DELL EMC

Technical Note

File-Based Backup and Restore of VxRail VCSA and PSC

Abstract

This document describes the procedures for the file-based backup and restore of VxRail vCenter Server Appliance (vCSA) and Platform Services Controller (PSC) in VxRail v4.5.

July 2019

H17869

TABLE OF CONTENTS

Executive Summary

vSphere 6.5 supports a file-based backup and restore mechanism that enables the recovery of an environment after failures. The Virtual Appliance Management Interface (VAMI) can be used to create a file-based backup of the vCenter Server Appliance (vCSA) and the Platform Services Controller (PSC). After a backup is created, the restore can be achieved by using the vCSA-UI installer.

VxRail 4.5 is based on vSphere 6.5, and as such, it can take advantage of VMware's native file-based backup and restore feature supported by vSphere 6.5. This document describes the procedures for the file-based backup and restore of VxRail vCSA and PSC in VxRail 4.5.

Intended Audience

This document is intended for customers and Dell EMC service providers who are authorized to work on a VxRail cluster and VxRail administrators.

Overview of VMware Native File-based Backup and Restore

The Virtual Appliance Management Interface (VAMI) can be used to perform a file-based backup of a vCenter Server's core configuration, inventory, and historical data of choice. The backed-up data is streamed over FTP, FTPS, HTTP, HTTPS or SCP to a remote system. The backup is not stored on the vCSA.

A file-based restore operation can be performed only for a vCSA that has been previously backed up using the VAMI. Such a restore operation is performed using the vCSA-UI installer. The process consists of deploying a new vCSA and copying the data from the file-based backup to the new appliance.

For more information on the native file-based backup and restore of vCSA, see the VMware document: https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.install.doc/GUID-3EAED005-B0A3-40CF-B40D-85AD247D7EA4.html

File-based Backup in VxRail 4.5

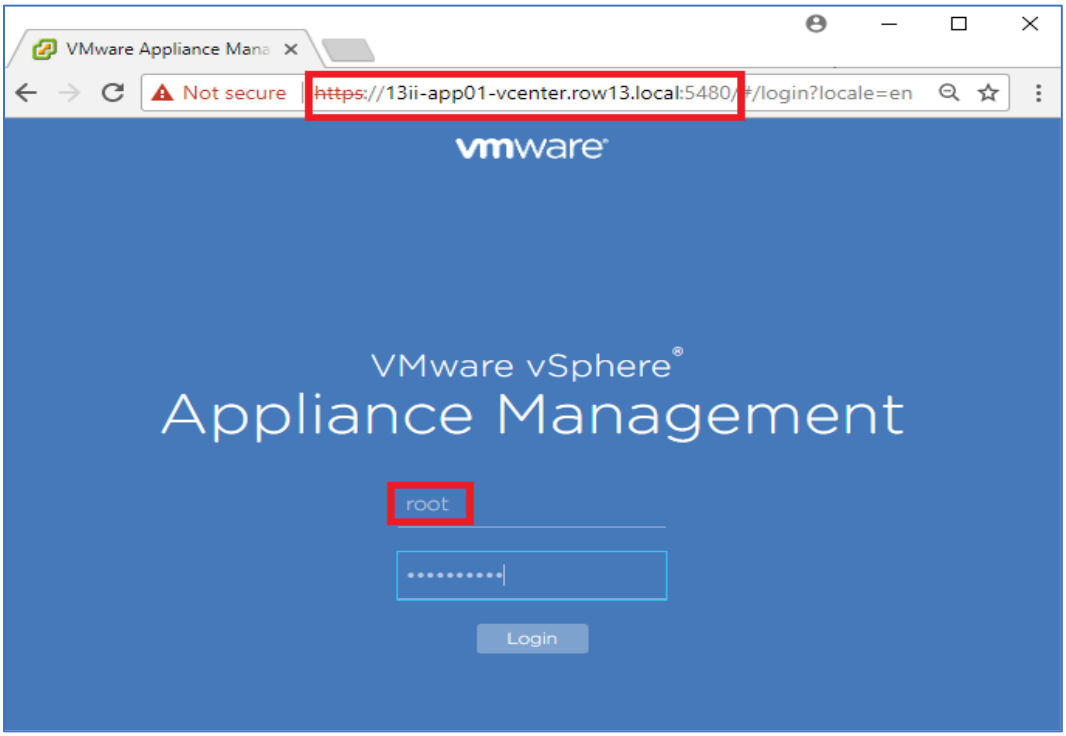
The procedure for file-based backup in VxRail 4.5 follows VMware's native file-based backup procedure. This built-in functionality supports the backup of vCSA and PSC both in internal and external deployment cases.

Backup Overview

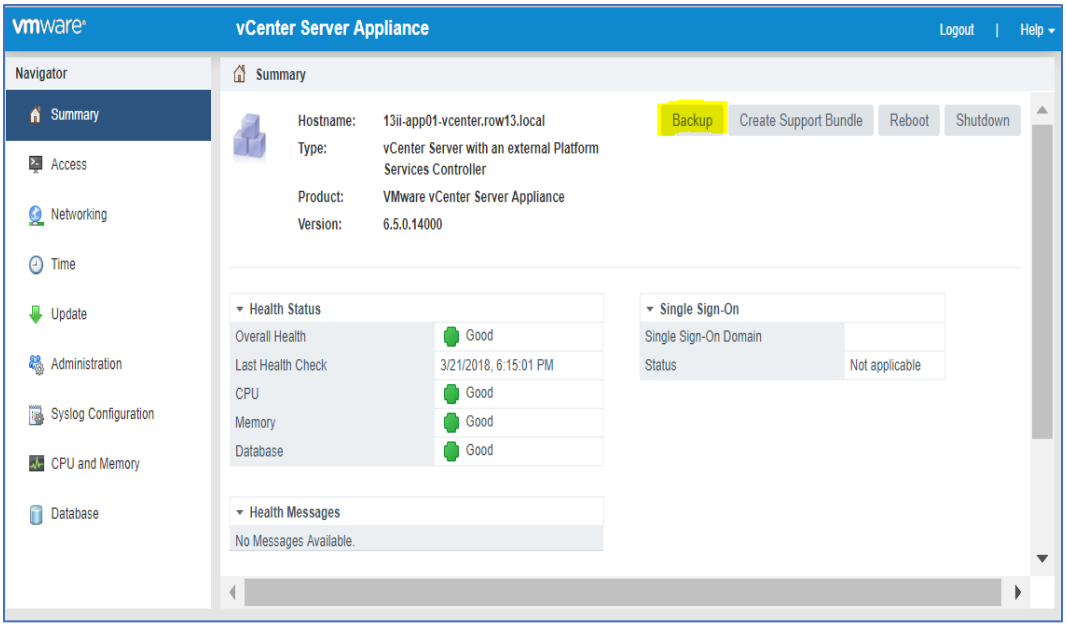
The file-based backup feature requires no quiescing or downtime of the selected appliance because the backup can be performed while the appliance is running. Furthermore, it does not require any agents; the backup can be started directly from the VAMI accessed using the FQDN or the IP address of the appliance at port 5480. From there, a wizard guides you through the backup process. You first select the protocol that you have already configured. VMware supports FTP, FTPS, HTTP, HTTPS and SCP protocols. You then specify the location where the backup will live and enter the username and password of the backup location. Optionally, you can encrypt the backup by using the AES 256, in which case you will be prompted for a password. This encryption password is not stored, and if lost, there is no way to recover the backup files. Therefore, this password must be stored in a safe location. By default, only the configuration and inventory data are backed up, but you can choose whether to include the historical and performance data in the backup. In the event of a disaster, the backup is used to recover the appliance.

Backup Procedure for vCSA and PSC

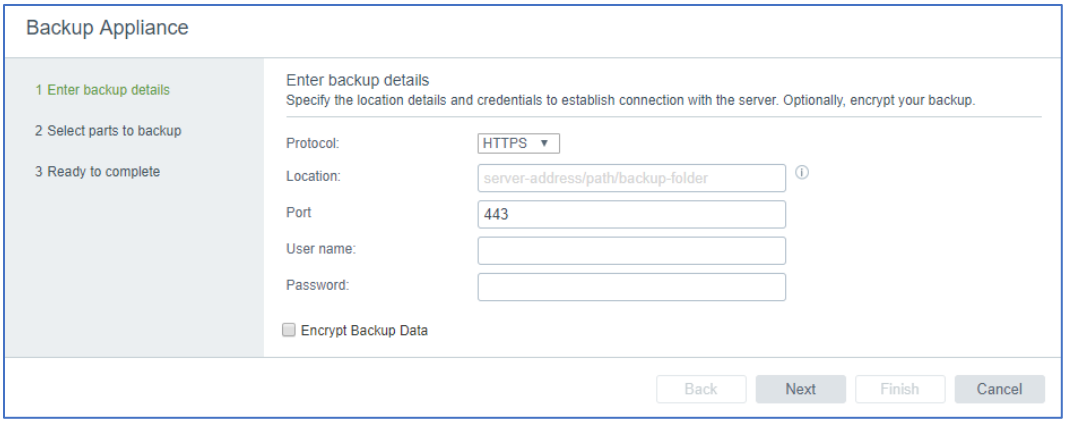
1. To begin the backup workflow, log into the VMware vSphere Appliance Management Interface (VAMI) as `root` using the FQDN or the IP address of the vCSA or PSC at port 5480.



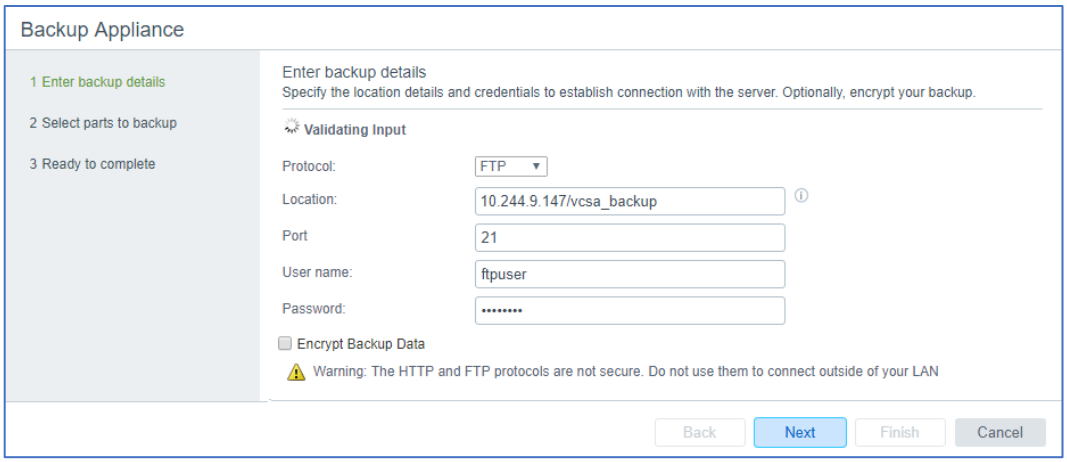
2. Click the **Summary** tab on the Navigator pane and then click the **Backup** button on the Summary pane to launch the Backup Appliance wizard.



The Backup Appliance wizard launches.



3. In the Backup Appliance wizard, enter the backup details.

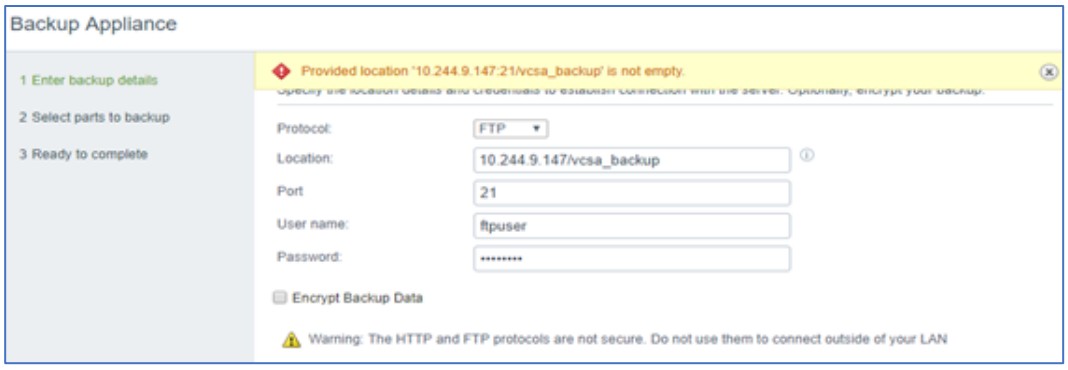


a. The backed-up data can be streamed over FTP, FTPS, HTTP, HTTPS, or SCP to a remote system. Select one of these protocols from the **Protocol** pull-down menu. The corresponding port number for the selected protocol is automatically filled in the **Port** field. The corresponding port numbers for these protocols are 21, 21, 80, 443, and 22 respectively.

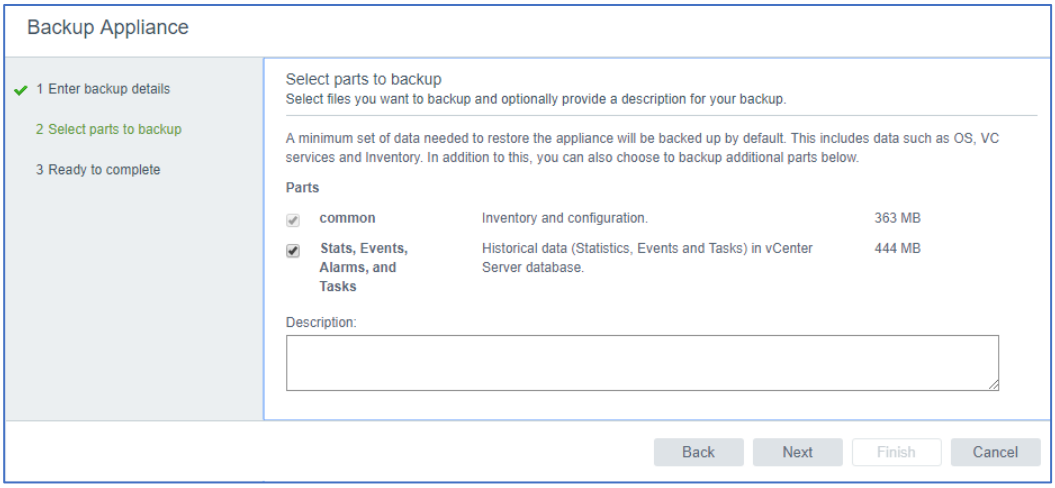
b. In the **Location** field, enter the backup target's IP address followed by the specific target folder in a simple syntax, such as **10.244.9.147/vcsa_backup**. You must also provide the required credentials in the **User name** and the **Password** fields to establish connection with the server.

   An option to encrypt the backup files using AES 256 is available by enabling a check-box named **Encrypt Backup Data** and entering a password. The encryption password is not stored, and if lost, there is no way to recover those backup files.

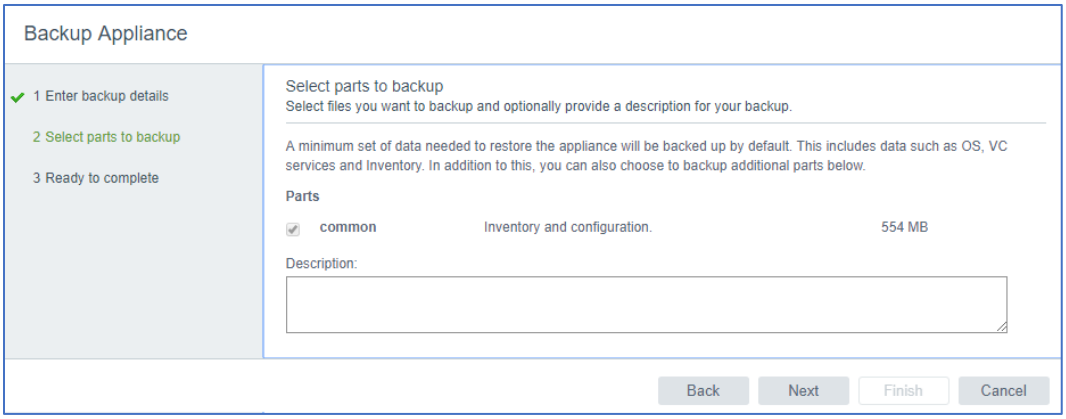
c. After you have entered the backup details, click **Next**. This step triggers an action for validating the entered information. If the information is not valid, you will be prompted to correct it. For instance, if the location does not exist, you will be notified as shown in the following figure.



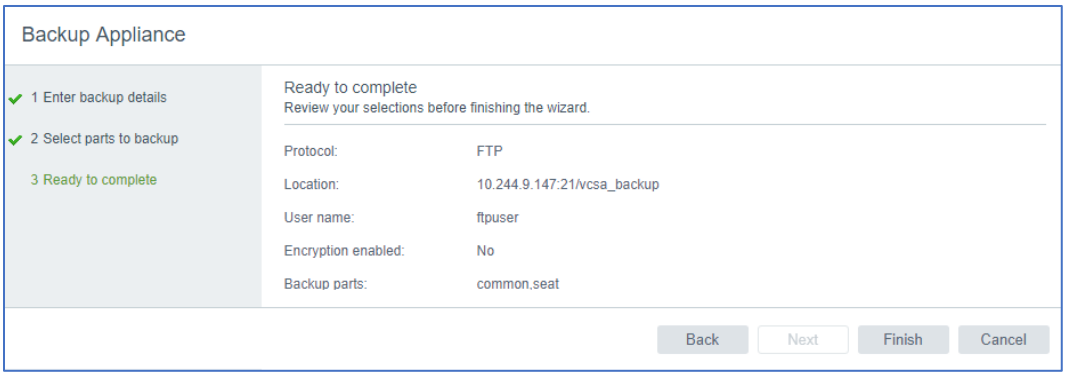
If the validation passes, you will move to the next step in the Backup Appliance wizard where you select the files you want to backup. By default, the inventory and configuration data of the vCSA are backed up. There is also the option of backing up the historical and performance data of the vCSA. Keep in mind that selecting this option could increase the backup time of the vCSA. The PSC will not have this option because all historical and performance data is kept in the vCSA database. You can optionally provide a description for your backup in the next screen. Click **Next** to proceed.



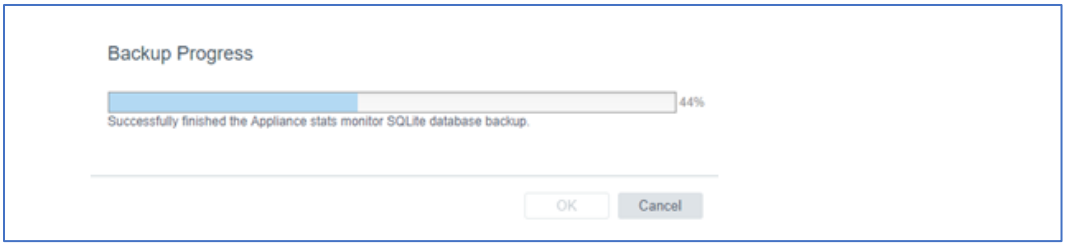
The following figure from a PSC backup workflow shows that unlike vCSA, the PSC does not have the option of backing up the historical and performance data.



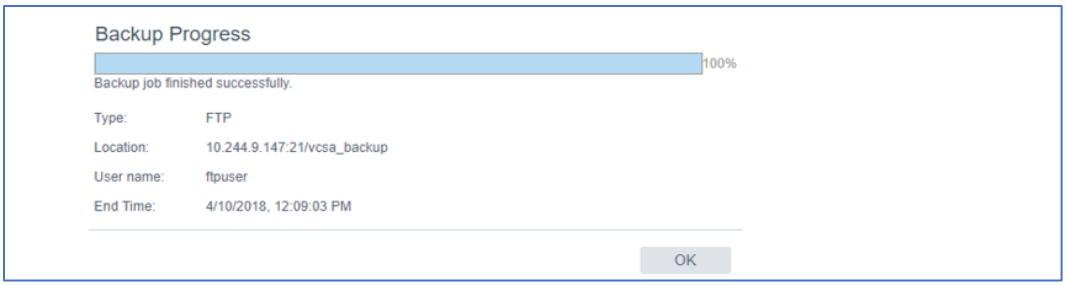
4. Review your selections presented in the Summary page before finishing the wizard. If you need to make changes, click **Back**. If everything looks okay, click **Finish**.



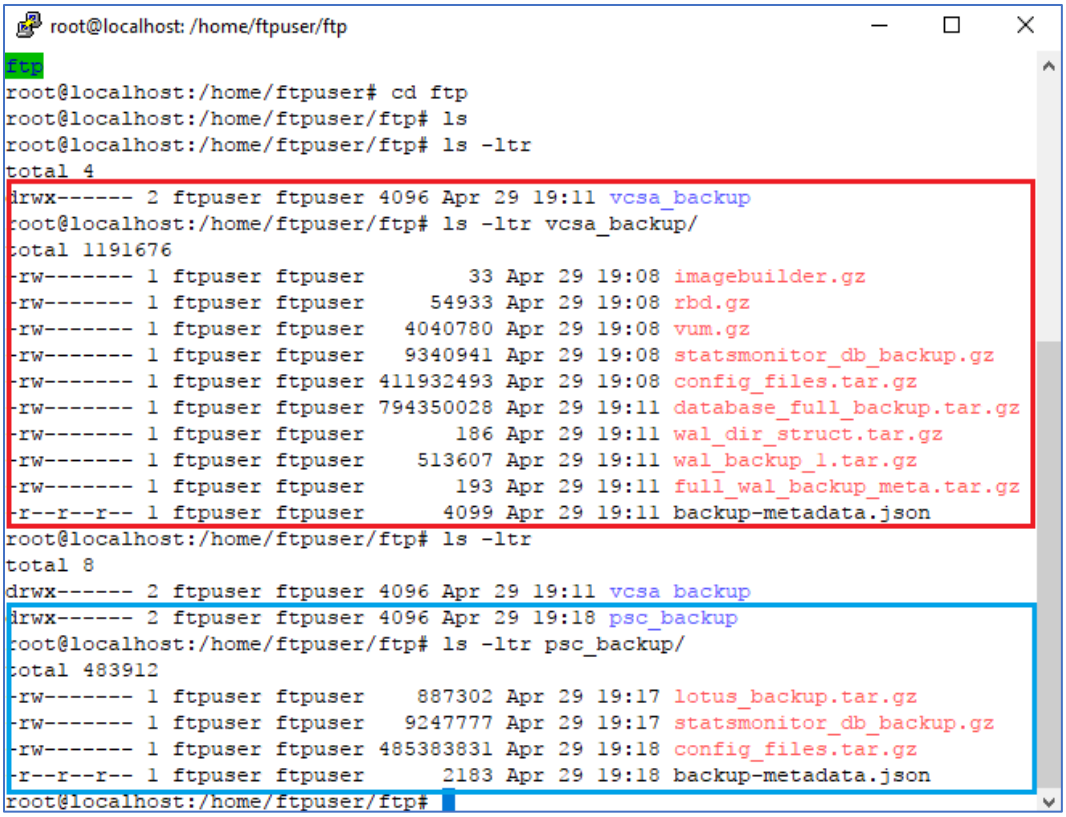
The backup files are then streamed to the backup target using the selected protocol. The backup process will produce a set of files for the designated appliance.



