VMware vSphere:
What's New

Lab Manual
ESXi 7 and vCenter Server 7

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

VMware vSphere: What's New [V6.7 to V7]

Lab Manual

ESXi 7 and vCenter Server 7

Part Number EDU-EN-VSWN7-LAB (04/2020)

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 Reconfiguring the Primary Network Identifier 1

Task 1: Change the FQDN and IP (PNID) Address of vCenter Server Appliance 1

Lab 2 Deploying and Managing Templates in the Content Library 3

Task 1: Check Out a VM Template in the vCenter Server Content Library 3

Task 2: Make Changes to a VM Template 5

Task 3: Check In a VM Template to the vCenter Server Content Library 5

Task 4: Revert to a Previous Version of a VM Template 6

Lab 3 Configuring Identity Federation to Use Windows ADFS 7

Task 1: Configure vCenter Server Identity Provider Federation 7

Task 2: Log In to vCenter Server Using an AD Account 9

Lab 4 Managing vCenter Server Certificates 11

Task 1: Renew a VMware CA Signed Machine SSL Certificate 11

Task 2: Replace the VMware CA Signed Machine SSL Certificate with a Custom Certificate 14

Task 3: Generate a CSR for a Machine SSL Certificate 16

Lab 5 Using vSphere vMotion to Migrate a VM with Attached Devices 17

Task 1: Use VMware Remote Console to Attach an ISO Image to a VM 17

Task 2: Migrate the VM with vSphere vMotion 18

Lab 6 Cloning and Decrypting VMs 20

Task 1: Verify That the Source VM Is Encrypted 20

Task 2: Clone the VM from the Storage Policy with Encryption to the Storage Policy with No Encryption 21

Task 3: Verify That the Cloned VM Is Not Encrypted 21

Lab 7 Assigning a vSphere Trust Authority Administrator 22
Task 1: Assign a vSphere Trust Authority Administrator 22
Lab 8 Enabling and Configuring vSphere Trust Authority 24
Task 1: Export the TPM Certificate and ESXi Image Metadata 24
Task 2: Export the Trusted User Principal 25
Task 3: Enable vSphere Trust Authority Services 26
Task 4: Import the Trusted Host Information to the Trust Authority Cluster 27
Task 5: Create a Trusted Key Provider on the Trust Authority Cluster 28
Task 6: Export the Trust Authority Cluster Settings 29
Task 7: Import the Trust Authority Cluster Settings into the Trusted Hosts Cluster 29
Task 8: Configure the Trusted Key Provider for the Trusted Hosts Cluster 30
Lab 9 Encrypting a Virtual Machine with a Trusted Key Provider 31
Task 1: Encrypt a VM with a Trusted Key Provider 31
Lab 10 Updating ESXi Hosts with vSphere Lifecycle Manager 33
Task 1: Import Updates 33
Task 2: Create a Cluster with vSphere Lifecycle Manager Enabled 35
Task 3: Add an ESXi Host to the Cluster 36
Task 4: Update ESXi Hosts with vSphere Lifecycle Manager 36
Task 5: Manage an Existing Cluster with a Cluster Image 37
Lab 11 (Optional) Upgrading vCenter Server Appliance 6.7 to 7.0 39
Task 1: Verify That vCenter Server Appliance 6.7 with External Platform Services Controller Is Running 40
Task 2: Run the vCenter Server Appliance 7.0 Installer and Perform Stage 1 of the Upgrade Process 41
Task 3: Monitor Stage 1 of the Upgrade Process 44
Task 4: Perform Stage 2 of the Upgrade Process 44
Task 5: Verify That the Upgrade Is Successful 46
Task 6: Decommission External Platform Services Controller Instance 47

Lab 1 Reconfiguring the Primary Network Identifier

Objective and Tasks

Reconfigure the primary network identifier (PNID):

1. Change the FQDN and IP (PNID) Address of vCenter Server Appliance

Task 1: Change the FQDN and IP (PNID) Address of vCenter Server Appliance

You change the FQDN and IP (PNID) address of the management network of vCenter Server Appliance.

You might need to change the PNID when vCenter Server network settings change.

1. From the student desktop, open Google Chrome.
2. Log in to the virtual appliance management interface (VAMI) for sa-vcsa-02.vclass.local.
   a. In Chrome, select **vSphere Site-A > VMware Appliance Management (SA-VCSA-02)**.
   b. If you get a website security warning message, click **Advance** and click **Proceed to sa-vcsa-02.vclass.local (unsafe).**
   c. Enter **`administrator@vsphere.local`** as the user name.
   d. Enter **`VMware1!`** as the password.

   NOTE

   The VM sa-vcsa-02.vclass.local is hosted on the ESXi server sa-esxi-09.vclass.local.

3. In the VAMI, navigate to the Networking page and click **EDIT** to edit Network Settings.

The Edit Network Settings wizard opens.

4. On the Select Network Adapter page, leave **NIC 0 (Management Network)** selected and click **NEXT**.
5. On the Edit settings page, delete the host name that appears and enter **`sa-vcsa-07.vclass.local`** in the **Hostname and DNS** text box.
6. Expand **NIC 0** and enter **`172.20.10.97`** in the **IPv4 address** text box.
7. Click **NEXT**.
8. On the SSO credentials page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password and click **NEXT**.
9. On the Ready to complete page, review your new settings and accept the acknowledgment that you made a backup of vCenter Server Appliance before continuing with the network configuration.

NOTE

Before continuing, verify that the new FQDN and IP address are set properly.

---

10. Click **FINISH**.

    A taskbar shows the status of the network update. When the network reconfiguration is complete, the UI redirects to the new IP address for sa-vcsa-07.vclass.local.

NOTE

It can take up to 20 minutes for the vCenter Server services to restart. The task is complete only when all services successfully start.

---

11. If you get a website security warning message, click **Advance** and click **Proceed to sa-vcsa-07.vclass.local (unsafe).**
12. Log in to the VAMI by entering **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
13. Click **Networking.**
14. Verify that the Hostname is sa-vcsa-07.vclass.local and that the IPV4 Address is 172.20.10.97/24**.**
15. Log out of the VAMI and close the browser tab.

Lab 2 Deploying and Managing Templates in the Content Library

Objective and Tasks

Manage template versioning in the vCenter Server content library:

1. Check Out a VM Template in the vCenter Server Content Library
2. Make Changes to a VM Template
3. Check In a VM Template to the vCenter Server Content Library
4. Revert to a Previous Version of a VM Template

Task 1: Check Out a VM Template in the vCenter Server Content Library

To update a template that is managed in the vCenter Server content library, you check out the VM template.

1. From the student desktop, log in to sa-vcsa-01.vclass.local as administrator@vsphere.local using the vSphere Client.
   a. From the bookmarks bar, select **vSphere Site-A > vSphere client (SA-VCSA-01)**.

      You can also enter the login URL `https://sa-vcsa-01.vclass.local/ui` in the address bar.

   b. Enter **`administrator@vsphere.local`** as the user name.

   c. Enter **`VMware1!`** as the password.

2. Review information about the VM template sa-vm-linux-template-01.
    a. Select **Menu > VMs and Templates**.
    b. In the left pane, expand **SA-Datacenter** and select the VM template **sa-vm-linux-template-01.**
    c. Select the **Summary** tab in the right pane.
    d. Review the summary information for the VM.
    e. Under Versioning, read the version information.
    f. Under VM Hardware, read the hardware information.
3. On the **Versioning** tab, click **CHECK OUT VM FROM THIS TEMPLATE.**

    The Check out VM from VM Template wizard opens.
4. On the Name and location page, configure the VM name and VM location.
    a. Enter **`sa-vm-linux-template-02`** in the **Virtual machine name** text box.
    b. For the virtual machine location, expand **SA-Datacenter** and select **Discovered virtual machine**.
    c. Click **NEXT.**
5. On the Select compute resource page, expand **SA-Cluster** and select **sa-esxi-01.vclass.local**.
6. Click **NEXT**.
7. On the Review page, review the VM information and click **FINISH.**

    NOTE

    This task might take some time to complete.

