VMware vSphere:
Operate, Scale and Secure [V8]

Lab Manual

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

VMware vSphere: Operate, Scale and Secure [V8]
Lab Manual
Part Number EDU-EN-VSOSS8-LAB (11-JUL-2023)

Typographical Conventions

The following typographical conventions are used in this course.

Conventions	Usage and Examples
`Monospace`	Identifies command names, command options, parameters, code fragments, error messages, filenames, folder names, directory names, and path names: • Run the `esxtop` command. • ... found in the `/var/log/messages` file.
`Monospace Bold`	Identifies user inputs: • Enter **`ipconfig /release`**.
Boldface	Identifies user interface controls: • Click the **Configuration** tab.
Italic	Identifies book titles: • *vSphere Virtual Machine Administration*
< >	Indicates placeholder variables: • <ESXi_host_name> • ... the `Settings/<Your_Name>.txt` file

Contents

Lab 1 Accessing the Lab Environment

Objective and Tasks

Access the lab environment and verify that vSphere licenses are valid:

1. Access Your Lab Environment
2. Verify That the vSphere Licenses Are Valid
3. (Optional) Assign Valid vSphere Licenses

Task 1: Access Your Lab Environment

You access and manage the lab environment from the student desktop.

The system assigned to you serves as an end-user terminal.

1. Verify that you are successfully logged into the student desktop.

   NOTE

   If not, log in to your student desktop by entering **`Student01`** as the user name and **`VMware1!`** as the password.

   ---

2. Log in to the vSphere Client on Site A.

   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.

   b. Select **vSphere Client (SA-VCSA-01)**.

   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**

      You should see **sa-vcsa-01.vclass.local** in the vSphere Client's navigation pane.

NOTE

On the vCenter Summary tab, you may see vSAN warning messages for SA-Compute-02. These warnings can be safely ignored. Select **Actions > Reset To green** to clear the warning message.

Task 2: Verify That the vSphere Licenses Are Valid

You verify that the licenses for the vCenter Server system and the ESXi hosts are valid for Site A.

1. Verify that the licenses for the vCenter Server system are not expired.

   a. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.

   b. Select **sa-vcsa-01.vclass.local**.

   c. In the right pane, click the **Configure** tab and click **Licensing** under Settings.

   d. Verify that the license expiration date for the vCenter instance is in the future.

2. Verify that the licenses for the ESXi hosts are valid.

   a. From the main menu, select **Administration** and select **Licenses** under licensing.

   b. On the Licenses page, click **Assets** and click the **HOSTS** tab.

   c. View the License Expiration column and conform that the license for host the ESXi hosts are not expired.

3. If any license has expired, proceed to task 3.

Task 3: (Optional) Assign Valid vSphere Licenses

You assign valid licenses to these vSphere components if the vCenter Server and ESXi host licenses are expired.

1. From the main menu, select **Administration**.
2. Assign a vCenter Server license key to the vCenter Server instance.
   a. In the navigation pane, select **Licenses** under Licensing.
   b. On the Licenses pane, click the **Licenses** tab.
   c. Click **ADD** to add new licenses.
   d. On the Enter license keys page, enter the vCenter Server and vSphere Enterprise Plus license keys in the **License keys** text box. For a list of license keys see: https://vmware.bravais.com/s/FMuCRtkwDwqlXWNrw5oF

      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 and click **Next.**
   g. On the Ready to complete page, click **Finish**.
   h. In the Licenses pane, click the **Assets** tab and select **VCENTER SERVER SYSTEMS**.
   i. Select the **sa-vcsa-01.vclass.local** check box and click **ASSIGN LICENSE**.
   j. Select the vCenter license and click **OK**.
3. Assign the vSphere Enterprise Plus license key to the ESXi hosts for Site A.
   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 5 objects.
   d. In the Assign License dialog box, select the vSphere Enterprise Plus license key and click **OK**.
4. Reconnect the ESXi hosts.
   a. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.
   b. In the navigation pane, select **SA-Datacenter**.
   c. In the right pane, click the **Hosts & Clusters** tab and select **Hosts**.

      If the ESXi hosts have a status of disconnected, perform substeps d and e.
   d. Right-click each disconnected host and select **Connection** > **Connect** if not connected.
   e. Verify that all ESXi hosts have a status of Connected.

Lab 2 Configuring a Centralized VMware Tools Installation Repository

Objective and Tasks

Create a shared VMware Tools repository:

1. Preconfigure the Environment
2. Copy the VMware Tools Packages to a Datastore
3. View the ESXi Advanced Settings
4. Re-create the `/productLocker` Symlink

Task 1: Preconfigure the Environment

You perform some preconfiguration in the vSphere Client and ESXi.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser and click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**

2. You enable the SSH service on your ESXi host.

   a. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.

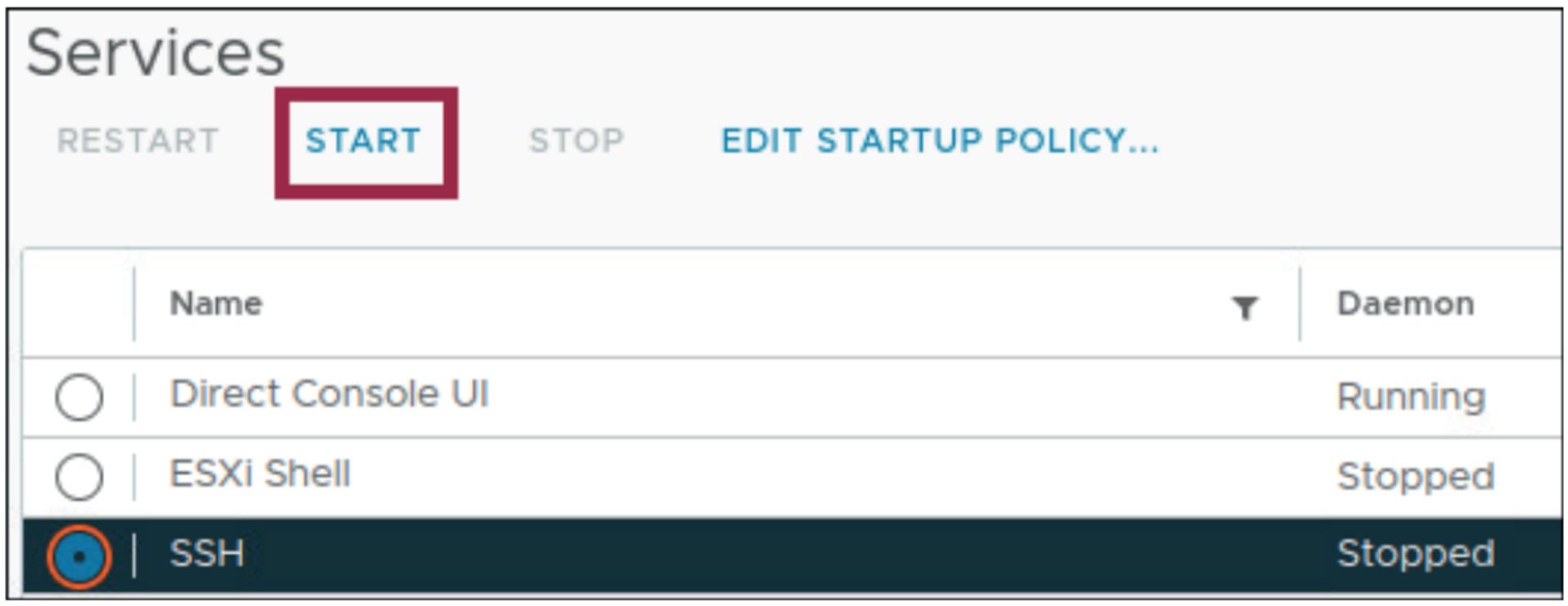
   b. In the navigation pane, expand **sa-vcsa-01.vclass.local**, **SA-Datacenter** and the **SA-Compute-02** cluster.

   c. In the navigation pane, select **sa-esxi-04.vclass.local**.

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

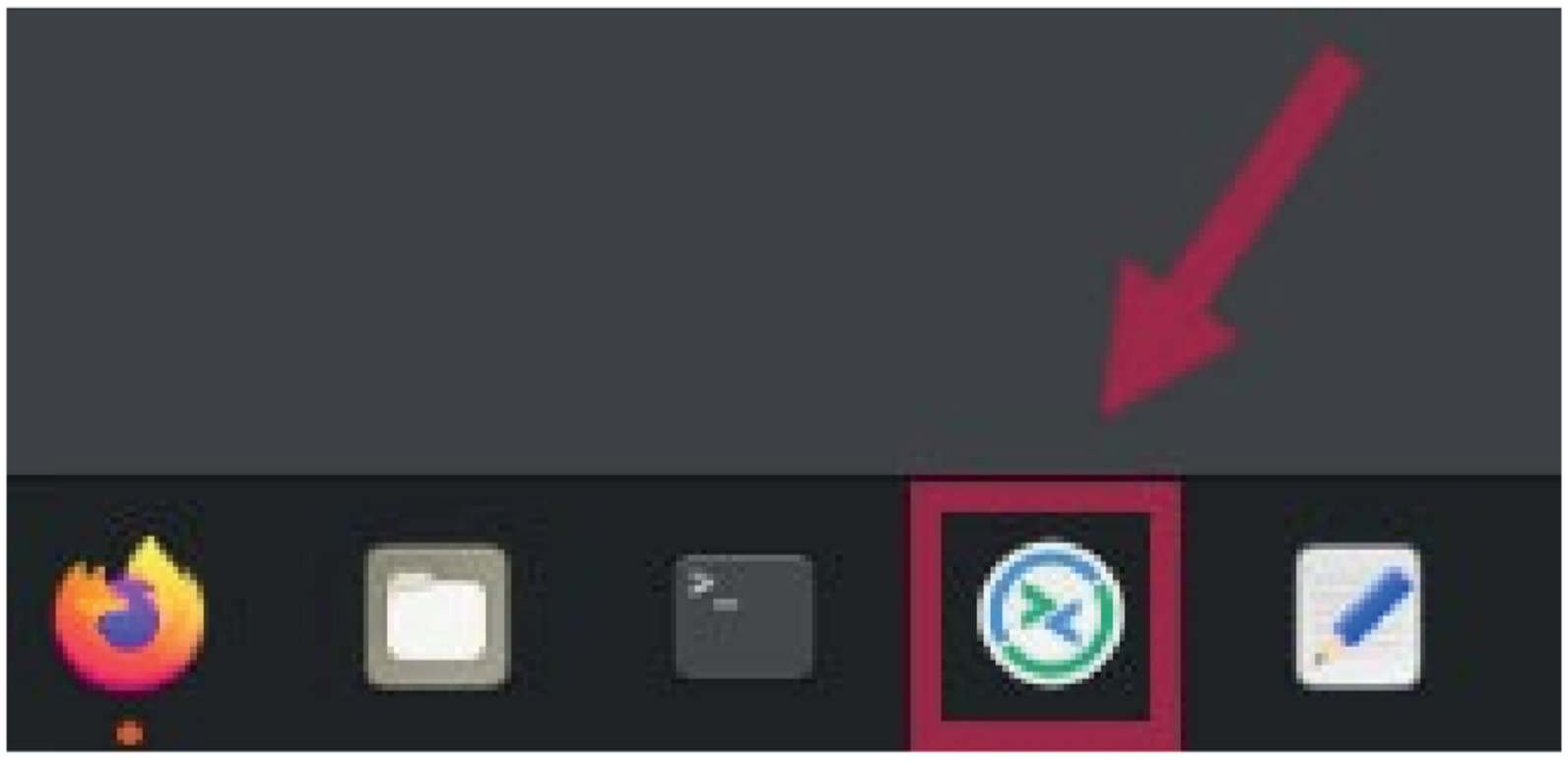
   e. Select **Services** under System.

   f. **Start** the **SSH** service.

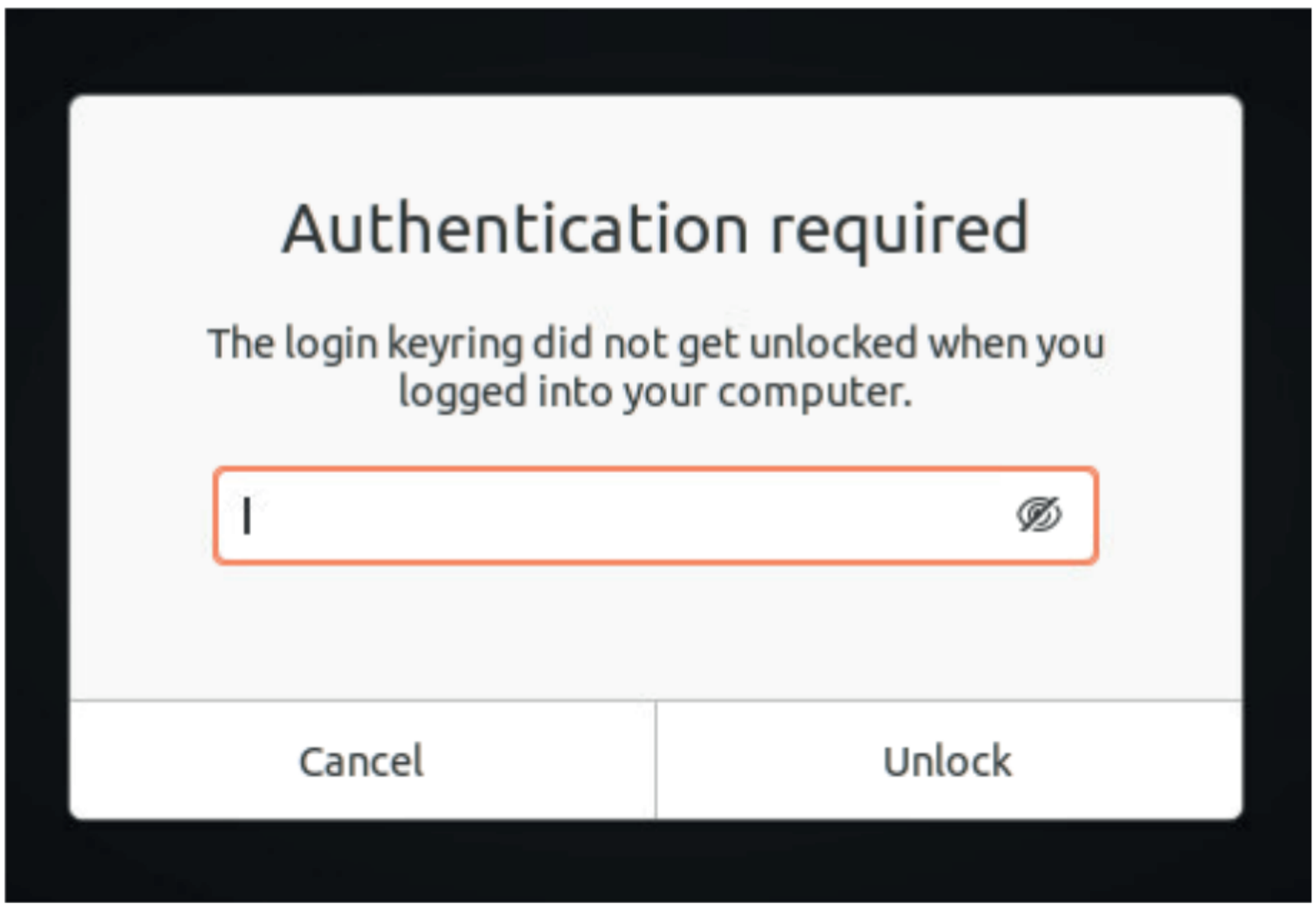


3. Open an SSH session to SA-ESXi-04.

   a. On the Linux taskbar, click **Remmina**



b. If the **Authentication required** pop-up appears, for the password enter: **`VMware1!`**



c. Double-click **SA-ESXi-04**.

You will be logged into sa-esxi-04.vclass.local as the root user.

NOTE

If prompted for login credentials, log in by entering user name **`root`** and password **`VMware1!`**

Task 2: Copy the VMware Tools Packages to a Datastore

Verify the VMware Tools packages are extracted and copy the files to a desired datastore accessible to your ESXi hosts.

1. On the ESXi host, verify **vmtools** and **floppies** sub-directories are located in /productLocker:

   ```
   cd /productLocker
   ls
   ```

2. Create **/vmtoolsRepo** directory in OPSCALE-Datastore:

   ```
   mkdir /vmfs/volumes/OPSCALE-Datastore/vmtoolsRepo
   ```

3. Copy the **vmtools** and **floppies** sub-directories to **/vmfs/volumes/OPSCALE-Datastore/vmtoolsRepo**

   ```
   cp -r * /vmfs/volumes/OPSCALE-Datastore/vmtoolsRepo
   ```

4. Verify **vmtools** and **floppies** sub-directories are located in the desired datastore:

   ```
   ls /vmfs/volumes/OPSCALE-Datastore/vmtoolsRepo
   ```

5. Close the Remmina window.

Task 3: View the ESXi Advanced Settings

View the current `productlocker` variable in the ESXi Advanced Settings from the vSphere Client.

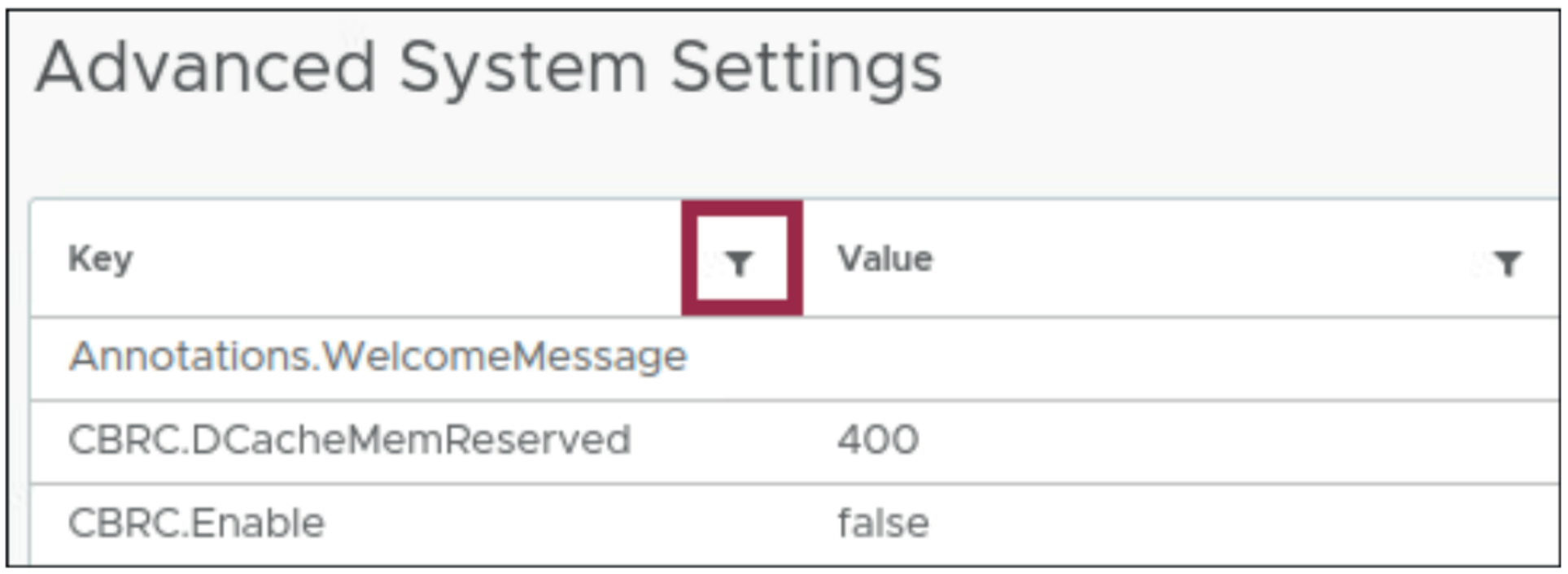
1. From the vSphere Client, filer for the UserVars.ProductLockerLocation key in Advanced System Settings.

   a. Return to the vSphere Client browser tab.

   b. Select the **sa-esxi-04.vclass.local** and select **Configure** tab.

   c. Click **Advanced System Settings** under System.

   d. Filter for **Locker** under Key.



   e. Record the value that appears in advanced settings.