5. When the backup job finishes successfully, click **OK**.



When the backup workflow completes successfully, the files become visible at the backup target. The backup workflow is nearly identical for vCSA and PSC. The following illustration shows the files at the backup target for both types of appliances.



File-based Restore in VxRail 4.5

The file-based restore procedure is for recovery of the VxRail vCSA in the event of a disaster where the vCSA, or the PSC, or both are no longer available.

Overview

You can perform a file-based restore of an appliance that has previously been backed up using the Virtual Appliance Management Interface (VAMI). You can perform such a restore operation using the vCSA-UI installer. You can mount the ISO of the vCSA from which you deployed and click the **Restore** button right from the installer. You must use the specific vCSA installer ISO, matching the vCSA version which was backed up (e.g., VMware-VCSA-all-6.5.0-7515524.iso). The Installer will then do a two-stage deployment: Stage 1 deploys the appliance, and Stage 2 configures and restores from the backup selected.

Restore Procedure

Primary Node Configuration Prior to Restore Operation

Before starting the restore operation, some prerequisite steps must be performed. In particular, the file-based restore operation requires a vSphere Standard Switch (vSwitch) or an ephemeral portgroup. By default, VxRail 4.5 with vCSA and PSC does not use a vSphere Standard Switch (VSS). You must create a temporary VSS on the primary node and take **vmnic1** out of the default Distributed Virtual Switch (DVS) before performing the restore operation. Generally, we can regard the first node as the primary-node. Even when VxRail vCSA and PSC are unavailable, the primary-node can still be accessed through its management IP because DVS configuration still works for the nodes.

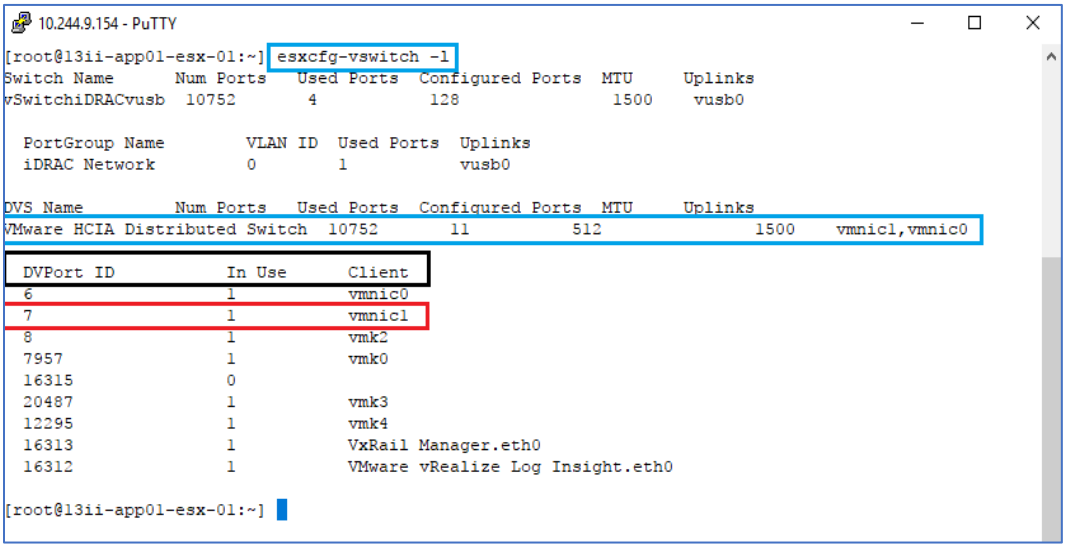
Perform the following steps to prepare the system for the actual restore operation:

1. Verify that the primary node is not in lockdown or maintenance mode.
2. Verify that DNS records for vCSA and PSC addresses exist.
3. [Important] If you are attempting to restore a vCSA or a PSC instance that is still running, power it off before starting the restore.

Note: Failure to power it off could compromise the restore operation and cause data corruption.

4. Enable the SSH service for the primary node using the node's web interface or the DCUI Troubleshooting menu.
5. SSH to the primary-node.
6. Run the following command to identify the **vmnic1 DVPort ID** in the DVS configuration.

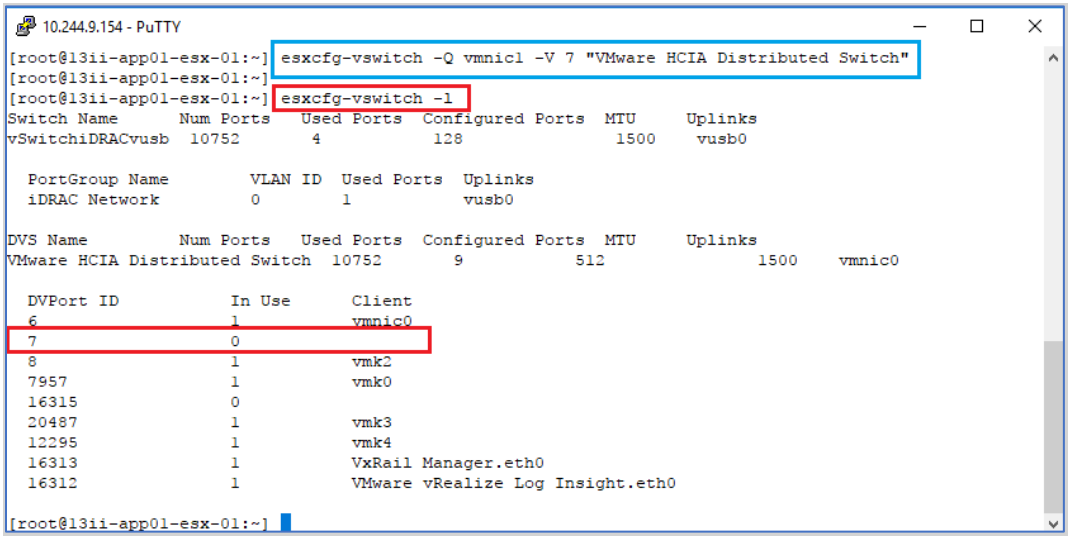
```
esxcfg-vswitch -l
```



In the sample command output, {DVS name is *VMware HCIA Distributed Switch*} and {vmnic1 DVPort ID is *7*}.

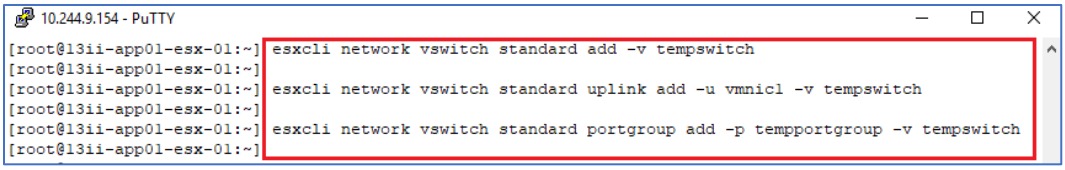
7. Having acquired the **vmnic1 DVPort ID**, run these commands to **remove the vmnic1 from the DVS** and to confirm that it was successfully removed:

```
esxcfg-vswitch -Q vmnic1 -V 7 "VMware HCIA Distributed Switch"
esxcfg-vswitch -l
```



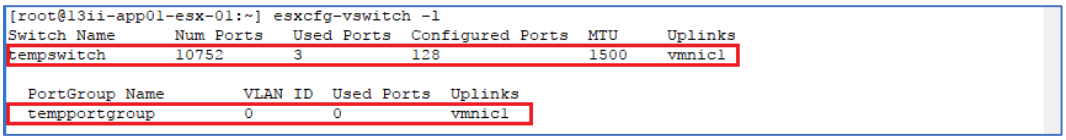
8. After confirming that the vmnic1 was removed from the DVS, run these commands to **create a temporary VSS and a portgroup with the vmnic1**:

```
esxcli network vswitch standard add -v tempswitch
esxcli network vswitch standard uplink add -u vmnic1 -v tempswitch
esxcli network vswitch standard portgroup add -p tempportgroup -v tempswitch
```



9. To confirm that VSS portgroup **tempportgroup** with **vmnic1** was created, run this command:

```
esxcfg-vswitch -l
```



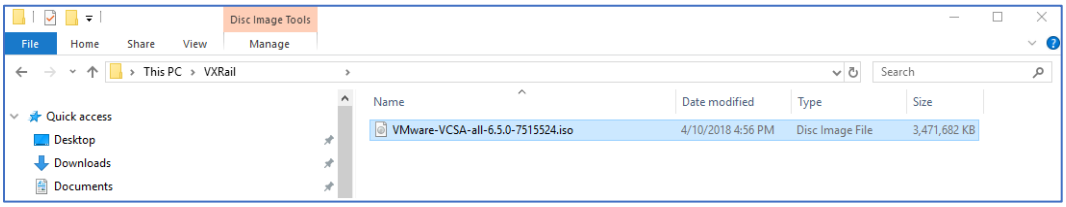
The system is ready for the actual restore operation.

Restore PSC to the Primary Node

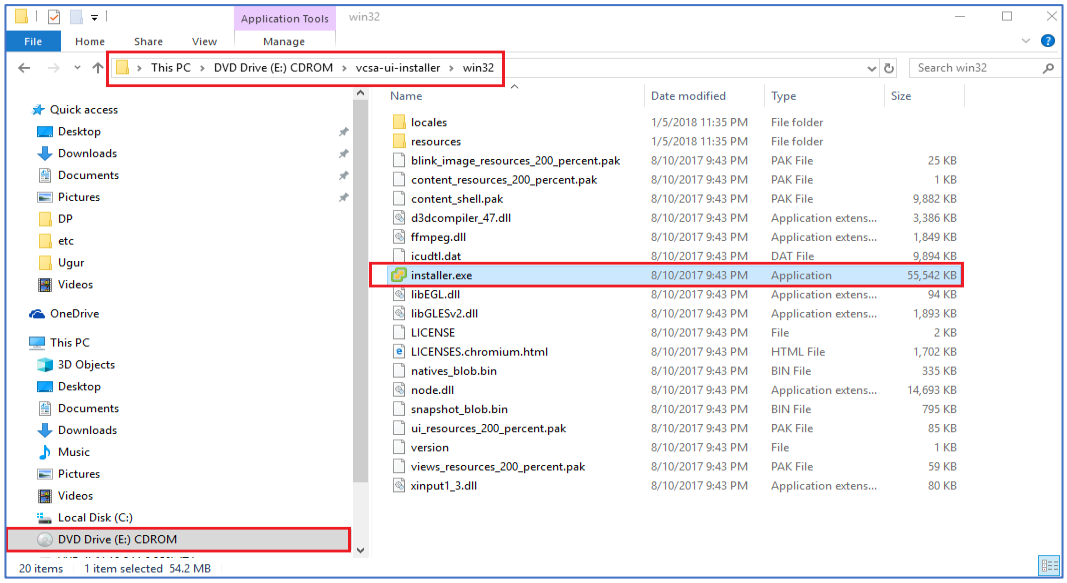
To begin the restore workflow, the VMware-VCSA-all-6.5.0.iso for vSphere 6.5 is required. You must use the specific vCSA installer ISO. It **must match** the vCSA version which was backed up (e.g., VMware-VCSA-all-6.5.0-7515524.iso).

To perform Stage 1 of the restore process:

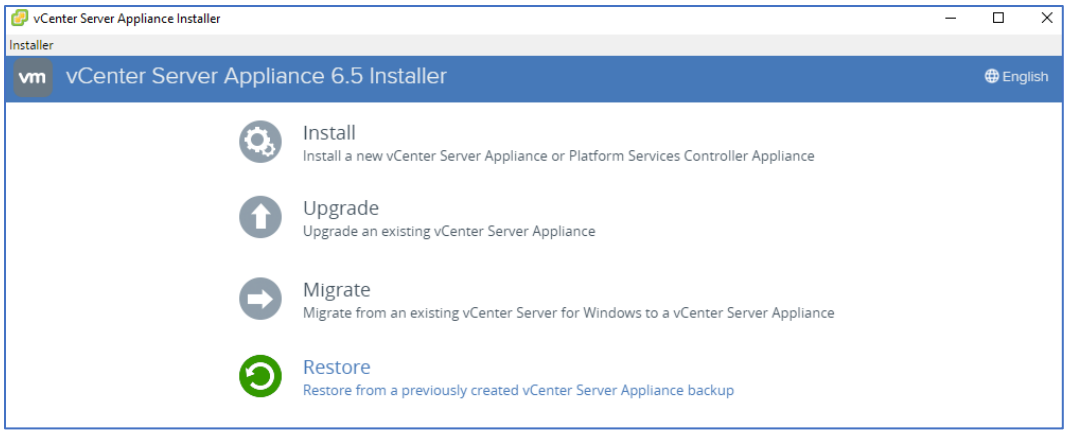
1. Mount the ISO file by double-clicking on the ISO file.



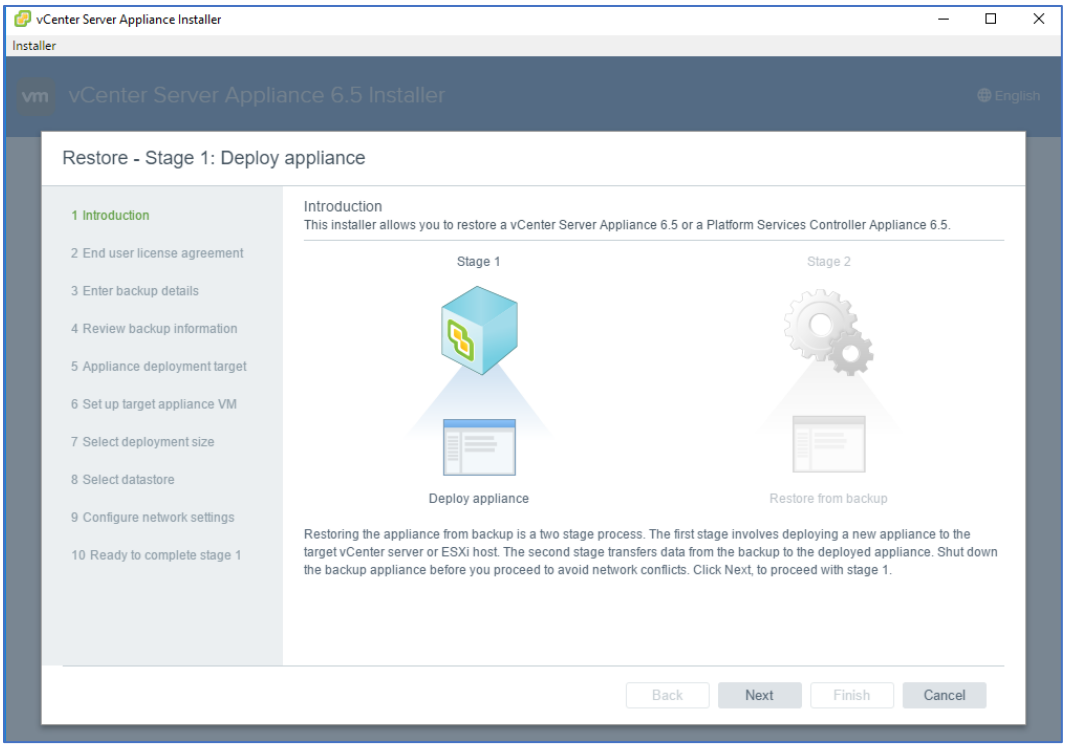
2. In the vCSA installer, navigate to the **vcsa-ui-installer** directory, and then to the subdirectory for your operating system, and run the **installer**.
   - For Windows OS, go to the *win32* subdirectory, and run the *installer.exe* file.
   - For Linux OS, go to the *lin64* subdirectory, and run the *installer* file.
   - For Mac OS, go to the *mac* subdirectory, and run the *Installer.app* file.



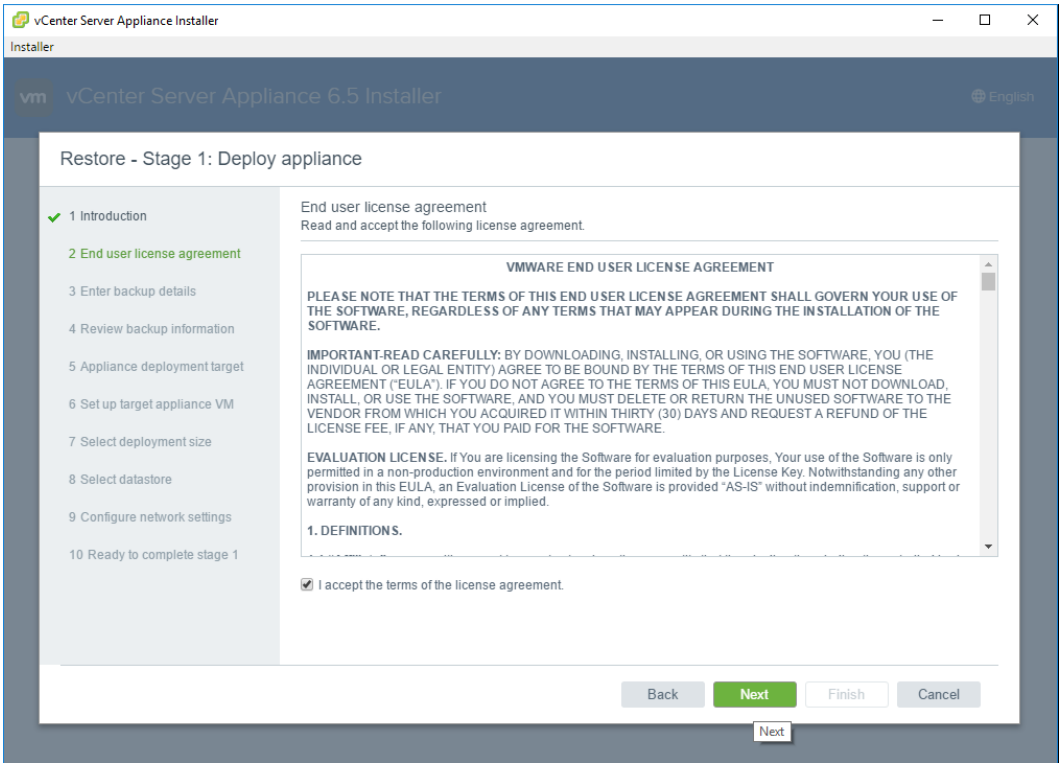
3. The vCenter Server Appliance Installer launches. The Installer allows you to restore a vCSA or a PSC. Click **Restore** to initiate the restore from a previously created appliance backup.



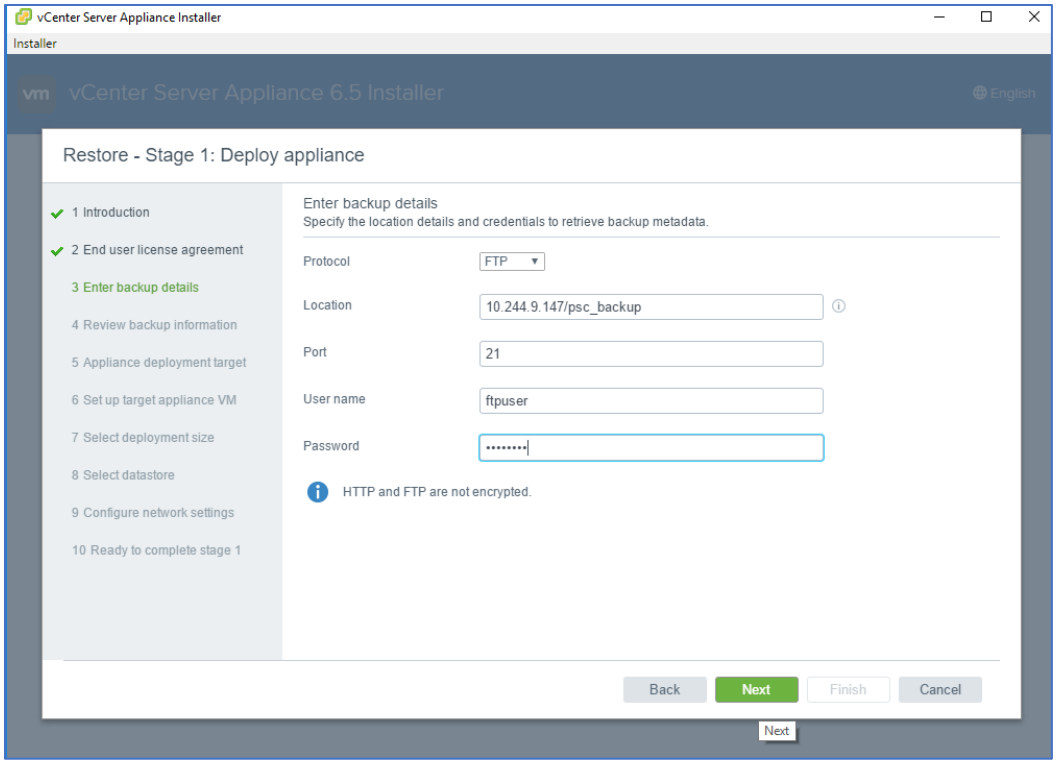
4. Restoring the appliance from backup is a two-stage process. The first stage is deploying a new appliance to the target ESXi host (i.e., the primary-node). The second stage transfers data from the backup to the deployed appliance. Click **Next** to proceed with Stage 1.