    ---

8. Under Versioning, verify that sa-vm-linux-template-02 appears.

    Two versions of the VM exist. The VM that is checked out is now available for updating.

Task 2: Make Changes to a VM Template

You change the VM template by increasing the number of virtual CPUs and memory.

1. In the left pane, expand the **Discovered virtual machine** folder and select **sa-vm-linux-template-02.**

   The **Summary** tab opens.

2. Change the vCPU and memory configuration for this VM.

   a. From the **ACTIONS** drop-down menu on the right, select **Edit Settings**.

   b. Increase the number of CPUs to **2**.

   c. Increase the memory to **4 GB.**

   d. Click **OK.**

3. Under VM Hardware, verify that the VM has 2 CPUs and 4 GB of memory.

NOTE

In this lab, only the VM hardware is modified, but the same steps can be followed for guest OS or guest application updates.

Task 3: Check In a VM Template to the vCenter Server Content Library

After the VM template is modified, you check in the modified version of the VM to the content library.

1. On the **Summary** tab for the VM sa-vm-linux-template-02, click **CHECK IN VM TO TEMPLATE.**

   The Check In VM window opens.

2. Enter **`CPU count increased to 2 vCPUs and memory increased to 4 GB`** in the **Check in notes** text box.

NOTE

Providing detailed notes is important for the version information of the VM template. **Check in notes** is a required field.

---

3. Click **CHECK IN.**

4. Monitor the Recent Tasks pane and wait for the tasks to complete.

5. Verify that the VM template called sa-vm-linux-template-02 is converted to the VM template sa-vm-linux-template-01 (3).
6. In the left pane, select **sa-vm-linux-template-01 (3)**.
7. Under Versioning on the **Summary** tab, verify that the information about the VM modifications appears.

NOTE

If the **Summary** tab does not display, select another VM and select **sa-vm-linux-template-01 (3)** again.

Task 4: Revert to a Previous Version of a VM Template

You revert to a previous version of a VM template in the vCenter Server content library.

1. In the left pane, select **sa-vm-linux-template-01 (3)**.

   Under Versioning, you should see two versions of the VM template.
2. Click the ellipsis (three dots) menu for the original version of the VM template sa-vm-linux-template-01 (2) and select **Revert to This Version**.

   The Revert to Version window opens.
3. Enter **`Reverting back to original configuration due to resource issues`** in the **Revert notes** text box.
4. Click **REVERT**.

   The VM template sa-vm-linux-template-01 (2) is renamed to sa-vm-linux-template-01 (4).
5. In the left pane, select **sa-vm-linux-template-01 (4).**
6. Under Versioning on the **Summary** tab, verify that the notes for the revert operation appear next to sa-vm-linux-template-01 (4).
7. Under VM Hardware, verify that the hardware for the VM template shows 1 CPU and 2,048 MB of memory.

Lab 3 Configuring Identity Federation to Use Windows ADFS

Objective and Tasks

Configure the vCenter Server identity provider federation with Microsoft ADFS:

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

Task 1: Configure vCenter Server Identity Provider Federation

You configure vCenter Server to use Microsoft ADFS.

vCenter Server identity provider federation supports only ADFS as an external identity provider.

1. From the student desktop, open a tab in the Google Chrome web browser.
2. From the student desktop, log in to the management vCenter Server (SA-VCSA-01) instance as administrator@vsphere.local using the vSphere Client.
    a. In Chrome, select **vSphere Site-A > vSphere Client (SA-VCSA-01)** in the bookmarks bar.
    b. If you get a website security warning message, click **Advance** and click **Proceed to sa-vcsa-01.vclass.local (unsafe)**.
    c. Enter **`administrator@vsphere.local`** as the user name.
    d. Enter **`VMware1!`** as the password.
3. Select **Menu > Administration**.

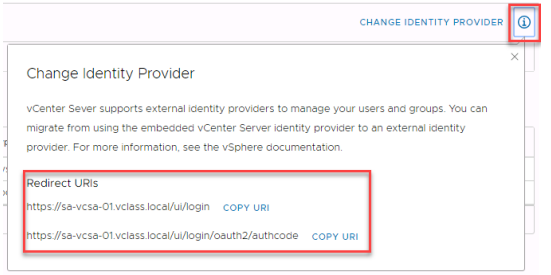
4. In the left pane under Single Sign On, click **Configuration**.

   The **Identity Provider** tab opens to the right.

5. Obtain the redirect URI links.

   a. In the **Identity Provider** tab, click the information icon next to the **CHANGE IDENTIFY PROVIDER** link.

   b. Verify that two redirect URIs are listed.



6. Click **CHANGE IDENTITY PROVIDER**.

   The Configure Main Identity Provider wizard opens.

7. On the Identity Provider page, leave **Microsoft ADFS** selected and click **NEXT**.

8. On the ADFS server page, configure the ADFS settings.

   a. On the student desktop, open the file **adfs_settings.txt** and review the ADFS configuration information.

You can copy and paste the information from this file to the appropriate text boxes on the ADFS server page.

   b. Return to the vSphere Client.

   c. Enter **88530659-7b70-4871-81f1-538c731c5d80** in the **Client Identifier** text box.

   d. Enter **j6aXzfMD57XzPv9w21AWak604KEzlUppNTUdQMdz** in the **Shared secret** text box.

   e. Enter **https://adfs.vclass.local/adfs/.well-known/openid-configuration** in the **OpenID Address** text box.

   f. Click **NEXT.**

9. On the Users and Groups page, configure the AD LDAP connection.
    a. Enter **cn=users,dc=vclass,dc=local** in the **Base distinguished name for users** text box.
    b. Enter **dc=vclass,dc=local** in the **Base distinguished name for groups** text box.
    c. Enter **administrator@vclass.local** in the **Username** text box.
    d. Enter **VMware1!** in the **Password** text box.
    e. Enter **ldaps://dc.vclass.local:636** in the **Primary server URL** text box.
    f. Next to SSL certificates, click **BROWSE.**
    g. Double-click the certificate **CAroot.cer** file on the student desktop.
    h. Click **NEXT**.
10. Review the ADFS configuration and click **FINISH.**
11. Verify that the ADFS server information appears on the **Identity Provider** tab.

Task 2: Log In to vCenter Server Using an AD Account

After configuring the ADFS identity source, you add permissions to vCenter Server for a user from the ADFS identity source. You log into vCenter Server as the user authenticated from ADFS.

1. Select **Menu > Hosts and Clusters.**
2. Add permissions to the ADFS user.
    a. In the left pane, select **sa-vcsa-01.vclass.local**.
    b. Select the **Permissions** tab in the right pane.
    c. Click the **Add Permission** icon (the plus sign).

    The Add Permission window opens.
    d. Change the Domain to **Microsoft ADFS**.
    e. Next to User/Group, search for **Administrator** and select it.
    f. Leave the **Administrator** role selected.
    g. Select the **Propagate to children** check box.
    h. Click **OK**.

NOTE

If the options or fields do not display correctly, you can refresh the vSphere Client to get the correct options and fields.

3. Log out of the vSphere Client.
4. Log in to the vSphere Client as administrator@vclass.local.

NOTE

You are redirected to the ADFS login page.

