the output table, find the Linux01 virtual machine statistics.

## Task 3: Record Statistics for Case 1: Single Thread and Single vCPU

You record statistics for the first test case.

1. After 30 seconds of statistics collection, record the values for the Linux01 virtual machine in the Case 1 column in the class configuration handout.
   - %USED
   - %RDY
   - %IDLE
2. Record the operations per minute (opm) value in the test script.
   a. In Firefox, click the **Linux01** console tab.
   b. Record the opm reported by the test script in the Case 1 column in the class configuration handout.

      The counter value is reported with each iteration that the test script performs. Use the counter reported in the last iteration.
3. Press Ctrl+C to stop the test script.
4. Close the **Linux01** console tab.

## Task 4: Run a Single-Threaded Program in a Dual-vCPU Virtual Machine

You modify the Linux01 virtual machine to have two vCPUs, and you restart the test script.

1. Go to the **vSphere Client** tab.
2. Shut down the Linux01 virtual machine.
3. Wait for the running indicator to be removed from the Linux01 virtual machine icon in the inventory tree.

   You might need to click the **Refresh** icon.
4. Add a second vCPU to the Linux01 virtual machine.
   a. In the left pane, right-click **Linux01** and select **Edit Settings**.
   b. On the **Virtual Hardware** tab in the Edit Settings dialog box, select **2** from the **CPU** drop-down menu and click **OK**.
   c. In the Recent Tasks pane, monitor the reconfiguration task to completion.
5. Power on the Linux01 virtual machine.
6. On the **Summary** tab, click the **Launch Web Console** link.
7. Wait for the virtual machine to complete its bootup process.

8. Log in as user root with the password VMware1!.
9. On the **Linux01** console tab, restart the test program.

   ```
   ./starttest1
   ```

   This script generates database operations to a medium-size database. The number of threads is set to 1. The script must run uninterrupted.

## Task 5: Record Statistics for Case 2: One Thread and Two vCPUs

You record statistics for the second test case.

1. Record the `esxtop` counter values.
   a. Switch to the MTPuTTY window.
   b. Enter **e**.
   c. Enter the GID for Linux01.
   d. Examine the two lines in the NAME column that start with vmx-vcpu.

      These two lines show the activity of each of the vCPUs in the Linux01 virtual machine.
   e. After 30 seconds of statistics collection, record the values for vCPU0 and vCPU1 in the Case 2 column in the class configuration handout.
      - %USED
      - %RDY
      - %IDLE
      - opm
2. Record the operations per minute value in the test script.
   a. In Firefox, click the **Linux01** console tab.
   b. Record the opm value reported by the test script in the Case 2 column in the class configuration handout.

      The counter value is reported with each iteration that the test script performs. Use the counter reported in the last iteration.
3. Press Ctrl+C to stop the test script.

## Task 6: Run a Dual-Threaded Program in a Dual-vCPU Virtual Machine

You configure the third case parameters by running a two-threaded test program on a virtual machine with two vCPUs.

1. On the **Linux01** console tab, start the two-threaded test program.

   ```
   ./starttest2
   ```

   This script generates database operations to a medium-size database. The number of threads is set to 2. The script must run uninterrupted.

## Task 7: Record Statistics for Case 3: Two Threads and Two vCPUs

You record statistics for the final test case.

1. Record the `esxtop` counter values.
   a. Switch to the MTPuTTY window.
   b. Examine the two lines in the NAME column that start with vmx-vcpu.

      These two lines show the activity of each of the vCPUs in the Linux01 virtual machine.
   c. After 30 seconds of statistics collection, record the values for vCPU0 and vCPU1 in the Case 3 column in the class configuration handout.
      - %USED
      - %RDY
      - %IDLE
      - opm
2. Record the operations per minute value in the test script.
   a. In Firefox, click the **Linux01** console tab.
   b. Record the opm value reported by the test script in the Case 3 column in the class configuration handout.
3. Press Ctrl+C to stop the test script.
4. Stop the `esxtop` program.
   a. Switch to the MTPuTTY window.
   b. Enter **q** to stop `esxtop`.
5. Keep the SA-ESXi-01 MTPuTTY session open for the next lab.
6. Keep the **Linux01** console tab open for the next lab.
7. Keep the **vSphere Client** tab open for the next lab.

## Task 8: Analyze the Test Results

You analyze the captured statistics and document your conclusions.

1. Review statistics that you recorded in the class configuration handout in tasks 3, 5, and 7.
2. Record conclusions that you can draw from the data. _____

# *Lab 9* Monitoring Memory Performance

## Objective: Use the esxtop command to monitor memory performance under load

In this lab, you perform the following tasks:

1. Generate Database Activity in the Test Virtual Machine
2. Check for Overcommitment of Virtual Machine Memory
3. Configure esxtop to Report Virtual Machine Memory Statistics
4. Observe Memory Statistics
5. Start a Memory Test on ResourceHog01 and ResourceHog02
6. Record Memory Statistics
7. Clean Up for the Next Lab

## Task 1: Generate Database Activity in the Test Virtual Machine

You start the test program to generate database activity.

1. In Firefox, click the **Linux01** console tab.
2. If necessary, log in to the Linux01 virtual machine as user root with the standard lab password.
3. In the Linux01 console, enter `./starttest2`.

   This test program performs continuous database operations to a medium-size database. The number of threads is set to 2. The script must run uninterrupted.

## Task 2: Check for Overcommitment of Virtual Machine Memory

You use resource allocation reports to determine whether memory is overcommitted for a virtual machine.

1. In Firefox, click the **vSphere Client** tab and log in, if necessary.
2. In vSphere Client, select **Hosts and Clusters** from the **Menu** drop-down menu.
3. In the left pane, select the **Linux01** virtual machine.
4. In the right pane, click the **Monitor** tab and click **Utilization** on the left.
5. Find the Virtual Machine Memory panel.
6. Record the value for VM Consumed. _____
7. Find the Guest Memory panel in the lower-left corner of the pane.
8. Record the value for Active Guest Memory. _____

**Q1. Is the consumed host memory greater than the active guest memory?**

If the consumed host memory is greater than the active guest memory, memory is not overcommitted. If the consumed host memory is less than active guest memory, then overcommitment is occurring and might cause degraded performance.

## Task 3: Configure esxtop to Report Virtual Machine Memory Statistics

You start `esxtop` and configure it for memory statistics.

1. Switch to the MTPuTTY window for sa-esxi-01.vclass.local.
   a. If you need to restart the SSH session to sa-esxi-01.vclass.local, click the **MTPuTTY** shortcut on the taskbar.
   b. In the Servers pane on the left, double-click **SA-ESXi-01**.
   c. When the PuTTY security alert appears, click **Yes**.

      You are automatically logged in to sa-esxi-01.vclass.local as user root.
2. Start `esxtop`.
3. In `esxtop`, enter **`m`** to view the memory statistics screen.
4. Set a 10-second update delay.
   a. Enter **`s`** to display the delay prompt.
   b. At the delay prompt, enter **`10`**.
5. Enter uppercase **`V`** to filter only the display virtual machine statistics.
6. Remove all statistics columns from the output table, except D, H, J, and K.

   Removing counters that are not monitored during the test can make isolation of the desired counters easier.
   a. Enter **`f`** to access the field order screen.
   b. For fields other than D, H, J, and K, if an asterisk appears to the left of the field name, press the corresponding letter to remove the asterisk.
   c. For the D, H, J, and K fields, if an asterisk does not appear to the left of the field name, press the corresponding letter to add an asterisk.
   d. Press Enter to return to the memory statistics output.