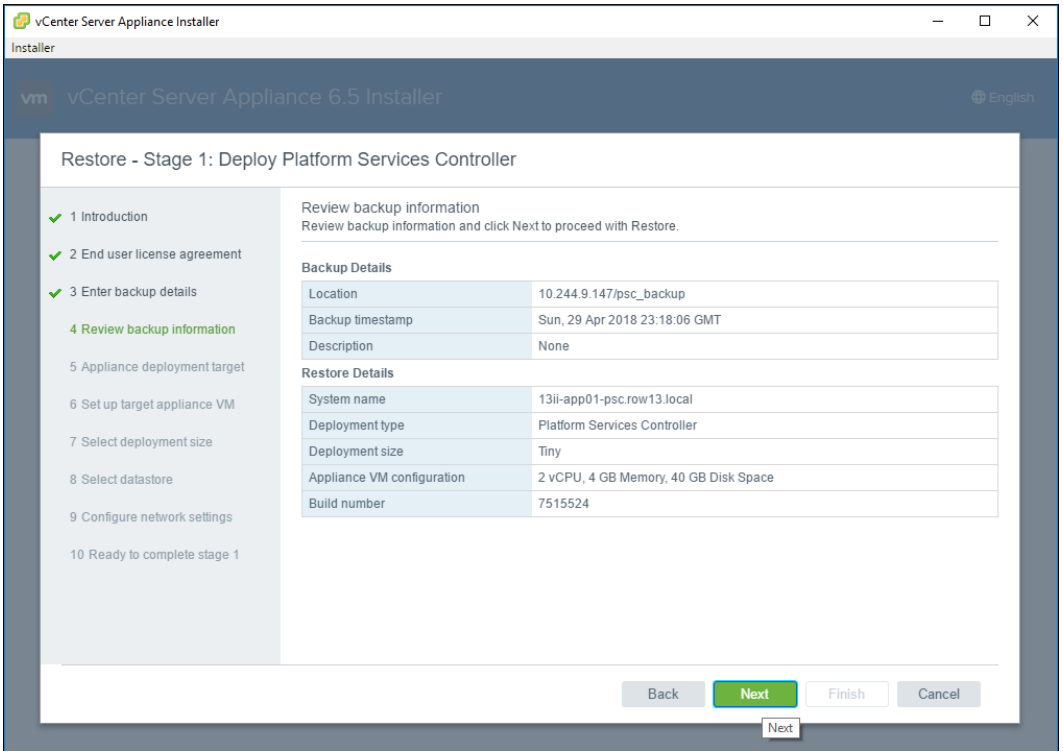
5. Accept the **End User License Agreement** (EULA) and click **Next**.



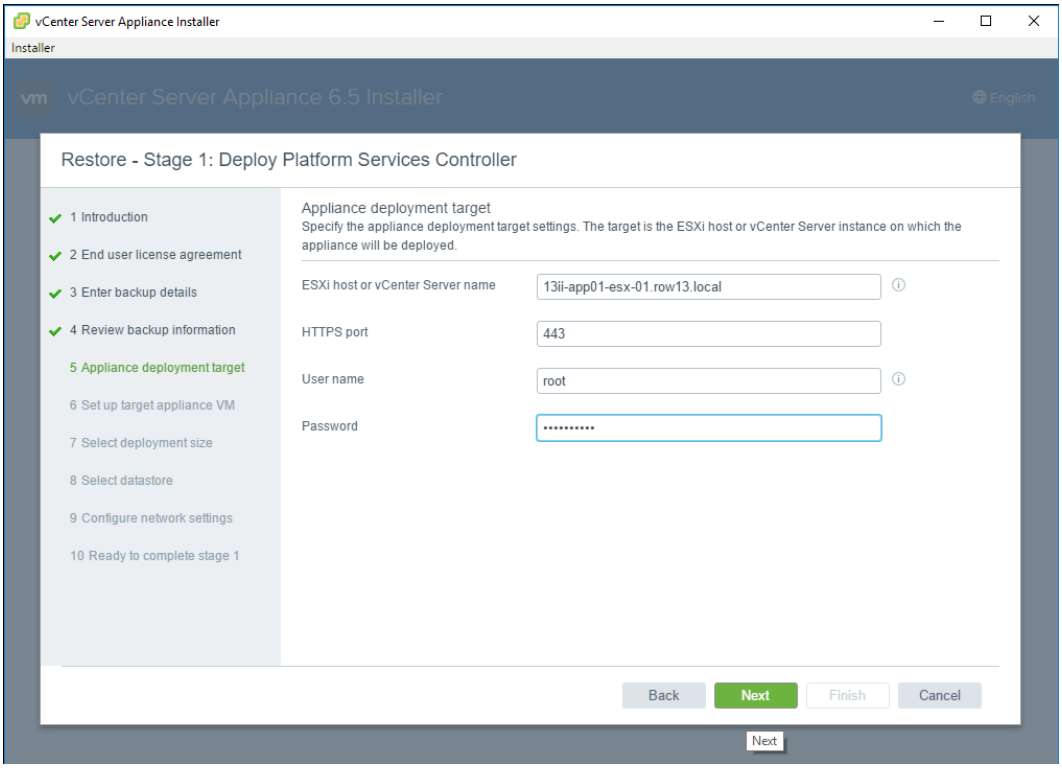
6. In the **Enter backup details** step, select the protocol and enter location details and credentials to retrieve backup metadata. Click **Next**.



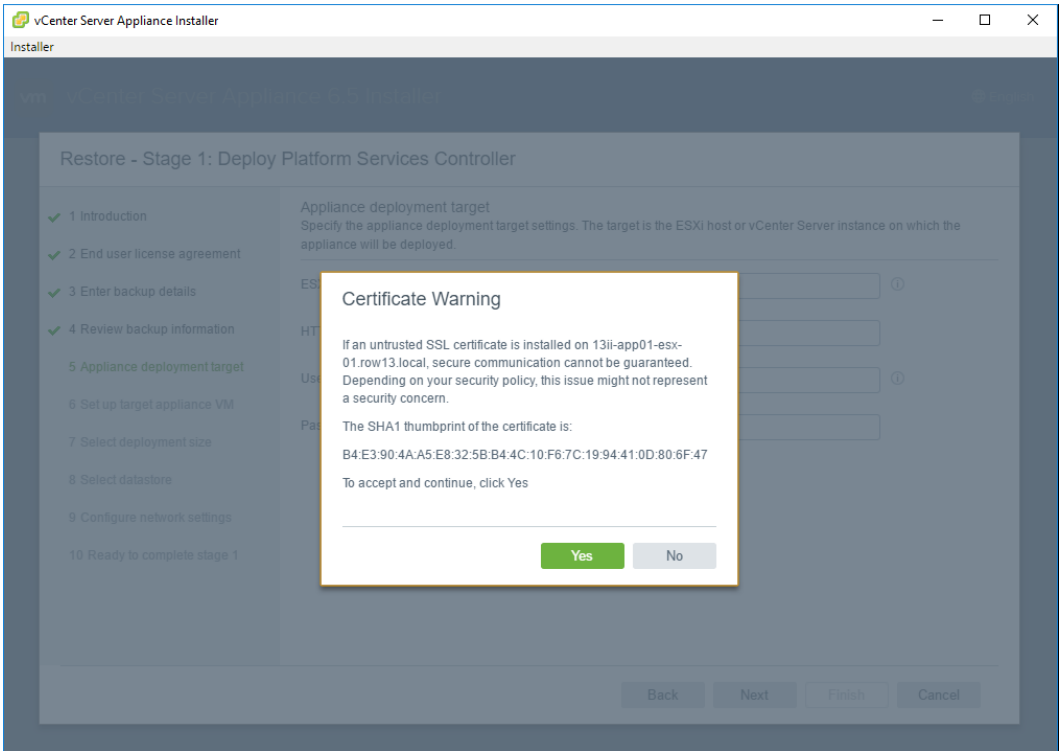
7. Review your backup information and click **Next** to proceed with the restore.



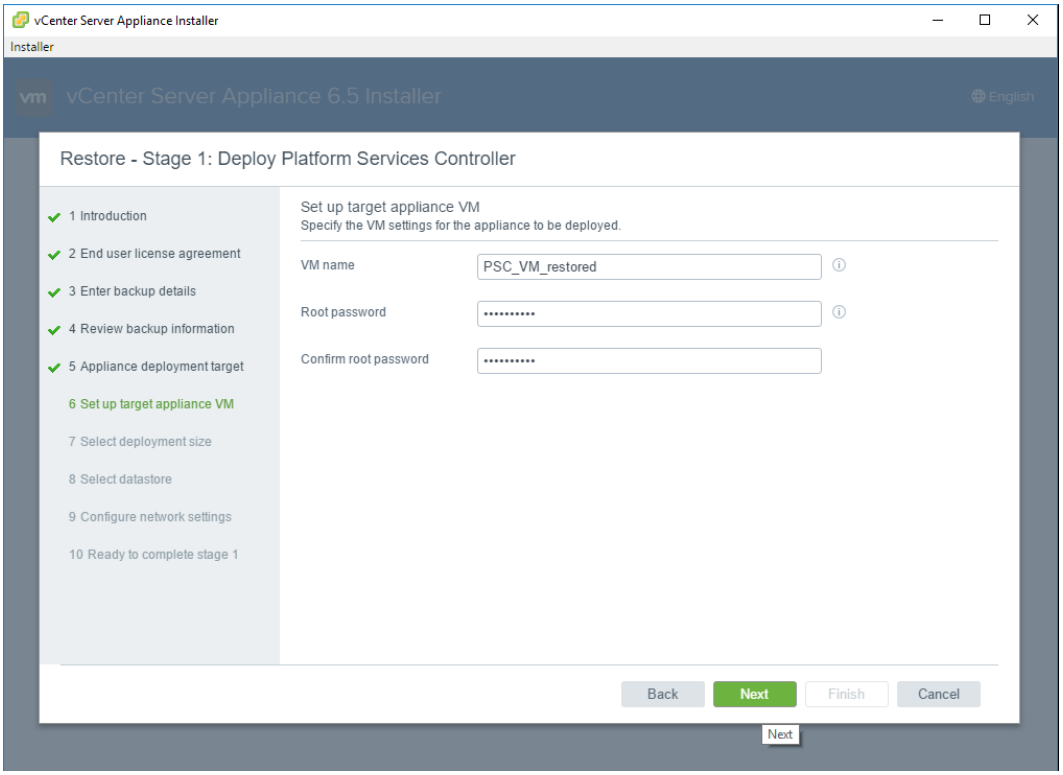
8. In the **Appliance deployment target** step, specify the appliance deployment target settings. The target is the ESXi host on which the appliance will be deployed. In this example, the primary ESXi node configured earlier with the temporary VSS must be set as the deployment target. Click **Next**.



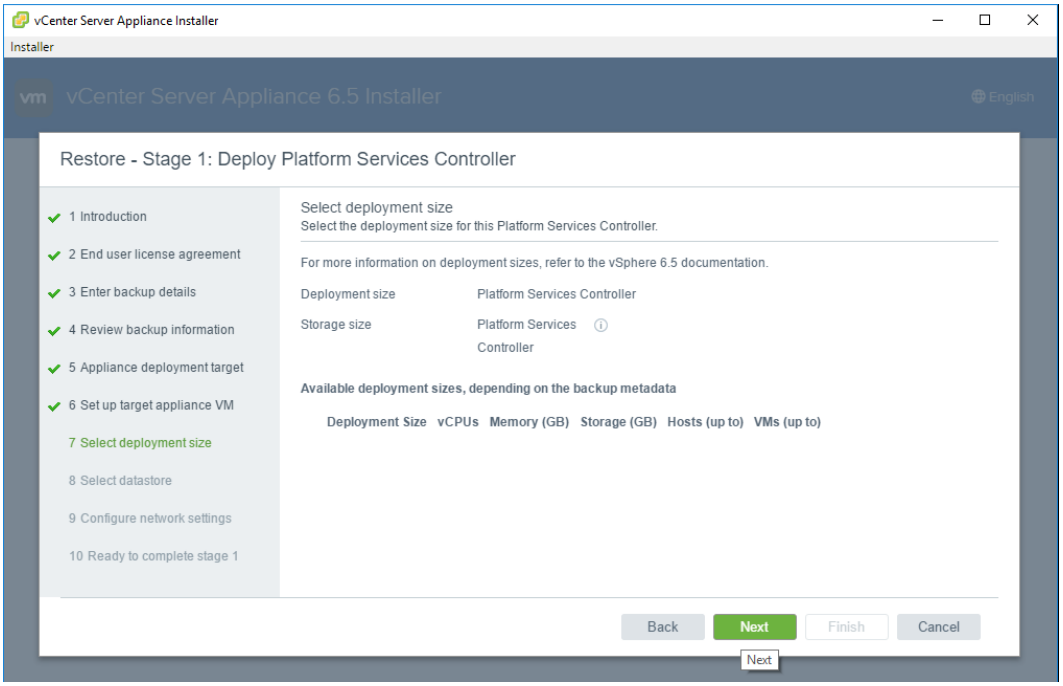
9. A Certificate Warning is presented. To accept and continue, click **Yes**.



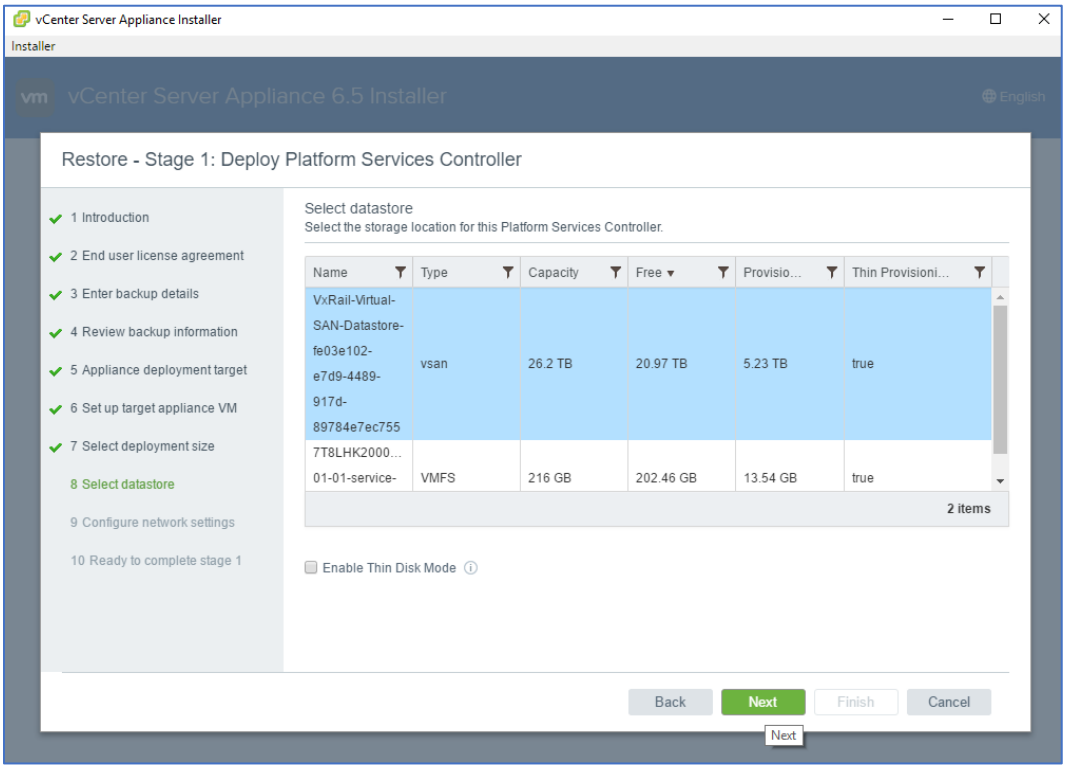
10. In the **Set up target appliance VM** step, specify the settings for the target appliance VM to be deployed. In this example, we named the VM *PSC_VM_restored*. Using the password of the old PSC for the target PCS is recommended. Click **Next**.



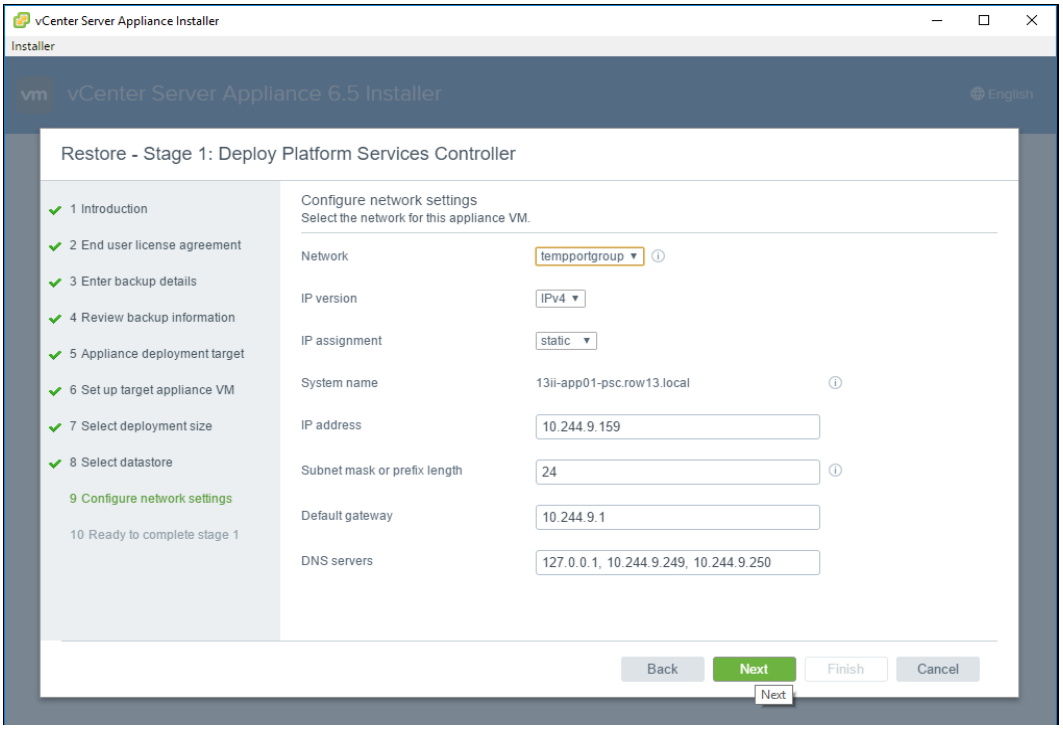
11. Depending on the backup metadata, available deployment sizes are listed. If there are choices, select one. For PSC, typically, there is no choice. Click **Next** to continue.



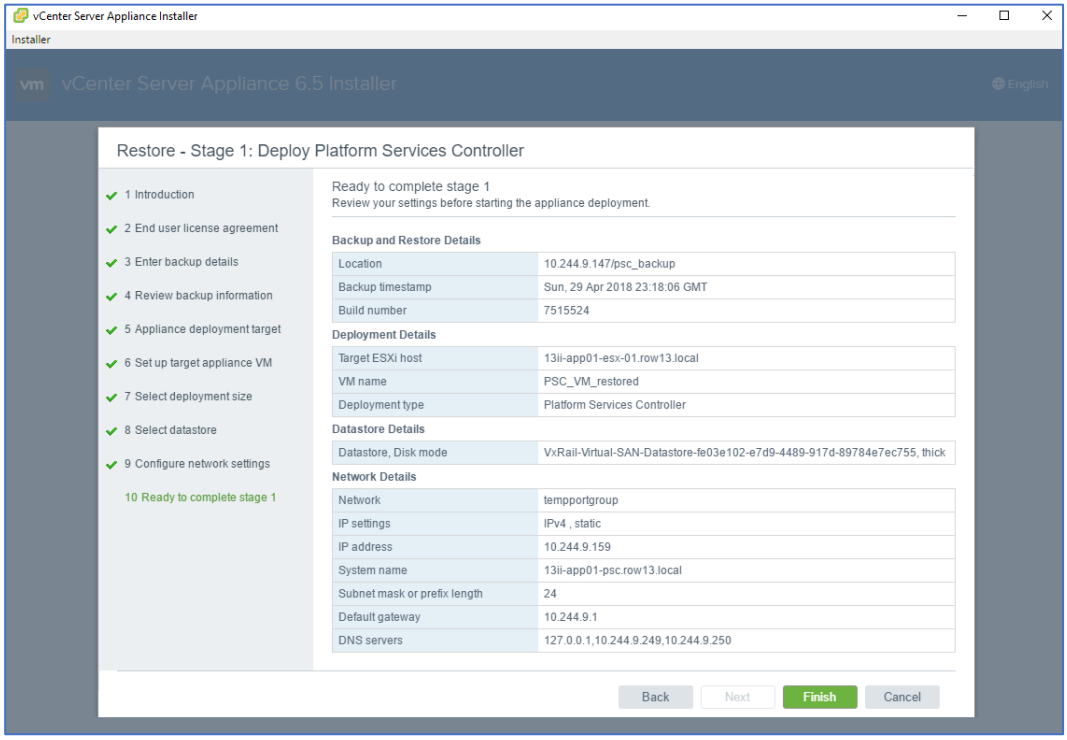
12. In the **Select datastore** step, select the **VSAN datastore** as the storage location for the PSC VM. Click **Next**.



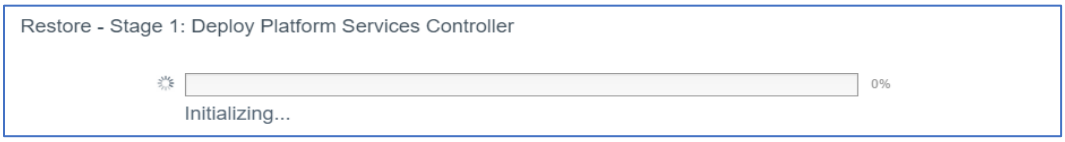
13. In the **Configure network settings** step, configure the network settings for the appliance VM. Select the **tempportgroup** created earlier. Note that the file-based restore procedure is for failed VxRail VCSA or PSC only. Do not make changes to the IP address, subnet mask, gateway and DNS in this step. If the IP address is changed, you will have to fix the VxRail Manager configuration after the restore. Refer to *Change the Internal vCSA Virtual Machine IP Address* or *Change the Internal PSC Virtual Machine IP Address* procedures in SolVe.