5. Provide the credentials for the AD user administrator@vclass.local.
   a. Enter **`administrator@vclass.local`** for the user name.
   b. Enter **`VMware1!`** for the password.
6. Verify that the login is successful.
7. Log out of the vSphere Client and close the browser tab.

Lab 4 Managing vCenter Server Certificates

Objective and Tasks

Use the vSphere Client to replace and renew VMware CA signed machine SSL certificates and to generate a certificate signing request:

1. Renew a VMware CA Signed Machine SSL Certificate
2. Replace the VMware CA Signed Machine SSL Certificate with a Custom Certificate
3. Generate a CSR for a Machine SSL Certificate

Task 1: Renew a VMware CA Signed Machine SSL Certificate

You use the vSphere Client to replace a VMware CA signed SSL certificate with a new certificate.

VMware CA issues the new certificate by using the currently configured VMware CA root certificate.

1. From the student desktop, select **vSphere Site-B > vSphere Client (SB-VCSA-01)** in the Google Chrome bookmarks bar.

   IMPORTANT

   You are logging in to vCenter Server on Site B.

   ---

2. Log in to the vSphere Client.
   a. Enter `administrator@vsphere.local` as the user name.
   b. Enter `VMware1!` as the password.

3. Navigate to the Certificate Management page.
   a. Select **Menu** > **Administration**.
   b. In the left pane under Certificates, click **Certificate Management.**
4. On the Certificate Management page, verify that sb-vcsa-01.vclass.local appears in the upper-right corner.
5. Under Machine SSL Certificate, click **VIEW DETAILS**.

   The screenshot is an example only. Your certificate information is different.

6. Record the certificate information.

   Valid from _____
   Valid until _____
   Thumbprint _____

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

7. Renew the VMware CA signed machine SSL certificate for vCenter Server SB-VCSA-01.

   a. Click **BACK TO CERTIFICATE MANAGEMENT**.

   b. Under Machine SSL Certificate, select **ACTIONS > Renew**.

      A warning message about renewing the certificate appears.

   c. Click **RENEW**.

   IMPORTANT

   vCenter Server services restart automatically. You must log back in because restarting the services ends the UI session.

   ---

8. Wait for the vCenter Server services to restart.

   This task takes a few minutes.

9. Verify the certificate replacement.

   a. In the vSphere Client, log in to vCenter Server SB-VCSA-01.

   b. Navigate to the Certificate Management page.

   c. Under Machine SSL Certificate, click **VIEW DETAILS**.

10. Record the valid dates and thumbprint information and compare it with the certificate information that you previously recorded.

    Valid from _____
    Valid until _____
    Thumbprint _____

    IMPORTANT

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

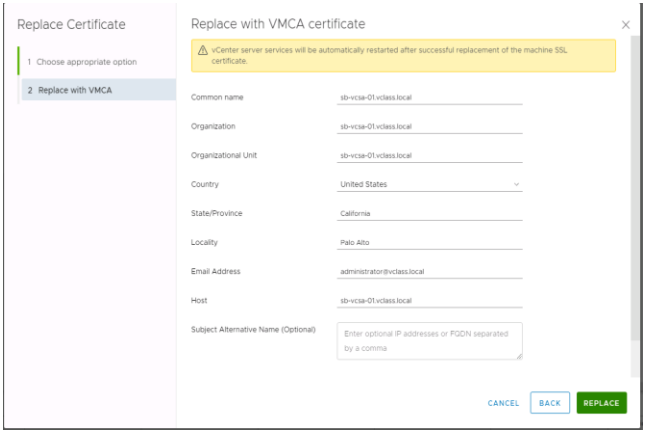
Task 2: Replace the VMware CA Signed Machine SSL Certificate with a Custom Certificate

Using the vSphere Client, you replace the VMware CA signed certificate with a custom VMware CA signed certificate.

1. Replace the VMware CA signed machine SSL certificate for vCenter Server SB-VCSA-01.
   a. Click **BACK TO CERTIFICATE MANAGEMENT**.
   b. Under Machine SSL Certificate, select **ACTIONS > Import and Replace Certificate**.

      The Replace Certificate wizard opens.
   c. On the Choose type of certificate to replace page, leave **Replace with VMCA certificate** selected and click **NEXT**.

      VMware CA generates a CSR to replace the current certificate.
2. On the Replace with VMCA certificate page, configure the required values.
   a. For **Organization**, enter **`sb-vcsa-01.vclass.local`**.
   b. For **Organizational Unit**, enter **`VMware Engineering`**.
   c. For **State/Province**, enter **`California`**.
   d. For **Locality**, enter **`Palo Alto`**.
   e. For **Email Address**, enter **`administrator@vclass.local`**.



3. Click **REPLACE.**

IMPORTANT

vCenter Server services restart automatically. The restart can take up to 10 minutes. You must log back in because restarting the services ends the UI session.

---

4. Verify the certificate replacement.
   a. In the vSphere Client, log in to vCenter Server SB-VCSA-01.
   b. Navigate to the Certificate Management page.
   c. Under Machine SSL Certificate, click **VIEW DETAILS**.
5. Record the valid dates and thumbprint information and verify that the information is different from what you recorded previously.
   Valid from_____
   Valid until _____
   Thumbprint _____

IMPORTANT

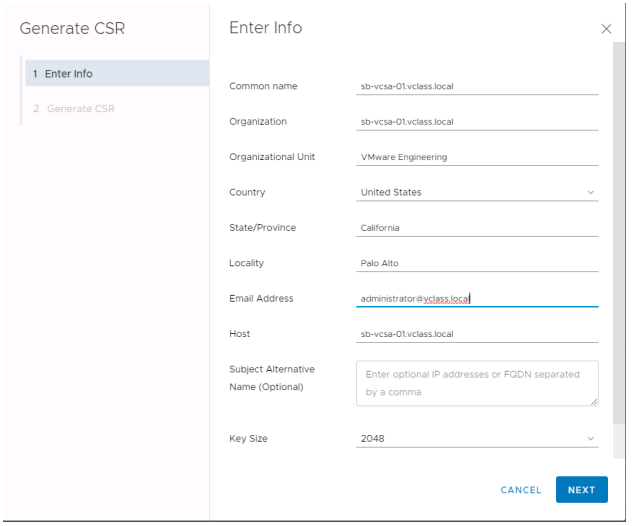
The valid dates and thumbprint of the current certificate should be different from the previous certificate.

Task 3: Generate a CSR for a Machine SSL Certificate

You use the vSphere Client to generate a CSR for the machine SSL certificate.

1. Click **BACK TO CERTIFICATE MANAGEMENT**.
2. Under Machine SSL Certificate, select **ACTIONS > Generate Certificate Signing Request (CSR)**.

   The Generate CSR wizard opens.
3. On the Enter Info page, configure the required values.
   a. For **Organization**, enter **`sb-vcsa-01.vclass.local`**.
   b. For **Organizational Unit**, enter **`VMware Engineering`**.
   c. For **State/Province**, enter **`California`**.
   d. For **Locality**, enter **`Palo Alto`**.
   e. For **Email Address**, enter **`administrator@vclass.local`**.



4. Click **NEXT**.
5. On the Generate CSR page, click **DOWNLOAD.**
6. Save the `sb-vcsa-01.vclass.local.csr` file to the desktop.
7. Click **FINISH**.

   You provide the CSR to your certificate authority.
8. Log out of the vSphere Client and close the browser tab.