   _____

Task 4: Re-create the /productLocker Symlink

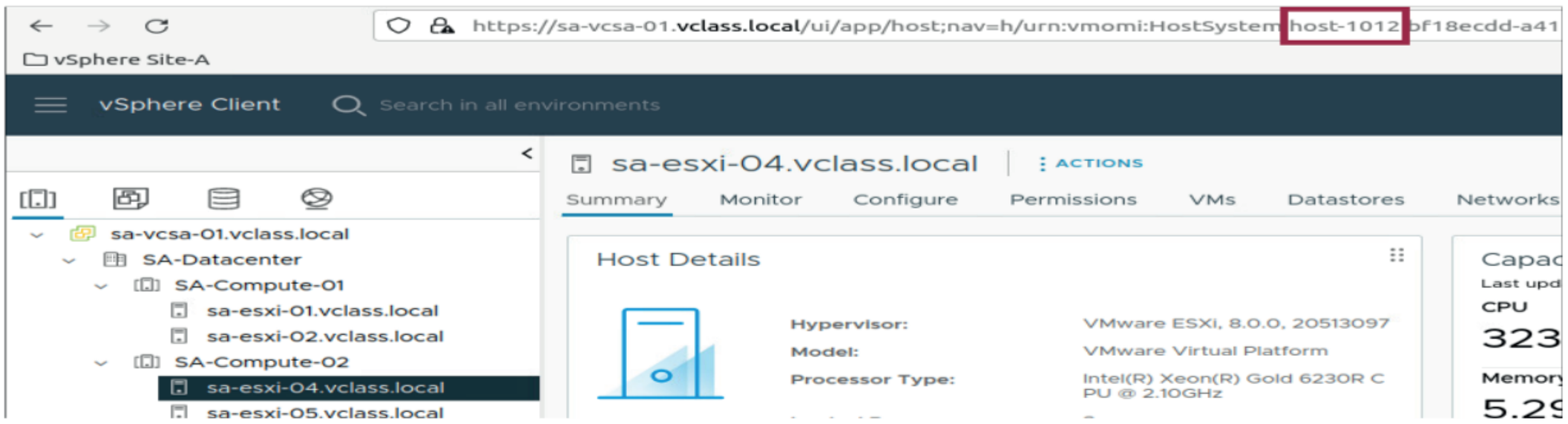
Re-create the `/productLocker` Symlink on the vCenter Managed Object Browser (MOB)

1. In the vSphere Client, verify the Host ID from the URL.

   a. Click on **sa-esxi-04.vclass.local.**

   b. Record the Host ID that appears in the URL.

      _____



2. Open the **UpdateProductLockerLocation_Task** vSphere API directly using the Host ID:

   a. In Firefox, open a new tab and enter **https://<vcenter_fqdn>/mob/?moid=<host ID>&method=updateProductLockerLocation** in the URL replacing the vCenter FQDN and Host ID

      For example:

      https://**sa-vcsa-01.vclass.local**/mob/?moid=**host-1012**&method=updateProductLockerLocation.

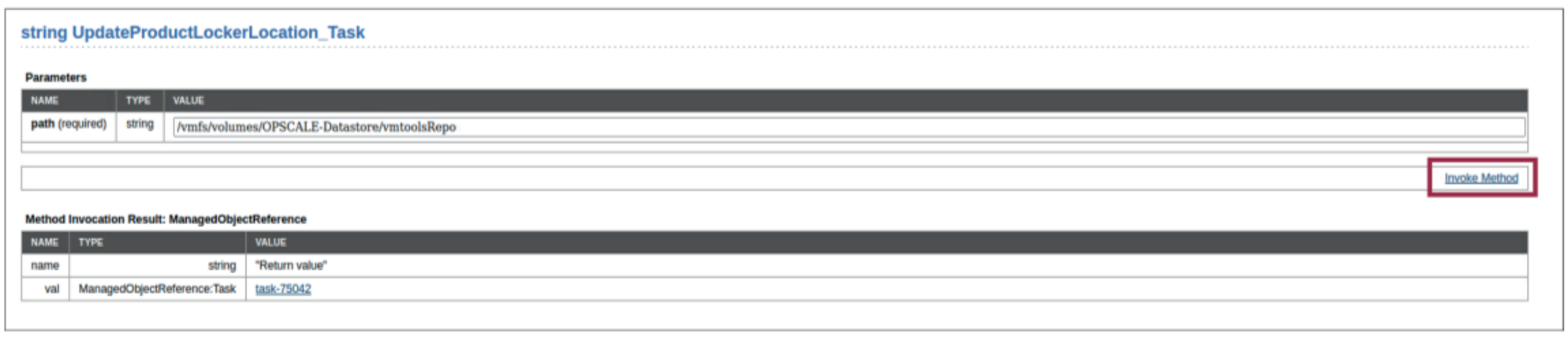
3. Log in to sa-vcsa-01.vclass.local MOB by entering **`administrator@vsphere.local`** for the user name and **`VMware1!`** for the password.

4. Update the /productLocker symlink by invoking updateProductLockerLocation vSphere API with the datastore containing the vmtools directory:

   a. In the MOB, update the **VALUE** tab with the datastore: **/vmfs/volumes/OPSCALE-Datastore/vmtoolsRepo**

   b. Click on **Invoke Method** to apply the setting.

      You will see a task created below.

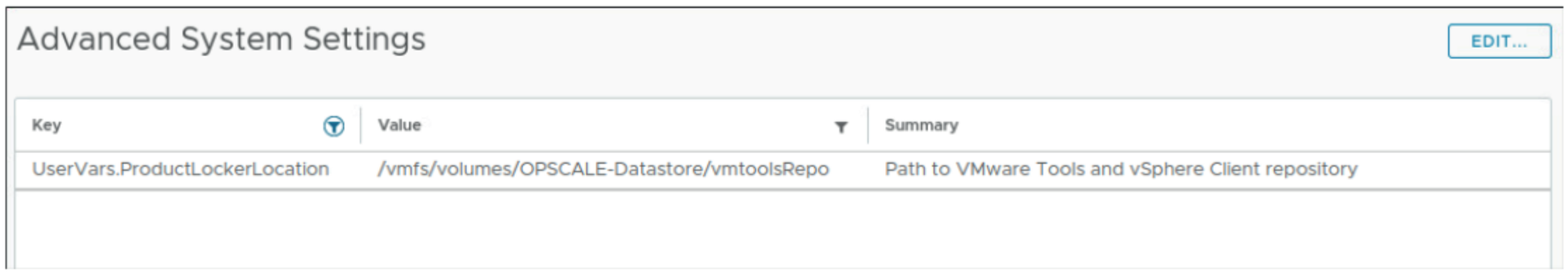


5. View the updated `productlocker` variable in the ESXi Advanced Settings from the vSphere Client.

   a. Return to the vSphere Client browser tab.

   b. Select the **sa-esxi-04.vclass.local** and select **Configure** tab.

   c. In the **Advanced System Settings** view, filter for **ProductLockerLocation** and verify the value has been updated.



6. Close the **Managed Object Browser** tab in the browser.

7. Return to the **vSphere Client** and disable the **SSH** service on your ESXi host.

   a. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.

   b. In the navigation pane, select **sa-esxi-04.vclass.local**.

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

   d. Select **Services** under System.

   e. **Stop** the **SSH** service.

Lab 3 (Simulation) Deploying vSphere Replication and Site Recovery Instances

Objective and Tasks

Deploy vSphere Replication and Site Recovery Instances:

1. Deploy and Register the On-Premises vSphere Replication Instance with vCenter
2. Deploy and Register the On-Premises Site Recovery Instance with vCenter

---

IMPORTANT

Do not perform the steps from this simulation in your actual lab environment.

Do not refresh, navigate away from, or minimize the browser tab hosting the simulation. These actions might pause the simulation, and the simulation might not progress.

Task 1: Lab Simulation

You deploy and register the on-premises vSphere Replication and Site Recovery Components on your vCenter, so you can replicate workloads running on physical and virtual machines.

1. In your local desktop, open a web browser.
2. Go to https://core-vmware.bravais.com/s/TFjUb4lK5KiycL5Mljz2 to open the simulation.
3. After you complete the simulation, close the simulation browser tab.

Lab 4 (Simulation) Configuring Replication for a Single VM

Objective and Tasks

Configure replication for a single VM:

1. Configure replication for the virtual machine
2. Verify the replication status

IMPORTANT

Do not perform the steps from this simulation in your actual lab environment.

Do not refresh, navigate away from, or minimize the browser tab hosting the simulation. These actions might pause the simulation, and the simulation might not progress.

Task 1: Lab Simulation

You configure replication for a virtual machine to vCenter.

1. In your local desktop, open a web browser.
2. Go to https://core-vmware.bravais.com/s/l6WbyI52AYFIPCYpysjh to open the simulation.
3. After you complete the simulation, close the simulation browser tab.

Lab 5 Managing Resource Pools

Objective and Tasks

Create and use resource pools:

1. Re-configure VMs
2. Create CPU Contention
3. Create Resource Pools
4. Verify Resource Pool Functionality
5. Knowledge Check

Task 1: Re-configure VMs

You configure a VM to facilitate CPU contention.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. From the main menu, select **Inventory** and select the **Hosts and Clusters** icon.
3. Confirm **SA-Compute-02** is expanded.

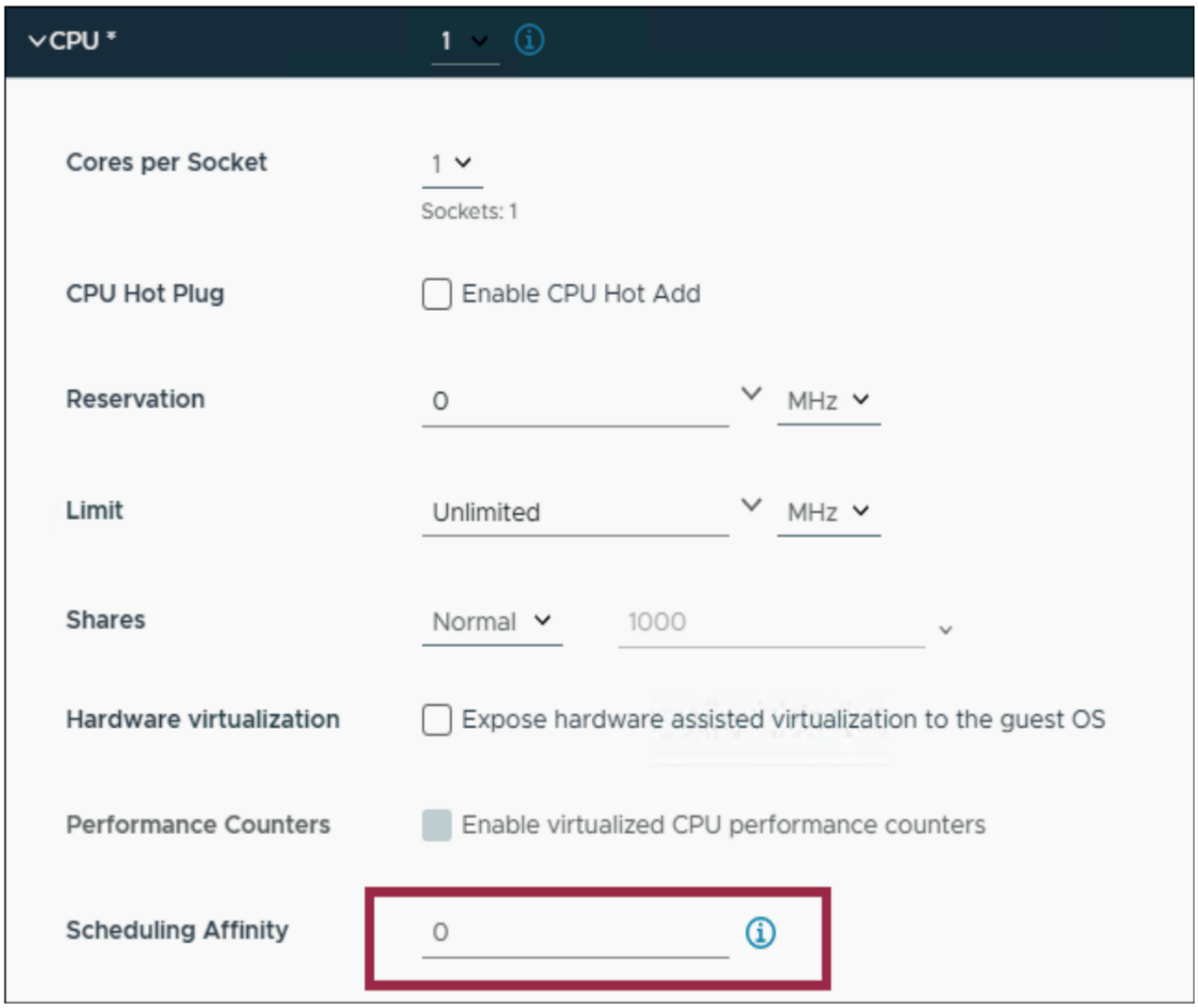
4. Configure the powered off VMs.

   a. In the Navigation pane, right-click the **Linux-CPU-01** virtual machine and select **Edit Settings**.

   b. On the **Virtual Hardware** tab, expand **CPU** to view more details.

   c. In the **Scheduling Affinity** text box, enter 0.

      This affinity setting forces the Linux-CPU-01 to run only on logical CPU 0.



   CAUTION

   Scheduling affinity is used here to create CPU contention for training purposes. VMware strongly discourages the use of this feature in a production environment.

   d. To apply these CPU configuration change, click **OK**.

5. Repeat this step for the Linux-CPU-02, Linux-CPU-03, Linux-CPU-04 and Linux-CPU-05 VMs.

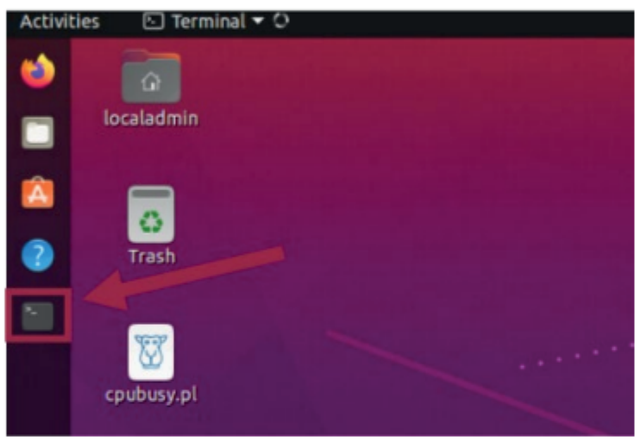
6. After preconfiguration is complete, power on all the Linux-CPU-XX VMs.

Task 2: Create CPU Contention

You use a tool to create CPU contention in your lab environment for testing. You force the VMs to compete for and share a single logical CPU on the ESXi host, which might lead to performance degradation.

1. Verify that the Linux-CPU-01, Linux-CPU-02, Linux-CPU-03, Linux-CPU-04 and Linux-CPU-05 VMs are powered on and running on sa-esxi-05.vclass.local.
2. Start the `CPUBUSY` script on the VM desktops.
   a. Select **Linux-CPU-01** in the navigation pane.
   b. From the Summary tab, select **LAUNCH WEB CONSOLE.**

      If you are asked to choose between VMRC and Web Console, choose the web console.
   c. Open the Linux Terminal and run the **CPUBUSY** script located on the Desktop.



`./Desktop/cpubusy.pl`

This script runs continuously. It stabilizes in 1 to 2 minutes. This script performs floating-point computations repeatedly. The script displays the duration (wall-clock time) of a computation, for example, `I did ten million sines in # seconds`.

d. Repeat steps a through c on the Linux-CPU-02, Linux-CPU-03, Linux-CPU-04 and Linux-CPU-05 VMs.

   You use the number of seconds reported as a performance estimate. The script `CPUBUSY` should run at approximately the same rate in each VM.

3. Leave the `CPUBUSY` script to run for 2 or more minutes so that the processes can reach their steady state.

Task 3: Create Resource Pools

You create resource pools to delegate control of a host's or a cluster's resources, and to compartmentalize resources in a cluster. To create resource pools in the cluster, you must firstly enable DRS.

1. Return to the vSphere Client.
2. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.
3. Enable DRS on SA-Compute-02
   a. Select the cluster **SA-Compute-02**.
   b. Click the **Configure** tab.
   c. Select **vSphere DRS** under the Services menu.
   d. In the right pane, click **EDIT**.
   e. Turn on the **vSphere DRS** toggle.
   f. Leave all other settings at defaults and click **OK.**
4. Right-click **SA-Compute-02** in the navigation pane and select **New Resource Pool**.
5. Assign properties to the resource pool.

Option	Action
Name	Enter: **`RP-Test`**.
CPU Shares	Select **Low** from the **Shares** drop-down menu.
All other settings	Leave the default settings.

6. Click **OK**.
7. In the Navigation pane, right-click **SA-Compute-02** and select **New Resource Pool**.
8. Assign properties to the resource pool.

Option	Action
Name	Enter: **`RP-Production`**.
CPU Shares	Select **High** from the **Shares** drop-down menu.
All other settings	Leave the default settings.

9. Click **OK**.
10. Expand the resource pools in the navigation pane.

Task 4: Verify Resource Pool Functionality

You assign VMs to resource pools with different resource settings to monitor and compare the performance.

1. Select the **RP-Test** resource pool in the navigation pane and click the **Summary** tab. From here, you can scroll down and inspect the number of shares in the RP-Test resource pool.

   Q1. What is the number of shares for this RP-Test (Low) resource pool?

2. Select the **RP-Production** resource pool in the navigation pane and click the **Summary** tab. From here, you can scroll down and inspect the number of shares in the RP-Production resource pool.

   Q2. What is the number of shares for this RP-Production (High) resource pool?

3. Drag the **Linux-CPU-01** VM to the **RP-Production** resource pool.

4. Drag the **Linux-CPU-02** to the **RP-Test** resource pool.

5. Switch between VM consoles to monitor the results of the `CPUBUSY` script.

   Wait a couple of minutes for the performance of the VMs to change.

   The contention should be evidenced on the Linux-CPU-02 console by increased duration for the same executions. For example, calculations might have taken 8 seconds before the VM was placed in the resource pool, and now it might take 12 seconds because of lower shares in the resource pool.

   Q3. What is the difference in performance between the two virtual machines?

6. Drag the **Linux-CPU-03**, **Linux-CPU-04** and **Linux-CPU-05** VMs to the **RP-Production** resource pool.

7. Switch between VM consoles to monitor the results of the `CPUBUSY` script.

   Wait a couple of minutes for the performance of the VMs to change.

   In the Resource Pools, the shares are distributed in a ratio of 4:1. Among the VMs, 4 of them have High shares, while 1 VM has Low shares. As a result, all 4 High-share VMs should receive comparable amounts of CPU cycles.