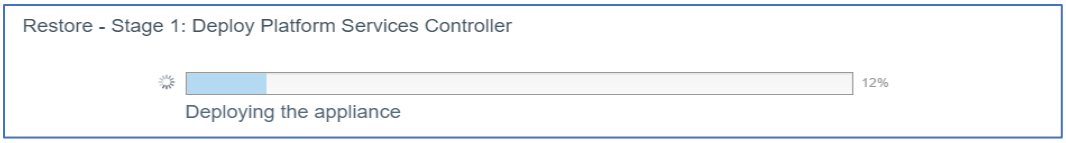


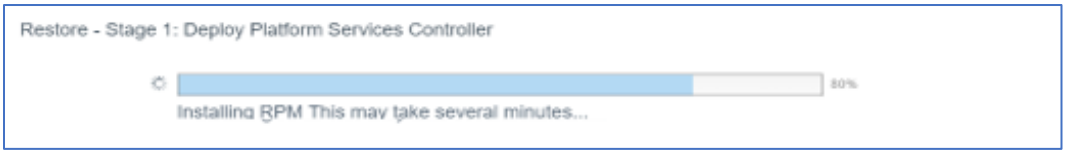
14. Review your settings, and then click **Finish** to start the appliance deployment.

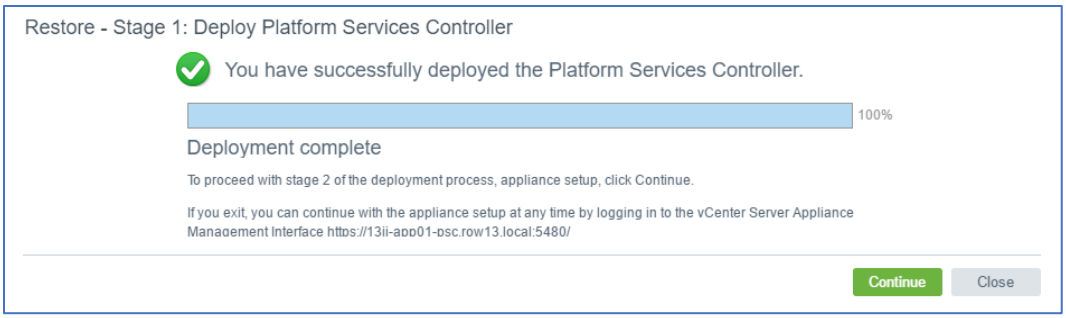


15. The appliance deployment is initiated. Observe the progress of the deployment process until it successfully completes. The completion of the deployment marks the end of the Stage 1 of the restore process. Click **Continue** to proceed to Stage 2.



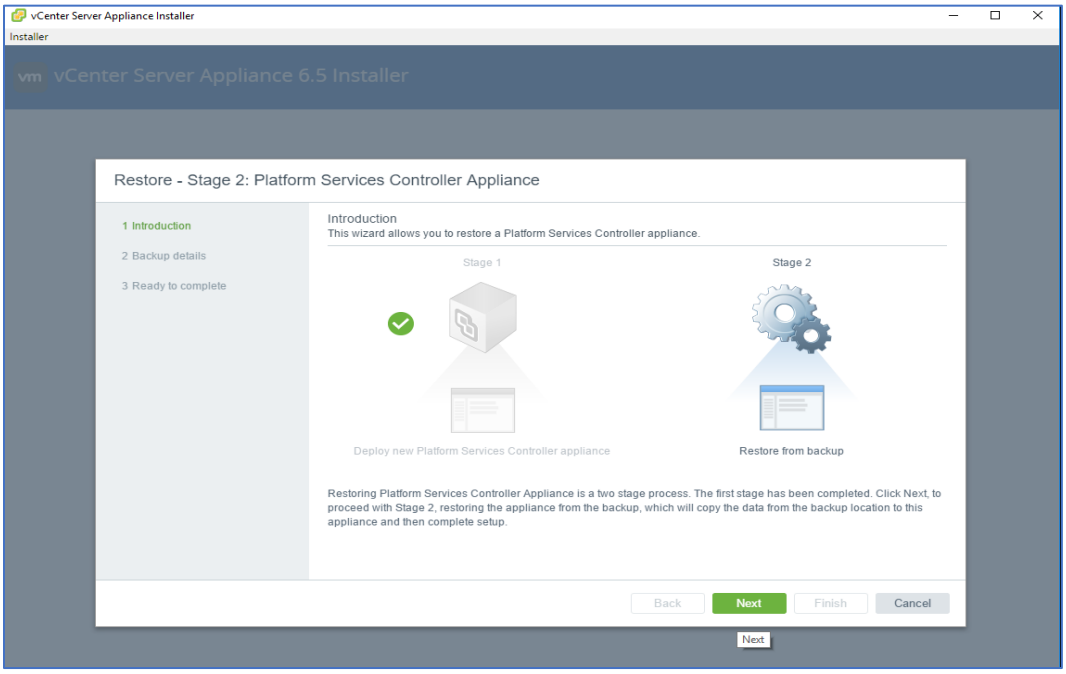




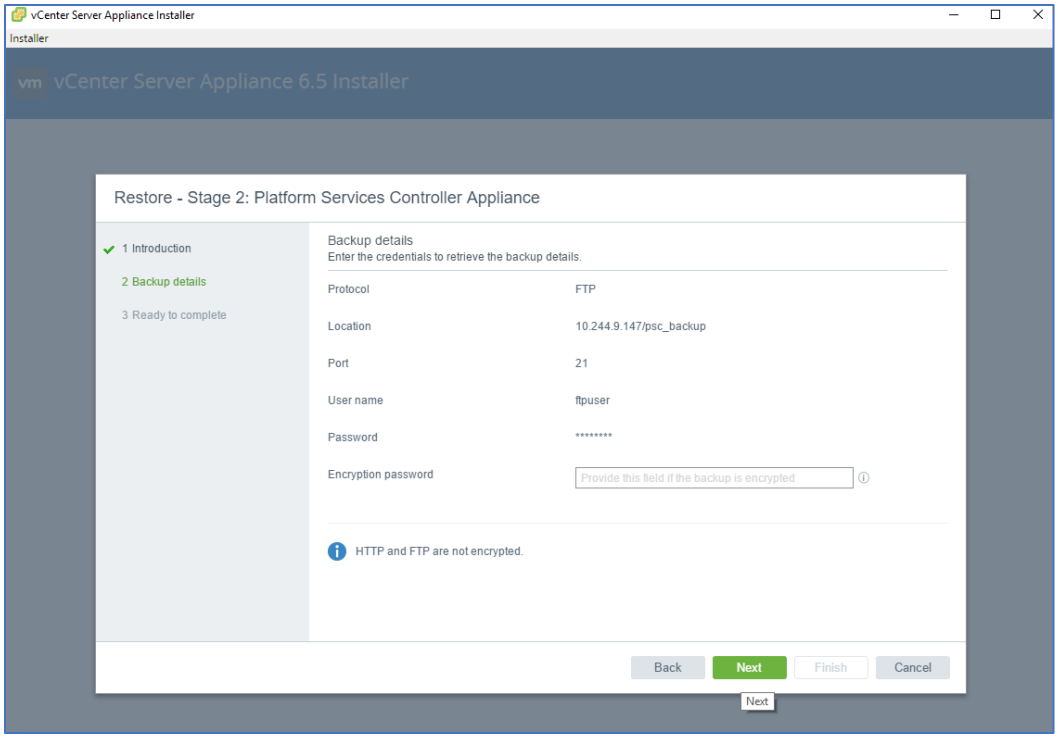


To perform Stage 2 of the restore process, follow these steps:

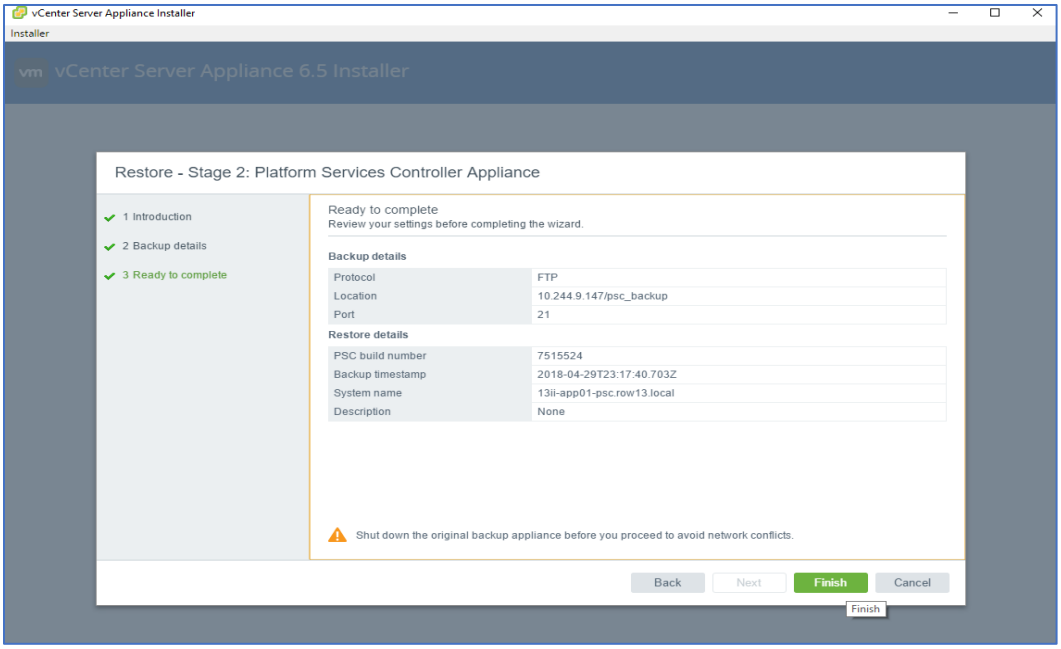
1. When the Stage 1 completes, the installer prompts for the Stage 2, which will copy the data from the backup location to this appliance and then complete the setup. In the **Introduction** step, click **Next** to proceed with Stage 2.



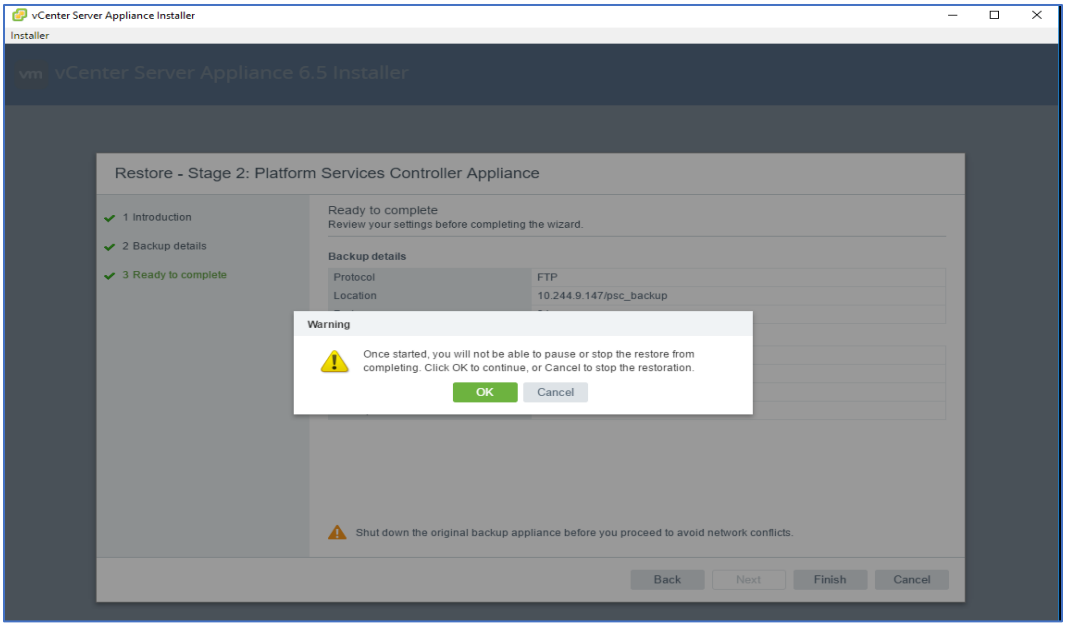
2. In the **Backup details** step, enter the credentials to retrieve the backup details. If the backup was performed with encryption, enter the encryption password here also. Click **Next**.



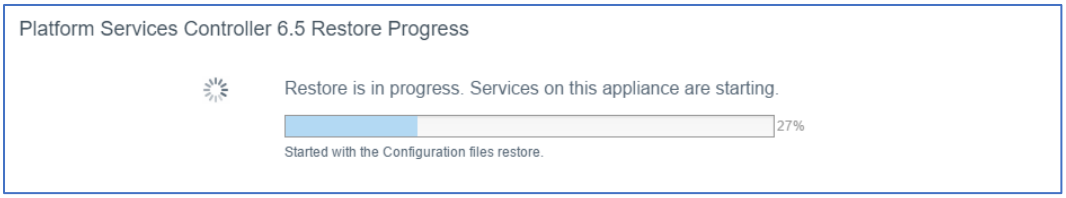
3. Review your settings before completing the wizard. Notice the warning at the bottom of the page that reminds you to shut down the original appliance to avoid network conflicts. Verify at this point that the original PSC is powered off. If you have not already done so per instructions stated earlier, power off the original PSC now. Click **Finish**.

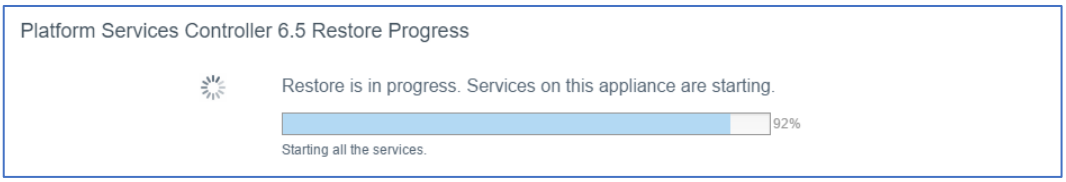


4. Once started, the restore operation cannot be paused or stopped. When presented with a warning message to that effect, click **OK** to start the restore operation.

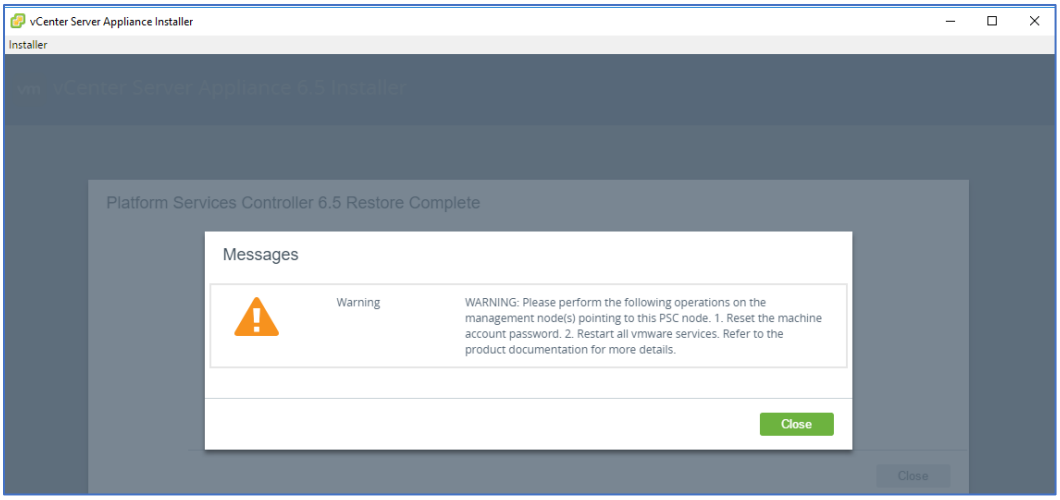


The restore operation starts.

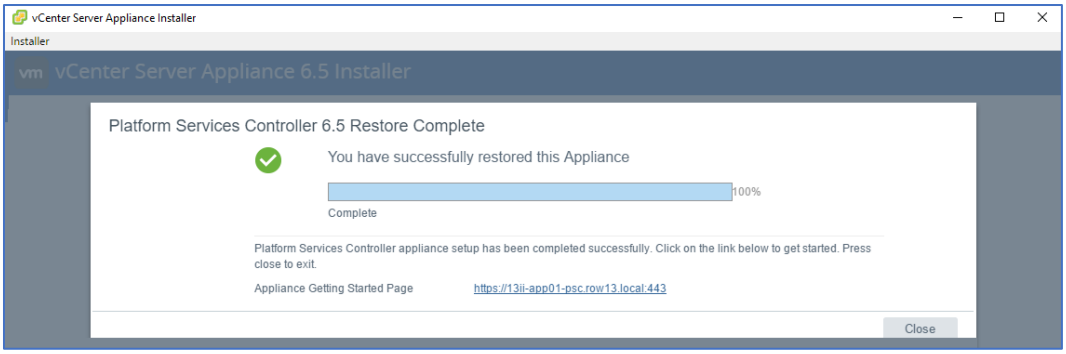




5. Just before the end of the restore operation, a warning is presented. This warning is for the vCSA service and it does not impact the PSC restore process. Click **Close**.



The restore operation completes. The PSC appliance is successfully restored.

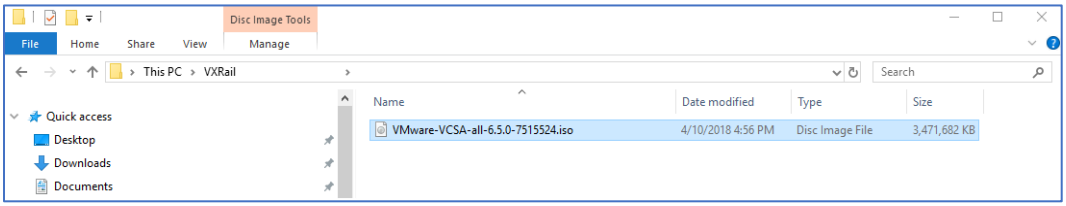


Restore vCSA to the Primary Node

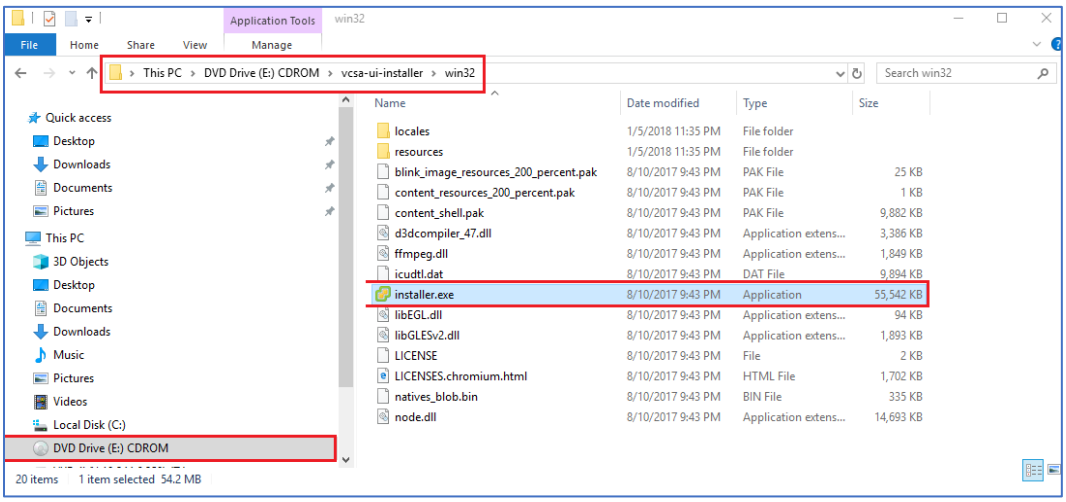
Once the internal PSC is restored, you can proceed to restore the internal vCSA. The restore process is the same for both types of appliances except for some minor differences. However, there is an additional and important post-restore step for vCSA only. To begin the restore workflow, the VMware-VCSA-all-6.5.0-xxxxxx.iso for vSphere 6.5 is required. You must use the specific vCSA installer ISO; it **must match** the vCSA version which was backed up (e.g., VMware-VCSA-all-6.5.0-7515524.iso).

To perform Stage 1 of the restore process:

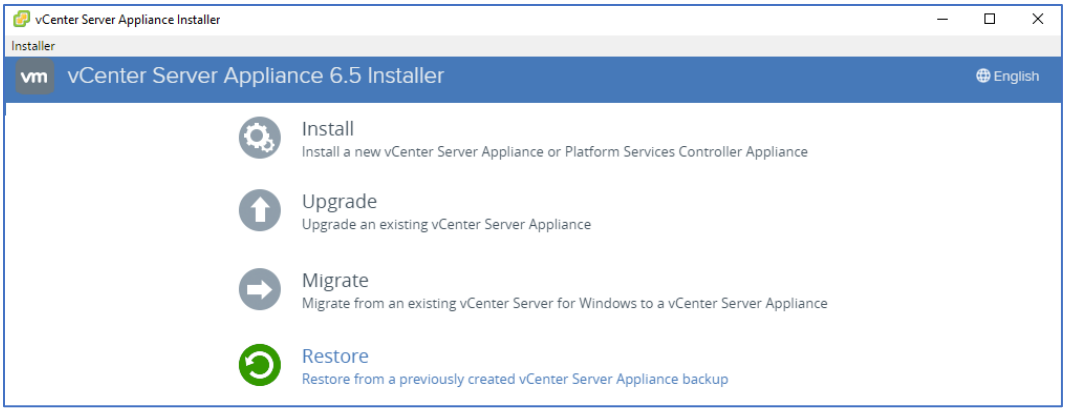
1. Mount the ISO file by double-clicking on the ISO file.