Lab 5 Using vSphere vMotion to Migrate a VM with Attached Devices

Objective and Tasks

Use the vSphere Client to migrate a virtual machine with vSphere vMotion while a device is attached through VMware Remote Console:

1. Use VMware Remote Console to Attach an ISO Image to a VM
2. Migrate the VM with vSphere vMotion

Task 1: Use VMware Remote Console to Attach an ISO Image to a VM

Using VMware Remote Console, you attach an ISO image to a VM and power on the VM.

1. From the student desktop, log in to sa-vcsa-01.vclass.local as administrator@vsphere.local using the vSphere Client.
   a. From the bookmarks bar, select **vSphere Site-A > vSphere Client (SA-VCSA-01)**.
   b. If you get a website security warning message, click **Advance** and click **Proceed to sa-vcsa-01.vclass.local (unsafe)**.
   c. Enter **`administrator@vsphere.local`** for the user name.
   d. Enter **`VMware1!`** for the password.
2. Select **Menu > VMs and Templates**.
3. In the left pane, power on the **Photon-VM-1** VM.
4. Connect to Photon-VM-1's remote console.
   a. On Photon-VM-1's **Summary** tab, click the **Launch Remote Console** link.
   b. In the browser, click **Open VMware Remote Console** to allow this website to open the program.

The VMware Remote Console window for Photon-VM-1 opens.

NOTE

Monitor the VMware Remote Console. When a login prompt appears, the Photon OS is running.

5. Connect an ISO image to the CD/DVD drive.
   a. From the **VMRC** drop-down menu in the upper-left corner, select **Removable Devices > CD/DVD drive 1 > Connect to Disk Image File (iso)...**
   b. Select the **xpud-0.9.2.iso** file located in **`C:\Materials\Downloads`**.
   c. Click **Open**.
6. Select **VMRC > Removable Devices > CD/DVD drive 1** and verify that the `xpud-0.9.2.iso` file is connected.

Task 2: Migrate the VM with vSphere vMotion

Using vSphere vMotion, you migrate the VM with a local ISO image that is attached through VMware Remote Console.
The local ISO image does not prevent the migration from happening, and the ISO image remains connected.

1. Return to the vSphere Client.
2. In the left pane, select **Photon-VM-1**.
3. On the **Summary** tab, record the ESXi host where the VM resides. _____
4. Select **ACTIONS > Migrate.**

   The Migrate wizard opens.
5. On the Select a migration type, leave **Change compute resource only** selected and click **NEXT**.
6. On the Select a compute resource page, select a different host from the host name that you recorded previously and click **NEXT**.
7. On the Select networks page, leave the destination network as **VM Network** and click **NEXT**.
8. On the Select vMotion priority page, leave **Schedule vMotion with high priority (recommended)** selected and click **NEXT**.
9. On the Ready to complete page, click **FINISH**.

10. Monitor the Recent Tasks pane and wait for the vMotion task to complete.
11. In the VMware Remote Console for Photon-VM-1, select **VMRC > Removable Device > CD/DVD drive 1** and verify that the ISO file is marked as connected.
12. In the VMware Remote Console for Photon-VM-1, select **VMRC > Removable Device > CD/DVD drive 1** and disconnect the ISO.
13. Close the VMware Remote Console by selecting **VMRC > Exit.**
14. In the left pane, select **Photon-VM-1** and select **ACTIONS > Power > Power Off** to shut down the VM.
15. Click **Yes** to confirm.
16. Log out of the vSphere Client and close the browser tab.

Lab 6 Cloning and Decrypting VMs

Objective and Tasks

Use the vSphere Client to clone an encrypted VM to an unencrypted copy:

1. Verify That the Source VM Is Encrypted
2. Clone the VM from the Storage Policy with Encryption to the Storage Policy with No Encryption
3. Verify That the Cloned VM Is Not Encrypted

Task 1: Verify That the Source VM Is Encrypted

You power on a VM and verify that the VM is encrypted.

The powered-on VM is cloned and decrypted by placing it on the default storage policy.

1. From the student desktop, log in to the management vCenter Server instance as administrator@vsphere.local using the vSphere Client.
   a. In Chrome, select **VCSA-MGMT** on the bookmarks bar.
   b. If you get a website security warning message, click **Continue to this website**.
   c. Enter **`administrator@vsphere.local`** for the user name.
   d. Enter **`VMware1!`** for the password.
2. Select **Menu > VMs and Templates**.
3. In the navigation pane, select the VM **sa-encrypt-01**.
4. Select **ACTIONS > Power > Power On**.

5. Under Guest OS on the **Summary** tab, verify that the VM sa-encrypt-01 is encrypted with the standard key provider.

   NOTE

   If you cannot see the Encryption status, click **SWITCH TO NEW VIEW** in the right corner of the central pane.

6. Under Storage Policies on the **Summary** tab, verify that the VM uses the VM Encryption Policy and that the VM is compliant.

Task 2: Clone the VM from the Storage Policy with Encryption to the Storage Policy with No Encryption

You clone the encrypted VM to an unencrypted version.

1. In the vSphere Client, select the VM **sa-encrypt-01** in the left navigation pane.
2. Under **ACTIONS**, select **Clone > Clone to Virtual Machine.**
3. Configure the clone.
   a. In the **Virtual machine name** text box, enter **`sa-decrypt-01`**.
   b. Select **MGMT-Datacenter** and click **NEXT**.
   c. Expand **MGMT-Cluster**, select the ESXi host **sa-esxi-08.vclass.local**, and click **NEXT**.
   d. Under VM Storage Policy, select **Datastore Default** , select **SA-Shared-01 datastore**, and click **NEXT**.
   e. Click **NEXT**.
   f. Review the Clone configuration and click **FINISH.**
4. Verify that the clone task completes and that a VM called sa-decrypt-01 is created.

Task 3: Verify That the Cloned VM Is Not Encrypted

You verify that the cloned VM is not encrypted.

1. In the vSphere Client, select **sa-decrypt-01** in the navigation pane.
2. Click the **Summary** tab.
3. Under Guest OS, verify that the encryption status for the VM sa-decrypt-01 appears as Not encrypted.
4. Log out of the vSphere Client and close the browser tab.

Lab 7 Assigning a vSphere Trust Authority Administrator

Objective and Tasks

Assign a vSphere Trust Authority Administrator role to allow a user to configure and manage vSphere Trust Authority:

1. Assign a vSphere Trust Authority Administrator

Task 1: Assign a vSphere Trust Authority Administrator

You assign a vSphere Trust Authority Administrator by adding a user to the TrustedAdmins Single Sign-On group.

1. From the student desktop, log in to the management vCenter Server (SA-VCSA-01) instance as administrator@vsphere.local using the vSphere Client.
   a. In Chrome, select **vSphere Site-A > vSphere Client (SA-VCSA-01)** in the bookmarks bar.
   b. Enter **`administrator@vsphere.local`** as the user name.
   c. Enter **`VMware1!`** as the password.
2. Select **Menu > Administration**.
3. Select **Single Sign-On > Users and Groups**.
4. Select the **Groups** tab and select **TrustedAdmins**.
5. Click **ADD MEMBERS**.
6. In the search text box, enter **`trustedadmin`** and select this user from the search results.

7. Click **SAVE**.
8. Confirm that the trustedadmin@vsphere.local user appears in the TrustedAdmins Single Sign-On group.

Lab 8 Enabling and Configuring vSphere Trust Authority

Objective and Tasks

Enable and configure vSphere Trust Authority:

1. Export the TPM Certificate and ESXi Image Metadata
2. Export the Trusted User Principal
3. Enable vSphere Trust Authority Services
4. Import the Trusted Host Information to the Trust Authority Cluster
5. Create a Trusted Key Provider on the Trust Authority Cluster
6. Export the Trust Authority Cluster Settings
7. Import the Trust Authority Cluster Settings into the Trusted Hosts Cluster
8. Configure the Trusted Key Provider for the Trusted Hosts Cluster

Task 1: Export the TPM Certificate and ESXi Image Metadata

You export the Trusted Platform Module (TPM) certificate and ESXi image metadata from the host to be attested.
This information is imported into the vSphere Trust Authority Cluster.