## Task 4: Observe Memory Statistics

You observe `esxtop` counters to determine memory conditions.

1. Examine `esxtop` statistics.
   a. In the `esxtop` output, view the Linux01 virtual machine statistics.
   b. Verify that the MCTLSZ, MCTLTGT, SWCUR, SWTGT, SWR/s, and SWW/s values are at or near zero.
   c. If you cannot see all values listed in step b, close the left pane.
2. Record the operations per minute (opm) value in the test script.
   a. Switch to the **Linux01** console tab.
   b. Record the opm value reported by the test script. _____

      The counter value is reported with each iteration that the test script performs. Use the counter reported in the last iteration.

## Task 5: Start a Memory Test on ResourceHog01 and ResourceHog02

You start a memory test on the ResourceHog01 and ResourceHog02 virtual machines.

1. Power on, open a console, and boot to the ResourceHog01 virtual machine.

   You must enter the console within 30 seconds.
   a. Return to the **vSphere Client** tab.
   b. In the left pane, select **ResourceHog01**.
   c. Right-click **ResourceHog01** and select **Power** > **Power On**.
   d. Click the **Summary** tab of ResourceHog01 and click the **Launch Web Console** link.
   e. Click anywhere in the console window.
   f. At the BIOS screen, press Enter.
   g. At the `boot:` prompt, press Enter to load the Ultimate Boot CD menu.

      If you see a `Booting...` prompt, you did not enter the console within 30 seconds. You must return to substep a. Power off and power on the virtual machine and enter the console to the virtual machine within 30 seconds. Repeat this process until the Ultimate Boot CD menu appears.

h. Use the arrow keys and the Enter key to select **Mainboard Tools** > **Memory Tests > Memtest86+ V1.70**.

   The exact keystroke sequence is Enter, down arrow, down arrow, Enter, down arrow, down arrow, Enter.

i. After the memory test utility is running, press Ctrl+Alt to release the pointer focus.

2. Repeat step 1 for the ResourceHog02 virtual machine.

## Task 6: Record Memory Statistics

You record and evaluate memory statistics with a significant load consuming ESXi host memory.

1. Switch to the MTPuTTY window.
2. After at least one minute of statistics collection, record the values for the ResourceHog02, ResourceHog01, and Linux01 virtual machines in the class configuration handout.
   - MCTL?
   - MCTLSZ
   - MCTLTGT
   - SWCUR
   - SWTGT
   - SWR/s
   - SWW/s
   - %SWPWT

   **Q1. For Linux01, does the value of MCTLSZ converge with the value of MCTLTGT?**

   **Q2. For Linux01, does the value of SWCUR converge with the value of SWTGT?**

3. Monitor the statistics output until the host reaches a steady state where the counters in each set are close in value to each other.

   If the counters in each set are close in value to each other, the host has reached a steady state.

4. To determine which virtual machines do not have the balloon driver installed, examine the MCTL? value for each virtual machine.

   The MCTL? field indicates the presence of the balloon driver. If the MCTL? value is Y, then that virtual machine has a balloon driver installed. Otherwise, the virtual machine lacks a balloon driver.

   **Q3. Which virtual machines do not have the balloon driver installed?**

5. To determine whether the virtual machines are swapping, examine the values for SWR/s and SWW/s for each virtual machine.

   **Q4. Which virtual machines are swapping?**

6. Determine which virtual machines have experienced degraded performance due to swapping.
   a. Enter lowercase **c** to switch to the CPU screen.
   b. Enter uppercase **V** to display only virtual machine statistics.
   c. Examine the %SWPWT value for each virtual machine identified as actively swapping.

      %SWPWT is the percentage of time the world is waiting for the ESX VMkernel swapping memory. As %SWPWT exceeds 5 percent, the performance of the virtual machine degrades significantly. If you do not see the %SWPWT field, expand your console window.

      **Q5. What are the %SWPWT values for each of the virtual machines?**

7. Enter **m** to return to the `esxtop` memory screen.

   The memory state can be found at the end of the third row from the top of the esxtop output.

   **Q6. What is the memory state: high, clear, soft, hard, or low?**

8. Record the opm value in the test script.
   a. Switch to the **Linux01** console tab.
   b. Record the opm value reported by the test script. _____
   c. Compare this opm value with the value that you recorded in task 4, step 2, substep b.

      **Q7. Has the performance of the test script degraded?**

## Task 7: Clean Up for the Next Lab

You stop the test script on the Linux01 virtual machine. You also stop the memory tests on ResourceHog01 and ResourceHog02.

1. In the MTPuTTY window, select **View** > **Servers** to display the Servers pane on the left.
2. Keep `esxtop` running in the MTPuTTY window.
3. Switch to the **Linux01** console tab and press Ctrl+C to stop the test script.

   Keep the console tab open.
4. Close the **ResourceHog01** and **ResourceHog02** console tabs.
5. Power off the ResourceHog01 and ResourceHog02 virtual machines.
6. Keep the **vSphere Client** tab open for the next lab.

# *Lab 10* Monitoring Storage Performance

## Objective: Use the esxtop command to monitor disk performance across a series of tests

In this lab, you perform the following tasks:

1. Prepare to Run Tests
2. Measure Continuous Sequential Write Activity to a Virtual Disk on a Remote Datastore
3. Measure Continuous Random Write Activity to a Virtual Disk on a Remote Datastore
4. Measure Continuous Random Read Activity to a Virtual Disk on a Remote Datastore
5. Measure Continuous Random Read Activity to a Virtual Disk on a Local Datastore
6. Analyze the Test Results

## Task 1: Prepare to Run Tests

You use several test scripts on the Linux01 virtual machine to generate continuous random and sequential I/O operations against both local and remote (network) datastores.

The Linux01 virtual machine is located on sa-esxi-01.vclass.local and is configured with two hard drives to serve as local and remote I/O targets. The SCSI drive is stored on the 11GBLocal local datastore. The SCSI drive is stored on the 11GBRemote remote datastore.

You monitor storage preparation tasks to completion and change folders.

1. In the Firefox window, click the **Linux01** console tab.
2. If necessary, log in as user root with the password VMware1!.
3. Configure storage.

   ```
   ./storageconfig.sh
   ```

   The storage preparation might take a few minutes to complete. The script must run uninterrupted to completion.
4. When the script is complete, navigate to the test scripts folder.

   ```
   cd aio-stress
   ```

## Task 2: Measure Continuous Sequential Write Activity to a Virtual Disk on a Remote Datastore

You run the `logwrite.sh` test script to generate continuous sequential write activity to the hard disk on the remote datastore.

1. In the Linux01 console, start the `logwrite.sh` test script.

   ```
   ./logwrite.sh
   ```
2. Allow the script to run uninterrupted.
3. View the MTPuTTY session to the sa-esxi-01 host.

   MTPuTTY should be logged in to SA-ESXi-01 and `esxtop` should be running.
4. If you are not logged in to MTPuTTY and `esxtop` is not running, start a new MTPuTTY session to sa-esxi-01.vclass.local.
   a. In the MTPuTTY window, open a connection to SA-ESXi-01.
   b. Enter **`esxtop`** at the command prompt.
   c. Set a 10-second update delay by entering **`s`** and entering **`10`**.