8. Enable Scalable Shares on SA-Compute-02.

   a. Select the cluster **SA-Compute-02**.

   b. Click the **Configure** tab.

   c. Select **vSphere DRS** under the Services menu.

   d. In the right pane, click **EDIT**.

   e. Select the **Additional Options** tab.

   f. Select the **Enable scalable shares for the resource pools on this cluster** check box.

   g. Click **OK.**

9. Switch between VM consoles to monitor the results of the `CPUBUSY` script.

   Wait a couple of minutes for the performance of the VMs to change.

   The VMs within RP-Production will retain a significantly higher CPU priority due to the allocation of high CPU shares in the resource pool.

10. In the vSphere Client, change the CPU shares of the RP-Test resource pool to **Normal**.

    a. Right-click the resource pool **RP-Test** in the Navigation pane and click **Edit Resource Settings**.

    b. Under **CPU**, select **Normal** for the Shares setting and click **OK**.

    c. In each VM console, leave the script to run for a few minutes and compare the performance of the `CPUBUSY` script on each VM.

       As the limited CPU resources are reapportioned between the 5 VMs, a difference in performance is noticeable on the Linux-CPU-02 VM. For example, now, the performance of the VM assigned as Linux-CPU- 02 is approximately twice as fast as each of the VMs labeled as 01, 03, 04, and 05. The reason for this is that VM 01 has exclusive access to 4000 shares, while the remaining 4 VMs are sharing a total of 8000 shares, resulting in an allocation of 2000 shares per VM.

11. Repeat the previous step to change CPU shares for the RP-Production resource pool to **Normal**.

    It takes a few seconds for the VMkernel scheduler to implement the new share values. After some time, you should observe that VM Linux-CPU-02 is running approximately four times faster than each of the other four VMs. This is because the shares allocated to VMs in the two Resource Pools are the same, but there are four VMs in one RP and only one VM in the other

12. Press **Ctrl+C** in each Web Console window for all Linux-CPU-XX VMs to stop the `CPUBUSY` script.

13. Close the Linux-CPU-01, Linux-CPU-02, Linux-CPU-03, Linux-CPU-04 and Linux-CPU-05 web consoles.

Task 5: Knowledge Check

You are tasked to create a resource pool and add virtual machines.

1. Create a new resource pool called: **`RP-Student`** in SA-Compute-02
2. Configure **Normal** CPU Shares for RP-Student.
3. Add **Linux-CPU-02** to RP-Student.
4. Shut down Linux-CPU-01, Linux-CPU-02, Linux-CPU-03, Linux-CPU-04 and Linux-CPU-05.
5. Disable DRS on the cluster **SA-Compute-02**.

   Doing this removes all the resource pools from the cluster.

Lab 6 Enabling vCLS Retreat Mode

Objective and Tasks

Enable vCLS retreat mode on a vSphere luster:

1. Verify the Cluster Domain ID
2. Enable vCLS Retreat Mode and Monitor vCLS VMs
3. Revert the Changes

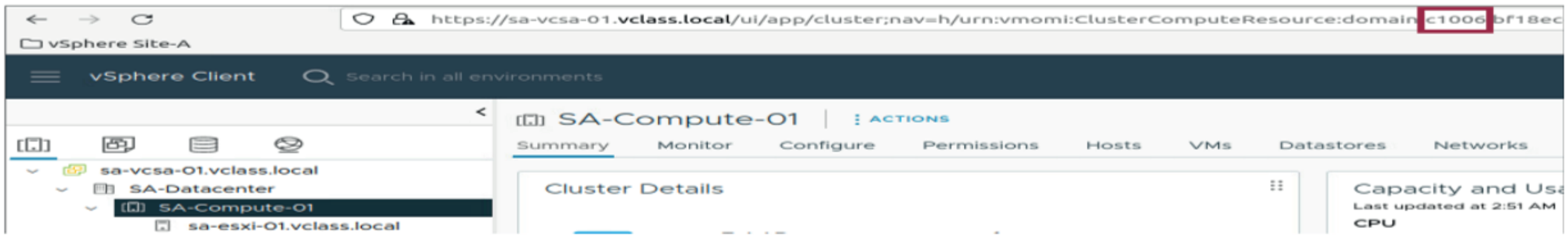
Task 1: Verify the Cluster Domain ID

You login to vCenter and to verify the cluster domain ID.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. From the main menu, select **Host and Clusters**.
3. Select **SA-Compute-01.**
4. Select the **VM** tab and verify the vCLS VMs are listed.
5. Record the cluster domain ID from the URL of the browser. It is the numbers following: domain-c until the colon.

   _____



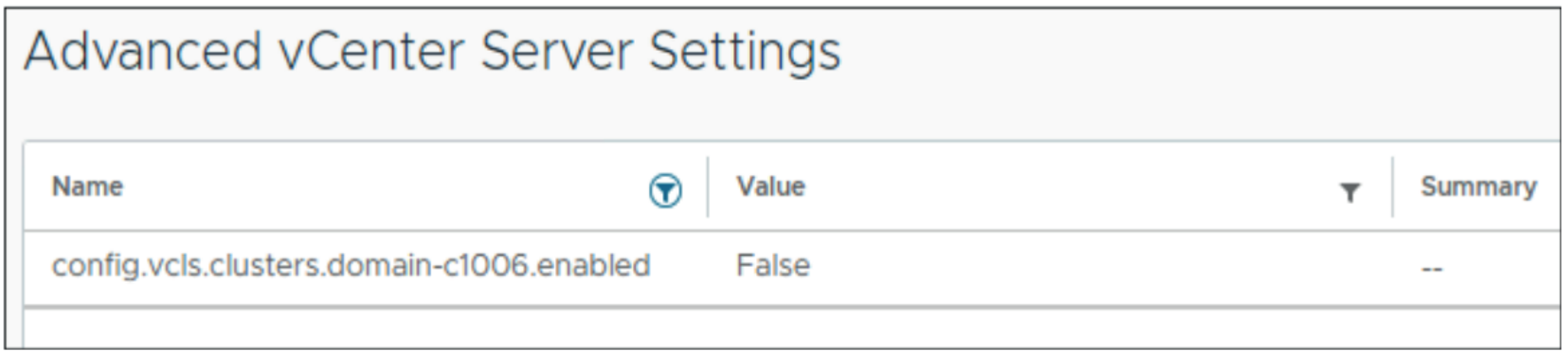
Task 2: Enable vCLS Retreat Mode and Monitor vCLS VMs

You enable retreat mode on SA-Compute-01 and monitor the vCLS VMs. Retreat mode lets you disable the vSphere Cluster Services to automatically remove the vCLS VMs.

1. Select **sa-vcsa-01.vclass.local**.
2. In the right pane, click the **Configure** tab and click **Advanced Settings**.
3. Click **EDIT SETTINGS.**
4. Add a new entry **`config.vcls.clusters.domain-c`**`<number>`**`.enabled`** in the name text box.

   Use the domain ID for `<number>` from Task 1.
5. Set the Value to **`False`**.
6. Select **ADD** and click **Save**.

   If you filter for **`vcls`**, you should see the advanced setting added to your vCenter.



7. Select **SA-Compute-01**.
8. Select the **VM** tab and monitor the vCLS VMs.

   Monitor to completion using Recent Tasks. The vCLS VMs will be powered off and deleted.

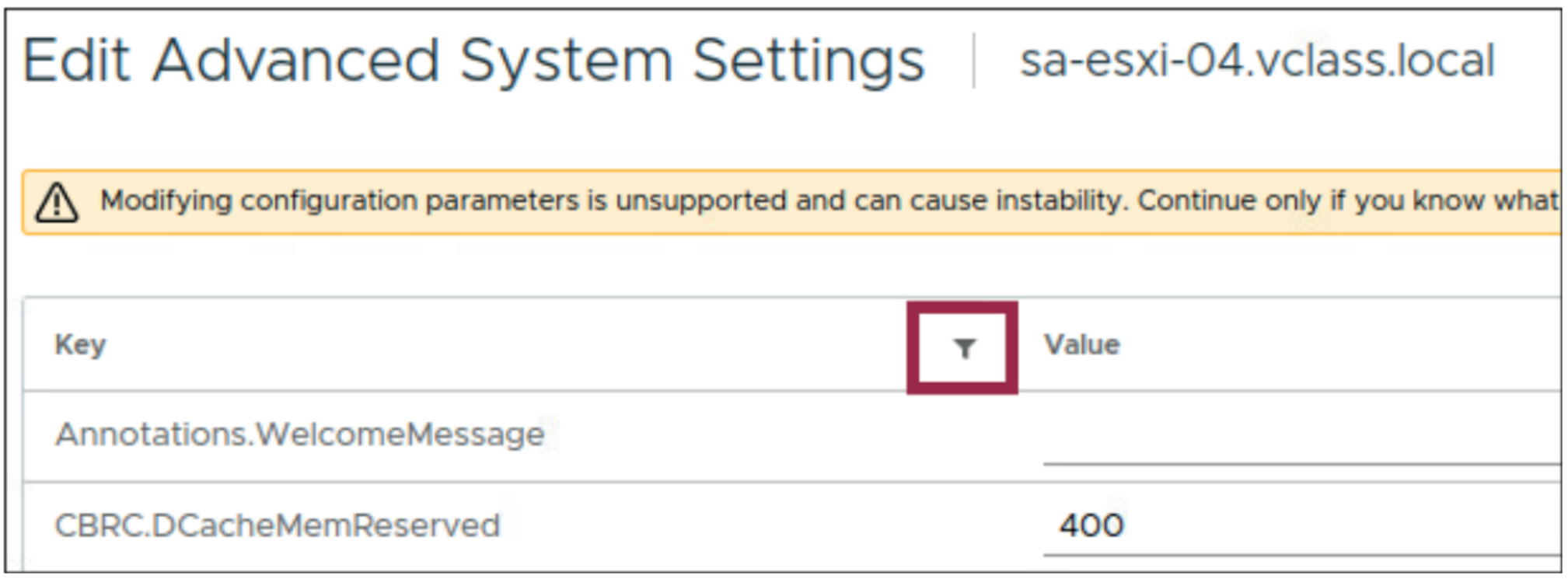
NOTE

After the retreat mode is enabled, DRS is not functional, even if it is activated, until vCLS is reconfigured by removing it from Retreat Mode. Also, vSphere HA does not perform optimal placement during a host failure scenario. HA depends on DRS for placement recommendations. HA will still power on the VMs but these VMs might be powered on in a less optimal host.

Task 3: Revert the Changes

You revert the changes made to the cluster.

1. Select **sa-vcsa-01.vclass.local**.
2. In the right pane, click the **Configure** tab and click **Advanced Settings**.
3. Click **EDIT SETTINGS.**
4. Filter for **vcls** to find the entry `config.vcls.clusters.domain-c<number>.enabled` from Task 2.



5. Set the Value to **`True`**.
6. Click **Save**.
7. Monitor the cluster to see the new vCLS VMs being deployed and powered-on.
   a. Select **SA-Compute-01**.
   b. Select the **VM** tab and monitor the vCLS VMs.
      Q1. What is the number of vCLS VMs deployed?

Lab 7 Configuring vSphere Distributed Switch

Objective and Tasks

Create and configure a distributed switch:

1. Create a Distributed Switch
2. Add ESXi Hosts to the Distributed Switch
3. Examine Your Distributed Switch Configuration
4. Migrate VMs to Another Distributed Switch Port Group

Task 1: Create a Distributed Switch

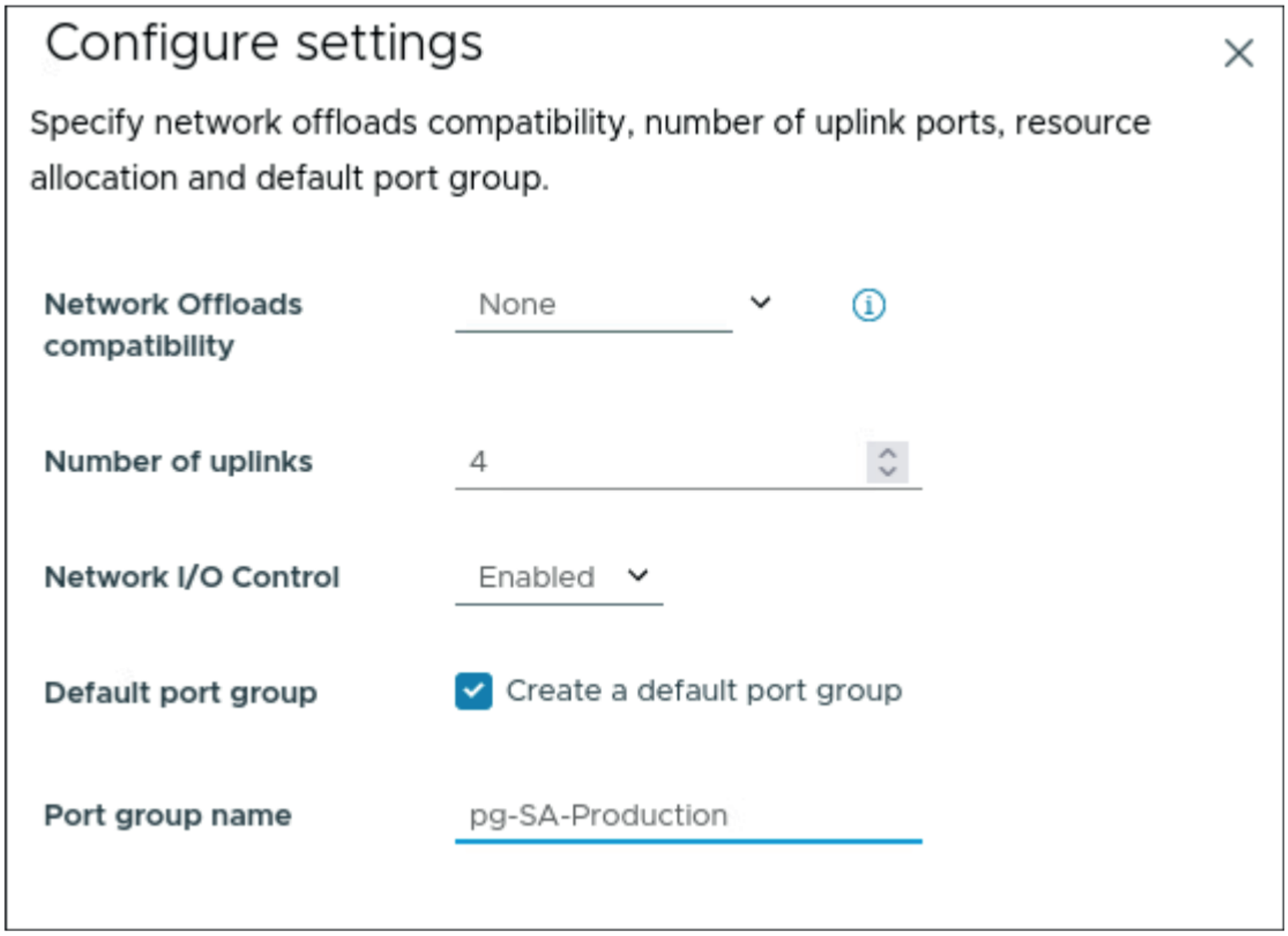
You create a distributed switch that functions as a single virtual switch across all associated hosts in your vSphere environment.

1. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar, and select **vSphere Client (SA-VCSA-01)**.

   If you are not logged in from a previous activity, log in using the vCenter Server lab credentials:
   User name **`administrator@vsphere.local`**
   Password **`VMware1!`**
2. From the main menu, select **Inventory** and click the **Networking** icon
3. In the navigation pane, expand **sa-vcsa-01.vclass.local**.
4. Right-click **SA-Datacenter** and select **Distributed Switch** > **New Distributed Switch**.

   The New Distributed Switch wizard appears.
5. Create a distributed switch.
   a. On the **Name and location** page, enter **`vds-Lab`** in the text box and click **NEXT**.
   b. On the **Select version** page, leave **8.0.0 - ESXi 8.0 and later** selected and click **NEXT**.

c. On the **Configure settings** page, enter **`pg-SA-Production`** in the Port group text box, keep all other default values, and click **NEXT**.



d. On the **Ready to complete** page, review the configuration settings and click **FINISH**.

6. In the navigation pane, expand **SA-Datacenter** and verify that the vds-Lab distributed switch appears.

7. Configure the pg-SA-Production port group to use only Uplink 1.

   a. In the navigation pane, expand **vds-Lab** distributed switch.

   b. Right-click **pg-SA-Production** port group and select **Edit Settings**.

   c. In the Edit Settings window, select **Teaming and failover**.

   d. Under Failover Order, move **Uplink 2**, **Uplink 3** and **Uplink 4** down until they appear under Unused uplinks.

      You can select multiple uplinks at once and move all at the same time.

   e. To apply these changes, click **OK**.

Task 2: Add ESXi Hosts to the Distributed Switch

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

1. In the navigation pane, right-click **vds-Lab** and select **Add and Manage Hosts.**
2. On the Select task page, leave **Add hosts** selected and click **NEXT**.
3. Select the check box for the hosts listed here and click **OK**.

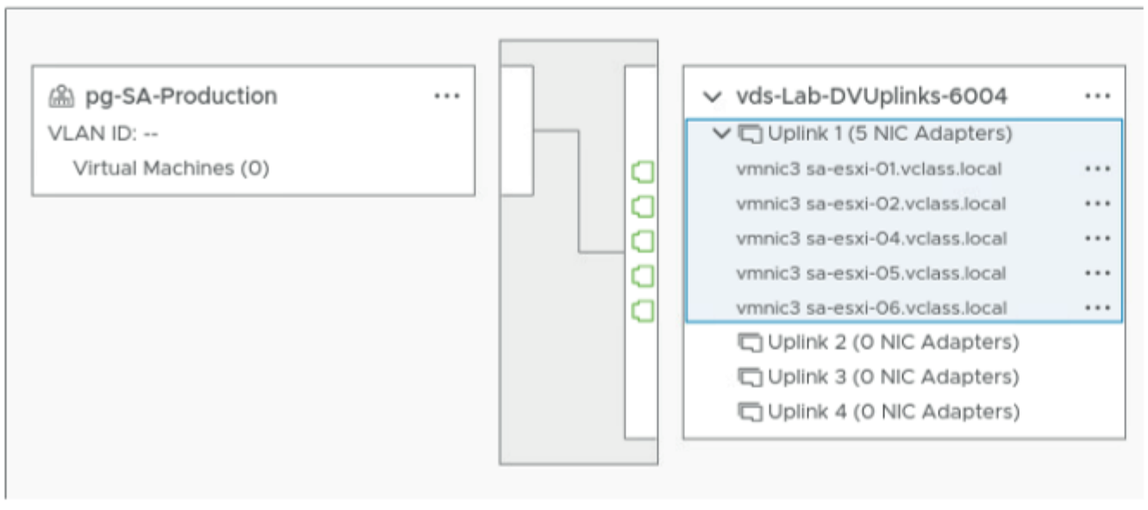
   sa-esxi-01.vclass.local
   sa-esxi-02.vclass.local
   sa-esxi-04.vclass.local
   sa-esxi-05.vclass.local
   sa-esxi-06.vclass.local

4. Click **NEXT**.
5. On the **Manage physical adapters** page, assign **vmnic3** to **Uplink 1**.
   a. In the vmnic3 row, click on the dropdown in the Assign uplink column and select **Uplink 1.**
   b. When ready, click **NEXT**.
6. On the **Manage VMkernel adapters** page, click **NEXT**.
7. On the **Migrate VM networking** page, click **NEXT**.
8. On the **Ready to complete** page, review settings and click **FINISH**.