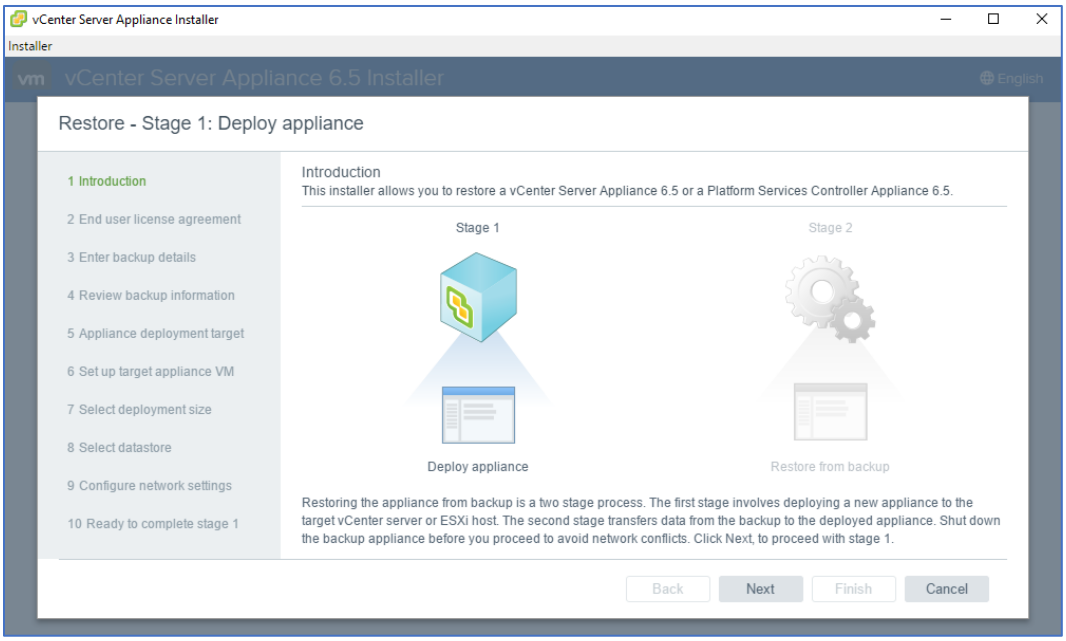
2. In the vCSA installer, navigate to the **vcsa-ui-installer** directory, and then to the subdirectory for your operating system, and run the **installer**.
   - For Windows OS, go to the *win32* subdirectory, and run the *installer.exe* file.
   - For Linux OS, go to the *lin64* subdirectory, and run the *installer* file.
   - For Mac OS, go to the *mac* subdirectory, and run the *Installer.app* file.



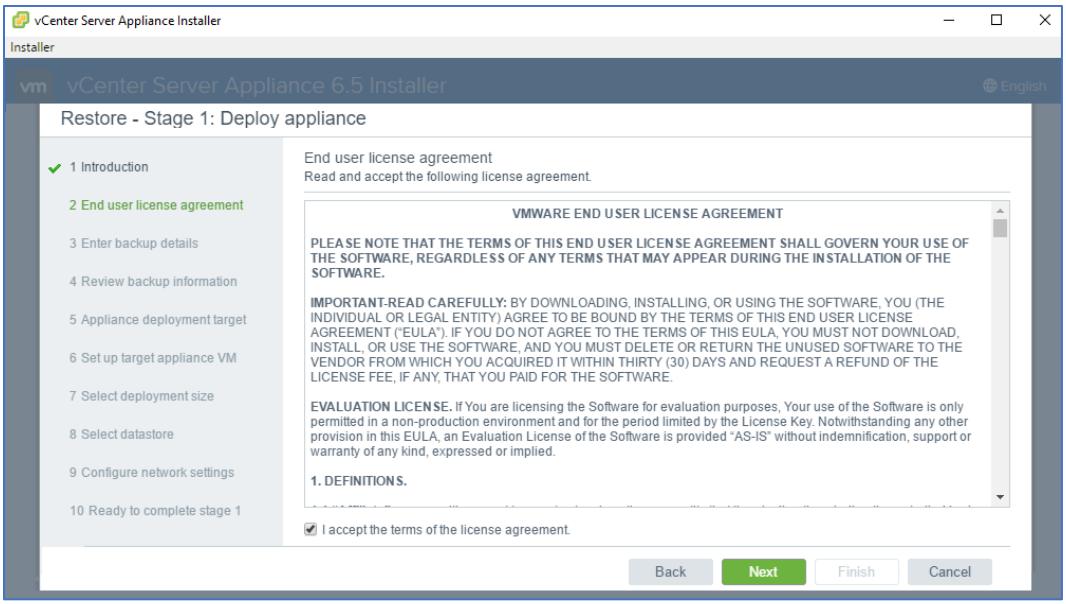
3. The vCenter Server Appliance Installer launches. The Installer allows you to restore a vCSA or a PSC. Click **Restore** to initiate the restore from a previously created appliance backup.



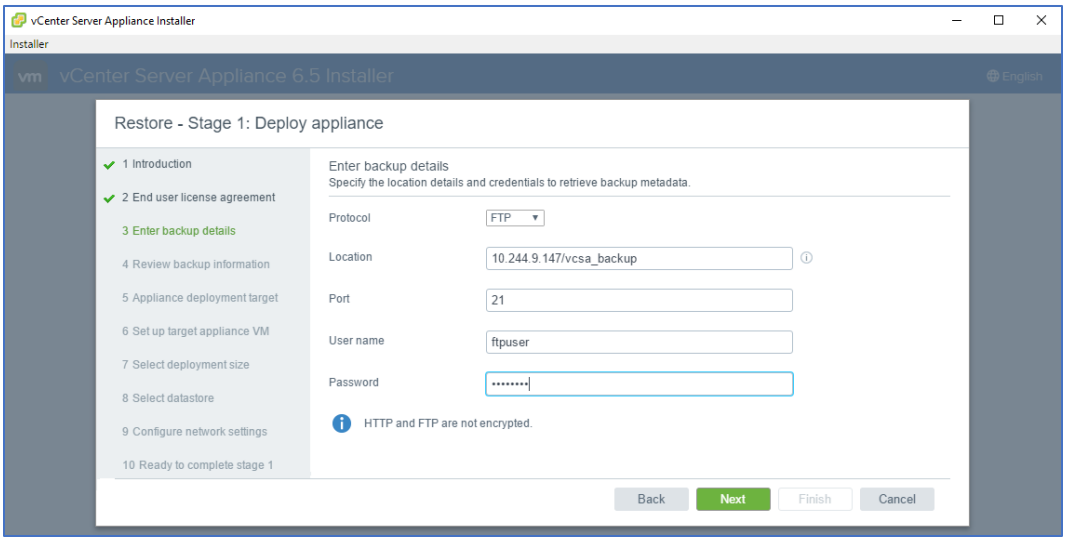
4. Restoring the appliance from backup is a two-stage process. The first stage deploys a new appliance to the target ESXi host (i.e., the primary-node). The second stage transfers data from the backup to the deployed appliance. Click **Next** to proceed with Stage 1.



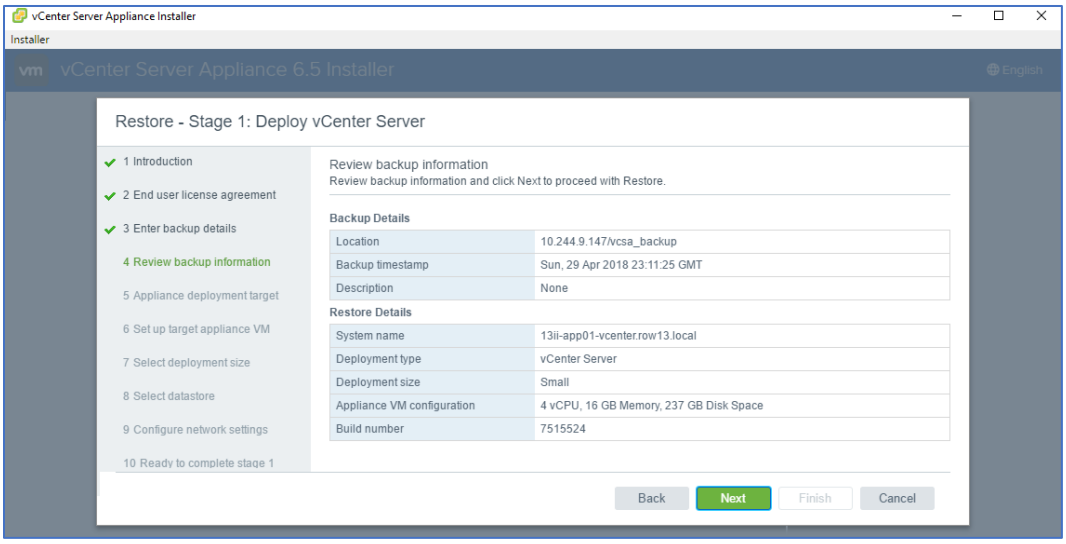
5. Accept the **End User License Agreement** (EULA) and click **Next**.



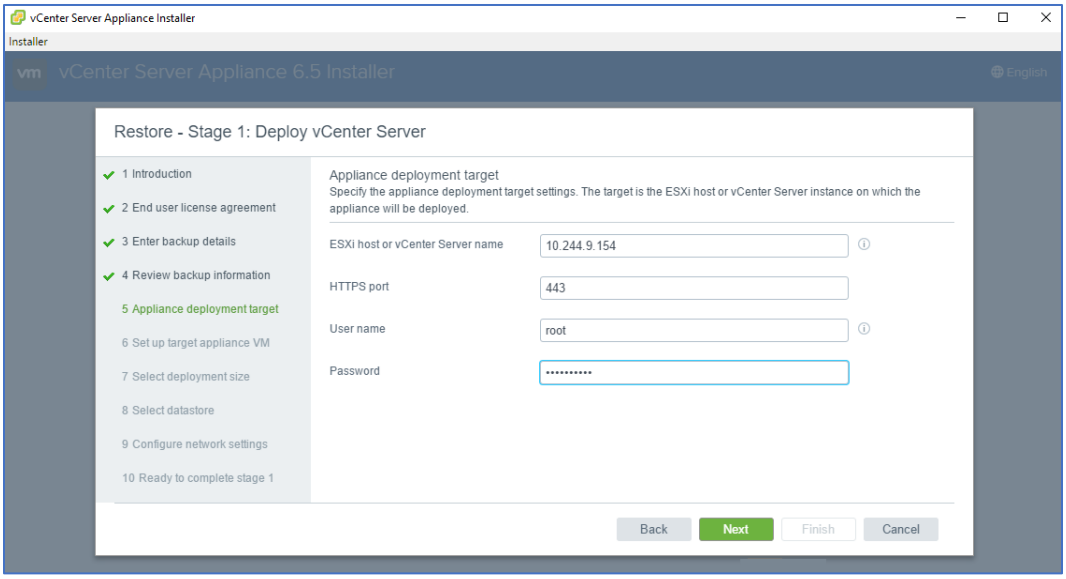
6. In the **Enter backup details** step, select the protocol and enter location details and credentials to retrieve backup metadata. Click **Next**.



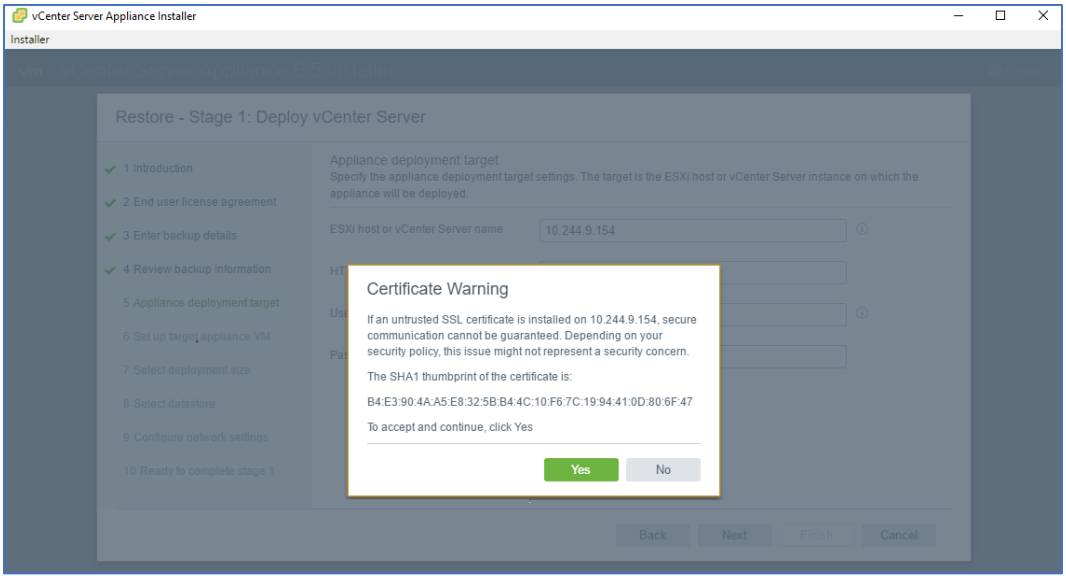
7. Review your backup information and click **Next** to proceed with the restore.



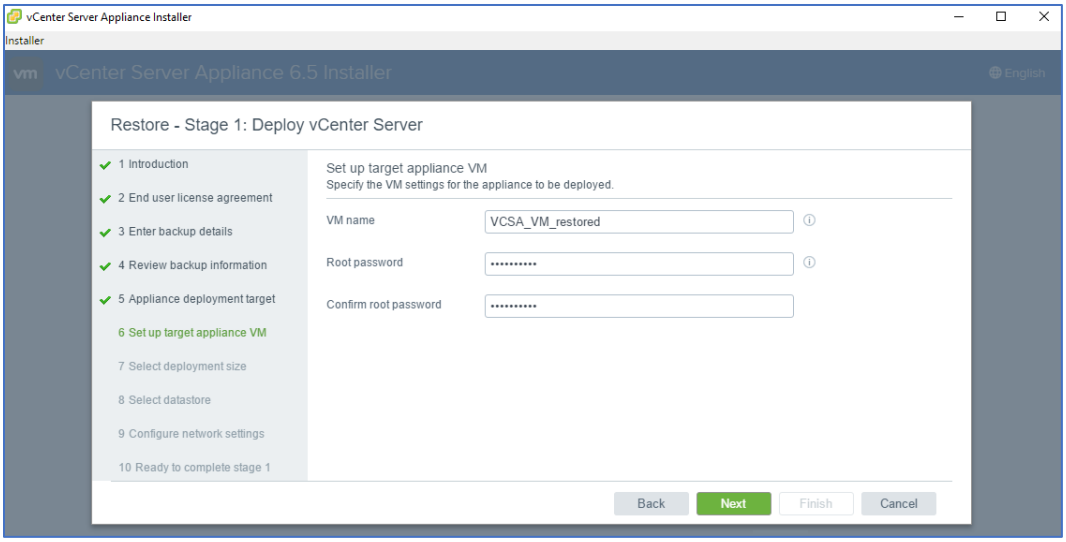
8. In the **Appliance deployment target** step, specify the appliance deployment target settings. The target is the ESXi host on which the appliance will be deployed. In this example, the primary ESXi node configured earlier with the temporary VSS was set as the deployment target. Click **Next**.



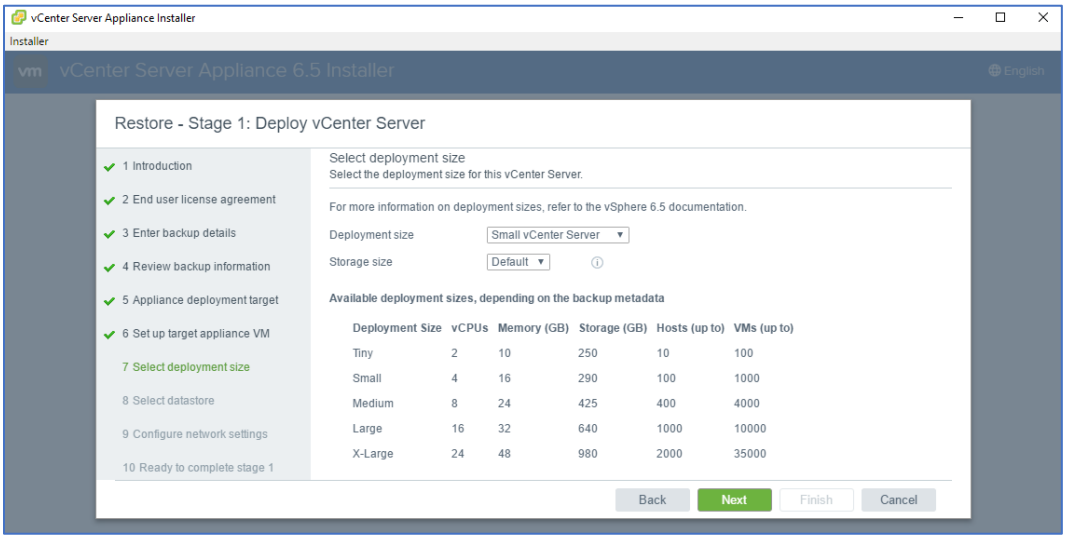
9. A Certificate Warning is presented. To accept and continue, click **Next**.



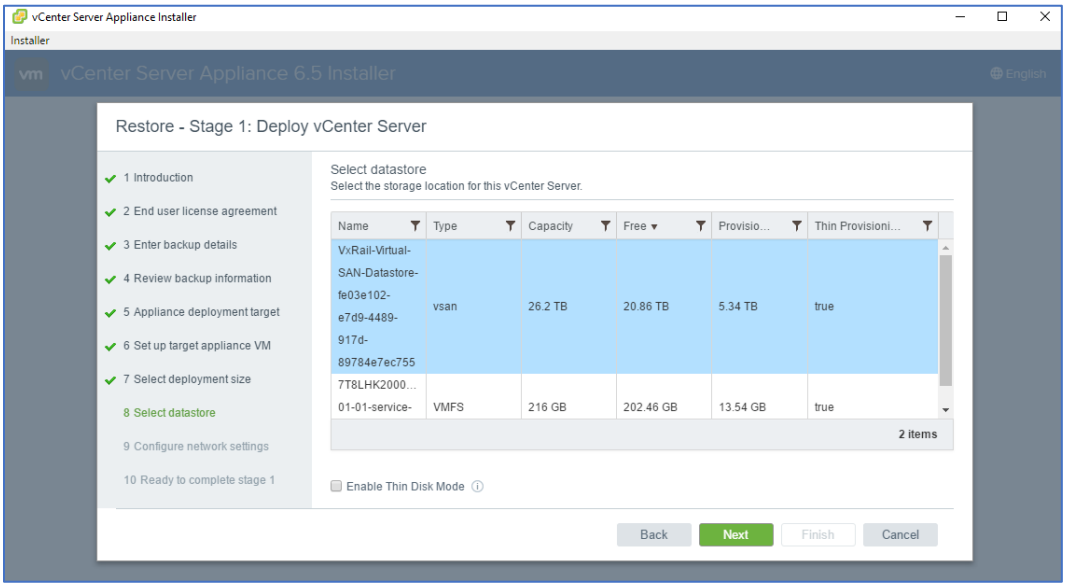
10. In the **Set up target appliance VM** step, specify the settings for the target appliance VM to be deployed. In this example, we named the VM *VCSA_VM_restored*. Using the password of the old VCSA for the target VCSA is recommended. Click **Next**.



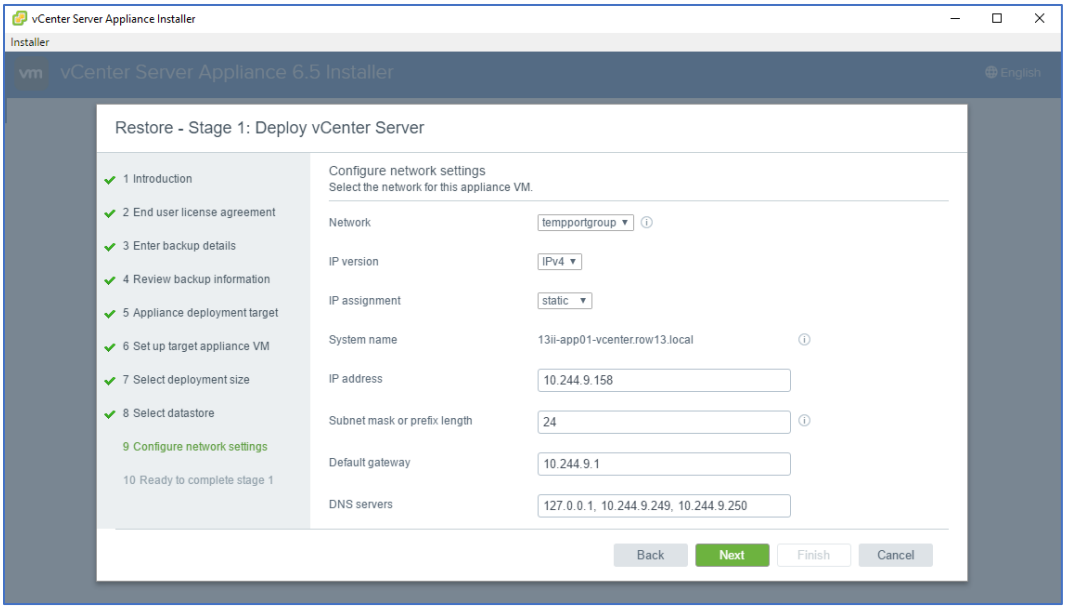
11. Depending on the backup metadata, available deployment sizes are listed. If there are choices, select one. However, the default values are recommended. Click **Next** to continue.