5. Enter **d** to display device adapter output and examine the reads and writes to the adapter paths.

   **Q1. Which adapter has the most disk I/O activity?**

6. Enter **u** to display individual device output and examine the reads and writes to the devices.

   One of the remote devices has more disk I/O activity than the others.

7. Enter **v** to display virtual machine output.
8. After 30 seconds of statistics collection, record the values for the Linux01 virtual machine in the Sequential Writes/Remote Datastore column in the class configuration handout.
   - READS/s
   - WRITES/s
9. In the Firefox window, click the **Linux01** console tab.
10. Press Ctrl+C to stop the test script.

## Task 3: Measure Continuous Random Write Activity to a Virtual Disk on a Remote Datastore

You run the `datawrite.sh` test script to generate continuous random write activity to the virtual machine hard disk on the remote datastore.

1. In the Linux01 console, start the `datawrite.sh` test script.

   ```
   ./datawrite.sh
   ```

2. Allow the script to run uninterrupted.
3. Return to the MTPuTTY window.
4. Enter **d** to display device adapter output and examine the reads and writes to the adapter paths.
5. Enter **u** to display individual device output and examine the reads and writes to the devices.
6. Enter **v** to display virtual machine output.
7. After 30 seconds of statistics collection, record the values for Linux01 in the Random Writes/ Remote Datastore column in the class configuration handout.
   - READS/s
   - WRITES/s
8. In the Firefox window, click the **Linux01** console tab.
9. Press Ctrl+C to stop the test script.

## Task 4: Measure Continuous Random Read Activity to a Virtual Disk on a Remote Datastore

You run the `fileserver2.sh` test script to generate continuous random read activity from the hard disk on the remote datastore.

1. In the Linux01 console, start the `fileserver2.sh` test script.

   ```
   ./fileserver2.sh
   ```

2. Allow the script to run uninterrupted.
3. Return to the MTPuTTY window.
4. Enter **`d`** to display device adapter output and examine the reads and writes to the adapter paths.
5. Enter **`u`** to display individual device output and examine the reads and writes to the devices.
6. Enter **`v`** to display virtual machine output.
7. After 30 seconds of statistics collection, record the values for Linux01 in the Random Reads/ Remote Datastore column in the class configuration handout.
   - READS/s
   - WRITES/s
8. In the Firefox window, click the **Linux01** console tab.
9. Press Ctrl+C to stop the test script.

## Task 5: Measure Continuous Random Read Activity to a Virtual Disk on a Local Datastore

You run the `fileserver1.sh` test script to generate continuous random read activity from the virtual machine hard disk on the local datastore attached to the ESXi host.

1. In the Linux01 console, start the `fileserver1.sh` test script.

   ```
   ./fileserver1.sh
   ```

   This test script first creates the file to be read, which can take 5 minutes or more.

   The test script must run uninterrupted.

2. Monitor the script output.

   The output remains silent during file creation.

3. After the `Starting with random read` message appears, view information in `esxtop`.
   a. Enter **d** to display device adapter output.

      **Q1. Which adapter has the most disk I/O activity?**

   b. Enter **u** to display individual device output.

      One of the local devices, rather than a remote device, is used for this test.

   c. Enter **v** to display virtual machine output.
4. After 30 seconds of statistics collection, record the values for Linux01 in the Random Reads/ Local Datastore column in the class configuration handout.
   - READS/s
   - WRITES/s
5. In the Firefox window, click the **Linux01** console tab.
6. Press Ctrl+C to stop the test script.

## Task 6: Analyze the Test Results

Your instructor conducts an in-class review to compare test results from each group.

1. Record the conclusions that you draw from the test data collected in tasks 2 through 5.

   _____

2. Keep the **Linux01** console tab and the **vSphere Client** tab open for the next lab.

# *Lab 11* Monitoring Network Performance

## Objective: Use the esxtop command to monitor network performance

In this lab, you perform the following tasks:

1. Prepare to Monitor Network Performance
2. Prepare the Client and the Server Virtual Machines
3. Measure Network Activity on an ESXi Physical Network Interface
4. Use Traffic Shaping to Simulate Network Congestion
5. Position the Client and the Server on the Same Port Group
6. Restart the Test and Measure Network Activity
7. Stop the Test and Analyze Results
8. Clean Up for the Next Lab

### Task 1: Prepare to Monitor Network Performance

You use the `esxtop` network statistics screen to monitor network performance.

1. View the MTPuTTY session to the sa-esxi-01 host.

   MTPuTTY should be logged in to the sa-esxi-01 host and `esxtop` should be running.

2. If MTPuTTY is not logged in and `esxtop` is not running, start a new MTPuTTY session to sa-esxi-01.vclass.local.

   a. In the MTPuTTY window, open a connection to SA-ESXi-01.

   b. Enter **`esxtop`** at the command prompt.

   c. Set a 10-second update delay.

3. Enter **n** to switch to the network statistics screen.
4. Remove unused counters to make the `esxtop` network screen easier to monitor.
   a. Enter **f** to display the Current Field Order table.
   b. In the Current Field Order table, enter **g** and **j** to remove PKTRX/s and PKTTX/s from the `esxtop` display.
   c. Press Enter to return to the network statistics screen.

## Task 2: Prepare the Client and the Server Virtual Machines

You use scripts on the Linux01 and Linux02 virtual machines to generate network traffic so that network performance can be measured.

The Linux01 virtual machine acts as a client, and the Linux02 virtual machine acts as a server. The Linux01 virtual machine is connected to the pg-SA Production port group. You move the Linux02 virtual machine to the pg-SA-Management port group so that the virtual machines are connected to different virtual switches, forcing their traffic to traverse the physical network.

1. In the Firefox window, click the **vSphere Client** tab.
2. Log in to vSphere Client, if necessary.
3. Migrate the Linux02 virtual machine from the pg-SA-Production port group on dvs-Lab to the pg-SA-Management port group on dvs-SA-Datacenter.
   a. Select **Networking** from the **Menu** drop-down menu.
   b. In the left pane, expand the dvs-Lab.
   c. Right-click **pg-SA-Production** and select **Migrate VMs to Another Network**.

      The Migrate VMs to Another Network wizard appears.
   d. For the Destination network, click **Browse**.
   e. Select **pg-SA-Management** and click **OK**.
   f. Click **Next**.
   g. On the Select VMs to migrate page, select the **Linux02** check box and click **Next**.
   h. On the Ready to complete page, review settings and click **Finish**.
   i. In the Recent Tasks pane, monitor the task to completion.

4. View the IP address of the Linux02 virtual machine.
   a. Select **Hosts and Clusters** from the **Menu** drop-down menu.
   b. Power on the Linux02 virtual machine.

      Wait for the virtual machine to boot up completely.
   c. In the left pane, select **Linux02**.
   d. From the **Summary** tab in the right pane, record the Linux02 IP address. _____

      The Linux02 IP address starts with 172.20.10 (the management network DHCP range).
5. View the IP address of the Linux01 virtual machine.
   a. In the left pane, select the **Linux01** virtual machine.
   b. From the **Summary** tab, record the Linux01 IP address. _____

      The Linux01 IP address starts with 172.20.11 (the production network DHCP range).
6. Start the server on Linux02.
   a. In the left pane, select **Linux02**.
   b. In the right pane, click the **Launch Web Console** link on the **Summary** tab.
   c. In the Linux02 console window, log in as user root with the password VMware1!.
   d. Navigate to the network scripts folder.

      ```
      cd netperf
      ```
   e. Start the server program.