Task 3: Examine Your Distributed Switch Configuration

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

1. In the navigation pane, select **vds-Lab**.
2. In the right pane, click the **Configure** tab and select **Topology** under Settings.
3. In the distributed switch topology diagram, expand **Uplink 1**.
4. Verify that the vmnic3 is attached and appears under Uplink 1 for ESXi hosts sa-esxi-01, sa-esxi-02, sa-esxi-04, sa-esxi-05, and sa-esxi-06.



5. Click the **pg-SA-Production** port group to highlight the active uplinks for this portgroup.
6. On the vds-Lab page, under settings, select **Properties** and verify the settings.
   - Number of uplinks is **4**.
   - Network I/O Control is **Enabled**.
   - The MTU size is **1500 Bytes**.
   - The Discover Protocol Type is set to **Cisco Discovery Protocol** and operation is set to **Listen**.
7. Under Settings, select each menu option to review the current configuration.
   - LACP: No entries are in the main window.
   - Private VLAN: No entries are in the main window.
   - NetFlow: No Collector IP address is set in the main window.
   - Port Mirroring: No entries are in the main window.
   - Health Check: All items are set to **Disabled** in the main window.
8. In the navigation pane, select the **pg-SA-Production** port group.
9. In the right pane, click the **Configure** tab and select **Properties** on the left.
10. Verify the distributed port group settings.
    - Port binding, is set to Static binding.
    - Port allocation, is set to Elastic.
    - Number of ports, is set to 8.

Task 4: Migrate VMs to Another Distributed Switch Port Group

You move VMs from their current port groups on the vds-SA-Datacenter distributed switch to the pg-SA-Production port group on the vds-Lab distributed switch.

1. Right-click on the **SA-Datacenter** and select **Migrate VMs to Another Network**.

   The **Migrate VMs to Another Network** wizard appears.
2. Migrate the VMs.
   a. On the **Select source network** page, select **pg-SA-Management** and click **NEXT**.
   b. On the **Select destination** networks page, select **pg-SA-Production** and click **NEXT**.
   c. On the **Select VMs to migrate** page, select VMs **Linux01** & **Linux02** and click **NEXT**.
   d. On the **Ready to complete** page, review settings and click **FINISH**.
   e. Monitor the task to completion using Recent Tasks.

3. Verify your distributed switch configuration.

   a. In the navigation pane, select **vds-Lab** and click **Hosts** in the right pane.

   b. Verify that sa-esxi-01, sa-esxi-02, sa-esxi-04, sa-esxi-05, and sa-esxi-06 are connected to the distributed switch.

      The state of the ESXi hosts should be Connected.

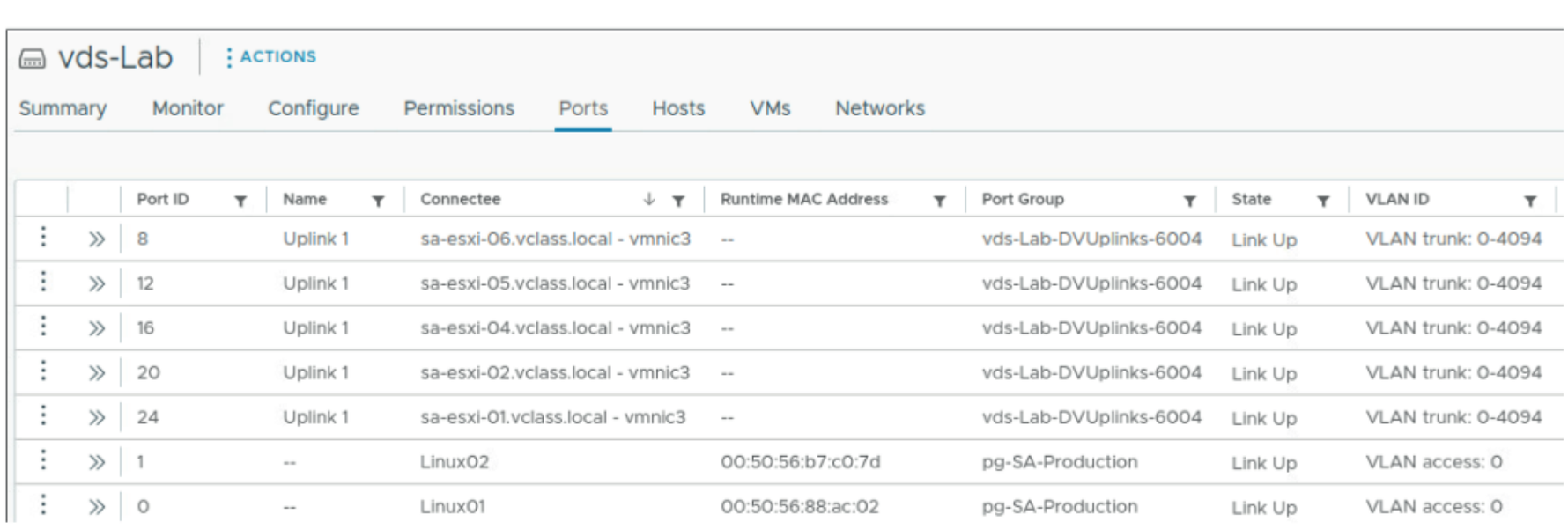
   c. Click **VMs** and verify that the Linux01 and Linux02 VMs are listed.

      If the VMs are listed, they reside on the new distributed switch.

   d. Click **Ports** and verify that pg-SA-Production is listed in the Port Group column.

   e. Verify that an uplink port group is listed which you previously mapped between vmnic3 and Uplink1.

      You can click the **Connectee** column to filter.



Port ID	Name	Connectee	Runtime MAC Address	Port Group	State	VLAN ID
8	Uplink 1	sa-esxi-06.vclass.local - vmnic3	--	vds-Lab-DVUplinks-6004	Link Up	VLAN trunk: 0-4094
12	Uplink 1	sa-esxi-05.vclass.local - vmnic3	--	vds-Lab-DVUplinks-6004	Link Up	VLAN trunk: 0-4094
16	Uplink 1	sa-esxi-04.vclass.local - vmnic3	--	vds-Lab-DVUplinks-6004	Link Up	VLAN trunk: 0-4094
20	Uplink 1	sa-esxi-02.vclass.local - vmnic3	--	vds-Lab-DVUplinks-6004	Link Up	VLAN trunk: 0-4094
24	Uplink 1	sa-esxi-01.vclass.local - vmnic3	--	vds-Lab-DVUplinks-6004	Link Up	VLAN trunk: 0-4094
1	--	Linux02	00:50:56:b7:c0:7d	pg-SA-Production	Link Up	VLAN access: 0
0	--	Linux01	00:50:56:88:ac:02	pg-SA-Production	Link Up	VLAN access: 0

4. Click the **Hosts and Clusters** icon from the inventory.

5. Log in to the Linux01 web console.

   a. In the navigation pane, click **Linux01** under SA-Datacenter > SA-Compute-02.

   b. In the right pane, click **LAUNCH WEB CONSOLE**.

   c. Click the **Linux01** web console tab in the browser and click in the window to capture keyboard input.

   d. Log in by entering user name **`root`** and password **`VMware1!`**

6. At the command prompt, ping 172.20.10.2 (the domain controller's IP address) to verify that the VM has full network connectivity.

   ```
   ping -c 3 172.20.10.2
   ```

7. If the `ping` command is successful, continue to Step 9.

8. If the `ping` command is unsuccessful, restart the networking in the VM.
    a. Enter the command to ensure that your VM has a valid DHCP-assigned IP address.

    `service network restart`

    b. Repeat steps 6 and 7.
9. Close the VM **Linux01** web console tab.

Lab 8 Managing vSphere Distributed Switches

Objective and Tasks

Use the vSphere Client to create and maintain a vSphere Distributed Switch (VDS) at the data center level:

1. Add a New Port Group to VDS
2. Enable the VDS Health Check
3. Investigate the VDS Health Check Status
4. Remediate the VDS Issue
5. Deactivate the VDS Health Check Service
6. Back Up the VDS Configuration
7. Knowledge Check

Task 1: Add a New Port Group to VDS

You add a port group to the vds-Lab vSphere distributed switch.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, and click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. From the main menu, select **Inventory** and click the **Networking** icon.
3. Right-click **vds-Lab** and select **Distributed Port Group > New Distributed Port Group**.
4. On the Name and location page, enter **`pg-SA-Testing`** in the text box and click **NEXT**.
5. On the Configure settings page, select **VLAN** under **VLAN type** from the drop-down menu, enter **`10`** for the **VLAN** number, and click **NEXT**.
6. On the Ready to complete page, review the information about your new VDS port group and click **FINISH**.

Task 2: Enable the VDS Health Check

You enable the VDS health check service on the vds-Lab vSphere distributed switch to verify its configuration for errors or mismatches.

1. In the navigation pane, select **vds-Lab**.
2. Select the **Configure** tab and select **Health Check** under Settings.
3. Click **EDIT** in the top-right corner.
4. Under VLAN and MTU, select **Enabled** from the **State** drop-down menu.
5. Under Teaming and failover, select **Enabled** from the **State** drop-down menu.
6. Click **OK**.

NOTE

After the health check is enabled, the VDS health check begins testing for selected configuration options (VLAN and MTU, Teaming and Failover, or both) by creating many fictitious MAC addresses. These MAC addresses continue to be created and sent through the vSphere and physical networks as long as the VDS health check is enabled.

Task 3: Investigate the VDS Health Check Status

You check for results from the VDS health check service.

The health check can take some time.

1. Select **vds-Lab** in the navigation pane.
2. Select the **Monitor** tab and select **Health** in the Monitor page menu.
3. Observe the Host Name list in the right pane.

   This list should comprise all hosts that were added to vSphere Distributed Switch.

   This list continuously updates with health check results while the health check service is enabled.
4. Highlight a host listing, where a warning appears, to view the additional information displayed below it.

   VLAN is the default tab under Health status details. To check MTU or other settings, you must click the individual tabs.

   When you set a VLAN in task 1, we didn't configure the physical environment to match.

Task 4: Remediate the VDS Issue

You fix the incorrect VLAN configured on your new port group that you confirmed through the VDS health check.

1. Confirm **vds-Lab** is expanded.
2. Right-click the **pg-SA-Testing** port group and select **Edit settings.**
3. On the VLAN page, select **None** for the **VLAN type** drop-down.

   Selecting **None** for this value removes any previously applied VLAN tags on the pg-SA-Testing port group.

   NOTE

   VMkernel port configuration is managed independently. However, VDS port group configuration can affect VMkernel port configuration.

   ---
4. To apply the VLAN change, click **OK**.
5. Verify your change.
   a. Select **vds-Lab** in the navigation pane.
   b. Select the **Monitor** tab and select **Health** to verify that VLAN Health Status has changed and now indicates Normal.

Task 5: Deactivate the VDS Health Check Service

You deactivate the VDS health check service on the vds-Lab vSphere distributed switch.

Deactivating the VDS health check service is important because of the many fictitious MAC addresses generated at one-minute intervals to facilitate troubleshooting efforts in the network infrastructure. The environment needs time for those MAC addresses to time out of the infrastructure, according to the network policy after the VDS health check is deactivated.

1. In the navigation pane, select **vds-Lab**.
2. Select the **Configure** tab and select **Health Check** under Settings.
3. Click **EDIT**.
4. Under VLAN and MTU, select **Disabled** from the **State** drop-down menu.
5. Under Teaming and failover, select **Disabled** from the **State** drop-down menu.
6. Click **OK**.

Task 6: Back Up the VDS Configuration

You back up the configuration for the vds-Lab vSphere distributed switch.

1. In the navigation pane, right-click **vds-Lab** and select **Settings** > **Export Configuration**.
2. In the Export Configuration dialog box, leave **Distributed switch and all port groups** selected and click **OK**.
3. Save the distributed switch configuration to the desktop with the filename `vds-Lab-backup.zip`.

Task 7: Knowledge Check

You are tasked to create and configure a vSphere Distributed Switch.

1. Create a new distributed switch called: **`vds-Student`**
2. Create a new port group called: **`pg-SA-Test`**
3. Add **sa-esxi-04.vclass.local** to vds-Student and assign **vmnic4** to **Uplink 1**.

Lab 9 Using Port Mirroring

Objective and Tasks

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

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 VM to capture and monitor mirrored traffic.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.
      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.
3. In the navigation pane, expand SA-Datacenter and select **SA-Compute-02**.
4. In the navigation pane, select the **Linux01** VM.

   The Linux01 VM will be used as the Port Mirroring destination.
5. In the right pane, click **Summary** and click **LAUNCH WEB CONSOLE**.
6. If not already logged in, click in the window to capture keyboard input.
   a. Log in by entering user **`root`** with password **`VMware1!`**

7. In the Linux01 web console, enter the `tcpdump` command at the command prompt.

   `tcpdump -nn icmp`

   This command line is used to monitor ICMP network traffic.

```
[root@localhost ~]# tcpdump -nn icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
_
```

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

   The `tcpdump` output does not have any information to display until ICMP traffic detects ping packets arriving on the VM's vNIC.

9. Leave the console window open with the `tcpdump` command running uninterrupted.

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

11. In the navigation pane, select the **Linux02** VM.

12. In the right pane, click **Summary** and click **LAUNCH WEB CONSOLE**.

13. Click the Linux02 **Web Console** tab in the browser and click in the window to capture keyboard input.

    a. Log in by entering user **`root`** with password **`VMware1!`**

       The Linux02 VM is used as the traffic source to be mirrored.

14. At the Linux02 command prompt, enter the `ping` command.

    `ping 172.20.10.2`

    This command pings the default router IP address.

15. If the `ping` command does not work, enter the following command to restart network services and then repeat step 14.

    `service network restart`

16. After the `ping` command begins to work, click the **Linux01** console tab.

17. In the Linux01 console window, verify that the running `tcpdump` command output remains silent and did not capture any ICMP traffic.

Task 2: Configure Port Mirroring on the Distributed Switch

You configure port mirroring so that the port connected to the Linux02 VM is the mirror source and the port connected to the Linux01 VM is the mirror destination.

All the traffic present on the Linux02 port is forwarded to the Linux01 port for examination.

IMPORTANT

Ensure that the **Linux01** and **Linux02** VMs both reside on **sa-esxi-06.vclass.local**. During a previous lab, DRS may have placed either VM on another ESXi. If so, proceed to Migrate the VM back to sa-esxi-06.vclass.local.

---

1. Open the **vSphere Client** tab.
2. From the main menu, select **Inventory** and click the **Networking** icon.
3. Select **vds-Lab.**
4. In the right pane, click **Configure** and select **Port Mirroring** on the left.
5. Add a port mirroring session.
   a. On the Port Mirroring panel, click **NEW.**

      The Add Port Mirroring Session wizard appears.

   b. On the Select session type page, leave **Distributed Port Mirroring** selected 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.

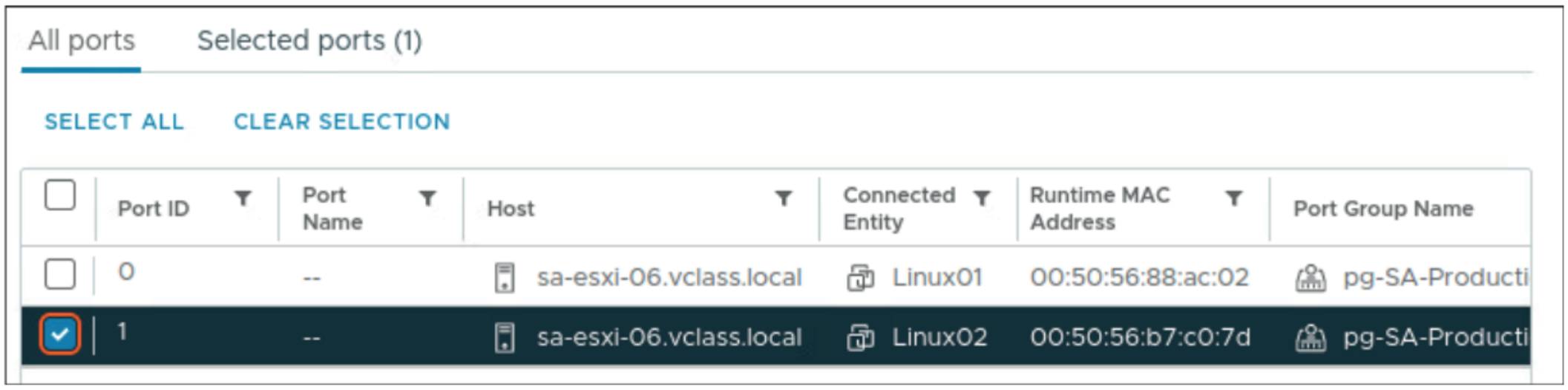
   c. On the Edit properties page, configure the port mirroring session.

      i. From the **Status** drop-down menu, select **Enabled**.

      ii. From the **Normal I/O on destination ports** drop-down menu, select **Allowed** and click **NEXT.**

d. On the Select sources page, configure the port mirroring source.

i. On the All ports tabs, select the check box for **Linux02** below Connected Entity.



ii. Click **NEXT**.

e. On the Select destinations page, configure the port mirroring destination.

i. On the All ports tabs, select the check box for **Linux01** below Connected Entity.

ii. Click **NEXT**.

f. On the Ready to complete page, review the configuration and click **FINISH.**

g. Monitor to completion using Recent Tasks.

Task 3: Verify That Port Mirroring Is Capturing Traffic

With port mirroring 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. Go to the **Linux01** console tab.
4. In the Linux01 console, examine the `tcpdump` output in the terminal window.

   The output looks similar to the following screenshot.

```
12:13:54.713364 IP 172.20.10.117 > 172.20.10.2: ICMP echo request, id 39705, seq
 67, length 64
12:13:54.713661 IP 172.20.10.2 > 172.20.10.117: ICMP echo reply, id 39705, seq 6
7, length 64
12:13:55.713772 IP 172.20.10.117 > 172.20.10.2: ICMP echo request, id 39705, seq
 68, length 64
```

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

   _____

   The local address begins with 172.20.10.

6. In the Linux01 console window, press Ctrl+C to stop the `tcpdump` command.

   a. If pressing Ctrl+C does not work, click anywhere inside the command prompt and repeat.

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, use `ifconfig` to examine the IP configuration.

   `ifconfig`

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. From the main menu of the vSphere Client, select **Inventory** and click the **Hosts and Clusters** icon.

    b. In the navigation pane, click **SA-Compute-02** and select the **VM** tab.

    c. Click the check box for **Linux01** and **Linux02**.

    d. Right-click the highlighted VMs and select **Power** > **Shut Down Guest OS**.

    e. In the pop-up window, click **Yes** to confirm the shutdown operation.

Task 4: Restore the Distributed Switch Configuration

You restore the vSphere distributed switch (vds-Lab) configuration to reset changes made since the configuration was saved.

1. From the main menu, select **Inventory** and click the **Networking** icon.

2. In the navigation pane, right-click **vds-Lab** and select **Settings** > **Restore Configuration**.

   The Restore Configuration wizard appears.

3. On the Restore switch configuration page, click **BROWSE**, select the file `/Desktop/vds-Lab-backup.zip`, and click **Open**.

4. Leave **Restore distributed switch and all port groups** selected and click **NEXT**.

5. On the Ready to complete page, review the settings and click **FINISH**.

   If you lose connection to the vSphere Client, restart Firefox.

6. After the switch configuration is restored, verify the configuration. View the port mirroring configuration and verify that the vds-Lab has no sessions configured.

   a. In the navigation pane, click vds-Lab and select the Configure tab.

   b. In the middle pane, select Port Mirroring under Settings.

      The port mirroring configuration was removed by the VDS restore operation.