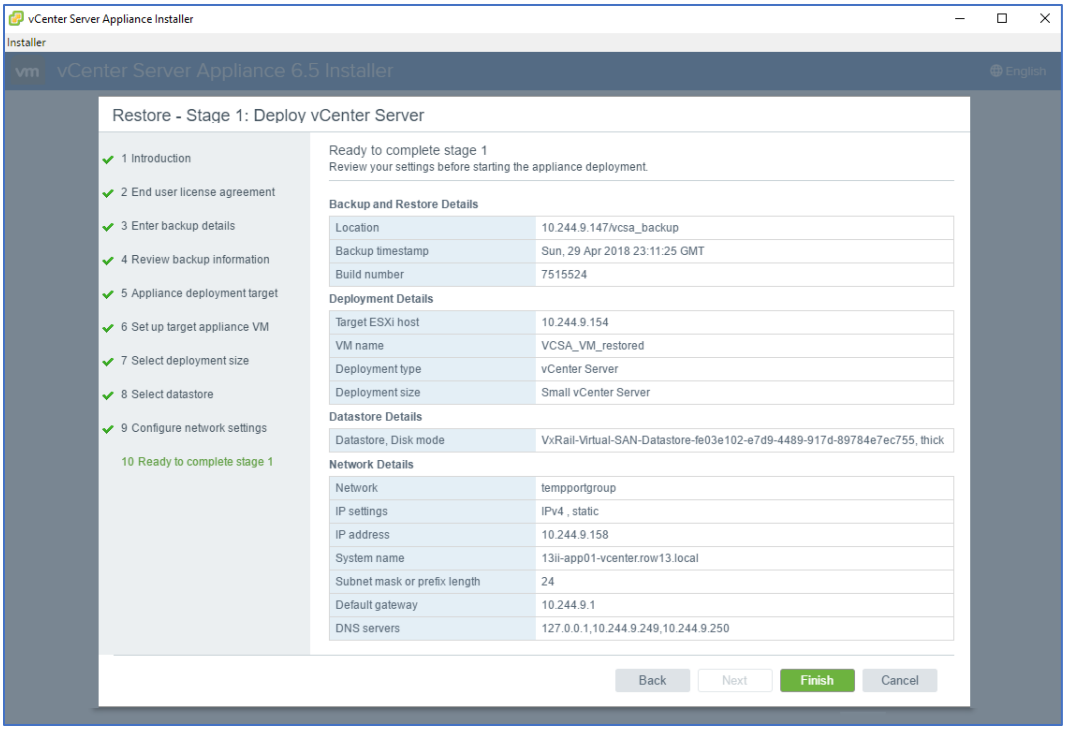
12. In the **Select datastore** step, select the **VSAN datastore** as the storage location for the VCSA VM. Click **Next**.



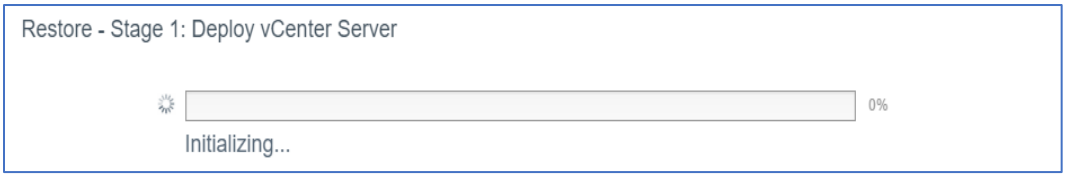
13. In the **Configure network settings** step, configure the network settings for the appliance VM. Select the **tempportgroup** created earlier. Note that the file-based restore procedure is only for failed VxRail VCSA or PSC. Do not make changes to the IP address, subnet mask, gateway and DNS in this step. If the IP address is changed, you will have to fix the VxRail Manager configuration after the restore. Refer to *Change the Internal vCSA Virtual Machine IP Address* or *Change the Internal PSC Virtual Machine IP Address* procedures in SolVe.

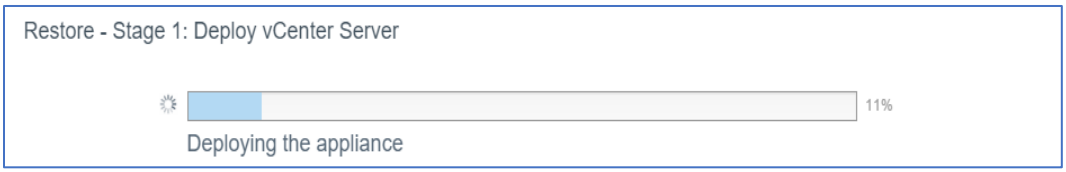


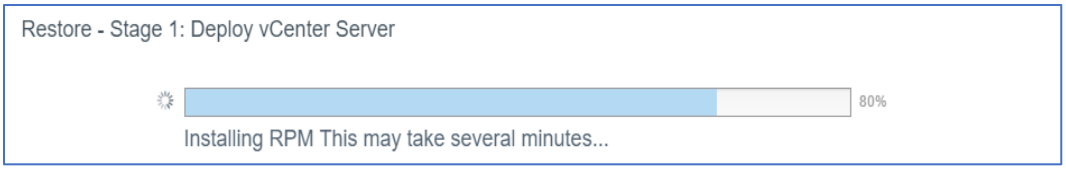
14. Review your settings, and then click **Finish** to start the appliance deployment.

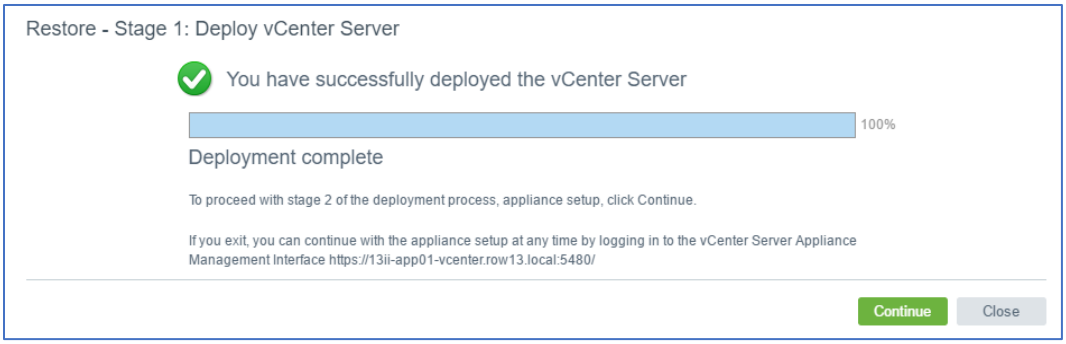


15. The appliance deployment is initiated. Observe the progress of the deployment process until it successfully completes. The completion of the deployment marks the end of the Stage 1 of the restore process. Click **Continue** to proceed to Stage 2.



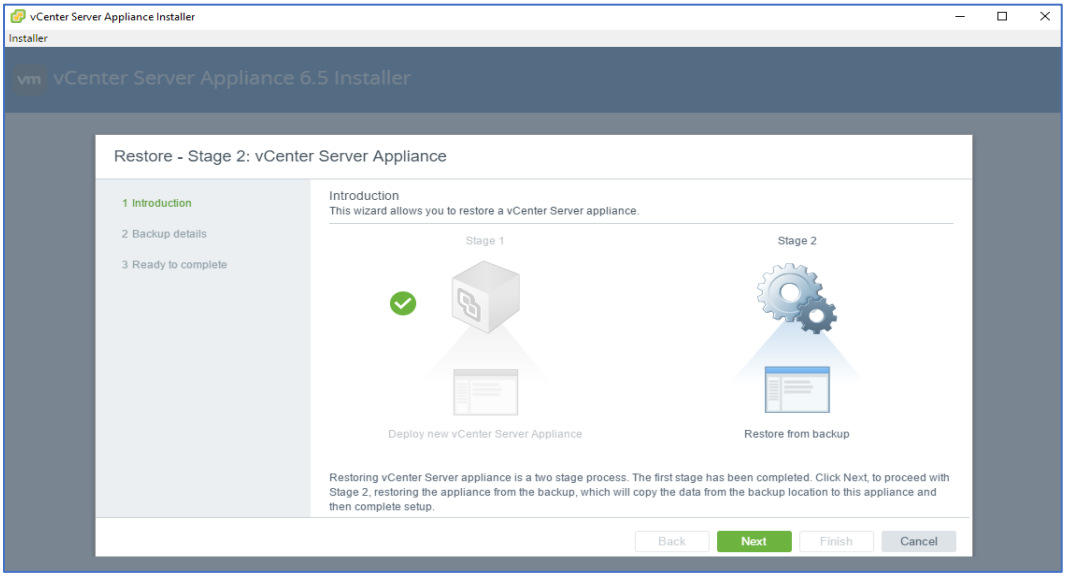




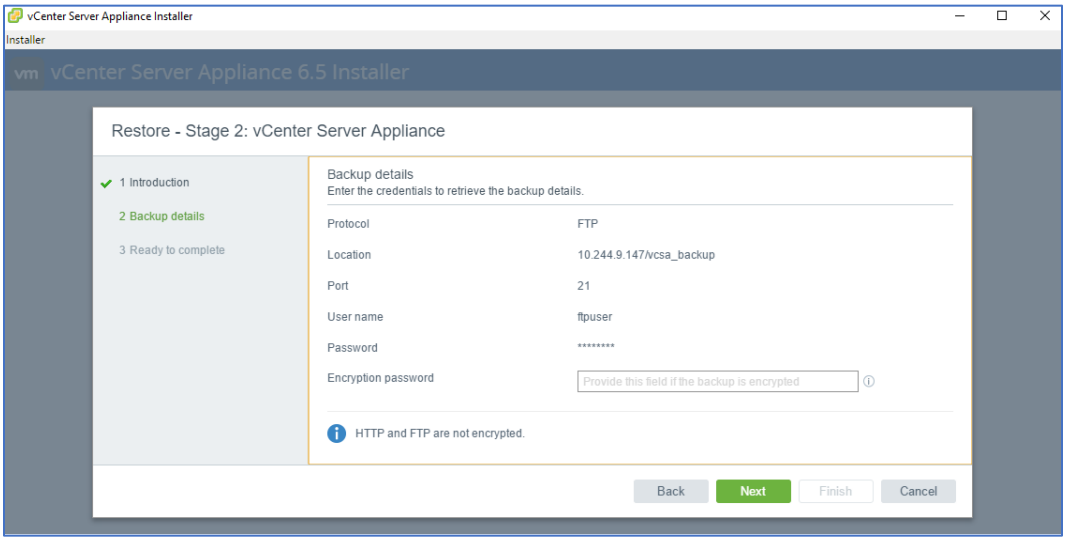


To perform Stage 2 of the restore process:

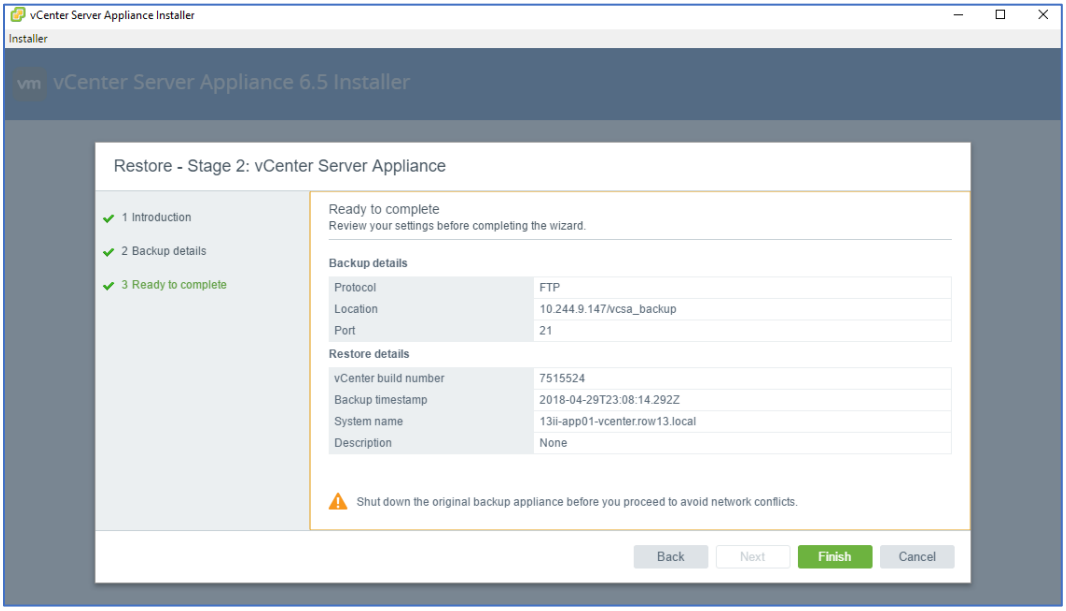
1. When the Stage 1 completes, the installer prompts for the Stage 2, which will copy the data from the backup location to this appliance and then complete the setup. In the **Introduction** step, click **Next** to proceed with Stage 2.



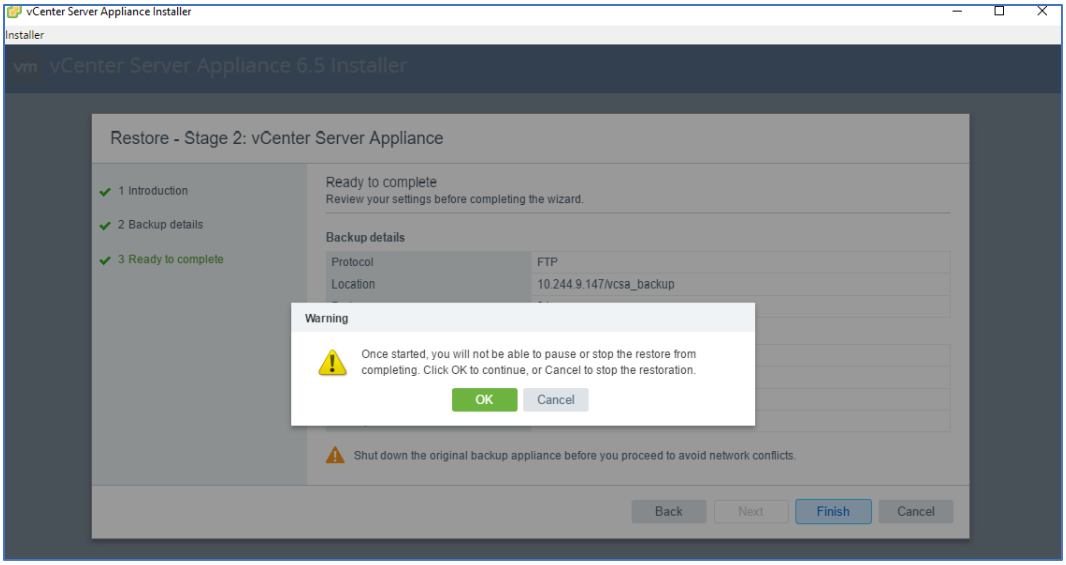
2. In the **Backup details** step, enter the credentials to retrieve the backup details. If the backup was performed with encryption, enter the encryption password here also. Click **Next**.



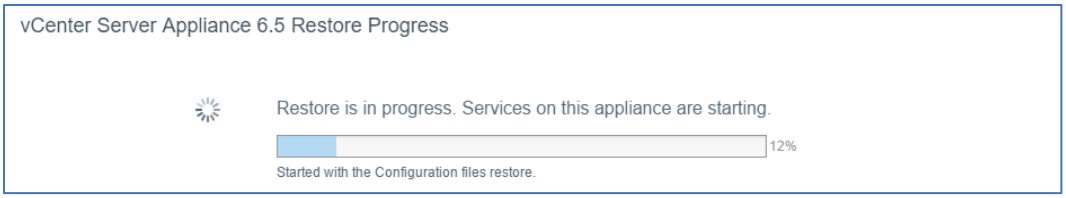
3. Review your settings before completing the wizard. Notice the warning at the bottom of the page that reminds you to shut down the original appliance to avoid network conflicts. Verify at this point that the original PSC is powered off. If you have not already done so, power off the original PSC now. Click **Finish**.

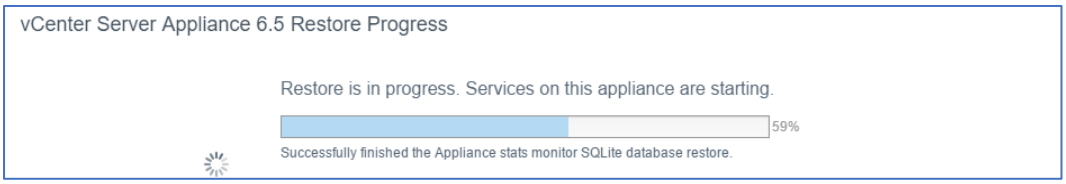


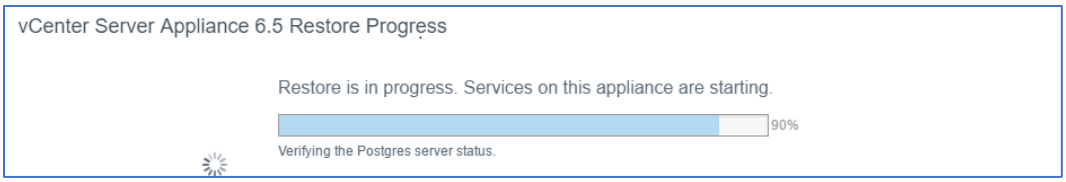
4. Once started, the restore operation cannot be paused or stopped. When presented with a warning message to that effect, click **OK** to start the restore operation.

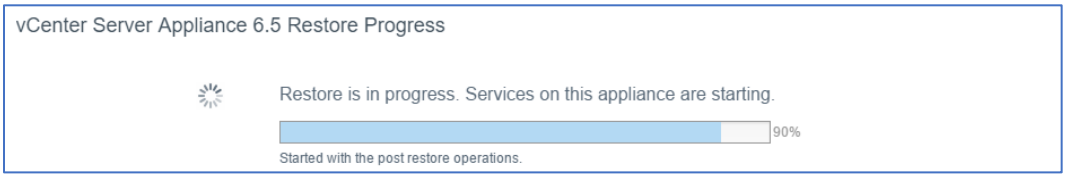


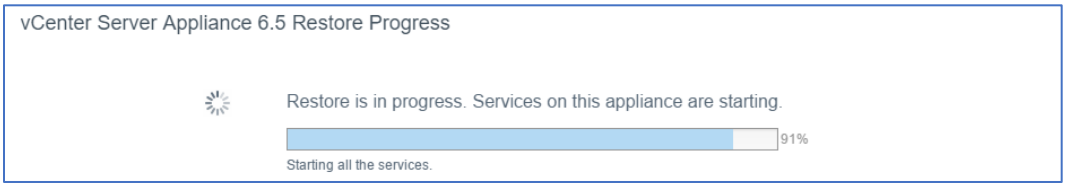
The restore operation starts.



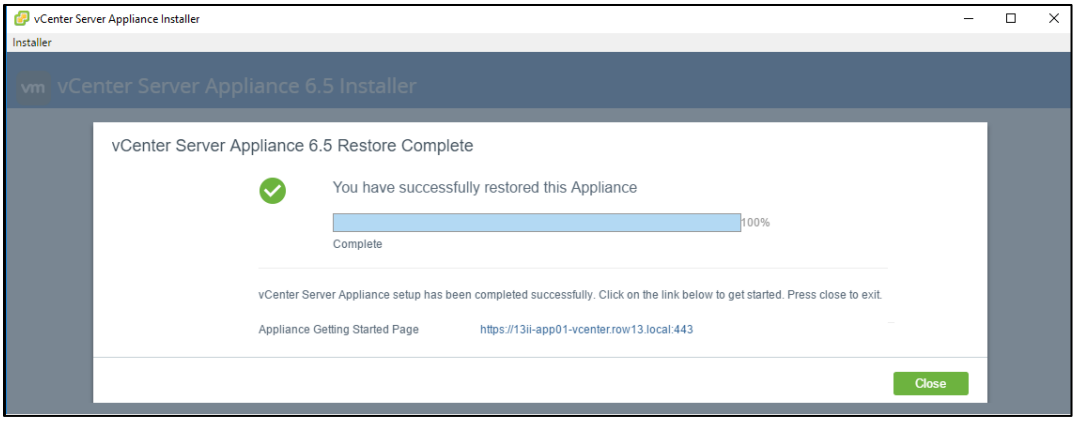




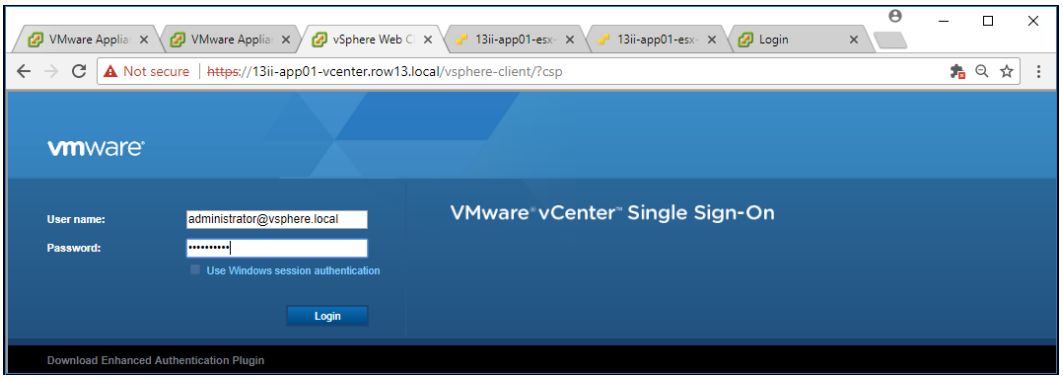


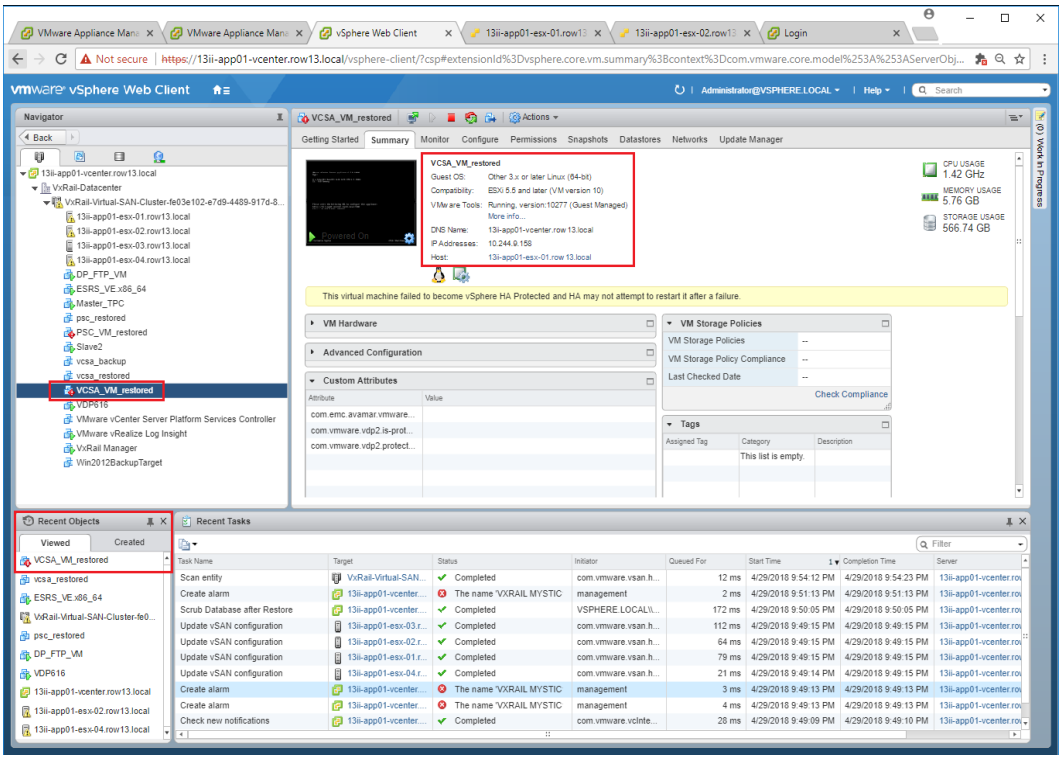


The restore operation completes. The vCSA appliance is successfully restored.