      ```
      ./netserver
      ```

      The server program runs as a background process.

      ```
      Starting netserver at port 12865
      Starting netserver at hostname 0.0.0.0 port 12865
      ```
   f. Verify that the server program is running.

      ```
      ps -ef | grep netserver
      ```

      The server and `grep` processes are listed.

      ```
      00:00:00 ./netserver
      00:00:00 grep netserver
      ```

## Task 3: Measure Network Activity on an ESXi Physical Network Interface

You measure the network performance of the ESXi host network interface with the Linux01 and Linux02 virtual machines positioned on different physical network segments across a router.

Requests sent from the Linux01 client enter the physical network through the ESXi network interface vmnic2 that is bound to a dvs-Lab distributed switch uplink. Using the pg-SA-Management port group on the dvs-SA-Datacenter distributed switch, the client requests are routed to the management network where the Linux02 server is positioned.

1. Switch to the **Linux01** console tab.
2. Start the client on Linux01.
   a. Navigate to the network scripts folder.

      ```
      cd /root/netperf
      ```

   b. Start the client test script.

      ```
      ./nptest1.sh server_IP_address
      ```

      *server_IP_address* is the Linux02 IP address that you recorded in task 2.

      The client and server programs must run uninterrupted.
3. Monitor network activity and record your findings.
   a. Switch to the MTPuTTY window.
   b. In the `esxtop` output, find the vmnic2 physical network interface.
   c. After 30 seconds of statistics collection, record the values for vmnic2 in the vmnic2 column in the class configuration handout.
      - MbTX/s
      - MbRX/s

## Task 4: Use Traffic Shaping to Simulate Network Congestion

You use traffic shaping to control the network speed to simulate congestion.

1. Return to the **vSphere Client** tab.
2. Select **Networking** from the **Menu** drop-down menu.
3. In the left pane, right-click the **pg-SA-Production** port group and select **Edit Settings**.
4. In the Edit Settings dialog box, click **Traffic shaping** on the left.
5. Select **Enabled** from the **Status** drop-down menus for ingress traffic shaping and egress traffic shaping.
6. Configure ingress and egress traffic shaping.

| Option | Action |
|---|---|
| **Average bandwidth (kbit/s)** | Enter `10000`. |
| **Peak bandwidth (kbits/s)** | Enter `10000`. |
| **Burst size (KB)** | Enter `10000`. |

7. Verify that you configured both ingress and egress traffic shaping and click **OK**.
8. Monitor network performance and record your findings.
   a. Switch to the MTPuTTY window.
   b. In the `esxtop` output, find the vmnic2 physical interface item.
   c. After 30 seconds of statistics collection, record the values for vmnic2 in the vmnic2 10 Mb/s column in the class configuration handout.
      - MbTX/s
      - MbRX/s
9. Disable ingress and egress traffic shaping.
   a. Return to the **vSphere Client** tab.
   b. In the left pane, right-click **pg-SA-Production** and select **Edit Settings**.
   c. Click **Traffic shaping**.
   d. For both ingress and egress traffic shaping, select **Disabled** from each **Status** drop-down menu.
   e. Click **OK**.

## Task 5: Position the Client and the Server on the Same Port Group

You migrate the Linux02 virtual machine back to the pg-SA-Production port group to show that virtual machines communicating on the same ESXi host and virtual switch port group can communicate at a faster rate than the rate dictated by the physical network hardware.

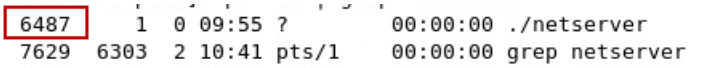
1. Stop the network client.
   a. Return to the **Linux01** console tab.
   b. In the Linux01 console, press Ctrl+C to stop the test script.
2. Stop the network server.
   a. Click the **Linux02** console tab.
   b. In the Linux02 console, end the server program.

      ```
      ps -ef | grep netserver
      ```

      ```
      kill process_id
      ```

      In the `kill` command, *process_id* is the netserver process ID as reported by the `ps` command.

      In the example `ps` output, the netserver process ID is 6487. The screenshot does not include the leftmost columns of the `ps` output.

      
      ```
      6487     1  0 09:55 ?        00:00:00 ./netserver
      7629  6303  2 10:41 pts/1    00:00:00 grep netserver
      ```

3. Migrate the Linux02 virtual machine from the pg-SA-Management port group to the pg-SA-Production port group on dvs-Lab
   a. Return to the **vSphere Client** tab.
   b. In the left pane, expand dvs-SA-Datacenter, right-click **pg-SA-Management**, and select **Migrate VMs to Another Network**.
   c. For the Destination network, click **Browse**.
   d. Select **pg-SA-Production** and click **OK**.
   e. Click **Next**.
   f. On the Select VMs to migrate page, select the **Linux02** check box and click **Next**.
   g. On the Ready to complete page, review settings and click **Finish**.
   h. In the Recent Tasks pane, monitor the task to completion.

4. Restart the network service and verify that the IP address is within the production network DHCP range.
   a. Click the **Linux02** console tab.
   b. In the terminal window, restart the network service.

      ```
      service network restart
      ```

      The network service might take up to a minute to restart and acquire a new DHCP address.
   c. Verify that a new DHCP-assigned address was acquired.

      ```
      ifconfig
      ```
   d. In the `ifconfig` command output, verify that the IP address starts with 172.20.11 (the production network DHCP range).
   e. Record the postmigration Linux02 IP address. _____

## Task 6: Restart the Test and Measure Network Activity

You measure network activity when the client and the server communicate across a virtual network contained within a single ESXi host and port group.

1. In the Linux02 console window, start the server program.

   ```
   ./netserver
   ```
2. Return to the **Linux01** console tab.
3. Start the client script.

   ```
   ./nptest1.sh server_IP_address
   ```

   *server_IP_address* is the postmigration Linux02 IP address that you recorded in task 5.
4. Monitor network activity and record your findings.
   a. Switch to the MTPuTTY window.
   b. In the `esxtop` output, find the vmnic2 row and verify that the traffic is no longer traversing the physical interface.
   c. Find the Linux01.eth0 row.
   d. After 30 seconds of statistics collection, record the values for Linux01.eth0 in the Linux01.eth0 column in the class configuration handout.
      - MbTX/s
      - MbRX/s

## Task 7: Stop the Test and Analyze Results

You use samples that you recorded to determine whether network performance was affected by the simulated congestion in an expected manner and to determine the fastest network configuration.

1. Stop the test.
   a. Return to the **Linux01** console tab.
   b. In the Linux01 console, press Ctrl+C to stop the client script.
   c. Return to the **Linux02** console tab.
   d. In the Linux02 console, stop the server process to end the server program.

      ```
      ps -ef | grep netserver
      kill process_id
      ```

      *process_id* is the `netserver` process ID that appears in the `ps` command output.
2. Review the sample values that you recorded in task 6.

   **Q1. Do you see an obvious difference in network throughput for each test?**

   **Q2. Which test resulted in the highest throughput (highest values)?**

   **Q3. Why was this test the fastest?**

## Task 8: Clean Up for the Next Lab

You end `esxtop` and you close the **Linux01** and **Linux02** console tabs. You also change the vSphere DRS automation mode to Fully Automated.

1. In the MTPuTTY window, enter **`q`** to end `esxtop`.
2. Close the MTPuTTY session.
3. Close the **Linux01** and **Linux02** console tabs.
4. On the **vSphere Client** tab, power off Linux01 and Linux02.
5. Migrate the local storage of Linux01 to shared storage.
   a. In the left pane, right-click **Linux01** and select **Migrate**.