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

Lab 10 Viewing a vSAN Datastore Configuration

Objective and Tasks

View a vSAN datastore configuration and a virtual machine's components on the vSAN datastore:

1. View a vSAN Datastore Configuration
2. View the vSAN Default Storage Policy
3. View a Virtual Machine on the vSAN Datastore

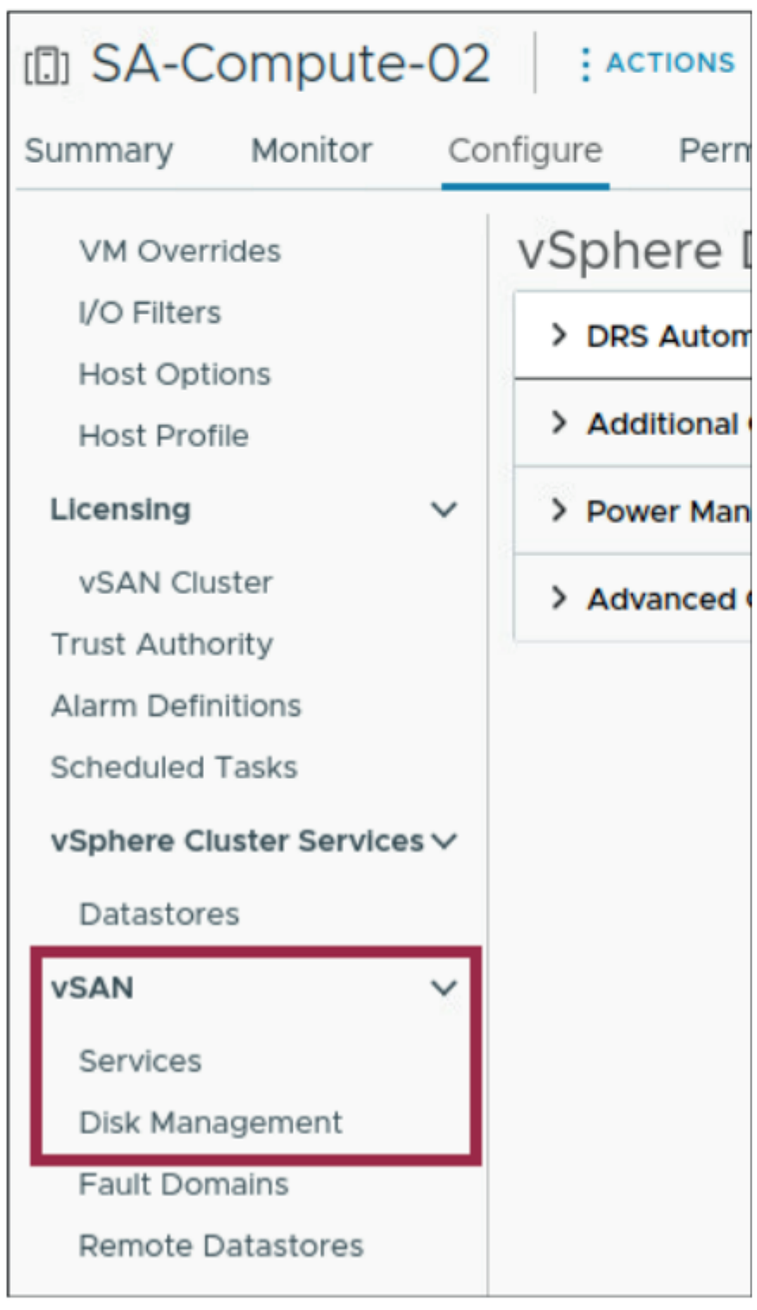
Task 1: View a vSAN Datastore Configuration

You view an existing vSAN datastore configuration in the SA-Compute-02 cluster to familiarize yourself with where to find vSAN information in the vSphere Client.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **administrator@vsphere.local**
      Password: **VMware1!**

2. Verify that vSAN is activated on the SA-Compute-02 cluster.
   a. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.
   b. In the navigation pane, expand **SA-Datacenter** and select **SA-Compute-02**.
   c. In the right pane, click the **Configure** tab.
   d. Under Configuration, select **Quickstart**.
   e. Verify that vSAN appears as one of the selected services.
3. View the ESXi hosts that belong to the vSAN cluster.
   a. In the right pane, click the **Summary** tab.
   b. Scroll down to the Cluster Resources tile to view the number of hosts in the vSAN cluster.
   c. Click the **Hosts** tab to view the names of the ESXi hosts in the cluster.
4. View the disk group configuration on the hosts in the vSAN cluster.
   a. In the right pane, click the **Configure** tab.
   b. Under vSAN, select **Disk Management**.



c. For the first ESXi host in the list, select **VIEW DISKS** and expand the **Disk group** to view its details.

Information about the disk group appears in the lower pane.

Q1. How many storage devices are in this disk group?

Q2. What are the drive types?

Q3. What tier does each drive belong to?

d. View the disk groups for the other ESXi hosts.

Select the drop-down next to SA-ESXI-04.VCLASS.LOCAL on the middle pane to navigate between hosts.

The number of storage devices, drive types, and tier assignments are the same as the first host.

5. View the VMkernel adapter configuration that is used to access the vSAN network.

   a. In the navigation pane, select **sa-esxi-04.vclass.local**.

   b. Click the **Configure** tab.

   c. Under Networking, select **VMkernel adapters**.

   d. In the VMkernel adapters list, expand **vmk1** to view its details.

   e. Click the **Properties** tab for vmk1.

   f. Verify that vSAN appears as an Enabled service.

6. View storage capacity information for the vSAN cluster.

   a. In the navigation pane, select **SA-Compute-02**.

   b. In the right pane, click the **Summary** tab.

   c. Scroll down and review the information about vSAN.

   This vSAN Capacity tile shows current storage capacity used.

   d. For vSAN Usage, click **VIEW CAPACITY** on the vSAN Capacity tile.

   The **Monitor** tab appears, and the vSAN > Capacity > Capacity Overview pane shows used space and free space in the vSAN cluster.

Task 2: View the vSAN Default Storage Policy

You view information about the vSAN Default Storage Policy, and you estimate the usable storage capacity of this policy.

1. From the main menu, select **Policies and Profiles.**
2. In the navigation pane, verify **VM Storage Policies** is selected.
3. In the right pane, scroll down the list of policies and select **vSAN Default Storage Policy**.
4. In the **Rules** tab, view the rule set for this storage policy.

   This storage policy uses RAID 1 (mirroring).
5. Estimate the usable storage capacity of the vSAN default storage policy.
   a. From the main menu, select **Inventory** and click the **Storage** icon.
   b. In the navigation pane, expand **sa-vcsa-01.vclass.local** and expand **SA-Datacenter**.
   c. In the navigation pane under SA-Datacenter, select **vsanDatastore**.
   d. In the right pane, click the **Monitor** tab.
   e. Under vSAN, select **Capacity**.

      Confirm the **CAPACITY USAGE** tab is selected and review the Capacity Overview and What if analysis panes. From here, you can estimate the effective free space available on the vSAN datastore if you deploy a VM with the specified storage policy. The policy selected is **vSAN Default Storage Policy**.

      Q1. Why is the policy's effective free space the value that it is?

Task 3: View a Virtual Machine on the vSAN Datastore

You confirm a virtual machine is located on the vSAN datastore, and you familiarize yourself with the vSAN components that make up the VM.

1. Verify that **vsanDatastore** is selected in the navigation pane.
2. In the right pane, click the **VMs** tab.

   A virtual machine named Photon-03 appears in the list.
3. Click **Photon-03**.

   Verify that the VMs and Templates view appears and Photon-03 is selected in the navigation pane.
4. View the vSAN components that make up the Photon-03 virtual machine.
   a. In the right pane, click the **Monitor** tab.
   b. Under vSAN, select **Physical disk placement**.
   c. Review the virtual machine's objects and the components for each object.

Lab 11 Using Policy-Based Storage

Objective and Tasks

Use policy-based storage to create tiered storage for VMFS datastore without a VASA provider:

1. Add Datastores for Use by Policy-Based Storage
2. Use vSphere Storage vMotion to Migrate a VMs Storage
3. Configure Storage Tags
4. Create VM Storage Policies
5. Assign Storage Policies to VMs

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

You create two small datastores, as simple tiered storage, for use by your vCenter instance.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. From the main menu, select **Inventory** and click the **Storage** icon.

3. Create a datastore named ds-gold.
   a. In the navigation pane, right-click **SA-Datacenter** and select **Storage** > **New Datastore**.

      The New Datastore wizard appears.
   b. On the Type page, leave **VMFS** selected and click **NEXT**.
   c. On the Name and device selection page, enter **`ds-gold`** in the Name text box.
   d. From the **Select a host** drop-down menu, select ESXi host **sa-esxi-04.vclass.local**.
   e. From the LUN list, select LUN 7 with the entry description **FreeNAS ISCSI Disk (naa..)** and capacity **8.00 GB**, and click **NEXT**.

      Local drives are labeled as Local VMware Disk. Do not select these drives.
   f. On the VMFS version page, leave **VMFS 6** selected and click **NEXT.**
   g. On the Partition configuration page, keep the default values and click **NEXT.**
   h. On the Ready to complete page, review settings and click **FINISH**.
   i. In the Recent Tasks pane, verify that the task was completed.
   j. Verify that the datastore ds-gold appears in the navigation pane.
4. Create a datastore named ds-silver.
   a. In the navigation pane, right-click **SA-Datacenter** and select **Storage** > **New Datastore**.

      The New Datastore wizard appears.
   b. On the Type page, leave **VMFS** selected and click **NEXT**.
   c. On the Name and device selection page, enter **`ds-silver`** in the Name text box.
   d. From the **Select a host** drop-down menu, select ESXi host **sa-esxi-04.vclass.local**.
   e. From the LUN list, select LUN 8 with the entry description **FreeNAS ISCSI Disk (naa..)** and capacity **12.00 GB**, and click **NEXT**.

      Local drives are labeled as Local VMware Disk. Do not select these drives.
   f. On the VMFS version page, leave **VMFS 6** selected and click **NEXT**.
   g. On the Partition configuration page, keep the default values and click **NEXT**.
   h. On the Ready to complete page, review settings and click **FINISH**.
   i. In the Recent Tasks pane, verify that the task was completed.
   j. Verify that the datastore ds-silver appears in the navigation pane.

Task 2: Use vSphere Storage vMotion to Migrate a VMs Storage

You use vSphere Storage vMotion to migrate the Photon-01 VM to the ds-gold datastore.

1. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon
2. In the navigation 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 datastore **ds-gold**, leave all other settings with 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 need to refresh the vSphere Client to see that the migration is complete.

   a. In the navigation pane, select **Photon-01**.

   b. In the right pane, click the **Datastores** tab and verify that the ds-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. From the main menu, select **Tags & Custom Attributes**.
2. Click the **Tags** tab.
3. Configure a new tag category and the Gold Tier identifier tag.

   a. Click **NEW**.

   b. In the **Name** text box, enter **`Gold Tier`**.

   c. Click the **Create New Category**.

   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. For the Associable Object Types, deselect the **All objects** check box.

   f. Select the **Datastore** check box and click **CREATE**..

   g. In the Create Tag dialog box, click **CREATE**.

4. Create a Silver Tier identifier tag.
    a. Click **NEW**.
    b. In the **Name** text box, enter **`Silver Tier`**.
    c. In the **Category** drop-down menu, select **Storage Tiers** and click **CREATE**.
5. Assign the Gold Tier tag to the ds-gold datastore.
    a. From the main menu, select **Inventory** and click the **Storage** icon.
    b. In the navigation pane, right-click **ds-gold** and select **Tags & Custom Attributes** > **Assign Tag**.
    c. Select the **Gold Tier** check box and click **ASSIGN**.
    d. In the navigation pane, select **ds-gold**.
    e. In the Tags tile on the **Summary** tab, verify that the Gold Tier tag is associated with the ds-gold datastore.
6. Assign the Silver Tier tag to the ds-silver datastore.
    a. In the navigation pane, right-click the **ds-silver** datastore and select **Tags & Custom Attributes** > **Assign Tag**.
    b. Select the **Silver Tier** check box and click **ASSIGN**.
    c. In the navigation pane, select the datastore **ds-silver**.
    d. Under Tags on the **Summary** tab, verify that the Silver Tier tag is associated with the ds-silver datastore.

Task 4: Create VM Storage Policies

You assign storage policies to VMs, and you specify the configuration settings to be enforced.

1. From the main menu, select **Policies and Profiles.**
2. Verify that **VM Storage Policies** is selected in the navigation pane.
3. Create a Gold Tier storage policy.
    a. In the VM Storage Policies page, click **CREATE**.

       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, and under "Datastore specific rules" , select **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 **Gold Tier**, click **OK**, and click **NEXT**.

f. On the Storage compatibility page, verify that the datastore ds-gold is listed under Compatible storage and click **NEXT**.

g. On the Review and finish page, click **FINISH**.

4. Repeat 3 steps to create Silver Tier Policy by using the **Silver Tier** tag.

5. Verify that Gold Tier Policy and Silver Tier Policy are entries in the Name column.

   If the entries cannot be found, repeat steps to add the entries.

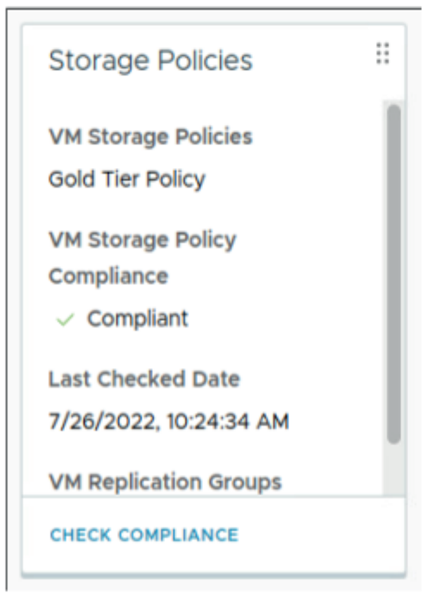
Task 5: Assign Storage Policies to VMs

You assign the Gold and Silver storage policies to individual VMs and you mitigate compliance issues.

A storage policy can be assigned to a VM while the VM is powered on or powered off.

1. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon
2. In the navigation pane, expand **SA-Datacenter** and the cluster **SA-Compute-02**.
3. Apply the Gold Tier storage policy to the Photon-01 VM.
   a. Right-click **Photon-01** and select **VM Policies** > **Edit VM Storage Policies**.
   b. On the Edit VM Storage Policies page, select **Gold Tier Policy** from the **VM storage policy** drop-down menu and click **OK**.
4. Verify that Gold Tier Policy was successfully applied to Photon-01.
   a. In the navigation pane, select **Photon-01**.
   b. In the right pane, click the **Summary** tab.
   c. Scroll down to the **Storage Policies** tile, if necessary.
   d. Verify that Gold Tier Policy appears and that Photon-01 is compliant.

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



5. Apply the Silver Tier storage policy to the Photon-02 VM.

   a. In the navigation pane, right-click **Photon-02** and select **VM Policies** > **Edit VM Storage Policies**.

   b. On the Edit VM Storage Policies page, select **Silver Tier Policy** from the **VM storage policy** drop-down menu and click **OK**.

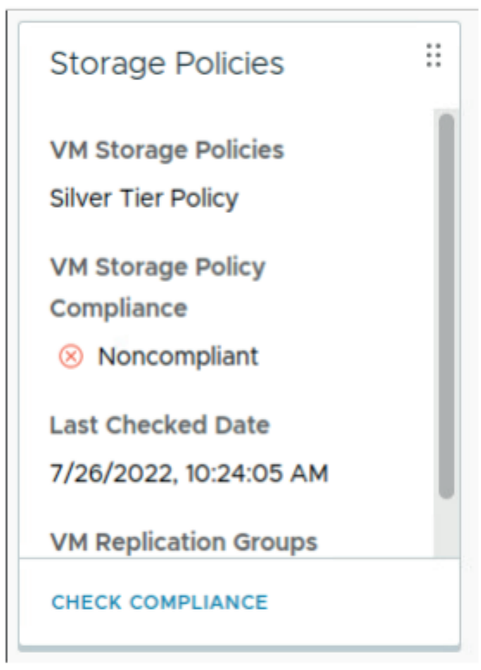
6. Verify that Silver Tier Policy was applied to Photon-02 but is displayed as Noncompliant.

   a. In the navigation pane, select **Photon-02**.

   b. In the right pane, click the **Summary** tab.

   c. View the VM Storage Policies tile, verify that Silver Tier Policy appears and that Photon-02 is not compliant.

      The Photon-02 VM is Noncompliant because its data is stored on a datastore that is not tagged as a part of the assigned policy.



7. Remediate the compliance issue for Photon-02.

   a. In the navigation 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 datastore **ds-silver**.

      With a VM storage policy assigned to the Photon-02 VM, 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.

8. Verify that Photon-02 is reported as compliant.
    a. In the right pane, verify that the status in the VM Storage Policies tile is Compliant.
    b. If the status is Noncompliant, click **Check Compliance** in the VM Storage Policies tile.
    c. Verify that the status changes to Compliant.

Lab 12 Creating vSAN Storage Policies

Objective and Tasks

Create and review vSAN storage policies:

1. Examine the Default Storage Policy
2. Create a Custom Policy with No Failure Tolerance
3. Assign the Custom Policy to a VM
4. Make the VM Compliant

Task 1: Examine the Default Storage Policy

You examine the vSAN Default Storage Policy.

A vSAN datastore has been preconfigured for you.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser and click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **administrator@vsphere.local**
      Password: **VMware1!**
2. From the main menu, select **Policies and Profiles.**
3. Verify that **VM Storage Policies** is selected in the navigation pane.
4. In the right pane, select **vSAN Default Storage Policy** and click **EDIT**.
5. On the Name and description page, click **NEXT**.

6. On the vSAN page, examine the rules under the **Availability**, **Storage Rules, Advanced Policy Rules**, and **Tags** tabs.

   Q1. How many failures can be tolerated?

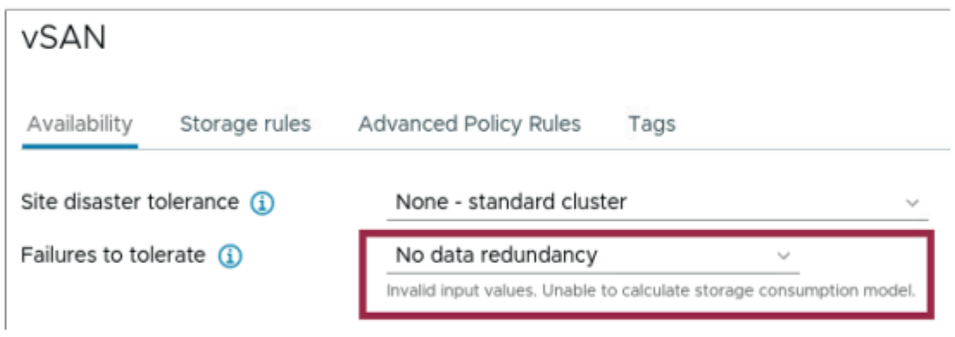
7. Click **CANCEL**.

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**.
2. On the Name and description page, enter **`vSAN-VM-Custom-Policy-FTT0`** in the **Name** text box and click **NEXT**.
3. On the Policy structure page, and under Datastore specific rules, select **Enable rules for "vSAN" storage** check box and click **NEXT**.
4. On the vSAN page **Availability** tab under Failures to tolerate, select **No data redundancy** from the drop-down menu.

   View the consumed storage space information below the drop-down menu.



   Q1. Why is the storage space size equal to the VM size?