1. On the Desktop, click the **Trust Authority** icon to start PowerCLI.
2. In PowerCLI, connect to the host that is to be attested, namely, the sa-esxi-01.vclass.local host, by using the root credentials.

   ```
   Connect-VIServer -server sa-esxi-01.vclass.local -User root
   -Password VMware1!
   ```

3. Assign the ESXi host to a variable.

   ```
   $vmhost = Get-VMHost
   ```

4. Inspect the TPM endorsement key of the ESXi host.

   ```
   Get-Tpm2EndorsementKey -VMHost $vmhost
   ```

5. Assign the TPM endorsement key to a variable.

   ```
   $tmp2 = Get-Tpm2EndorsementKey -VMHost $vmhost
   ```

6. Using the TPM endorsement key, export the TPM device CA certificate to the `C:\vta\` directory on the student desktop.

   ```
   Export-Tpm2CACertificate -Tpm2EndorsementKey $tmp2 -FilePath
   C:\vta\cacert.zip
   ```

   NOTE

   You perform this step only once because both ESXi hosts are running the same TPM 2.0 hardware.

7. Export the ESXi image metadata from the ESXi host.

   ```
   Export-VMHostImageDb -VMHost $vmhost -FilePath
   C:\vta\image.tgz
   ```

8. Disconnect existing PowerCLI sessions.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   ```

Task 2: Export the Trusted User Principal

You export the trusted user principal from the vCenter Server system that manages the Trusted (attested) Cluster.
This information is imported into the vCenter Server system that manages the vSphere Trust Authority Cluster.

1. In PowerCLI, connect to the vCenter Server system that manages the Trusted (attested) Cluster by using the Trust Authority Administrator credentials.

   ```
   Connect-VIServer -server sa-vcsa-01.vclass.local -User
   trustedadmin@vsphere.local -Password VMware1!
   ```

2. Export the trusted user principal to the `C:\vta\` directory on the student desktop.

   ```
   Export-TrustedPrincipal -FilePath C:\vta\principal.json
   ```

3. Disconnect existing PowerCLI sessions.

```
Disconnect-VIServer -server * -Confirm:$false
```

Task 3: Enable vSphere Trust Authority Services

You enable vSphere Trust Authority services on the vSphere Trust Authority Cluster.

1. In PowerCLI, connect to sb-vcsa-01.vclass.local using the Trusted Administrator credentials.

```
Connect-VIServer -server sb-vcsa-01.vclass.local -User
trustedadmin@vsphere.local -Password VMware1!
```

2. Get the current Trusted Services state of the Trust Authority Cluster.

```
Get-TrustAuthorityCluster "SB-Cluster"
```

NOTE

The cluster should report the Trusted Services state as disabled.

---

3. Assign the current Trusted Services state of the Trust Authority Cluster to a variable.

```
$TAcluster = Get-TrustAuthorityCluster "SB-Cluster"
```

4. Enable Trusted Services on the Trust Authority Cluster.

```
Set-TrustAuthorityCluster -TrustAuthorityCluster $TAcluster
-State Enabled
```

   a. Enter **y** to confirm that you want to enable SB-Cluster.

NOTE

The cluster, called SB-Cluster, is enabled as a vSphere Trust Authority Cluster. The attestd and kmxd services on the Trust Authority hosts are started.

---

5. Leave the PowerCLI session open to this vCenter Server system.

Task 4: Import the Trusted Host Information to the Trust Authority Cluster

You import the trusted host information to the Trust Authority Cluster.

1. In PowerCLI, import the trusted user principal from the Trusted Cluster into the Trust Authority Cluster.

   ```
   New-TrustAuthorityPrincipal -TrustAuthorityCluster
   $TAcluster -FilePath C:\vta\principal.json
   ```

2. To verify that the previous import was successful, return the trusted user principal from the Trusted Cluster.

   ```
   Get-TrustAuthorityPrincipal -TrustAuthorityCluster
   $TAcluster
   ```

3. Import the TPM CA certificate from the Trusted Cluster into the Trust Authority Cluster.

   ```
   New-TrustAuthorityTpm2CACertificate -Name tpmca -
   TrustAuthorityCluster $TAcluster -FilePath C:\vta\cacert.zip
   ```

   NOTE

   This step dictates which TPM devices are trusted by the Trust Authority Cluster.

4. Import the ESXi image metadata from the Trusted Cluster into the Trust Authority Cluster.

   ```
   New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster
   $TAcluster -FilePath C:\vta\image.tgz
   ```

   NOTE

   This step dictates which versions of ESXi are trusted by the Trust Authority Cluster

5. Leave the PowerCLI session open to this vCenter Server system.

Task 5: Create a Trusted Key Provider on the Trust Authority Cluster

You create a trusted key provider on the Trust Authority Cluster so that the Trust Authority Cluster can request encryption keys from a key management server (KMS).

1. Add the key management server, called SB-KMS-01, as a Trust Authority key provider.

   ```
   New-TrustAuthorityKeyProvider -TrustAuthorityCluster
   $TAcluster -MasterKeyId 1 -Name SB-KMS-01 -KmipServerAddress
   172.20.110.193
   ```

   NOTE

   The MasterKeyId is typically in the form of a longer UUID. In this lab, you use an internal PyKMIP KMS. This value differs depending on the KMS that is used. Refer to the KMS vendor documentation.

   IMPORTANT

   You might encounter an error message. You can ignore this message and continue.