      The Migrate wizard appears.
   b. On the Select the migration type page, click **Change storage only** and click **Next**.

c. On the Select storage page, select **OPSCALE-Datastore** and click **Next**.

d. On the Ready to complete page, click **Finish**.

e. In the Recent Tasks pane, monitor the migration task to completion.

6. Keep the **vSphere Client** tab open for the next lab.

# *Lab 12* Configuring Lockdown Mode

## Objective: Configure and test lockdown mode

In this lab, you perform the following tasks:

1. Start the vSphere ESXi Shell and SSH Services
2. Test the SSH Connection
3. Enable and Test Lockdown Mode
4. Disable Lockdown Mode
5. Examine the DCUI.Access List

### Task 1: Start the vSphere ESXi Shell and SSH Services

You use vSphere Client to verify that the VMware vSphere® ESXi™ Shell and SSH services are running on sa-esxi-01.vclass.local.

1. In Firefox, click the **vSphere Client** tab and log in, if necessary.
2. In vSphere Client, select **Host and Clusters** from the **Menu** drop-down menu.
3. In the left pane, select **sa-esxi-01.vclass.local**.
4. In the right pane, click the **Configure** tab.
5. On the left under System, click **Services**.
6. Verify that the vSphere ESXi Shell service is running and that the startup policy is set to start and stop with the host.
7. Verify that the SSH service is running and that the startup policy is set to start and stop with the host.

   By default, the vSphere ESXi Shell and SSH services are not configured to start with the host. This setting was enabled as part of the lab kit configuration.

## Task 2: Test the SSH Connection

You use MTPuTTY to connect to the ESXi host and verify that SSH is working.

1. Click **MTPuTTY** in the Windows desktop taskbar.

   The MTPuTTY utility window appears.

2. In the left pane, double-click **SA-ESXi-01**.

   A new **SA-ESXi-01** tab opens in the right pane.

   MTPuTTY is configured to automatically log in to the ESXi host as user root.

3. If the login is successful, enter `exit`.

## Task 3: Enable and Test Lockdown Mode

You enable lockdown mode for your assigned ESXi host.

1. Return to the **vSphere Client** tab.

   sa-esxi-01.vclass.local should be selected in the left pane.

2. In the right pane, click the **Configure** tab.

3. In the left pane under System, click **Security Profile**.

4. Enable normal lockdown mode.

   a. In the right pane, click **Edit** next to Lockdown Mode.

      The Lockdown Mode wizard appears.

   b. On the Lockdown Mode page, click **Normal**.

   c. Click **Exception Users** on the left.

      Users are not listed.

   d. Click **OK**.

5. Verify that normal lockdown mode works properly.

   The user root will be denied access in this SSH session.

   In lockdown mode, all users except those defined in the Exception Users list are denied direct access to the host vSphere ESXi Shell, SSH, and DCUI.

   a. Go to the **MTPuTTY** window.

   b. In the left pane, double-click **SA-ESXi-01**.

      MTPuTTY automatically tries to log in as root.

   c. Verify that user root is not logged in and that the `Access Denied` message appears.

   d. Close the MTPuTTY window.

## Task 4: Disable Lockdown Mode

You disable lockdown mode.

1. Return to the **vSphere Client** tab.
2. Click **Edit** next to Lockdown Mode.
3. On the Lockdown Mode page, click **Disabled**.
4. Click **OK**.

## Task 5: Examine the DCUI.Access List

You examine the DCUI.Access list. The DCUI.Access list is a list of local users on an ESXi host. These users have rights to disable lockdown mode when a catastrophic failure occurs and administrators need direct host access again. These users do not need the administrator role on the ESXi host.

1. In the right pane on the left, click **Advanced System Settings** under System.
2. In the Advanced System Settings pane, click the filter icon in the Key column.
3. Enter **`dcui`** and click **Filter**.

   The DCUI.Access entry appears.

4. Examine the value of the DCUI.Access setting.

   The root user is added to the DCUI.Access list by default. Thus, the root user can disable lockdown mode but cannot bypass lockdown mode.

5. Keep the **vSphere Client** tab open for the next lab.

# *Lab 13* Working with Certificates

## Objective: Generate and replace a vCenter Server certificate

In this lab, you perform the following tasks:

1. Examine vSphere Certificates
2. Create a Windows 2012 Certificate Authority Template for vSphere
3. Create a Certificate Signing Request
4. Download the CSR to the Student Desktop
5. Request a Signed Custom Certificate
6. Replace a Machine Certificate with the New Custom Certificate

## Task 1: Examine vSphere Certificates

You examine the default certificates issued by VMware Certificate Authority in a nonproduction vCenter Server system.

1. In Firefox, click the **vSphere Client** tab and log in, if necessary.
2. Select **Administration** from the **Menu** drop-down menu.
3. In the left pane, select **Certificate Management**.
4. In the right pane, enter vCenter Server credentials to manage certificates.
   a. In the **Server IP/FQDN** text box, enter **`sa-vcsa-01.vclass.local`**.
   b. In the **Username** text box, enter **`administrator@vsphere.local`**.
   c. In the **Password** text box, enter **`VMware1!`**.
   d. Click **Login and Manage Certificates**.

      Various certificates appear in the Certificate Management panel.

      **Q1. How many active certificates are in the certificate store for this node?**

      **Q2. How long are the certificates valid for?**

5. Scroll down and click **View Details** for the first certificate under Trusted Root Certificates.

   **Q3. Who issued the certificate?**

6. At the top of the right pane, click **Back to Certificate Management**.

   **Q4. How many solution certificates do you see?**

   **Q5. What are the names of the solution users that have certificates (from the Subject field)?**

## Task 2: Create a Windows 2012 Certificate Authority Template for vSphere

You create a vSphere 6.7 certificate template on a Windows 2012 Server domain controller that you can use to create certificates that work with vSphere 6.7. The certificate template can be used to create machine SSL or solution user certificates in VMware CA.

1. Open a console to dc.vclass.local.
   a. Click the **Remote Desktop Connection Manager** icon in the Windows desktop toolbar.

      The Remote Desktop Connection Manager window appears.

   b. In the left pane, double-click **DC (vclass.local)**.

      The desktop for dc.vclass.local appears in the right pane.

      You are automatically logged in as a domain administrator.
2. Open the certification authority console.
   a. Click the Windows **Start** button on the dc.vclass.local desktop.
   b. On the Apps page, click the up arrow icon.
   c. Click **Administrative Tools**.
   d. In the Administrative Tools window, double-click **Certification Authority**.

      The Certification Authority window appears.
3. Open the certificate templates console.
   a. Expand **vclass-DC-CA**.
   b. Right-click **Certificate Templates** and select **Manage**.
4. Configure a new certificate template.
   a. Right-click the existing **Web Server** template and select **Duplicate Template**.

      The Properties of New Template dialog box appears.

   b. Click the **General** tab and enter **`vSphere67`** in the **Template display name** text box.
   c. Click the **Extensions** tab.
   d. Select **Key Usage** and click **Edit**.
   e. In the Edit Key Usage Extension dialog box, select the **Signature is proof of origin (nonrepudiation)** and **Allow encryption of user data** check boxes.
   f. Click **OK**.
   g. Select **Application Policies** and click **Edit**.

h. In the Edit Application Policies Extension dialog box, click **Add** and select **Client Authentication**.

i. Click **OK**.

j. Click the **Request Handling** tab and select the **Allow private key to be exported** check box.

k. Click **OK** to save the new certificate template.

l. Close the Certificate Templates Console window.