5. To complete the vSAN page, click **NEXT**.
6. On the Storage compatibility page, click **NEXT**.

   Only the vsanDatastore is listed under Compatible storage.

7. On the Review and finish page, click **FINISH**.
8. Verify that the vSAN-VM-Custom-Policy-FTT0 storage policy is created and appears in the list.

   You might need to scroll through the VM Storage Policies list.

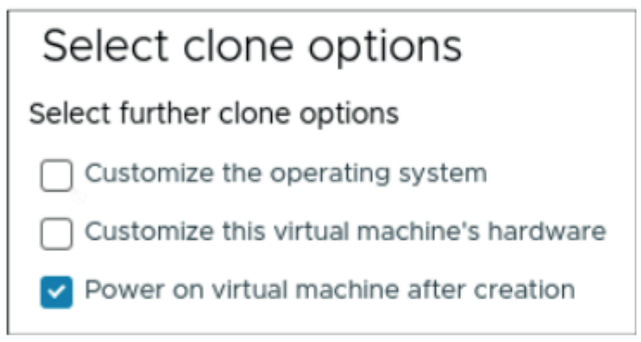
Task 3: Assign the Custom Policy to a VM

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

1. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.
2. Clone a VM from Photon-01.
   a. In the navigation 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, select **Lab VMs** for the location and click **NEXT**.
   c. On the Select a compute resource page, expand **SA-Datacenter** and **SA-Compute-02**, select **sa-esxi-05.vclass.local**, and click **NEXT**.

      You may see a compatibility warning for the ESXi host. This warning can be safely ignored.

   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 only **Power on virtual machine after creation** 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 VM is listed in the navigation pane and is powered on.

   If you do not see the VM listed and powered on, click the **Refresh** icon.

4. Assign the vSAN-VM-Custom-Policy-FTT0 storage policy to Payload-02.

   a. In the navigation pane, right-click **Payload-02** and select **VM Policies** > **Edit VM Storage Policies**.

   b. Select **vSAN-VM-Custom-Policy-FTT0** 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 navigation pane, select **Payload-02**.

6. On the **Summary** tab, review the Related Objects tile and the VM Storage Policies tile.

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

   Q2. On which datastore is the VM located?

   Q3. Which storage policy is the VM using?

   Q4. Is the VM compliant with its storage policy?

Task 4: Make the VM Compliant

You migrate the Payload-02 VM from the shared VMFS datastore to the vSAN datastore to make it compliant with its storage policy.

1. Migrate the Payload-02 VM to the vSAN datastore to ensure its compliance.

   a. In the navigation pane, right-click **Payload-02** and select **Migrate**.

   b. On the Select a migration type page, click **Change storage only** and click **NEXT**.

   c. On the Select Storage page, 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 tile and click **Check Compliance**.

   The compliance status might have been refreshed automatically by the vSphere Client. If so, clicking **Check Compliance** is not required.

3. Verify that the compliance status of Payload-02 changes to Compliant.

4. In the navigation pane, right-click **Payload-02** and select **Power > Power Off.**

Lab 13 Backing Up vCenter Appliance

Objective and Tasks

Access the vCenter Server Appliance Management Interface and create a backup of vCenter Appliance.

1. Backup vCenter Appliance

Task 1: Backup vCenter Appliance

You access vCenter VAMI and backup the Appliance.

1. Log in to the vCenter VAMI on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vCenter Appliance Management (SA-VCSA-01)**.
   c. On the VAMI login page, enter the vCenter root credentials.

      User name: **`root`**
      Password: **`VMware1!`**

      You should see **sa-vcsa-01.vclass.local** in the Summary page.

2. Backup the vCenter Appliance.

   a. In the navigation menu, select **Backup**.

   b. Select **BACKUP NOW**.

   c. Assign properties to the backup configuration.

Option	Action
Backup Location	Enter: **`nfs://172.20.10.15/mnt/NFS-POOL`**
User name	Enter: **`root`**
Password	Enter: **`VMware1!`**
Data	Uncheck **Stats, Events and Tasks**

   d. Select **START** and monitor the task to completion.

   e. Verify the backup file is created and stored in the Activity window.

3. Close the vCenter VAMI browser tab.

Lab 14 Using vSphere Configuration Profiles

Objective and Tasks

Transition a cluster from using baselines to using images and use vSphere configuration profiles to manage all the hosts in the cluster:

1. Configure a Cluster with a Single Image
2. Configure a Cluster with vSphere Configuration Profiles
3. Remediate the Hosts in a Cluster
4. View the Configuration Document

Task 1: Configure a Cluster with a Single Image

You configure a cluster to use a single image to manage the updates of all ESXi hosts in the cluster.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser and click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

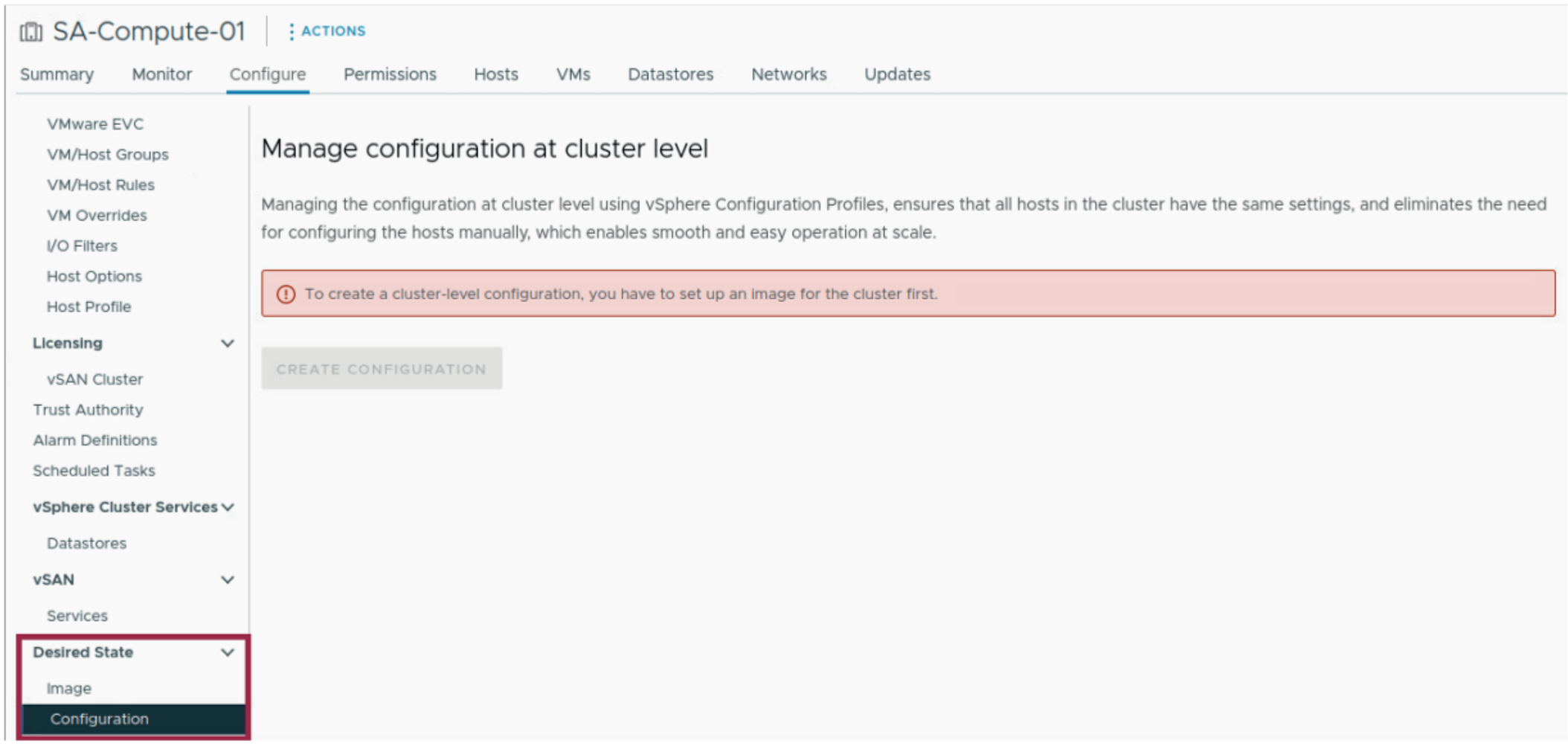
      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**

2. View the current configuration status of the cluster.

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

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

   c. Select **Configuration** under Desired State.



The cluster is currently managed with baselines.

3. Configure the cluster to use a single image.

   a. In the right pane, click the **Updates** tab.

   b. Read any warning and information messages and click **MANAGE WITH A SINGLE IMAGE**.

   c. Click **SETUP IMAGE**.

   d. From the **ESXi Version** drop-down menu, select **8.0 U1 - 21495797**.

   e. Click **VALIDATE**.

      The image is valid.

   f. Click **SAVE** and wait for the Check Image Compliance task to complete.

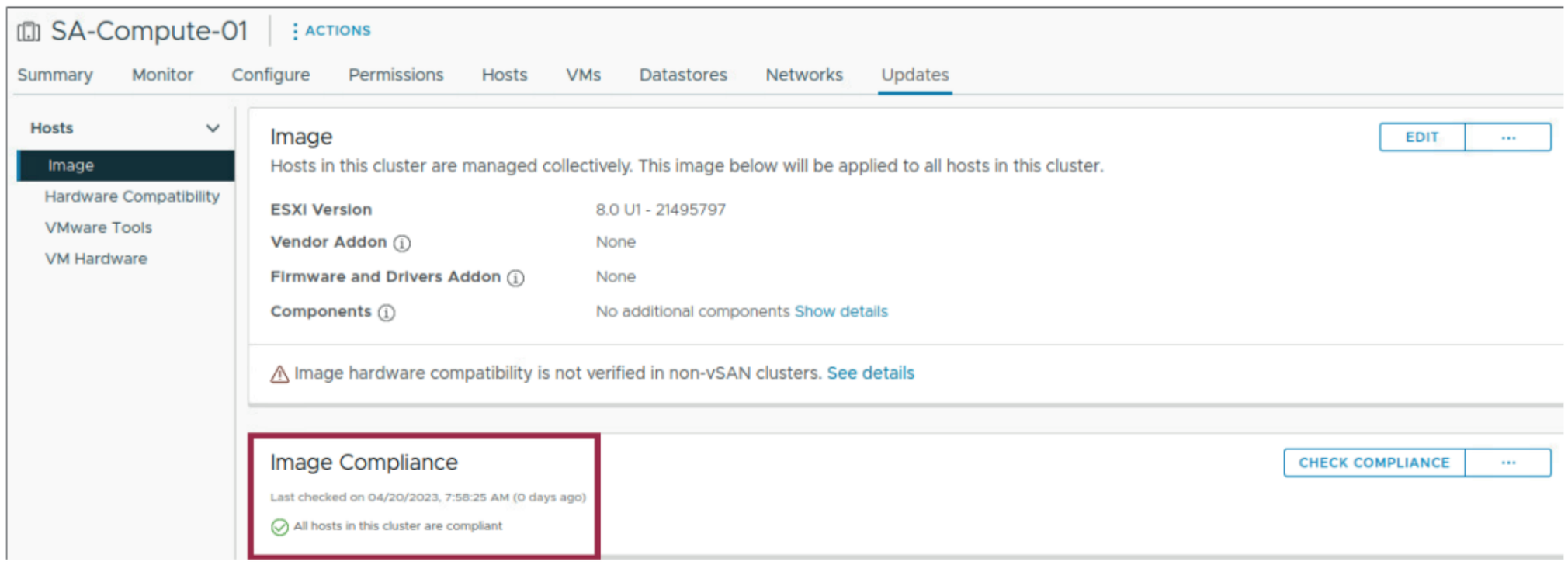
   g. Click **FINISH IMAGE SETUP**.

   h. Read the message and click **YES, FINISH IMAGE SETUP**.

   i. Monitor the Recent Tasks pane.

      Several tasks are started. Saving the changes to the image automatically starts the Check compliance of cluster with image task.

4. Verify that the hosts in the cluster are compliant.



Task 2: Configure a Cluster with vSphere Configuration Profiles

You configure a cluster to use a single configuration profile to manage the configuration of all ESXi hosts in the cluster.

1. In the right pane of the vSphere Client, click the **Configure** tab for SA-Compute-01.
2. Select **Configuration** under Desired State.
3. Convert the cluster to use vSphere Configuration Profiles.
   a. Click **CREATE CONFIGURATION**.
   b. In the Create configuration step, click **IMPORT FROM REFERENCE HOST**.
   c. Select **sa-esxi-01.vclass.local** and click **IMPORT**.
   d. Click **CLOSE** to close the wizard and select **NEXT**.
   e. In the Validate configuration step, wait until the validation completes and click **NEXT**.
   f. In the Pre-check and apply step, wait until the pre-check completes and click **FINISH AND APPLY**.
   g. Click **CONTINUE**.
4. Click **GO TO CONFIGURATION**.

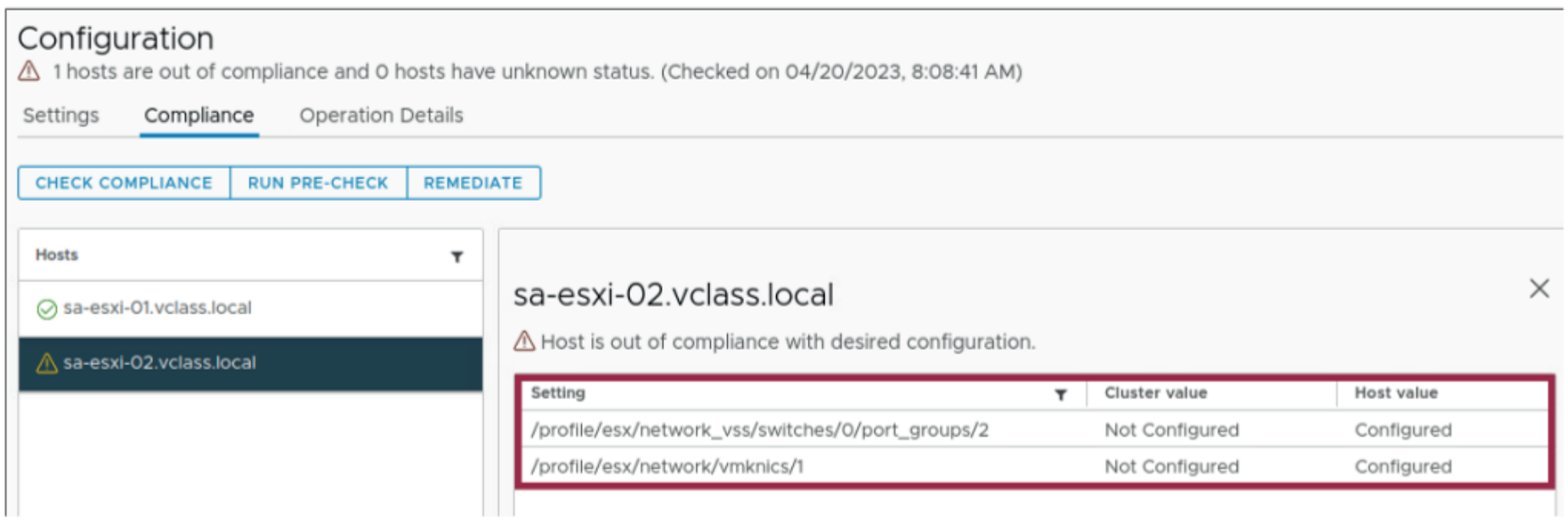
Task 3: Remediate the Hosts in a Cluster

You reconfigure a host and remediate it to be compliant with the cluster configuration profile.

1. Add a VMkernel to your ESXi host.
   a. In the left navigation pane, select **sa-esxi-02.vclass.local**.
   b. In the right pane, click the **Configure** tab.
   c. Select **VMkernel adapters** under Networking.
   d. Click **ADD NETWORKING**.
   e. Leave **VMkernel Network Adapter** selected and click **NEXT**.
   f. Select Select an existing standard switch.
   g. Select **vSwitch0** and click **NEXT**.
   h. Leave the default port properties selected and click **NEXT**.
   i. Leave **Obtain IPv4 settings automatically** selected and click **NEXT** and **FINISH**.

   vmk1 appears under VMkernel adapters.
2. Check compliance of the cluster with the configuration profile.
   a. Select the **SA-Compute-01** cluster.
   b. In the right pane, click the **Configure** tab.
   c. Select **Configuration** under Desired State.
   d. Select the **Compliance** tab and click **CHECK COMPLIANCE**.

   The host sa-esxi-02.vclass.local is out of compliance.



3. Remediate the cluster against the configuration profile.

   a. Click **REMEDIATE**.

      A pre-check automatically runs before you can continue.

   b. Expand each host to view the details of the pre-check.

   c. Click **NEXT** and review the impact details.

   d. Click **REMEDIATE**.

4. Monitor the Recent Tasks pane.

   The host might be rebooted as part of the remediation. When the host comes back online, a second compliance check automatically runs.

5. In the navigation pane, select **sa-esxi-02.vclass.local**.

   The host remediation removed the additional VMkernel adapter.

Task 4: View the Configuration Settings of the Cluster

You view the settings of the cluster configuration in the vSphere Client and in the configuration document.

1. In the vSphere Client, select the **SA-Compute-01** cluster in the navigation pane.
2. From the **Configure** tab, select **Configuration** under Desired State.
3. Under Configuration, click the **Settings** tab.
4. Explore the available settings.

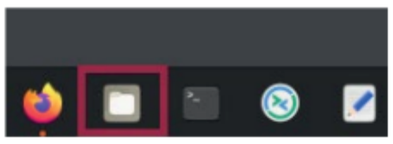
5. Export the configuration document to a JSON file.

   a. From the **Settings** tab, click **EXPORT**.

   b. Click **DOWNLOAD**.

   c. Review the details of the download and click **Save**.

6. On the Linux taskbar, click **Files**.



7. Click **Downloads**.
8. Right-click the **export-settings-config-xxxxxxxxxx.json** file and click **Open with Text Editor**.
9. Inspect the configuration settings in the JSON file.

   You can edit the JSON file manually and import it back into the cluster.
10. Close the text editor and the Files window.

Lab 15 Working with Certificates

Objective and Tasks

Generate and replace a vCenter certificate using the vSphere Client:

1. Examine the Machine SSL Certificate
2. Generate a Certificate Signing Request
3. Replace a Machine SSL Certificate with a Pregenerated CA Certificate

Task 1: Examine the Machine SSL Certificate

You investigate the vCenter machine SSL certificate using the vSphere Client.