5. Log into the vSphere Web Client to verify.



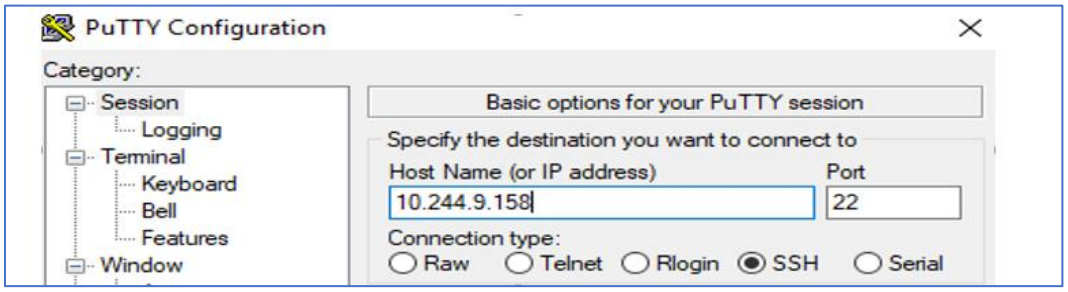


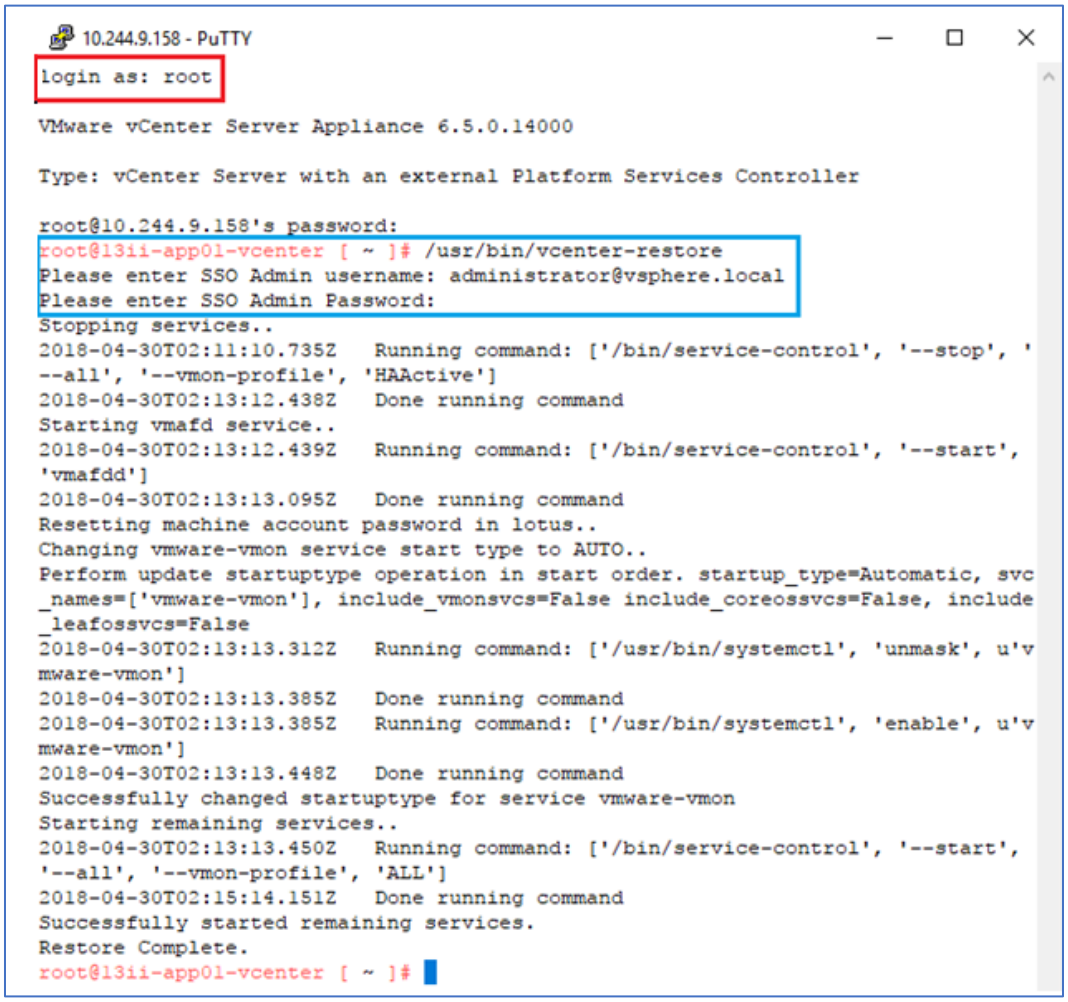
6. Run a post-recovery script to complete the restore process (this is only for vCSA, not applicable to PSC). Log into the bash shell of the newly restored vCSA via Putty or via the VM console on the vSphere Web Client, and run this command:

```
/usr/bin/vcenter-restore
```

- Note that the script prompts for the SSO administrator username and password (e.g., administrator@vsphere.local) to execute.
- Note that in vSphere 6.0, the script name is *psc-restore*, not *vcenter-restore*; i.e.,

```
/usr/bin/psc-restore
```





Delete the Old vCSA and PSC VMs

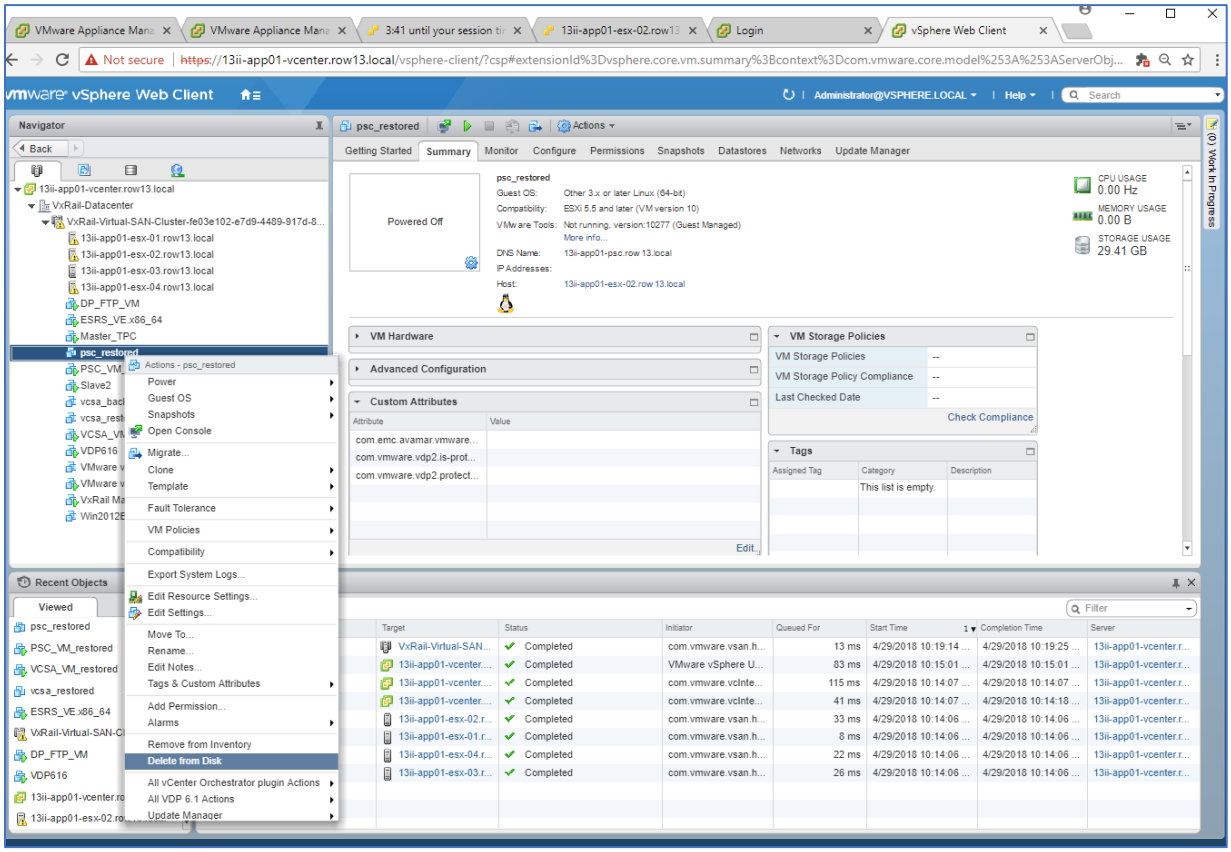
It is a best practice to delete the old vCSA and PSC VMs once the recovery operations are completed. Once the internal vCSA and PCS are restored, the vSphere Web Client becomes accessible. When logged into the vSphere Web Client, you might face either of these two situations:

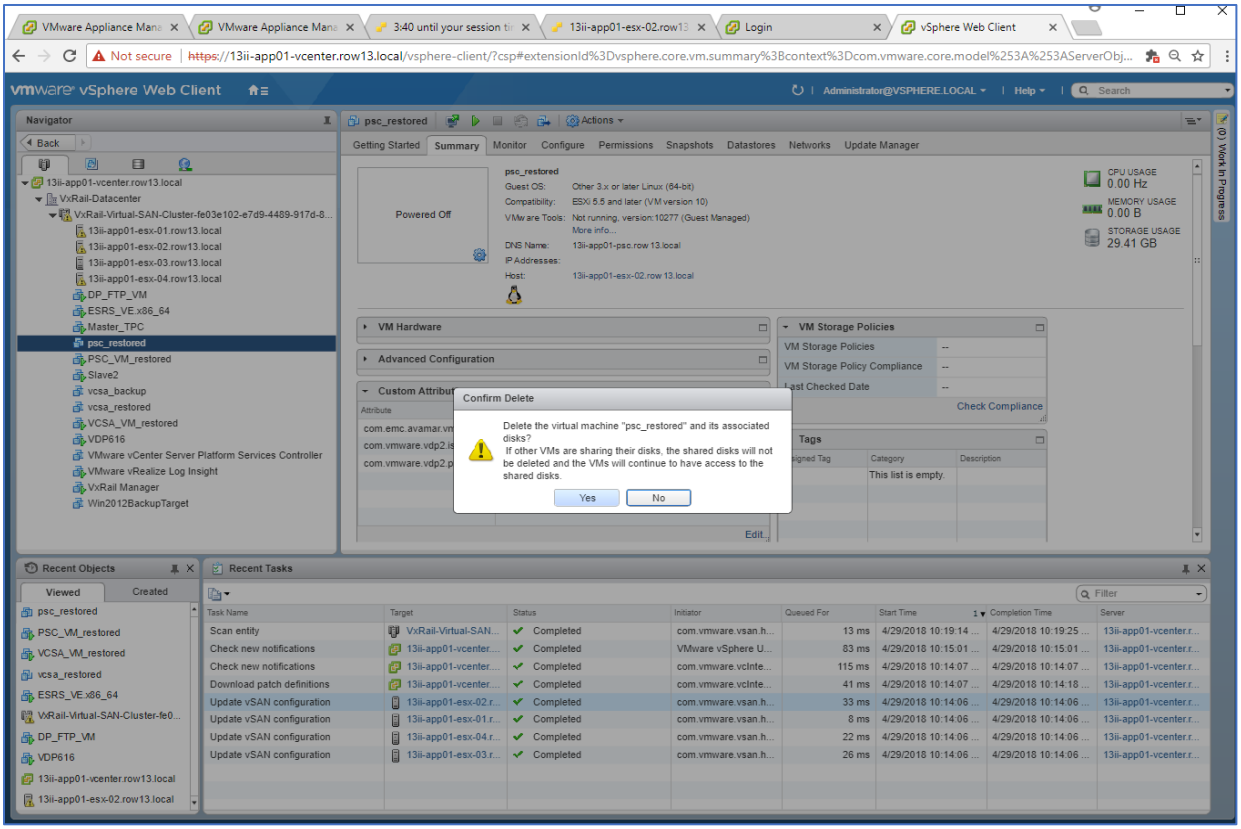
1. The old vCSA VM and/or the old PSC VM is in normal power off state.
2. The old vCSA VM and/or the old PSC VM is in orphaned state. This happens if the old VMs are removed before the restore procedure.

Deleting VMs in Power-off State

If an old VM is in the power-off state, you simply need to delete it from disk as follows:

1. **Right-click-VM > Delete from Disk** and then click **Yes** to confirm the delete action when prompted as shown in the following screen shots where the name of the old PSC VM is *psc_restored* and the name of the restored PSC is *PSC_VM_restored*.

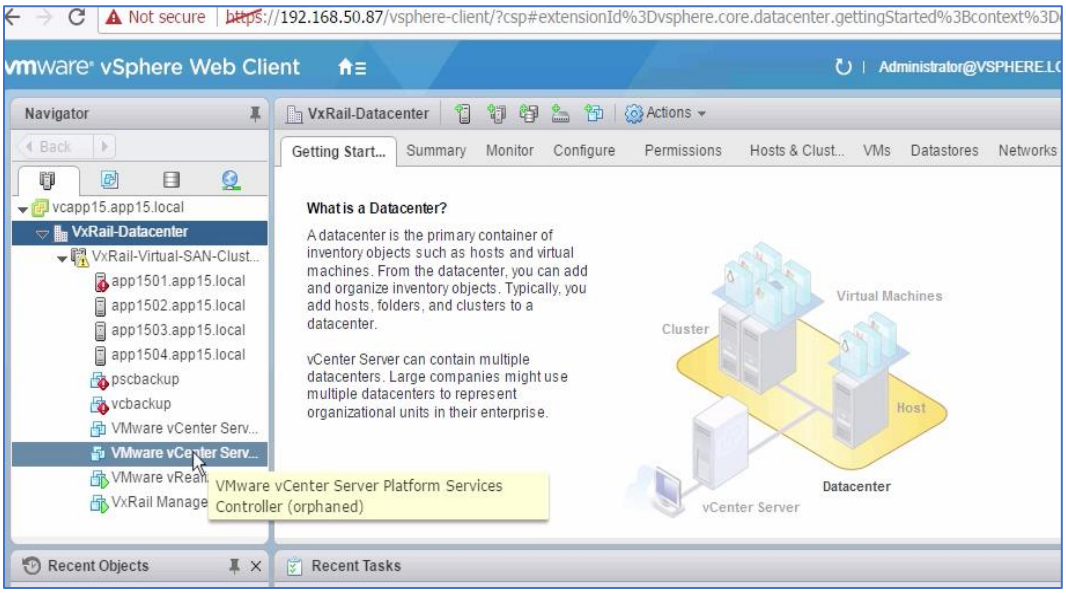


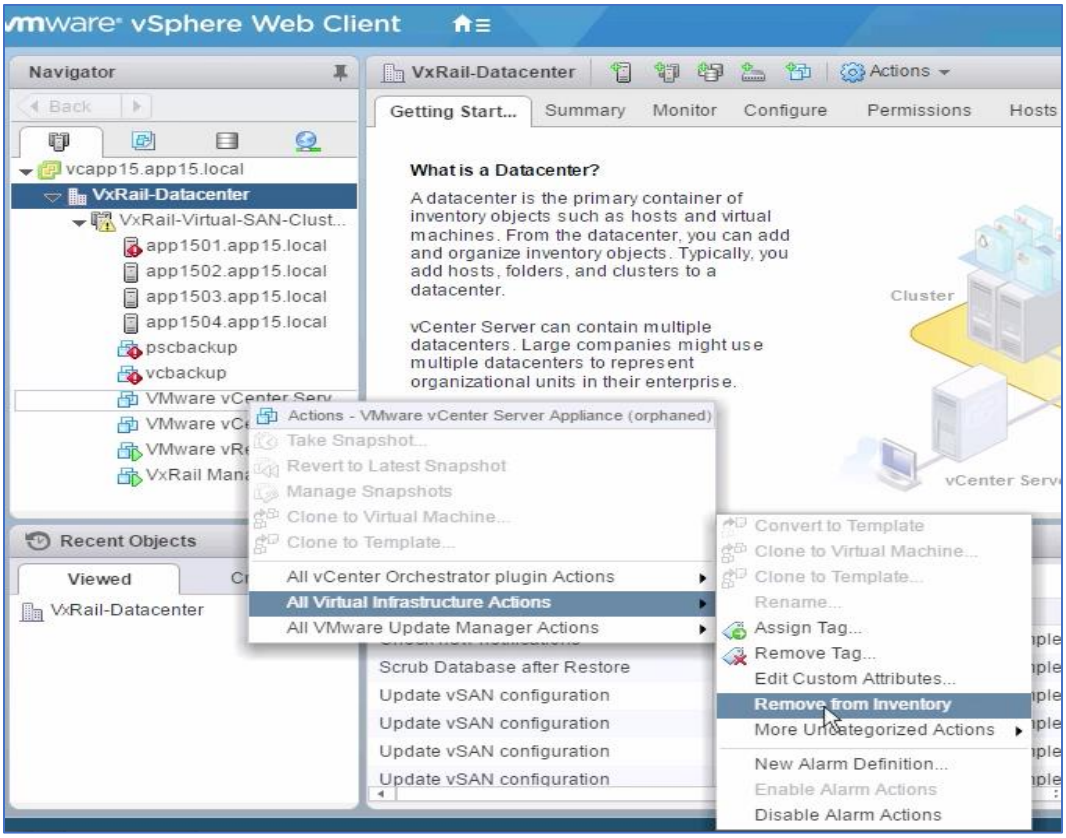


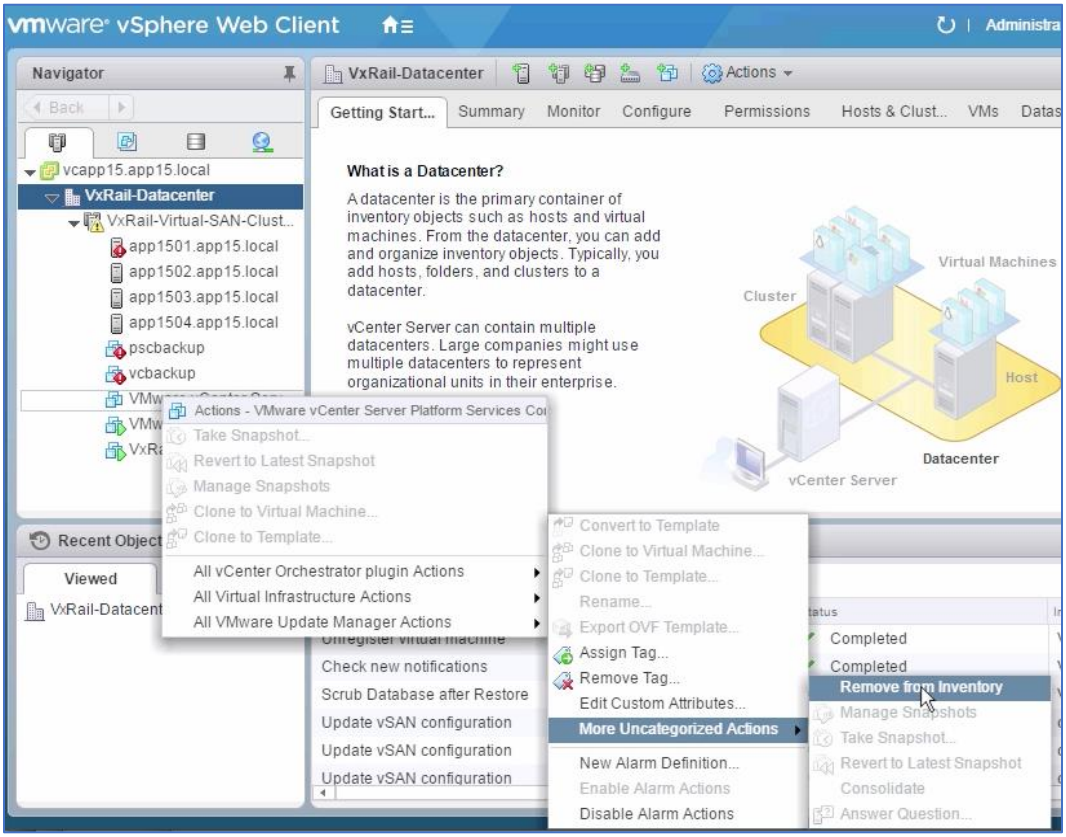
Deleting VMs in Orphaned State

If an old VM is in the orphaned state, delete it as follows:

1. Right-click-VM > All Virtual Infrastructure Actions > Remove from Inventory, or
2. Right-click-VM > All Virtual Infrastructure Actions > More uncategorized Actions > Remove from Inventory