2. Assign the key provider to a variable.

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
   $TAcluster
   ```

3. Create the trusted key provider client certificate.

   ```
   New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
   $kp
   ```

4. Return the KMS certificate.

   ```
   Get-TrustAuthorityKeyProviderServerCertificate -
   KeyProviderServer $kp.KeyProviderServers
   ```

5. Assign the KMS certificate to a variable.

   ```
   $cert = Get-TrustAuthorityKeyProviderServerCertificate -
   KeyProviderServer $kp.KeyProviderServers
   ```

6. Add the KMS certificate to the trusted key provider in a trusted state.

   ```
   Add-TrustAuthorityKeyProviderServerCertificate -
   ServerCertificate $cert
   ```

7. Leave the PowerCLI session open to this vCenter Server system.

Task 6: Export the Trust Authority Cluster Settings

You export the settings for the Trust Authority Cluster.
This information is imported into the Trusted Cluster.

1. Export the Trust Authority Cluster information to the `C:\vta\` directory on the student desktop.

   ```
   Export-TrustAuthorityServicesInfo -TrustAuthorityCluster
   $TAcluster -FilePath C:\vta\cluster_settings.json
   ```

   NOTE

   This file contains information about the Trust Authority attestation services and key provider services.

2. Disconnect existing PowerCLI sessions.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   ```

Task 7: Import the Trust Authority Cluster Settings into the Trusted Hosts Cluster

You import the Trust Authority Cluster settings into the trusted hosts cluster to establish a connection to the Trust Authority Cluster.

1. Using PowerCLI, connect to the vCenter Server system that manages the Trusted Cluster.

   ```
   Connect-VIServer -server sa-vcsa-01.vclass.local -User
   trustedadmin@vsphere.local -Password VMware1!
   ```

2. Assign the Trusted Cluster to a variable.

   ```
   $TrustedCluster = Get-TrustedCluster "SA-Cluster"
   ```

3. Import the Trust Authority Cluster information.

   ```
   Import-TrustAuthorityServicesInfo -FilePath
   C:\vta\cluster_settings.json
   ```

   a. At the confirmation prompt, enter **`y`** to accept the default.

4. Enable the Trusted Cluster.

   ```
   Set-TrustedCluster -TrustedCluster $TrustedCluster -State
   Enabled
   ```

   a. At the confirmation prompt, enter `y` to accept the default.

Task 8: Configure the Trusted Key Provider for the Trusted Hosts Cluster

You configure the trusted key provider for the trusted hosts cluster so that encryption keys can be received from the Trust Authority Cluster.
You perform this task using the vSphere Client, which is connected on the vCenter Server system that manages the Trusted Cluster.

1. Using the vSphere Client, log in to vCenter Server sa-vcsa-01.vclass.local as trustedadmin@vSphere.local.
   a. In Chrome, select **vSphere Site-A > vSphere Client (SA-VCSA-01)**.
   b. Enter **`trustedadmin@vsphere.local`** for the user name.
   c. Enter **`VMware1!`** for the password.
2. Select **Menu** > **Hosts and Clusters**.
3. In the navigation pane, select **sa-vcsa-01.vclass.local**.
4. Click the **Configure** tab and select **Key Providers** under Security.
5. Click **ADD TRUSTED KEY PROVIDERS**.

   The trusted key providers that are available have a status of Connected.
6. Select **SB-KMS-01** and click **ADD KEY PROVIDERS**.

   The trusted key provider is shown as Trusted and Connected. Because this trusted key provider is the first to be added, it is marked as the default.

   NOTE

   The trusted key provider becomes the default key provider for the entire vCenter Server system.
7. Log out of the vSphere Client.

Lab 9 Encrypting a Virtual Machine with a Trusted Key Provider

Objective and Tasks

Encrypt a VM with a trusted key provider:

1. Encrypt a VM with a Trusted Key Provider

Task 1: Encrypt a VM with a Trusted Key Provider

You encrypt a VM with a trusted key provider so that the VM can run only on trusted hosts attested by the vSphere Trust Authority Cluster.

1. From the student desktop, log in to the management vCenter Server (SA-VCSA-01) instance as administrator@vsphere.local using the vSphere Client.
   a. In Chrome, select **vSphere Site-A > vSphere Client (SA-VCSA-01)** in the bookmarks bar.
   b. Enter **`administrator@vsphere.local`** as the user name.
   c. Enter **`VMware1!`** as the password.
2. Select **Menu > VMs and Templates**.
3. In the navigation pane, select the VM called **Photon-VM-1**.
4. If the VM is powered on, shut it down by right-clicking the VM and selecting **Power > Shut Down Guest OS**.
5. Right-click **Photon-VM-1** and select **VM Policies > Edit VM Storage Policies**.
6. From the **VM storage policy** drop-down menu, select **VM Encryption Policy**.

7. Click **OK**.

   The VM is encrypted with the configured trusted key provider. The VM summary displays a padlock icon with a green tick to indicate that the VM is encrypted with a trusted key provider.

8. Power on the VM.

Lab 10 Updating ESXi Hosts with vSphere Lifecycle Manager

Objective and Tasks

Import updates from an offline bundle and configure clusters with vSphere Lifecycle Manager:

1. Import Updates
2. Create a Cluster with vSphere Lifecycle Manager Enabled
3. Add ESXi Hosts to the Cluster
4. Update ESXi Hosts with vSphere Lifecycle Manager
5. Manage an Existing Cluster with a Cluster Image

Task 1: Import Updates

You import updates so that you can update vSphere clusters with vSphere Lifecycle Manager.

1. In Chrome, select **vSphere Site-A** > **vSphere Client (SA-VCSA-01)** from the bookmarks bar.
   a. If prompted to open `vmware-ciplauncher.exe`, click **Cancel**.
2. Log in to vCenter Server by entering **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
3. In the vSphere Client, select **Menu** > **Lifecycle Manager**.

4. Import an ESXi image to the image depot.
    a. In the Lifecycle Manager pane, click **ACTIONS** > **Import Updates**.

       The Import Updates dialog box opens.

    b. In the Import Updates dialog box, click **BROWSE** and select **Desktop > Class Materials and Licenses > Downloads**.

    c. Double-click **VMware-ESXi-7.0.0-15847920-depot.zip**.

    d. Wait for the dialog box to close and the import to finish.
5. Import sample vendor add-ons and components to the image depot.
    a. Select **ACTIONS** > **Import Updates**.

    b. Click **BROWSE** and double-click **RC3_SampleAddonsComponents.zip** from `C:\Materials\Downloads`.

The dialog box closes but the import task continues to run.

    c. Monitor the Recent Tasks pane and wait for the import task to complete.

    d. Click **ACTIONS** > **Import Updates**.

    e. Click **BROWSE** and double-click **VMware-ESXi-7.0.0-15847920-vib-test-certs.zip** from `C:\Materials\Downloads`.

    f. Monitor the Recent Tasks pane and wait for the import task to complete.
6. On the **Image Depot** tab, select **ESXi** under ESXi versions.
7. Review the details and components that appear to the right.

   The ESXi version, release date, category, and a full list of components are provided.
8. Click **VENDOR ADDONS** and select the first imported add-on on the list.
9. Review the add-on details.

   You can check the add-on version, release date, category, and a list of added or removed components.
10. Click **COMPONENTS** and select the first imported component on the list.
11. Review the component details.

    You can check the component version, release date, category, and severity.

Task 2: Create a Cluster with vSphere Lifecycle Manager Enabled

You create a vSphere cluster to manage multiple ESXi hosts. You use a single image to maintain consistency in the cluster.

1. Select **Menu** > **Hosts and Clusters**.
2. In the navigation pane, right-click the **SA-Datacenter** object and select **New Cluster**.

   The New Cluster dialog box opens.
3. Configure the new cluster.

Option	Action
Name	Enter **SA-Compute-02**.
vSphere DRS	Leave the service turned off.
vSphere HA	Leave the service turned off.
vSAN	Leave the service turned off.
Manage all hosts in the cluster with a single image	Click the information icon, read the information provided, and close the box. Select the check box.
ESXi Version	Select **7.0 GA - 15847920**.
Vendor Addon (optional)	Leave the default values. Click **OK**.