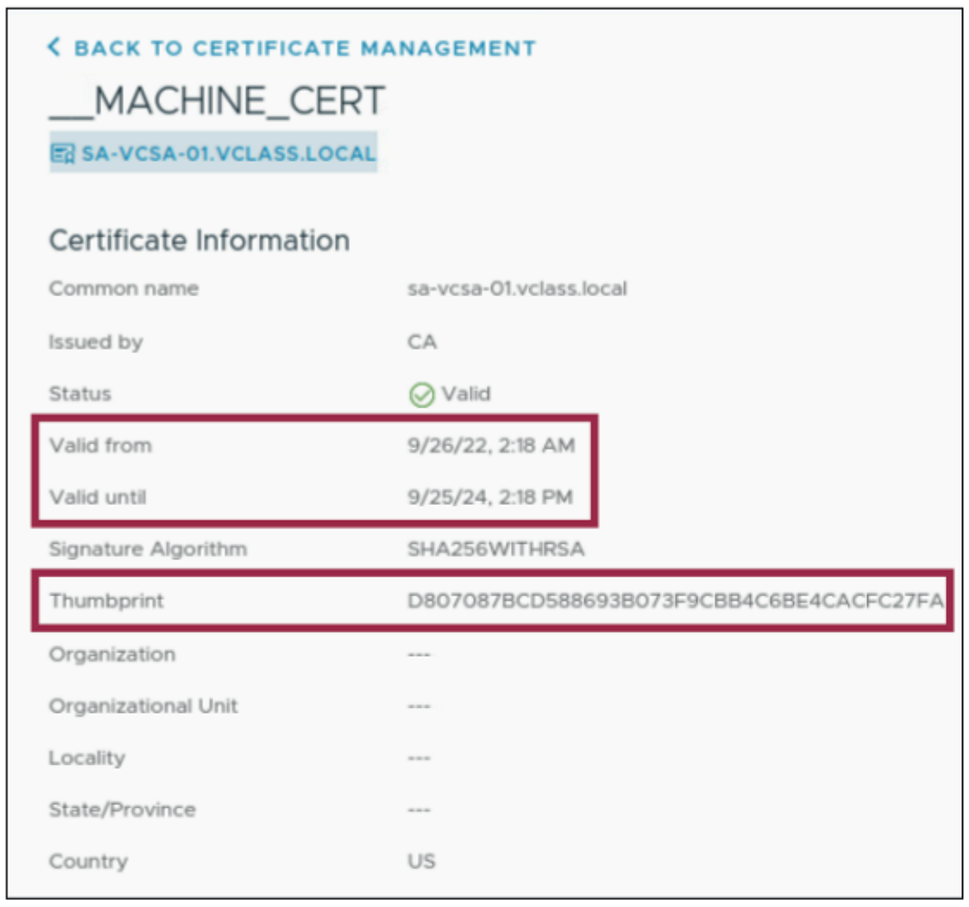
1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser and click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **administrator@vsphere.local**
      Password: **VMware1!**
2. From the main menu, select **Administration** and select **Certificate Management** under Certificates.

3. From the Machine SSL Certificate tile, select **VIEW DETAILS**.

NOTE

The following screenshot is an example. Your certificate information may be different.



4. Record the following certificate information for future comparison.

   Valid from: _____
   Valid until: _____

   Thumbprint: _____

   Each time a certificate is renewed, the current time is set as the **Valid from** time and the **Valid to** time is set as 2 years from that moment.
   The certificate thumbprint, also called a cert hash, is unique and changes with each certificate generated.

5. When you have finished reviewing the Machine SSL certificate details, click **BACK TO CERTIFICATE MANAGEMENT** at the top of the page.

6. Scroll down and click **VIEW DETAILS** for the first certificate under Trusted Root Certificates.

   Q1. Who issued the certificate?

7. When you have finished reviewing the Trusted Root certificate details, click **BACK TO CERTIFICATE MANAGEMENT** to return to Certificate Management.

Task 2: 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. Generate the CSR.

   a. Under Machine SSL Certificate, click **Actions** > **Generate Certificate Signing Request (CSR)**.

   b. Enter the required details to finish the certificate signing request.

Option	Action
Organization	Enter: **`VMware`**
Organization Unit	Enter: **`Education`**
Country	Select: **`United States`**
State/Province	Enter: **`California`**
Locality	Enter: **`Palo Alto`**
Email Address	Enter: **`cert.admin@vmware.com`**

   c. When finished, click **NEXT**.

2. Click **FINISH** to close the wizard.

   Generating the vCenter CSR in this task is for testing purposes only. You will use pre-signed certificates for importing and replacing the Machine SSL certificate on vCenter in the next task.

Task 3: Replace a Machine SSL Certificate with a Pregenerated CACertificate

You import and replace the VMware CA self-signed certificate with an external CA-signed certificate using the vSphere Client.

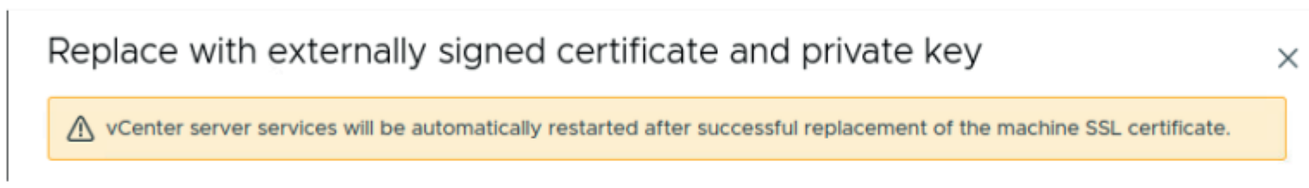
1. From the main menu, select **Administration** and select **Certificate Management** under Certificates.
2. Import and Replace the self-signed certificate.
   a. Under the Machine SSL Certificate tile, select **Actions > Import and Replace Certificate**.

      The Replace Certificate wizard starts.

   b. On the Choose type of certificate to replace, select **Replace with external CA certificate (requires private key)**.

   c. Click **NEXT**.

      A warning is placed in the interface for the user.

   d. Under the Machine SSL Certificate text box, click **BROWSE FILE**.

   e. From the folder `/Desktop/Class Materials and Licenses/linux_CA`, select **ca_vcsa.crt** and click **Open**.

      After selecting this file, the text box will be populated with the CA-signed certificate information.

   f. Under the Chain of trusted root certificates box, select **BROWSE FILE**.

   g. From the folder `/Desktop/Class Materials and Licenses/linux_CA`, select **RootCA.crt** and click **Open**.

      After selecting this file, the text box will be populated with the root and chain certificate information.

   h. Under the Private Key box, select **BROWSE FILE**.

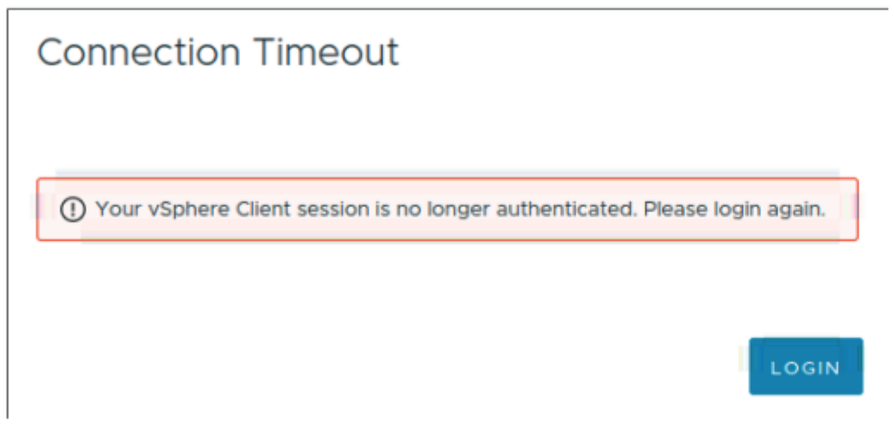
   i. From the folder `/Desktop/Class Materials and Licenses/linux_CA`, select **vmca_issued_key.key** and click **Open**.

      After selecting this file, the text box will be populated with the Private Key information.

j. On the Replace with external CA certificate page, click **REPLACE**.

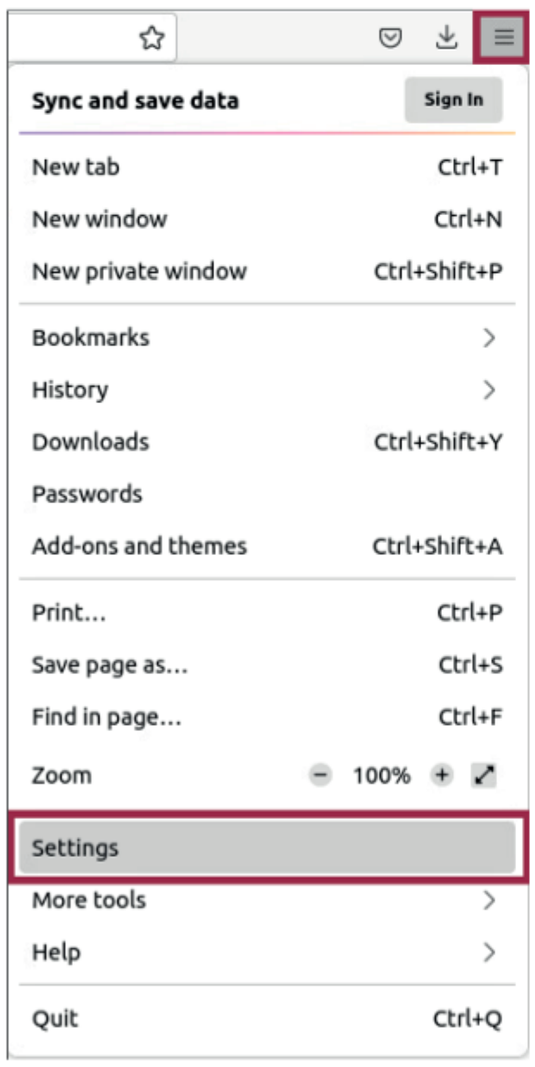
Shortly after the new CA-signed certificate import process successfully begins (in seconds), a message box indicating a connection timeout in the vSphere Client should display. This happens because replacing a security certificate causes vCenter services to restart including the vSphere Client UI.

You will need to restart the web browser to reconnect to the vSphere Client. You will do this at the end of the next step.



3. Clear the web cache and restart Firefox.

a. In a new Firefox tab, open the Firefox menu and select **Settings**.



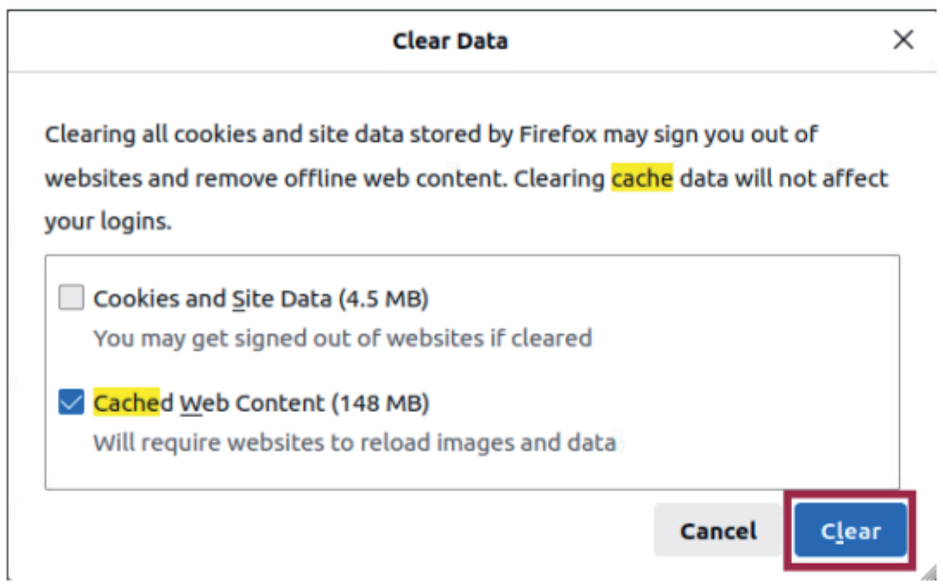
Alternatively, you can open a new Firefox browser tab and enter **`about:preferences`** in the Address box.

b. In the highlighted search box, search for **`cache`**.

c. Under Cookies and Site Data, select **Clear Data**.

d. In the Clear Data dialog box, deselect **Cookies and Site Data** and click **Clear**.

This action will clear the web cache of your Firefox browser.



e. Restart your Firefox browser.

4. Verify the certificate replacement.

After a longer wait (of at least 10 minutes), you must log back in to the vCenter instance because restarting the services ends the UI session.

a. Using the vSphere Client, log in to the vCenter sa-vcsa-01.vclass.local using your vCenter lab credentials.

b. If you get receive the security message `Warning: Potential Security Risk Ahead in your Firefox browser session`, click **Advanced...** and click **Accept the Risk and Continue** to proceed to the vCenter login page.

If you experience difficulties when attempting to log in to the vCenter instance in Site A, clear both Cached Web Content and Cookies and Site Data in the Firefox browser, then retry from step 4a.

If you cannot log in to vCenter after services have restarted, attempt to log in using a new private Firefox window.

c. From the main menu, select **Administration** and select **Certificate Management** under Certificates.

d. From the Machine SSL Certificate tile, select **VIEW DETAILS**.

e. Compare the valid dates and thumbprint information with the certificate information collected in an earlier task.

Valid from: _____
Valid until: _____

Thumbprint: _____

IMPORTANT

The valid dates and thumbprint of the current certificate should be different from the previous certificate.

Lab 16 Monitoring Virtual Machine Performance

Objective and Tasks

Use the system monitoring tools to review the CPU workload:

1. Create a CPU Workload
2. Use Performance Charts to Monitor CPU Use

Task 1: Create a CPU Workload

You run the `CPUBUSY` script in each virtual machine to create a heavy CPU workload in your lab environment.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. Power on Linux-CPU-01 and Linux-CPU-02.
   a. From the main menu of the vSphere Client, select **Inventory** and click the **Hosts and Clusters** icon.
   b. In the navigation pane, click **SA-Compute-02** and select the **VM** tab.
   c. Click the check box for **Linux-CPU-01** and **Linux-CPU-02**.
   d. Right-click the highlighted VMs and select **Power** > **Power On**.
3. From the main menu, select **Inventory** and click the **VMs and Templates** icon.
4. In the navigation pane, expand **sa-vcsa-01.vclass.local** and expand **SA-Datacenter**.
5. Expand **Lab VMs**.

6. On the Summary tab for **Linux-CPU-01** and **Linux-CPU-02**, click **LAUNCH WEB CONSOLE**.
7. On both virtual machine desktops, open the Linux Terminal and run `CPUBUSY`

   `./Desktop/cpubusy.pl`

Task 2: Use Performance Charts to Monitor Host CPU Use

You use Performance Charts to review the latest CPU readiness metrics for two virtual machines.

1. Return to the vSphere Client.
2. View the CPU performance chart for the Linux-CPU-01 virtual machine.
   a. In the navigation pane, select **Linux-CPU-01.**
   b. In the right pane, click the **Monitor** tab and select **Overview** under Performance.

      Scroll down and review the Performance Overview panes.
   c. Select **Advanced** under Performance.

      The real-time CPU usage graph appears.
   d. Click the **Chart Options** link.

      The Chart Options dialog box opens.
   e. In the Chart Metrics pane, verify that **CPU** is selected.
   f. In the **Timespan** drop-down menu, verify that **Real-time** is selected.
   g. Under Select object for this chart, deselect the **0** check box.

      The Linux-CPU-01 VM should be the only selected object.
   h. In the Select counters for this chart list, verify that the **Readiness** and **Usage** check boxes are the only boxes that are selected.
   i. Click **OK**.

      The CPU/Real-time chart for the Linux-CPU-01 virtual machine opens.
3. Open a new tab in the web browser and start a second vSphere Client instance.
   a. To start the vSphere Client, select **vSphere Site-A > vSphere Client (SA-VCSA-01)** in the bookmarks toolbar in Firefox.
4. In the second vSphere Client instance, repeat step 2 to view the CPU performance chart for the Linux-CPU-02 virtual machine.
5. In the vSphere Client windows that show the CPU charts for Linux-CPU-01 and Linux-CPU-02, view the Latest column for the Readiness metric in the Performance Chart Legend.

6. Record the latest CPU readiness value for each virtual machine and leave the Performance Chart windows open.
    - Linux-CPU-01 _____
    - Linux-CPU-02 _____
7. In each VM console, close the Linux Terminal window to stop the `CPUBUSY` script.

IMPORTANT

This script must be stopped in each virtual machine. If the script is left running, the performance of other labs might be affected.

---

8. In the vSphere Client windows that show the CPU charts for Linux-CPU-01 and Linux-CPU-02, view the Latest column for the Readiness metric.
9. Wait for the chart to be updated and compare the CPU ready value with what you recorded in step 6.

    Performance charts update every 20 seconds.

    Q1. Did the CPU ready value change? If it did, what is the reason for the change?
10. Close the Linux-CPU-01 and Linux-CPU-02 consoles and the second vSphere Client tab.

Lab 17 Using Alarms

Objective and Tasks

Create alarms to monitor virtual machine events and conditions:

1. Create a Virtual Machine Alarm to Monitor a Condition
2. Trigger the Virtual Machine Alarm
3. Create a Virtual Machine Alarm to Monitor an Event
4. Trigger the Virtual Machine Alarm
5. Deactivate Virtual Machine Alarms
6. Knowledge Check

Task 1: Create a Virtual Machine Alarm to Monitor a Condition

You create an alarm to monitor a condition that occurs on a virtual machine.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **administrator@vsphere.local**
      Password: **VMware1!**
2. From the main menu, select **Inventory** and click the **VM and Templates** icon.
3. Right-click **Linux-CPU-01** and select **Alarms > New Alarm Definition**.

   The New Alarm Definition wizard opens.

   Because you are creating an alarm for the Linux-CPU-01 virtual machine object, this alarm monitors only that object. If you set the alarm on an object higher in the vCenter inventory, the alarm applies to the parent object and all relevant child objects in the hierarchy.

4. On the Name and Targets page, enter **`Linux-CPU-01 CPU Usage`** in the **Alarm Name** text box.

   The target type is Virtual Machine, and the target object is Linux-CPU-01.

5. Click **NEXT.**

6. On the Alarm Rule 1 page, define the trigger condition.

   If VM CPU Usage is above 40% for 30 seconds, then trigger the alarm and show the alarm as Warning.

   a. From the first drop-down menu, select **VM CPU Usage**.

   b. From the **select an operator** drop-down for the IF condition, select **is above**.

   c. In the **%** text box, enter **40**.

   d. From the last drop-down menu, select **30 sec**.

   e. For the THEN condition, select **Show as Warning** from the select severity drop-down menu.

   f. Click **NEXT**.

7. On the Reset Rule 1 page, read the rule and do not change anything.

   The reset rule is to reset the alarm to Normal if the warning condition is no longer met.

8. Click **NEXT**.

9. On the Review page, review the alarm information.

   The alarm is active by default.

10. Click **CREATE**.

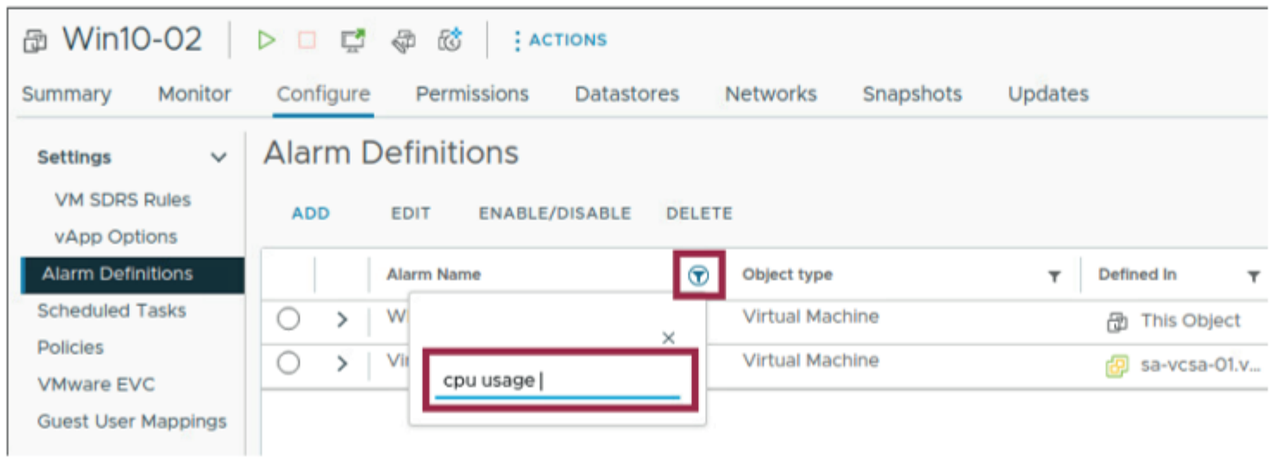
11. Verify that the alarm definition is created.

    a. In the navigation pane, select **Linux-CPU-01** and click the **Configure** tab.

    b. Select **Alarm Definitions**.

    c. Verify that the Linux-CPU-01 CPU Usage alarm appears in the alarm list.

    d. If you cannot easily find the alarm, use the filter in the Alarm Name column and search for some or all of the alarm name.