5. Enable the new certificate template.

   a. In the Certification Authority console window, right-click **Certificate Templates** and select **New > Certificate Template to Issue**.

      The Enable Certificate Templates window appears.

   b. Select **vSphere67** and click **OK.**

   c. Close all open windows.

   d. In the left pane of the Remote Desktop Connection Manager, right-click **DC (vclass.local)** and select **Disconnect server**.

6. Close the Remote Desktop Connection Manager window.

## Task 3: Create a Certificate Signing Request

You use vSphere Certificate Manager to create a certificate signing request (CSR) that you use to request a signed custom certificate from the domain controller certificate authority (CA) for the lab.

1. Start an SSH session with SA-VCSA-01.

   a. Click **MTPuTTY** in the Windows desktop toolbar.

      The MTPuTTY utility window appears.

   b. In the left pane, double-click **SA-VCSA-01**.

      A new **SA-VCSA-01** tab opens in the center pane.

   c. Enter **`shell`** to start a Bash shell.

2. Create a certificate signing request.

   a. Enter **`/usr/lib/vmware-vmca/bin/certificate-manager`**.

      The vSphere Certificate Manager program starts.

   b. Enter **`1`** to select the **Replace Machine SSL certificate with Custom Certificate** option.

   c. Press Enter to accept the default user name of Administrator@vsphere.local.

   d. Enter the password **`VMware1!`**.

e. Enter **1** to select the **Generate Certificate Signing Request** option.

f. For the output directory path, enter **/var/tmp**.

The /var/tmp directory on Linux and UNIX systems is a temporary directory. The contents of the/var/tmp directory are not deleted during a reboot.

3. Configure the certificate properties.

a. For **Country**, press Enter to accept the default.

b. For **Name**, enter **VMware**.

c. For **Organization**, enter **VMeduc**.

d. For **OrgUnit**, enter **vclass**.

e. For **State**, press Enter.

f. For **Locality**, press Enter.

g. For **IPAddress**, press Enter.

h. For **Email**, enter **certadmin@vclass.local**.

i. For **Hostname**, enter **sa-vcsa-01.vclass.local**.

j. For **Name**, enter **sa-vcsa-01.vclass.local**.

4. Enter **2** to exit vSphere Certificate Manager.

## Task 4: Download the CSR to the Student Desktop

You download the CSR from the vCenter Server system to your student desktop.

1. Enter **chsh -s /bin/bash** to temporarily change the login shell of the root account to /bin/bash.

This step is necessary for WinSCP to connect to the vCenter Server system so that you can download the CSR to your student desktop.

2. Start the WinSCP application.

a. On the student desktop taskbar, click the **WinSCP** icon.

b. In the left pane, double-click **SA-VCSA-01**.

c. In the Warning dialog box, click **Update** to accept and remember the Certificate Lab vCenter Server public key for SSH.

d. Click **Continue** to close the Authentication Banner dialog box.

In the WinSCP window, you should see the `C:\Materials\Downloads` folder on your student desktop in the left pane and the `/root` directory on the vCenter Server Appliance instance in the right pane.

3. Use the folder controls to navigate to the `/var/tmp` directory in the right pane.
4. If the left pane is not `C:\Materials\Downloads`, then use the folder controls to navigate to the `C:\Materials\Downloads` folder.
5. Drag the **vmca_issued_csr.csr** and **vmca_issued_key.key** files from the `/var/tmp` directory in the right pane to the `C:\Materials\Downloads` folder in the left pane.

   This action copies the files from the vCenter Server system to the `Downloads` folder on your student desktop.
6. Leave the WinSCP window open.

## Task 5: Request a Signed Custom Certificate

You request a signed custom certificate from the domain controller CA for the lab.

1. Copy the contents of the `vmca_issued_csr.csr` file to the clipboard.
   a. On your student desktop, open Windows Explorer and navigate to the `C:\Materials\Downloads` folder.
   b. Right-click the **vmca_issued_csr.csr** file and select **Edit with Notepad++**.
   c. Select all the text.
   d. Press Ctrl+C to copy the selected text to the clipboard.
2. Go to the certificate services program on the domain controller and request a certificate.
   a. On your student desktop, open a new Firefox tab and go to http://dc.vclass.local/certsrv.
   b. Log in with the user name administrator and the password VMware1!.
   c. On the Microsoft Active Directory Certificate Services page, click the **Request a certificate** link.
   d. Click the **advanced certificate request** link.
   e. Under Saved Request, press Ctrl+V to paste the CSR text into the **Base-64-encoded certificate request** text box.
   f. From the **Certificate Template** drop-down menu, select **vSphere67**.
   g. Click **Submit**.

h. Click **Base 64 encoded**.

i. Click the **Download certificate** link.

j. Save the file to the `C:\Materials\Downloads` folder as `machine_ssl.cer`.

**NOTE**

The filename is case-sensitive and must exactly match the correct filename for the script to use it.

3. Download the certificate chain.

a. On the **Firefox** tab, click the **Download certificate chain** link.

**Base 64 encoded** should still be clicked.

b. Save the file to the `C:\Materials\Downloads` folder as `cachain.p7b`.

**NOTE**

The filename is case-sensitive and must exactly match the correct filename for the script to use it.

c. Close the **Microsoft Active Directory Certificate Services** tab.

d. Close Notepad++.

4. Export the root certificate.

a. Switch to the Windows Explorer window and navigate to the `C:\Materials\Downloads` directory.

b. Right-click the **cachain.p7b** file and select **Open**.

The Certificate Manager Console opens.

c. In the left pane, expand the inventory tree until you see the `Certificates` folder.

d. Select the **Certificates** folder.

You should see two certificates: the root certificate for your domain controller and the custom certificate for your vCenter Server Appliance instance.

VMware appears under the Issued To column and vSphere67 appears under the Certificate Template column at the far right.

e. To export the root certificate, right-click the root certificate **vclass-DC-CA** and select **All Tasks** > **Export**.

The Certificate Export wizard appears.

f. Click **Next**.

g. On the Export File Format page, click **Base-64 encoded X.509 (.CER)** and click **Next**.

h. On the File to Export page, click **Browse**.

i. Navigate to the `C:\Materials\Downloads` folder.

j. Enter **`root-64.cer`** in the **File name** text box.

**NOTE**

The filename is case-sensitive and must exactly match the correct filename for the script to use it.

k. Click **Save**.

l. On the File to Export page, click **Next**.

m. Click **Finish**.

n. Click **OK**.

o. Close the Certificate Manager Console.

## Task 6: Replace a Machine Certificate with the New Custom Certificate

You replace the machine SSL certificate for vCenter Server with the new custom certificate so that VMware CA acts as a subordinate CA to the domain controller CA.

1. Copy the certificate files from the student desktop to the vCenter Server system.

   a. Switch to the WinSCP window.

   b. In the WinSCP window, drag the **machine_ssl.cer** and **root-64.cer** files from the `C:\Materials\Downloads` folder to the `/var/tmp` folder in the right pane.

      If you do not see the files refresh the files in the left pane.

      This action copies the certificate files from the student desktop to the vCenter Server system.