4. In the Recent Tasks pane, monitor the progress as the cluster is created.

Task 3: Add an ESXi Host to the Cluster

Using Cluster Quickstart, you add an ESXi host to the cluster.

1. In the navigation pane, select **SA-Compute-02** and click the **Configure** tab.
2. On the **Configure** tab, select **Quickstart** under Configuration in the menu on the left.
3. On the 2. Add Hosts card, click **ADD**.

   The Add hosts dialog box opens.
4. In the first **IP address or FQDN** text box, enter **`sa-esxi-03.vclass.local`**.
5. Enter **`root`** in the **Username** text box and **`VMware1!`** in the **Password** text box.
6. Click **NEXT**.
7. In the Security Alert dialog box, select **sa-esxi-03.vclass.local** and click **OK**.
8. On the Host summary page, expand **sa-esxi-03** to view the configuration details and click **NEXT**.
9. On the Review and finish page, review the information and click **FINISH**.
10. Monitor the Recent Tasks pane and wait for the task to finish.
11. Verify that sa-esxi-03.vclass.local is in the SA-Compute-02 cluster.

    The host is placed in maintenance mode.

Task 4: Update ESXi Hosts with vSphere Lifecycle Manager

You scan hosts for compliance and update them to use the defined cluster image.

1. In the navigation pane, select **SA-Compute-02** and click the **Updates** tab.
2. Click **RUN PRE-CHECK** in the Image Compliance pane.
3. On the Image Compliance card, click **See more** to view the details of the precheck task and wait for the task to complete.
4. Scroll down to view the compliance check results.
5. Click **REMEDIATE ALL**.

   The Review Remediation Impact dialog box opens.
6. Review the details and the End User License Agreement.
7. Ensure that the **I accept the terms of the end user license agreement** check box is selected and click **START REMEDIATION**.

8. Monitor the remediation progress in the Image Compliance pane.

   The remediation might take some time to complete.

9. Verify that the remediation completes successfully.

Task 5: Manage an Existing Cluster with a Cluster Image

You convert an existing vSphere 7 cluster to use vSphere Lifecycle Manager, and you update an ESXi host using a cluster image.

1. In the navigation pane, select **SA-Compute-01** and click the **Configure** tab.
2. Under Services, select **vSphere Availability** to verify that vSphere HA is turned off.
   a. If vSphere HA is turned on, click **EDIT** next to vSphere HA is Turned ON, disable vSphere HA, and click **OK**.
3. Click the **Updates** tab.

   The Baselines page opens.

4. On the Baselines page, read the information and click **MANAGE WITH A SINGLE IMAGE**.

   The Image page opens.

5. On the Image page, read the information and click **SETUP IMAGE**.

   The cluster is checked for readiness.

6. Wait for the task to finish and configure the image.

Option	Action
ESXi Version	Select **7.0 GA - 15847920**.
Vendor Addon	Select **VMWTestAddon1** and click **SELECT**.
Firmware and Drivers Addon	Leave the default values.
Components	Click **Show details** and click **ADD COMPONENTS**. Select **vmwTestComponent3** and **vmwTestComponent4** and click **SELECT**.

7. Click **VALIDATE**.

   A valid draft image is ready.

8. Click **SAVE**.

   Image compliance is automatically checked in the cluster.

   The host should be out of compliance with the image.

9. Click **FINISH IMAGE SETUP**.

   The Finish image setup dialog box opens.

   After the cluster is converted, the Baselines page disappears.

10. Log out of the vSphere Client and close the browser tab.

Lab 11 (Optional) Upgrading vCenter Server Appliance 6.7 to 7.0

Objective and Tasks

A demonstration of the upgrade process is available, but you can also perform the steps yourself in this optional lab.

Upgrade vCenter Server Appliance version 6.7 with external Platform Services Controller to version 7 with embedded Platform Services Controller:

1. Verify That vCenter Server Appliance 6.7 with External Platform Services Controller Is Running
2. Run the vCenter Server Appliance 7.0 Installer and Perform Stage 1 of the Upgrade Process
3. Monitor Stage 1 of the Upgrade Process
4. Perform Stage 2 of the Upgrade Process
5. Verify That the Upgrade Is Successful
6. Decommission the External Platform Services Controller Instance

Task 1: Verify That vCenter Server Appliance 6.7 with External Platform Services Controller Is Running

You verify that a vCenter Server Appliance 6.7 instance and an external Platform Services Controller 6.7 instance are running. You also record information about these VMs.

The vCenter Server Appliance 6.7 VM is called SA-VCSA-03 and the external Platform Services Controller 6.7 VM is called SA-VCPSC-03. Both VMs are on the ESXi host called sa-esxi-09.vclass.local.

1. Open a new tab in the Google Chrome web browser.
2. Using the vSphere Client, log in to management vCenter Server vcsa-mgmt.vclass.local as adminstrator@vsphere.local.
   a. In Chrome, select **VCSA-MGMT** on the bookmarks bar.
   b. Enter **administrator@vsphere.local** as the user name.
   c. Enter **VMware1!** as the password.
3. Select **Menu** > **Hosts and Clusters.**
4. In the navigation pane, expand **SA-ESXi-09** to show registered VMs.
5. Select and power on virtual machines **SA-VCSA-03** and **SA-VCPSC-03.**

   The VMs take a few minutes to start.
6. Open a new tab in the Google Chrome web browser.
7. Using the vSphere Client, log in to vCenter Server Appliance 6.7 as administrator@vsphere.local.
   a. In Chrome, select **vSphere Site-A > vSphere Client (SA-VCSA-03)**.
   b. If you get a website security warning message, click **Advance** and click **Proceed to sa-vcsa-03.vclass.local (unsafe)**.
   c. Enter **administrator@vsphere.local** as the user name.
   d. Enter **VMware1!** as the password.
8. Select **Menu** > **Hosts and Clusters**.
9. Verify that sa-vcsa-03.vclass.local appears in the navigation pane.
10. With **sa-vcsa-03.vclass.local** selected in the left pane, click the **Summary** tab in the right pane and verify that the running version is 6.7.

    You can find the version number under Version Information.
11. Log out of the vSphere Client and close the browser tab.

12. Return to the vSphere Client connected to VCSA-MGMT.
13. Select **Menu** > **Hosts and Clusters.**
14. In the navigation pane, expand the **MGMT-Datacenter** cluster.
15. Expand **sa-esxi-09.vclass.local** and select **SA-VCSA-03**.

    The **Summary** tab shows the details of the SA-VCSA-03 virtual machine.
16. Record the DNS Name and IP Address for the SA-VCSA-03 virtual machine.

    DNS name _____

    IP address _____
17. Select **SA-VCPSC-03** in the navigation pane.

    The **Summary** tab shows the details of the SA-VCPSC-03 virtual machine.
18. Record the DNS Name and IP Address for the SA-VCPSC-03 virtual machine.

    DNS name _____

    IP address _____
19. Log out of the vSphere Client.

Task 2: Run the vCenter Server Appliance 7.0 Installer and Perform Stage 1 of the Upgrade Process

You start the vCenter Server Appliance 7.0 installer and perform stage 1 of the converge upgrade process.

1. Mount the vCenter Server Appliance 7.0 installer ISO.
    a. On the Desktop, double-click the **Class Materials and Licenses** folder.
    b. Double-click **Downloads**.
    c. Double-click **VMware-VCSA-all-7.0.0-15952498.iso**.

The vCenter Server Appliance installer ISO file is mounted on the DVD drive.

2. Navigate to the `vcsa-ui-installer\win32` folder.

    This folder includes an application file called `installer.exe`.
3. Double-click **installer.exe** to start the vCenter Server installer.
4. Click **Upgrade**.

    The Upgrade - Stage 1: Deploy vCenter Server wizard opens.

5. On the Introduction page, read the information about the upgrade process and click **NEXT**.
6. On the End-user license agreement page, accept the license agreement and click **NEXT**.
7. On the Connect to source appliance page, configure the source vCenter Server Appliance 6.7 settings.
   a. Enter **`sa-vcsa-03.vclass.local`** in the **vCenter Server Appliance** text box.
   b. Click **CONNECT TO SOURCE**.
   c. Enter **`VMware1!`** in the **SSO Password** text box.
   d. Enter **`VMware1!`** in the **Appliance (OS) root password** text box.
   e. Enter **`sa-esxi-09.vclass.local`** in the **ESXi host or vCenter Server name** text box.