Task 2: Trigger the Virtual Machine Alarm

You trigger the virtual machine alarm, reset the virtual machine alarm, and view the events that occurred when the alarm was triggered.

1. Generate CPU activity in Linux-CPU-01 to trigger the Linux-CPU-01 CPU Usage alarm.
   a. On the **Summary** tab for Linux-CPU-01, click **Launch Web Console**.
   b. On Linux-CPU-01's desktop, open the Linux Terminal and run `CPUBUSY`.

      ```
      ./Desktop/cpubusy.pl
      ```

      The `CPUBUSY` script should generate enough activity to reach 40 percent CPU usage.
2. Return to the vSphere Client.
3. Verify that the Linux-CPU-01 CPU Usage alarm is triggered.
   a. On the Linux-CPU-01 page, select the Monitor tab and select **Triggered Alarms** under Issues and Alarms.
   b. Wait for at least 30 seconds and refresh the Triggered Alarms pane.
   c. Verify that the Linux-CPU-01 CPU Usage alarm appears in the Triggered Alarms list.
4. Under Tasks and Events, select **Events**.

   An entry states that the Linux-CPU-01 CPU Usage alarm changed from green to yellow.
5. Acknowledge the triggered alarm.
   a. In the right pane under Issues and Alarms, click **Triggered Alarms**.
   b. Select the check box next to **Linux-CPU-01 CPU Usage**.
   c. Click **ACKNOWLEDGE**.

      The Triggered Alarms pane shows the time that the alarm was acknowledged and the user that acknowledged the alarm.
6. Stop the `CPUBUSY` script.
   a. Return to the Linux-CPU-01 console tab.
   b. Close the Linux Terminal window to stop the `CPUBUSY` script.

7. Verify that Linux-CPU-01 returns to a normal state.
   a. Return to the vSphere Client.
   b. Refresh the Triggered Alarms pane and verify that the Linux-CPU-01 CPU Usage alarm no longer appears.

      You might have to wait a minute for CPU usage to decrease.
   c. In the navigation pane, verify that Linux-CPU-01 icon does not show the warning symbol.
   d. On the Triggered Alarms page, select **Events** under Tasks and Events.

      An entry states that the Linux-CPU-01 CPU Usage alarm changed from yellow to green.
8. Close the Linux-CPU-01 console tab.

Task 3: Create a Virtual Machine Alarm to Monitor an Event

You create an alarm to monitor an event that occurs on any virtual machine in SA-Compute-02.

1. In the navigation pane, click the **Host and Clusters** icon.
2. Select **SA-Compute-02** and click the **Configure** tab in the right pane.
3. Select the Alarm Definitions pane and click **ADD**.

   The New Alarm Definition wizard starts.
4. On the Name and Targets page, configure the alarm name and target type.
   a. Enter **`VM Suspended`** in the **Alarm Name** text box.
   b. Select **Virtual Machines** from the **Target type** drop-down menu.

      The target objects are all virtual machines in SA-Compute-02.
   c. Click **NEXT**.
5. On the Alarm Rule 1 page, define the trigger condition.

   If a VM is suspended, then trigger an alarm, and show the alarm as Warning.
   a. From the first drop-down menu, select **VM suspended**.

      The VM suspended event appears under the Power and Connection State category, or type Suspend in the search box.
   b. From the **select severity** drop-down menu, select **Show as Warning**.
   c. Click **NEXT**.

6. Configure the reset rule.

   If the VM is resuming, then reset the alarm to normal.

   a. On the Reset Rule 1 page, turn on the **Reset the alarm to green** toggle.

   b. Click the first drop-down menu for the IF condition and enter **`resuming`** in the **Search** box.

   c. Select **VM resuming** from the search results.

   d. Click **NEXT**.

7. On the Review page, review the alarm information.

   The alarm is active by default.

8. Click **CREATE**.

9. Verify that the alarm definition is created.

   If you cannot easily find the alarm, use the filter in the Alarm Name column and search for some or all of the alarm name.

Task 4: Trigger the Virtual Machine Alarm

You trigger the virtual machine alarm, reset the virtual machine alarm, and view the events that occurred when the alarm was triggered.

1. Trigger the VM Suspended alarm by suspending Linux-CPU-01.

   a. In the navigation pane, right-click **Linux-CPU-01** and select **Power** > **Suspend**.

   b. Click **YES** to confirm suspending the VM.

2. Verify that the VM Suspended alarm is triggered.

   a. In the navigation pane, select **SA-Compute-02** .

   b. In the right pane, click the **Monitor** tab and under Issues and Alarms, select **Triggered Alarms**.

   c. Monitor the Recent Tasks pane and wait for the Suspend virtual machine task to complete.

   d. Verify that the VM Suspended alarm appears in the Triggered Alarms list.

   e. Refresh the Triggered Alarms pane.

3. In the navigation pane, right-click **Linux-CPU-01** and select **Power > Power On**.

   Wait for Linux-CPU-01 to power on.

4. Verify that Linux-CPU-01 has returned to a normal state.

   a. In the navigation pane, verify that Linux-CPU-01's icon does not show the warning symbol.

   b. Refresh the Triggered Alarms pane.

      The VM Suspended alarm no longer appears in the list.

   c. Under Tasks and Events, select **Events**.

      You should see an entry stating that the VM Suspended alarm changed from yellow to green.

Task 5: Deactivate Virtual Machine Alarms

You deactivate the Linux-CPU-01 CPU Usage and the VM Suspended alarms.

1. Deactivate the Linux-CPU-01 CPU Usage alarm.

   a. In the navigation pane, select **Linux-CPU-01**.

   b. Click the **Configure** tab and select **Alarm Definitions**.

   c. Search for the Linux-CPU-01 CPU Usage alarm.

      If necessary, use the filter in the Alarm Name column to search for the alarm.

   d. Click the **Linux-CPU-01 CPU Usage** check box and click **DISABLE**.

   e. Verify that the Linux-CPU-01 CPU Usage alarm is deactivated.

2. Repeat step 1 to deactivate the VM Suspended alarm.

   Perform this step on the **SA-Compute-02** object because the alarm is defined on this object.

3. In the navigation pane, right-click Linux-CPU-01 and select **Power > Power Off**.

4. Verify that Linux-CPU-01 has powered off.

Task 6: Knowledge Check

You are tasked to create and trigger a virtual Machine alarm to monitor an event

1. Create a new alarm definition on Linux-CPU-02 called: **`VM Powered Off`**
2. Configure the alarm to **Show as Warning** and to **Reset the alarm to green** when the VM is **Powered on**
3. Trigger the alarm by powering off Linux-CPU-02
4. Power on Linux-CPU-02, confirm the alarm has reset and deactivate the alarm
5. Power off Linux-CPU-02 to finish this task.

Lab 18 Configuring Lockdown Mode

Objective and Tasks

Configure and test lockdown mode:

1. Start the SSH Service
2. Enable and Test Lockdown Mode
3. Disable Lockdown Mode
4. Knowledge Check

Task 1: Start the SSH Service

You use the vSphere Client to verify that the SSH service is running on sa-esxi-01.vclass.local.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser and click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.
      User name: **administrator@vsphere.local**
      Password: **VMware1!**
2. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.
3. In the navigation pane, select **sa-esxi-04.vclass.local**.
4. In the right pane, click the **Configure** tab.
5. Under System on the page menu to the left, click **Services**.
6. **Start** the **SSH** service if not already running.

Task 2: Enable and Test Lockdown Mode

You enable lockdown mode for your assigned ESXi host.

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 direct console user interface (DCUI).

1. In the navigation pane, select **sa-esxi-04.vclass.local**.
2. In right pane, click the **Configure** tab.
3. Under System, click **Security Profile**.
4. Enable normal lockdown mode.
   a. In the right pane, click **EDIT** next to Lockdown Mode.

      The Lockdown Mode page appears.

   b. On the Lockdown Mode page, click **Normal**.
   c. Select the **Exception Users** tab.

      The user list is empty.

   d. Click **OK**.
5. Verify that the user root is denied access in this SSH session.
   a. Click **Remmina** in the Linux taskbar.
   b. Double-Click **SA-ESXi-04** to login.

      Remmina automatically tries to log in as root. On the SSH credential page, click ok if prompted to log in as the root user.

   c. Verify that user root is not logged in to the SSH session.
   d. Close the Remmina window.
6. Verify that the SSH service is running on the ESXi host.
   a. In the navigation pane, select **sa-esxi-04.vclass.local**.
   b. In the right pane, click the **Configure** tab.
   c. At the left under System, click **Services**.

      You can see that the SSH service is not disabled and it is running on the ESXi host.

7. Verify the root user is denied access in the ESXi UI.

   a. Open the Firefox web browser, open a new tab and click **vSphere Site-A** on the bookmarks toolbar.

   b. Select **Host Client (SA-ESXI-04)**.

   c. On the login page, enter the ESXi lab credentials.

      User name: **`root`**
      Password: **`VMware1!`**

   d. Verify that user root is unable to log in.

   e. Close the browser tab for Host Client (SA-ESXI-04).

Task 3: Disable Lockdown Mode

You disable lockdown mode for your assigned ESXi host.

1. From the main menu, select **Inventory** and click the **Hosts and Clusters** icon.
2. In the navigation pane, select **sa-esxi-04.vclass.local**.
3. In the right pane, click the **Configure** tab.
4. In the navigation pane under System, click **Security Profile**.
5. You disable lockdown mode on your ESXi host.

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

      The Lockdown Mode page appears.

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

   c. Click **OK**.

6. Disable the SSH service on your ESXi host.

   a. Click the **Hosts and Clusters** icon in the inventory.

   b. In the navigation pane, select **sa-esxi-04.vclass.local**.

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

   d. At the left under System, click **Services**.

   e. **Stop** the **SSH** service.

Task 4: Knowledge Check

You are tasked to configure lockdown mode on an ESXi host

1. Configure lockdown mode on sa-esxi-01.vclass.local.
2. Confirm lockdown mode has been configured successfully.
3. Disable lockdown mode on sa-esxi-01.vclass.local.

Lab 19 (Simulation) Configuring Identity Federation to Use Microsoft ADFS

Objective and Tasks

Configuring Identity Federation to use Microsoft ADFS:

1. Configure vCenter Identity Provider Federation
2. Log In to vCenter Using an AD Account

IMPORTANT

Do not perform the steps from this simulation in your actual lab environment.

Do not refresh, navigate away from, or minimize the browser tab hosting the simulation. These actions might pause the simulation, and the simulation might not progress.

Task 1: Lab Simulation

You configure the ADFS identity source and add permissions to vCenter for a user from the ADFS identity source. You then log into vCenter as the user authenticated from ADFS.

1. In your local desktop, open a web browser.
2. Go to https://core-vmware.bravais.com/s/dfx0wDotmsZvWT6R9aiK to open the simulation.
3. After you complete the simulation, close the simulation browser tab.

Lab 20 Configuring vCenter to work with an external KMS

Objective and Tasks

Add a Key Management Server (KMS) to your vCenter from the vSphere Client:

1. Configure a KMS on vCenter
2. Establish Trust between KMS and vCenter

Task 1: Configure a KMS on vCenter

You configure KMS from the vSphere Client.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser, click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter Server lab credentials.

      User name: **administrator@vsphere.local**
      Password: **VMware1!**
2. From the main menu, select **Inventory** and click the **Host and Clusters** icon.
3. In the left pane, click **sa-vcsa-01.vclass.local** and select the **Configure** tab.
4. In the middle pane, select **Key Providers** under Security.
5. Click **ADD** and select **Add Standard Key Provider.**

6. In the wizard, assign the KMS configuration.

Name	sa-kms-01.vclass.local
KMS	sa-kms-01.vclass.local
Address	172.20.10.193
Port	5696

7. Click **ADD KEY PROVIDER.**
8. Click **TRUST** on the Make vCenter Trust Key Provider page.

   Verify the Key Management Server is added and appears under Key Providers.
9. Select **sa-kms-01.vclass.local (default)**.

   The Status of 1 KMS not connected will appear.

Task 2: Establish Trust between KMS and vCenter

You establish trust between the KMS server and vCenter.

1. On the Key Providers tab, click **sa-kms-01.vclass.local**.
2. Click **ESTABLISH TRUST** and select **Make KMS trust vCenter**.

   The Make KMS trust vCenter wizard appears.
3. For **Choose a method**, select **KMS certificate and private key** and click **NEXT**.
   a. For **KMS Certificate**, click **UPLOAD A FILE**, select `/Downloads/KMS Keys/root_certificate.pem` and click **Open**.
   b. For **KMS Private Key**, click **UPLOAD A FILE**, select `/Downloads/KMS Keys/root_key.pem` and click **Open**.
4. Click **ESTABLISH TRUST.**
5. Confirm trust is established between KMS and vCenter.

Lab 21 Creating an Encrypted Virtual Machine

Objective and Tasks

Encrypt a new VM with a standard key provider:

1. Deploy an Encrypted VM
2. Confirm the VM is Encrypted with a Standard Key Provider

Task 1: Creating an Encrypted Virtual Machine

You encrypt the virtual machine Photon-ENC using a virtual machine encryption policy.

1. Log in to the vSphere Client on Site A.
   a. Open the Firefox web browser and click **vSphere Site-A** on the bookmarks toolbar.
   b. Select **vSphere Client (SA-VCSA-01)**.
   c. On the login page, enter the vCenter lab credentials.

      User name: **`administrator@vsphere.local`**
      Password: **`VMware1!`**
2. From the main menu, select **Inventory** and click the **VMs and Templates** icon.
3. Right-click **Lab VMs** and select **New Virtual Machine**.

   The New Virtual Machine wizard appears.
4. On the Select creation type page, verify that **Create a new virtual machine** is selected and click **NEXT**.

5. On the Select a name and folder page, enter the VM name and choose the VM location.

   a. Enter **`Photon-ENC`** in the **Virtual machine name** text box.

   b. Leave **Lab VMs** selected and click **NEXT**.

6. On the Select a compute resource page, expand SA-Datacenter > SA-Compute-02, select **sa-esxi-06.vclass.local** and click **NEXT**.

7. On the Select storage page, select **Encrypt this virtual machine.**

   After selecting the Encrypt check box, the "Management Storage Policy - Encryption" policy is automatically selected. From the VM Storage Policy drop-down menu, it now only shows policies where encryption is enabled.

8. Select **vsanDatastore** and click **NEXT**.

9. On the Select compatibility page, keep the default and click **NEXT**.

10. On the Select a guest OS page, select Guest OS Family **Linux** and **VMware Photon OS (64bit)** from the **Guest OS Version** drop-down menu and click **NEXT**.

11. On the Customize hardware page, configure virtual hardware settings.

    a. Configure CPU, memory, and storage.

Option	Action
CPU	Select **1** from the drop-down menu
Memory	Enter **1 GB**
Hard Disk 1	Enter **2 GB**

    b. For **New Network**, verify that **VM Network** is selected.

    c. For **New CD/DVD Drive**, select **Datastore ISO File** from the drop-down menu.

    d. In the Select File window, click **OPSCALE-Datastore**.

    e. Click the **ISO** folder and select the Photon OS ISO image**: photon-3.0-a0f216d.iso**

    f. Click **OK**.

    g. Expand the **New CD/DVD Drive** to view more details.

    h. Select the **Connect At Power On** check box.

    i. Click **NEXT**.

12. On the Ready to complete page, review the information and click **FINISH**.

13. In the navigation pane, verify that the Photon-ENC VM appears in the Lab VMs folder.

Task 2: Confirm the VM is Encrypted with a Standard Key Provider

You verify that the VM is encrypted with a Standard Key Provider.

1. Select **Photon-ENC** in the navigation pane.
2. In the **Summary** tab, review the settings in the different panes and verify that the settings show the correct configuration for the VM.
3. In the **Virtual Machine Details** pane, verify that the VM is encrypted with a Standard Key Provider.

Answer Key

Lab 5 Managing Resource Pools

Q1. What is the number of shares for this RP-Test (Low) resource pool?

A1. 2,000.

Q2. What is the number of shares for this RP-Production (High) resource pool?

A2. 8,000.

Q3. What is the difference in performance between the two virtual machines?

A3. The RP-Test resource pool, and the virtual machine in it, have only one-fourth of the CPU shares that the RP-Production resource pool has. Therefore, the virtual machine in the RP-Test resource pool receives only one-fourth of the CPU cycles of the logical CPU to which the virtual machines are pinned.

Lab 6 Enabling vCLS Retreat Mode

Q1. What is the number of vCLS VMs deployed?

A1. Two vCLS VMs.

Lab 10 Viewing a vSAN Datastore Configuration

Q1. How many storage devices are in this disk group?

A1. Two.

Q2. What are the drive types?

A2. All storage devices are flash drives (SSD).

Q3. What tier does each drive belong to?

A3. One 5 GB flash drive is used for the cache tier and one flash drive is used for the capacity tier (if you mouse over the progress bar showing the currently used capacity, you can see it's a 10 GB disk)

Q1. Why is the policy's effective free space the value that it is?

A1. Because the storage policy uses RAID 1 (mirroring), RAID 1 provides full redundancy. A full copy of the VM is maintained and, therefore, the VM takes up twice the amount of space as a VM that is not mirrored.

Lab 12 Creating vSAN Storage Policies

Lab 15 Working with Certificates

Lab 16 Monitoring Virtual Machine Performance

Lab 12 Creating vSAN St

Task 1: Examine the Defau

Q1. How many failures can

A1. One.

Task 2: Create a Custom P

Q1. Why is the storage spa

A1. Because the number of created.

Task 3: Assign the Custom

Q1. Why do the VM home a

A1. The selected storage p currently on a VMFS da

Q2. On which datastore is t

A2. OPSCALE-Datastore.

Q3. Which storage policy is

A3. vSAN-VM-Custom-Poli

Q4. Is the VM compliant wit

A4. No. The status is Not A

Lab 15 Working with Cert

Task 1: Examine the Machi

Q1. Who issued the certific

A1. Under Issuer Informatio CA issued the certificat

Lab 16 Monitoring Virtual

Task 2: Use Performance

Q1. Did the CPU ready valu

A1. Yes. After the scripts s contention does not oc

Lab 12 Creating vSAN St

Task 1: Examine the Defau

Q1. How many failures can

A1. One.

Task 2: Create a Custom P

Q1. Why is the storage spa

A1. Because the number of created.

Task 3: Assign the Custom

Q1. Why do the VM home a

A1. The selected storage p currently on a VMFS da

Q2. On which datastore is t

A2. OPSCALE-Datastore.

Q3. Which storage policy is

A3. vSAN-VM-Custom-Poli

Q4. Is the VM compliant wit

A4. No. The status is Not A

Lab 15 Working with Cert

Task 1: Examine the Machi

Q1. Who issued the certific

A1. Under Issuer Informatio CA issued the certificat

Lab 16 Monitoring Virtual

Task 2: Use Performance

Q1. Did the CPU ready valu

A1. Yes. After the scripts s contention does not oc