2. In the MTPuTTY session, change the login shell of the root account back to the vCenter Server Appliance shell.

   a. Switch to the MTPuTTY window.

   b. If the SSH session to SA-VCSA-01 is not open, reconnect to SA-VCSA-01.

   c. If you see the `timed out waiting for input: auto-logout` message, enter **`shell`**.

   d. Enter **`chsh -s /bin/appliancesh`** to change the login shell of the root account back to the vCenter Server Appliance shell.

      This step returns the vCenter Server system to its more secure posture.

3. Replace the machine SSL certificate with the custom certificate.
   a. Enter **`cd /var/tmp`** to change to the `/var/tmp` directory.

      If you run vSphere Certificate Manager from the `/var/tmp` directory, you do not have to enter the full path for each of the certificate and key files that you import.

   b. Enter **`/usr/lib/vmware-vmca/bin/certificate-manager`** to start vSphere Certificate Manager.

   c. Enter **`1`** to select the **Replace Machine SSL certificate with Custom Certificate** option.

   d. Press Enter to use the default user name of Administrator@vsphere.local.

   e. When prompted, enter the password **`VMware1!`**.

   f. Enter **`2`** to select the **Import custom certificate(s) and key(s)** option.

   g. Import the custom certificate.

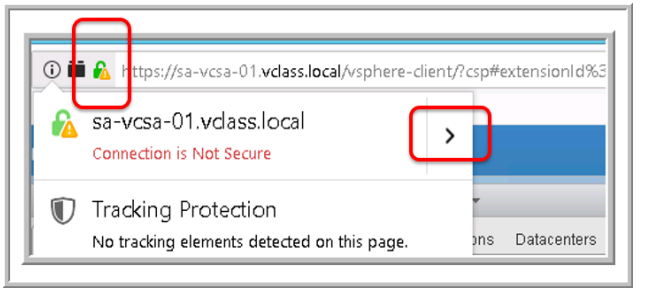
| Option | Action |
|---|---|
| **Please provide valid custom certificate for Machine SSL** | Enter **`machine_ssl.cer`**. |
| **Please provide valid custom key for Machine SSL** | Enter **`vmca_issued_key.key`**. |
| **Please provide the signing certificate of the Machine SSL certificate** | Enter **`root-64.cer`**. |
| **You are going to replace Machine SSL cert using custom cert. Continue operation: Option[Y/N]?:** | Enter **`y`**. |

      You must wait for the process to complete. This process takes several minutes while the services are restarted.

      During this operation, review the number of services that are updated.

   h. Wait until the `100% Complete [All tasks completed successfully]` message appears.

4. Close and reopen Firefox and log in to vSphere Client.
   a. Close the Firefox window.
   b. Start Firefox.
   c. From the Favorites bar, select **vSphere Site-A > vSphere Client (SA-VCSA-01)**.
   d. In the Insecure Connection window, click **Advanced**, click **Add Exception**, and click **Confirm Security Exception**.
   e. Log in to vSphere Client as administrator@vsphere.local with the password VMware1!.
5. In the Firefox browser, click the security report icon (padlock) to the left of the **Location** text box.




6. View information about the machine certificate.
   a. Click the **arrow** to the right of Connection is Not Secure.
   b. Click **More Information**.
   c. Click **View Certificate**.
   d. Click the **Details** tab.
   e. In the Certificate Fields panel, scroll down and select **Certificate Subject Alt Name**.

      **Q1. To which machine was the certificate issued?**

   f. Scroll up and select **Issuer**.

      **Q2. Who issued the certificate?**

g. Scroll down and select **Not Before**.

**Q3. On what day did the certificate become valid?**

**Q4. Why does Firefox on your student desktop trust the vCenter Server certificate?**

h. Click **Close**.

i. Close the dialog box.

7. Keep the **vSphere Client** tab open for the next lab.
8. Close all other windows.
   a. Close the WinSCP window.
   b. Close the MTPuTTY window.
   c. Close the Windows Explorer window.

# *Lab 14* Virtual Machine Encryption

## Objective: Register a key management server with vCenter Server and encrypt a virtual machine

In this lab, you perform the following tasks:

1. Verify Access to the Key Management Server
2. Register the KMS with vCenter Server
3. Create an Encryption Storage Policy
4. Encrypt a Virtual Machine
5. Use Encrypted vSphere vMotion to Migrate Virtual Machines

### Task 1: Verify Access to the Key Management Server

You verify that you can access the key management server (KMS).

The KMS used in this lab is a simple Python-based key server that keeps keys while the KMS is running.

1. Use MTPuTTY to log in to vCenter Server Appliance.
   a. On the taskbar, click the **MTPuTTY** icon.
   b. In the left pane, double-click **SA-VCSA-01**.

      You are logged in to vCenter Server Appliance as user root.

2. Ping the photon-client, which is the key management server.
   a. At the command prompt, enter **`shell`**.
   b. At the shell command prompt, ping the key management server.

      ```
      ping photon-client
      ```

   c. Verify that the ping is successful.
   d. Press Ctrl+C to end the `ping` command.
3. Exit the MTPuTTY session and close the MTPuTTY window.

## Task 2: Register the KMS with vCenter Server

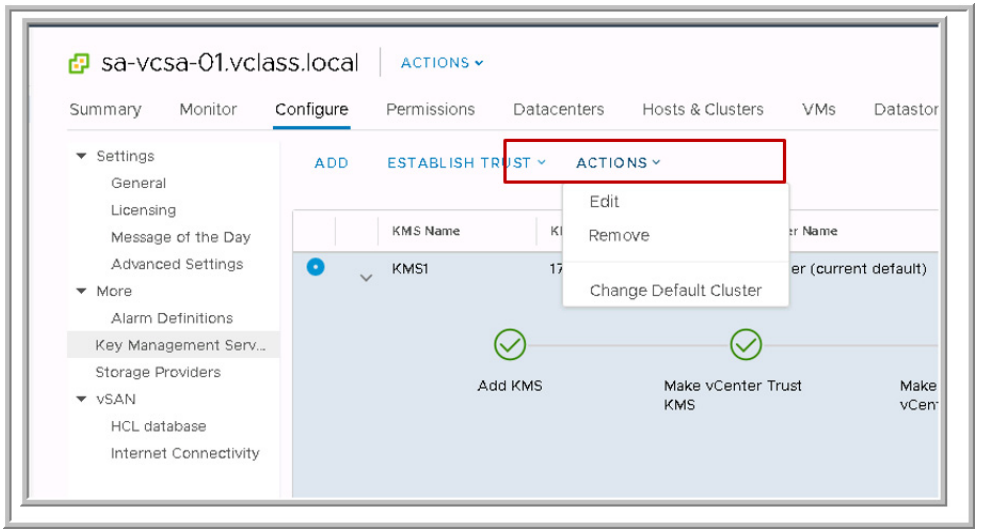
You register the KMS with vCenter Server, and you mark the KMS cluster as the default.

1. In Firefox, click the **vSphere Client** tab and log in, if necessary.
2. Select **Hosts and Clusters** from the **Menu** drop-down menu.
3. In the left pane, select **sa-vcsa-01.vclass.local**.
4. In the right pane, click the **Configure** tab and click **Key Management Servers** on the left.
5. Click **Add**.

   The Add KMS dialog box appears.
6. Click the text field to the right of KMS Cluster and select **Create New Cluster**.
7. Enter **`SA KMS-Cluster`** in the **New cluster name** text box.
8. In the **Server name** text box, enter **`KMS1`**.
9. In the **Server address** text box, enter **`172.20.10.193`**.