   f. Enter **`root`** in the **User name** text box.
   g. Enter **`VMware1!`** the **Password** text box.
   h. Click **NEXT**.
8. In the Certificate Warning window, click **YES** to continue.

   A message window states that the source vCenter Server instance is converged and upgraded to vCenter Server with embedded Platform Services Controller.
9. Click **YES** to continue.
10. On the vCenter Server deployment target page, configure the target settings.
    a. Enter **`sa-esxi-09.vclass.local`** in the **ESXi host or vCenter Server name** text box.
    b. Enter **`root`** in the **User name** text box.
    c. Enter **`VMware1!`** the **Password** text box.
    d. Click **NEXT**.
11. In the Certificate Warning window, click **YES** to continue.

12. On the Set up target vCenter Server VM page, configure the VM settings for the vCenter Server instance to be deployed.
    a. Enter **vCenter7_converge** in the **VM name** text box.
    b. Enter **VMware1!** in the **Set root password** text box.
    c. Enter **VMware1!** in the **Confirm root password** text box.
    d. Click **NEXT**.
13. On the Select deployment size page, select the deployment size.
    a. Select **Tiny** from the **Deployment size** drop-down menu.
    b. Select **Default** from the **Storage size** drop-down menu.
    c. Click **NEXT**.
14. On the Select datastore page, configure the storage location for the vCenter Server instance.
    a. Select **SA-ESXi-09-Local-02**.
    b. Select the **Enable Thin Disk Mode** check box.
    c. Click **NEXT**.
15. On the Configure network settings page, configure the vCenter Server network.
    a. Select **VM Network** from the **Network** drop-down menu.
    b. Select **IPv4** from the **IP version** drop-down menu.
    c. Select **static** from the **IP assignment** drop-down menu.
    d. Enter **172.20.10.99** in the **Temporary IP address** text box.
    e. Enter **255.255.255.0** in the **Subnet mask or prefix length** text box.
    f. Enter **172.20.10.10** in the **Default gateway** text box.
    g. Enter **172.20.10.10** in the **DNS servers** text box.
    h. Click **NEXT**.
16. On the Ready to complete stage 1 page, click **FINISH**.

    Stage 1 of the vCenter Server Deployment proceeds.

Task 3: Monitor Stage 1 of the Upgrade Process

You monitor the progress of the stage 1 deployment to ensure that no errors are reported.

The first stage of the vCenter Server deployment creates a vCenter Server Appliance instance in sa-esxi-09.

1. Using the vSphere Client, log in to management vCenter Server vcsa-mgmt.vclass.local as adminstrator@vsphere.local.
   a. In Chrome, select **VCSA-MGMT** on the bookmarks bar.
   b. Enter **`administrator@vsphere.local`** as the user name.
   c. Enter **`VMware1!`** as the password.
2. Select **Menu** > **Hosts and Clusters**.
3. Verify that a VM called vCenter7_converge is created on sa-esxi-09.vclass.local.
4. Log out of the vSphere Client and close the browser tab.
5. Return to the vCenter Server installer and wait for the deployment to complete.

   NOTE

   The deployment might take some time to complete.

   ---

6. When stage 1 is complete, select **CONTINUE** to proceed to stage 2.

Task 4: Perform Stage 2 of the Upgrade Process

You perform stage 2 of the two-stage upgrade process by copying data from the source appliance to the deployed vCenter Server instance.

1. In the vCenter Server installer, verify that you are on the Introduction page of stage 2 and click **NEXT**.

   Pre-upgrade checks are performed and might take a few minutes to complete.
2. Read the pre-upgrade check results and click **CLOSE**.
3. On the Configuration replication page, click **This is the first vCenter Server in the topology that I want to converge** and click **NEXT**.
4. On the Select upgrade data page, click **Configuration and Inventory** and click **NEXT**.

   A time estimate is provided.

5. On the Configure CEIP page, deselect the **Join the VMware's Customer Experience Improvement Program (CEIP)** check box, click **NEXT**, and close the warning message.
6. On the Ready to complete page, select the **I have backed up the source vCenter Server and all the required data from the database** check box.
    a. If a shutdown warning appears, close the notification.
7. Click **FINISH**.
8. Monitor the progress of stage 2 and wait for it to complete.
9. When stage 2 completes, read the results in the Message window and click **CLOSE**.
10. In the Upgrade - Stage 2: Complete window, click **CLOSE**.

Task 5: Verify That the Upgrade Is Successful

You verify the settings and data of the new vCenter Server Appliance instance.

After a successful upgrade, a vCenter Server Appliance with an embedded Platform Services Controller instance is created. The data from the source vCenter Server Appliance instance is copied to the new vCenter Server Appliance instance.

1. Using the vSphere Client, log in to management vCenter Server vcsa-mgmt.vclass.local as adminstrator@vsphere.local.
   a. In Chrome, select **VCSA-MGMT** on the bookmarks bar.
   b. Enter **administrator@vsphere.local** as the user name.
   c. Enter **VMware1!** as the password.
2. Select **Menu > Hosts and Clusters.**
3. Select the VM **vCenter7_converge** and verify that the VM is powered on.
4. In the **Summary** tab, verify that the DNS name is sa-vcsa-03.vclass.local and the IP address is 192.20.10.96.

   NOTE

   The IP address changes from the temporary IP address to the original IP address.

   ---

5. Log out of the vSphere Client and close the tab.
6. Using the vSphere Client, log in to vCenter Server Appliance 7.0 sa-vcsa-03.vclass.local as adminstrator@vsphere.local.
   a. In Chrome, select **vSphere Site-A > vSphere Client (SA-VCSA-03)**.
   b. Enter **administrator@vsphere.local** as the user name.
   c. Enter **VMware1!** as the password.
7. Select Menu > Administration.
8. Under Deployment, select **System Configuration**.

9. Verify that vCenter Server sa-vcsa-03.vclass.local with the embedded Platform Services Controller instance appears.

NOTE

The vCenter Server icon indicates that the vCenter Server instance has an embedded Platform Services Controller instance.
The external Platform Services instance is still shown because this system is not yet decommissioned.

10. Log out of the vSphere Client and close the tab.

Task 6: Decommission External Platform Services Controller Instance

You decommission the external Platform Services Controller instance.

You perform this step only when no other vCenter Server instances are connected to the external Platform Services Controller instance. It is safe to decommission the external Platform Services Controller instance because sa-vcsa-03 is no longer connected to sa-vcpsc-03.

1. Using the vSphere Client, log in to management vCenter Server vcsa-mgmt.vclass.local as adminstrator@vsphere.local.
   a. In Chrome, select **VCSA-MGMT** on the bookmarks bar.
   b. Enter **`administrator@vsphere.local`** as the user name.
   c. Enter **`VMware1!`** as the password.
2. Select **Menu** > **Hosts and Clusters**.
3. Select the VM **SA-VCPSC-03** and shut down the VM.
4. Log out of the vSphere Client.
5. From the student desktop, open MTPuTTY and connect to sa-vcsa-03.

   You are logged in as root
6. Type **`shell`** to switch to the vCenter Server command shell.

7. Decommission the external Platform Services Controller instance by running the `cmsso-util` command.

   `cmsso-util unregister --node-pnid sa-vcpsc-03.vclass.local --username administrator@vsphere.local --passwd VMware1!`

   During the decommission process, vCenter Server services are restarted.

8. Using the vSphere Client, log in to management vCenter Server sa-vcsa-03.vclass.local as adminstrator@vsphere.local.

   a. In Chrome, select **vSphere Site-A > vSphere Client (SA-VCSA-03)**.

   b. Enter **`administrator@vsphere.local`** as the user name.

   c. Enter **`VMware1!`** as the password.

9. Select **Menu** > **Administration**.

10. Under Deployment, select **System Configuration**.

11. Verify that the vCenter Server sa-vcsa-03.vclass.local with the embedded Platform Services Controller instance appears and that the external Platform Services Controller sa-vcpsc-03 instance is no longer shown.

12. Log out of the vSphere Client and close the browser tabs.