   172.20.10.193 is the IP address of the KMS.
10. In the **Server port** text box, enter **`5696`**.
11. Leave the remaining text boxes blank and click **Add**.
12. In the Make vCenter Trust KMS window, click **Trust**.
13. Verify that the KMS appears in the list.

14. From the **Actions** drop-down menu above the KMS servers, select **Change Default Cluster**.




15. Click **Save**.

## Task 3: Create an Encryption Storage Policy

You create a virtual machine storage policy that includes only the encryption common rule.

Although a prebuilt policy called VM Encryption Policy is available, you should understand how the policy is created.

1. Select **Policies and Profiles** from the **Menu** drop-down menu.
2. In the left pane, select **VM Storage Policies**.
3. In the right pane, click **Create VM Storage Policy**.

   The Create VM Storage Policy wizard appears.
4. On the Name and description page, enter **`SA Encryption Policy`** in the **Name** text box and click **Next**.
5. On the Policy structure page, select the **Enable host based rules** check box and click **Next**.
6. On the Host based services page, click **Custom** on the **Encryption** tab.

   The custom properties show that the provider is VMware VM Encryption and that I/O filters are not allowed before encryption.
7. Click **Next**.

8. On the Storage compatibility page, review the compatible storage.

   All storage is compatible with the encryption filter because the filter is applied as a common rule, so the filter is storage agnostic.

9. Click **Next**.
10. On the Review and finish page, click **Finish**.
11. Verify that your encryption policy appears in the storage policies list.

## Task 4: Encrypt a Virtual Machine

You encrypt a virtual machine.

1. Select **Hosts and Clusters** in the **Menu** drop-down menu.
2. In the left pane, right-click **Photon-01** and select **VM Policies** > **Edit VM Storage Policies**.
3. In the Edit VM Storage Policies dialog box, select **SA Encryption Policy** from the **VM storage policy** drop-down menu.
4. Click **OK**.
5. Verify that the virtual machine is encrypted.
   a. In the left pane, select **Photon-01**.
   b. In the right pane, expand the **VM Hardware** panel on the **Summary** tab.

      The panel states that the virtual machine configuration files and the hard disk are encrypted.

## Task 5: Use Encrypted vSphere vMotion to Migrate Virtual Machines

You use encrypted VMware vSphere® vMotion® to migrate Photon-01 (the encrypted virtual machine) and Photon-02 (an unencrypted virtual machine) to a different host.

1. View the vSphere vMotion encryption state on Photon-01.
   a. In the left pane, right-click **Photon-01** and select **Edit Settings**.
   b. Click the **VM Options** tab.
   c. Expand the Encryption panel.

      Because Photon-01 is encrypted, the Encrypted vMotion state is always Required and cannot be changed.

   d. Click **Cancel**.

2. View the vSphere vMotion encryption state on Photon-02.
   a. In the left pane, right-click **Photon-02** and select **Edit Settings**.
   b. Click the **VM Options** tab.
   c. Expand the Encryption panel.

      Because Photon-02 is not encrypted, the default state is Opportunistic.
   d. Keep the default value and click **Cancel**.
3. Power on Photon-01 and Photon-02.
4. Migrate Photon-01 and Photon-02 to sa-esxi-03.vclass.local.
   a. Right-click **Photon-01** and select **Migrate**.
   b. On the Select a migration type page, leave **Change compute resource only** clicked and click **Next**.
   c. On the Select a compute resource page, click **sa-esxi-03.vclass.local** and click **Next**.
   d. On the Select networks page, select **pg-SA-Management** for the destination network and click **Next**.
   e. On the Select vMotion priority page, click **Next**.
   f. On the Ready to complete page, click **Finish**.
   g. Click the **Summary** tab of Photon-01 and verify that Photon-01 is now on sa-esxi-03.vclass.local.
   h. Repeat substeps a through g to migrate Photon-02.
5. View the hot migration events that occurred.
   a. In the left pane, select **sa-vcsa-01.vclass.local**.
   b. In the center pane, click the **Monitor** tab.
   c. Click **Events** on the left.
   d. Click the down arrow next to the Description column header and select **Filter**.
   e. Enter **`encryption`** in the text box and click **Filter**.

      You should see two events that begin with Hot migrating Photon-02 and Hot migrating Photon-01.
   f. Select each of these events and view the description.

      The description mentions that a hot migration was performed with encryption.

# *Answer Key*

## **Lab 4:** Creating vSAN Storage Policies

Task 1: Examine the Default Storage Policy . . . . . .23

**1.** One failure

Task 2: Create a Custom Policy with No Failure Tolerance . . . . . .24

**1.** Because the number of failures to tolerate is zero, a mirrored copy of the virtual machine is not created.

Task 3: Assign the Custom Policy to a Virtual Machine . . . . . .25

**1.** Because the selected storage policy is only compatible with vSAN datastores and the virtual machine is currently located on a VMFS datastore.

**2.** OPSCALE-Datastore.

**3.** Custom01.

**4.** No. The status is Not Applicable.

Task 5: Create an Invalid Storage Policy . . . . . .27

**1.** Because the storage policy requires at least four fault domains contributing all-flash storage but only three were found.

## **Lab 7:** Using vSphere Auto Deploy

Task 8: Start the TFTP Service on vCenter Server Appliance . . . . . .51

**1.** ATFTPD_DIRECTORY = “/var/lib/tftpboot”.

**2.** Yes. The filename is undionly.kpxe.vmw-hardwired.

## **Lab 9:** Monitoring Memory Performance

Task 2: Check for Overcommitment of Virtual Machine Memory . . . . . .68

**1.** Answers vary depending on the current workload.

Task 6: Record Memory Statistics. . . . . .71

**1.** Yes, the values should converge over time.

2. Depending on many factors, the values might converge over time.
3. ResourceHog02 and ResourceHog01.
4. Although all three VMs might be swapping, the levels of swapping on ResourceHog01 and ResourceHog02 are going to be much larger than the level of swapping on Linux01.
5. ResourceHog01 and ResourceHog02 should experience high %SWPWT values because their memory is being swapped out and they must wait whenever those pages are accessed. Linux01 should experience low %SWPWT values, possibly zero.
6. Answers vary.
7. Answers vary.

## **Lab 10:** Monitoring Storage Performance



1. vmhba65, the software iSCSI adapter.



1. vmhba1, a local host bus adapter.

## **Lab 11:** Monitoring Network Performance



1. Yes. Network throughput values will vary.
2. The test with the client and server on the same port group.
3. Because network I/O did not pass through the physical network hardware.

## **Lab 13:** Working with Certificates



1. The total might vary. Typically, eight or more certificates are in the certificates management list.
2. By default, tickets issued by VMware CA are valid for 10 years. The machine certificate might have a different expiration date from the other certificates.
3. Under Issuer Information, the Issuer Name field contains CA, which indicates that VMware CA issued the certificate.
4. Four solution certificates and one Trusted Root Certificates are shown for this configuration.
5. Machine, vsphere-webclient, vpxd, and vpxd-extension.



1. The certificate was issued to the vCenter Server-Platform Services Controller system, sa-vcsa-01.vclass.local.
2. The domain controller CA issued the certificate.
3. The certificate was signed now, so it is valid from today.
4. The student desktop is a member of the same Active Directory domain, and Firefox is using the same certificate store. Because the vCenter Server certificate is signed by the domain controller CA, Firefox trusts the subordinate certificate.