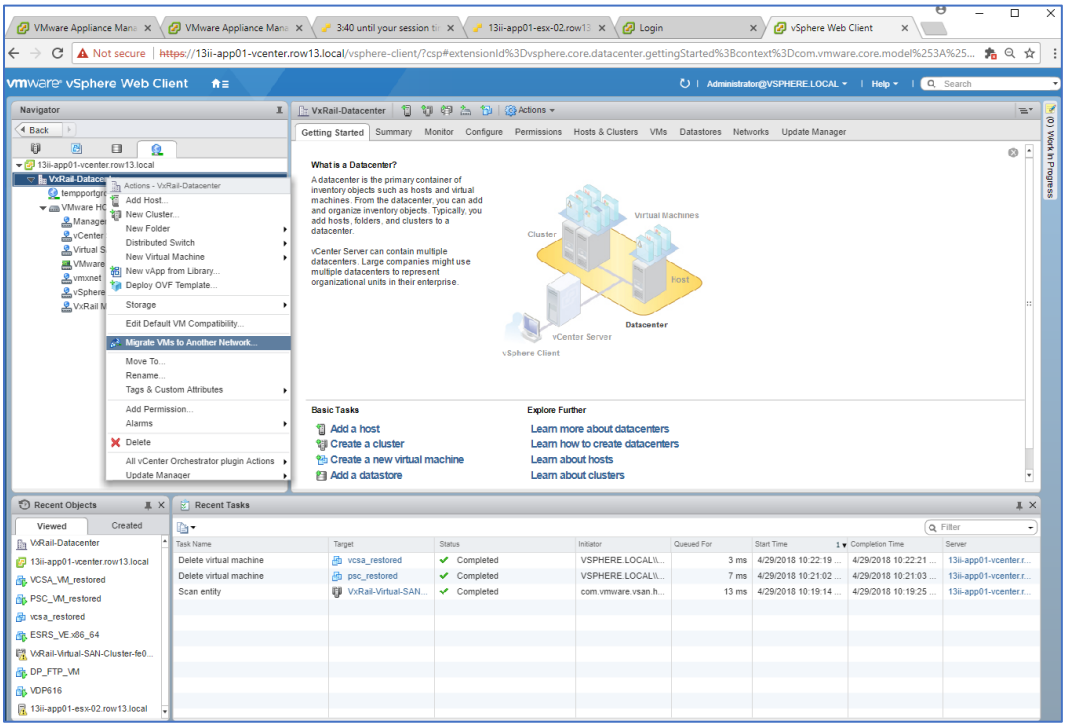




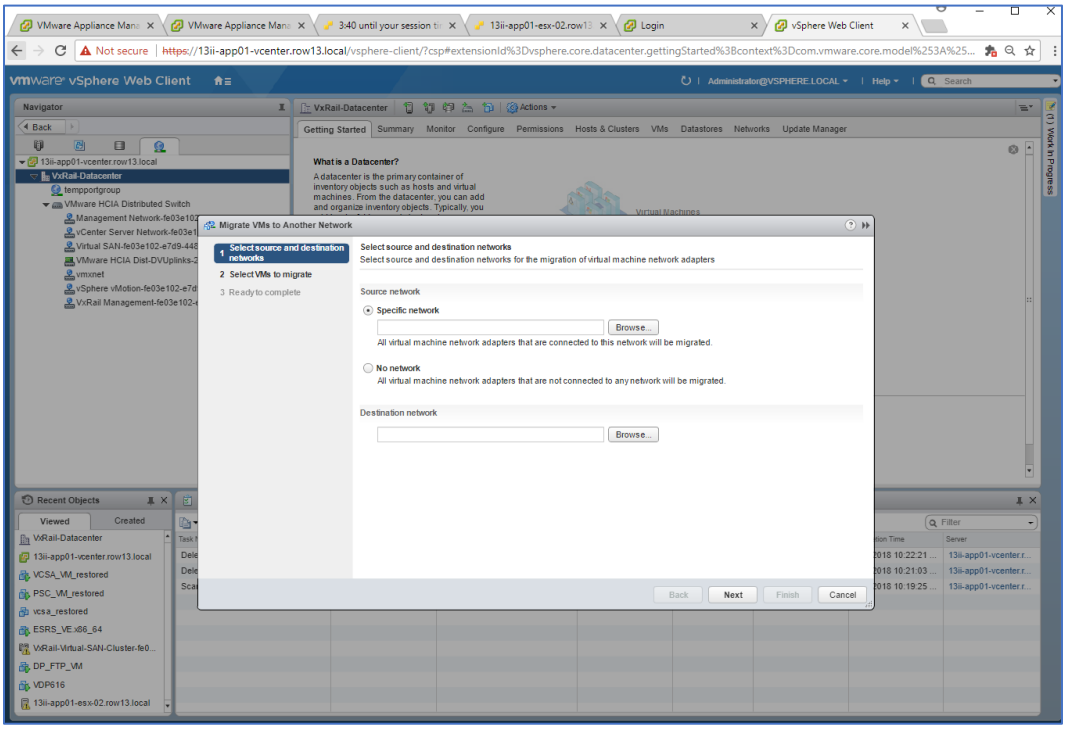
Migrate from tempportgroup to DVS vCenter Server portgroup

The next step is to bring vmnic1 back to DVS and remove the temporary VSS.

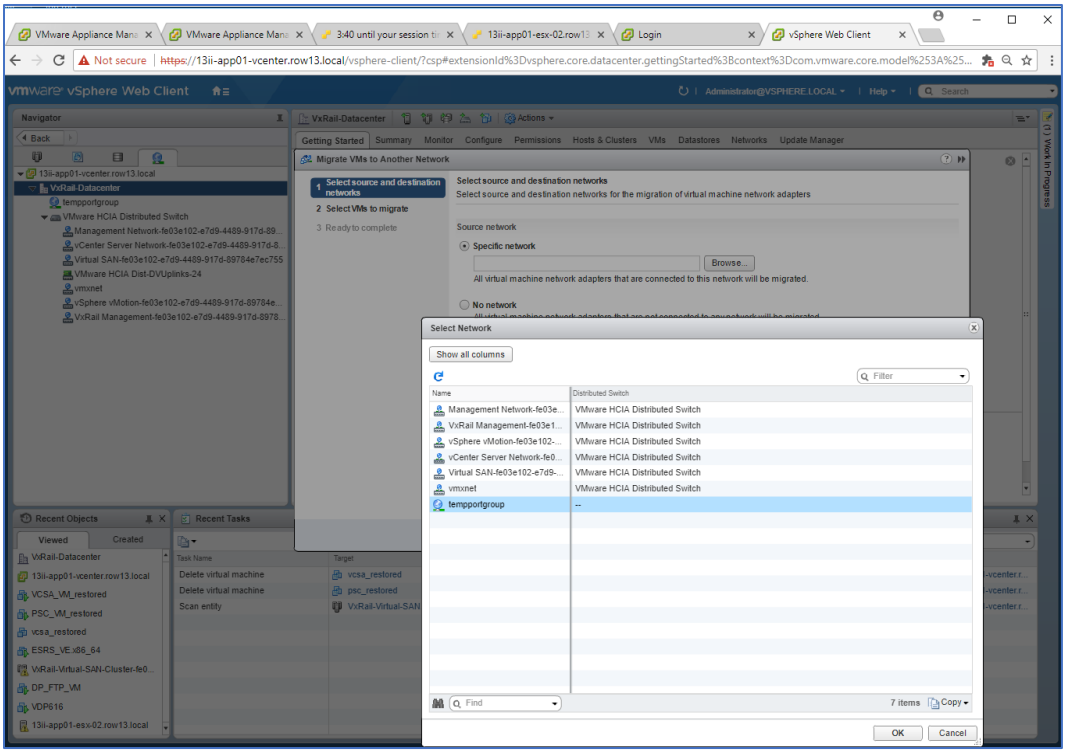
1. Log into vSphere Web Client.
2. Click on the **Networking** tab.
3. Right-click on the Datacenter > Select **Migrate VMs to Another Network…**



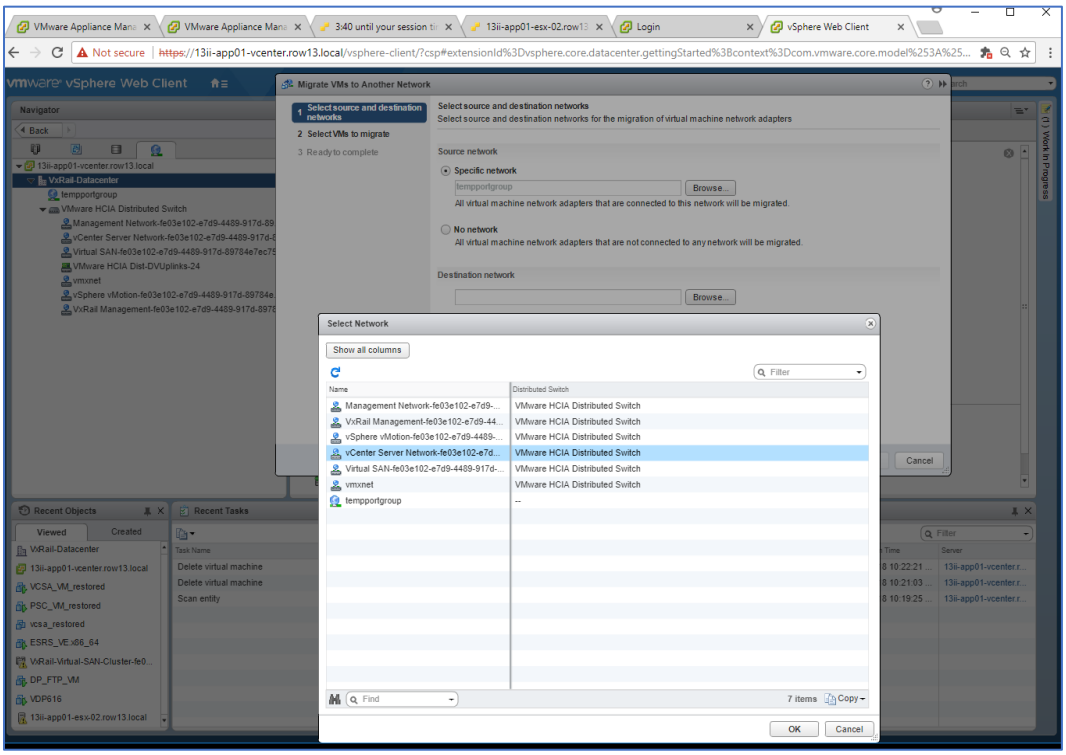
The Migrate VMs to Another Network window opens.



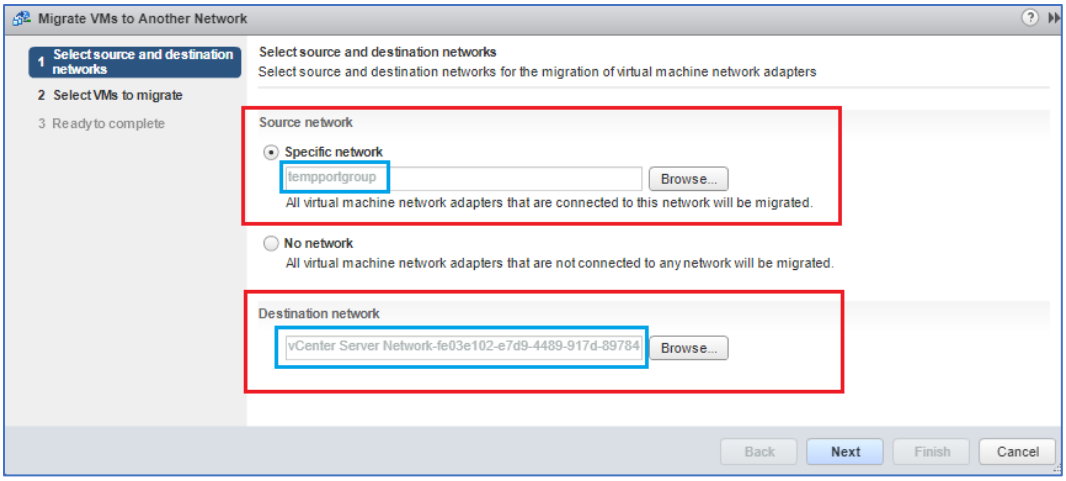
4. For Source network, click **Specific network**, then **Browse** and select **tempportgroup**.



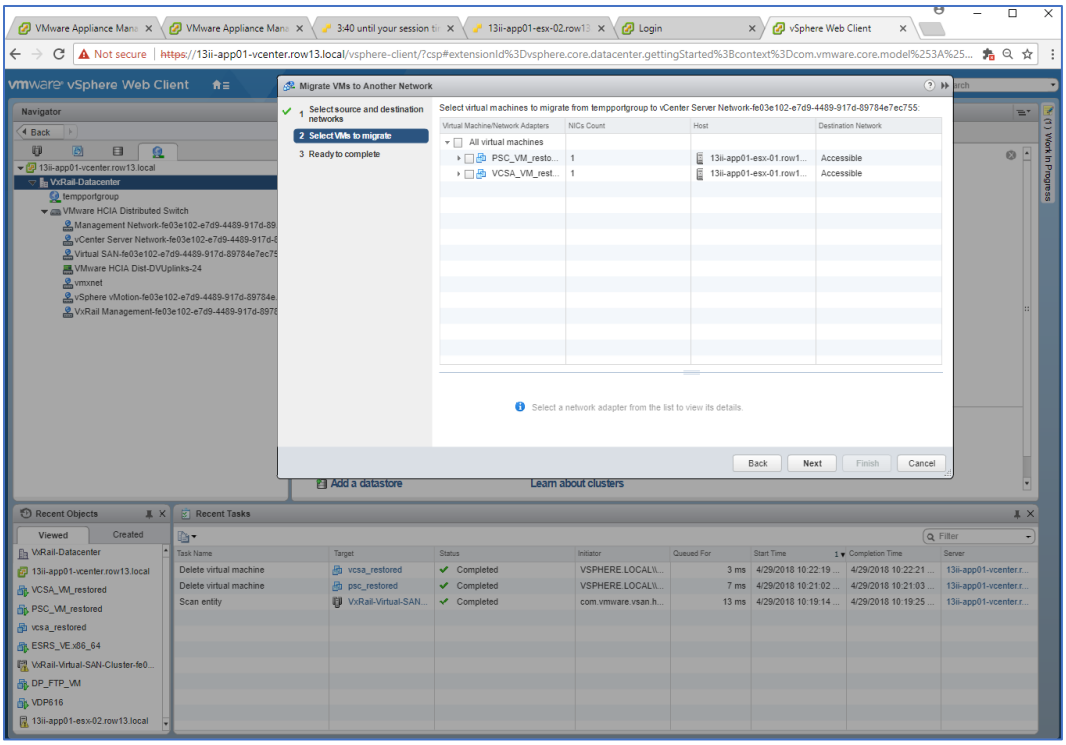
5. For Destination network, **Browse** and select **vCenter Server Network-####**



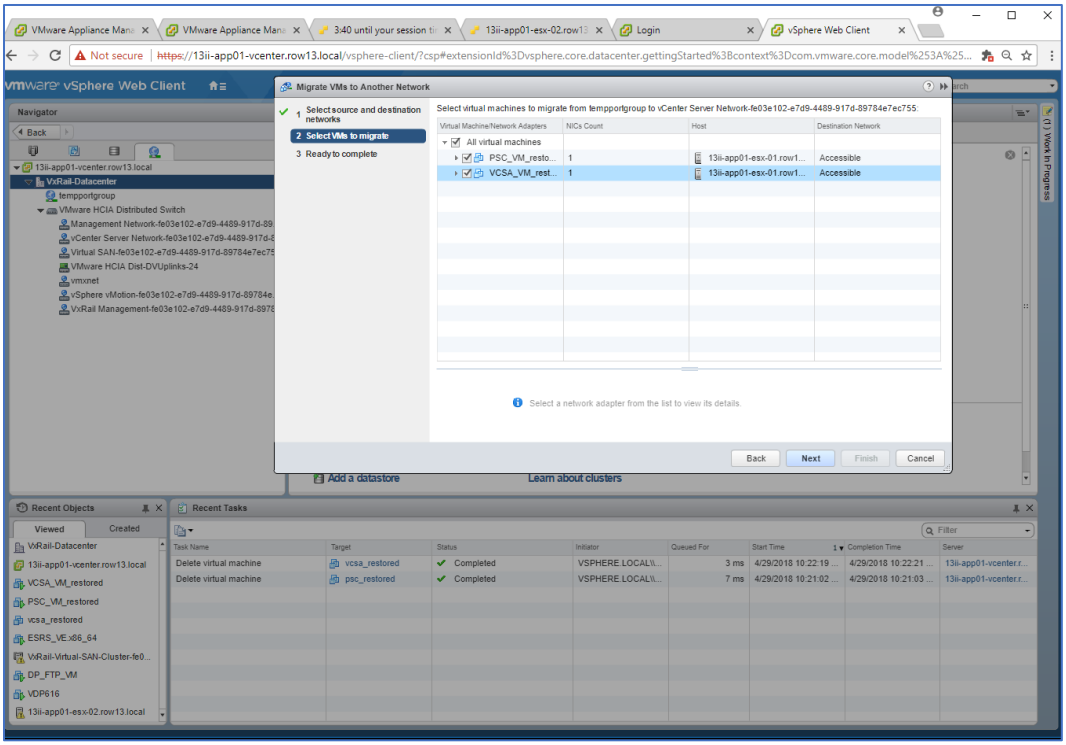
6. Click **Next** to select VMs to migrate.



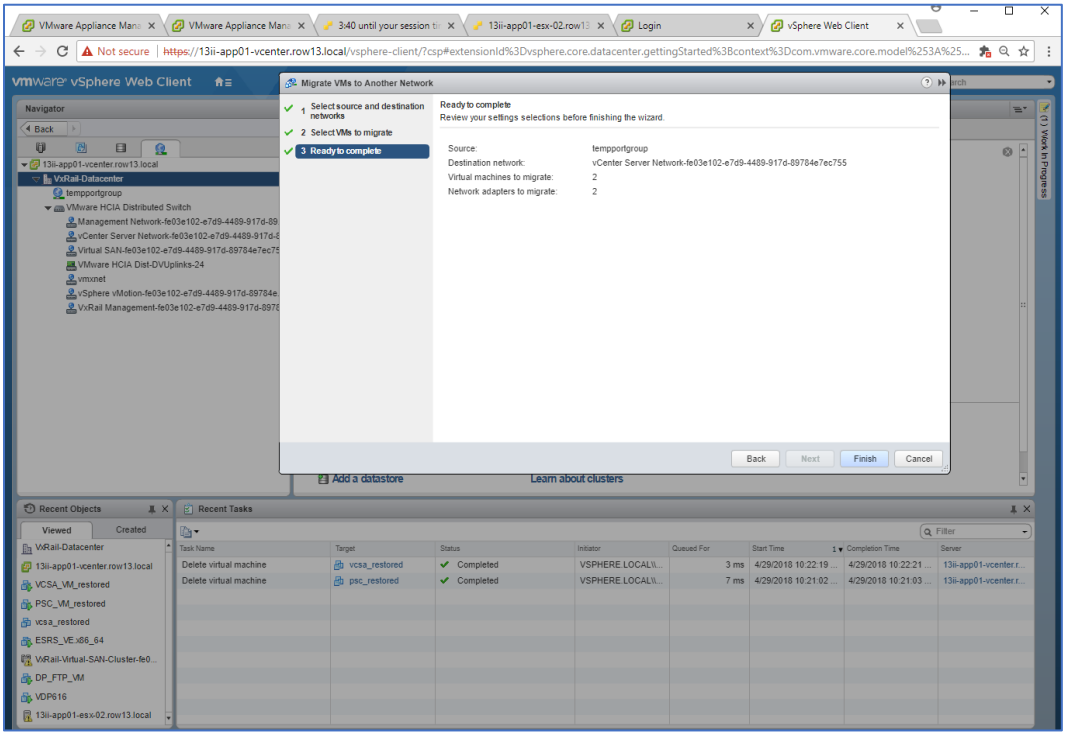
The newly restored VMs on the tempportgroup are displayed.



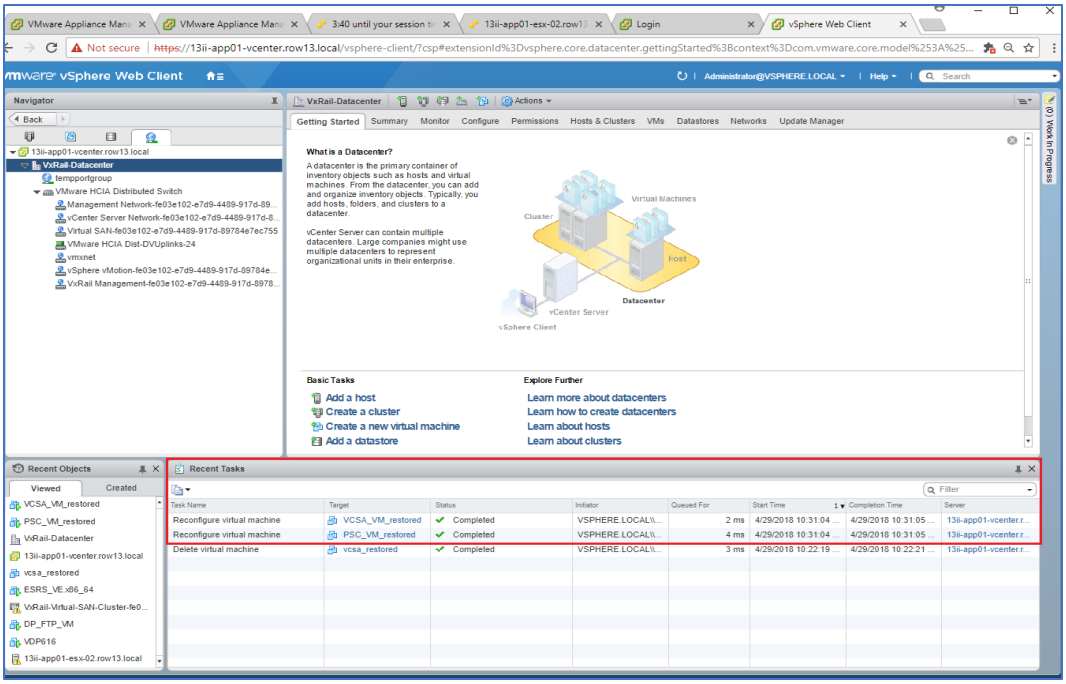
7. Select the VMs and click **Next**.



8. In the Summary page, review the settings and click **Finish**.

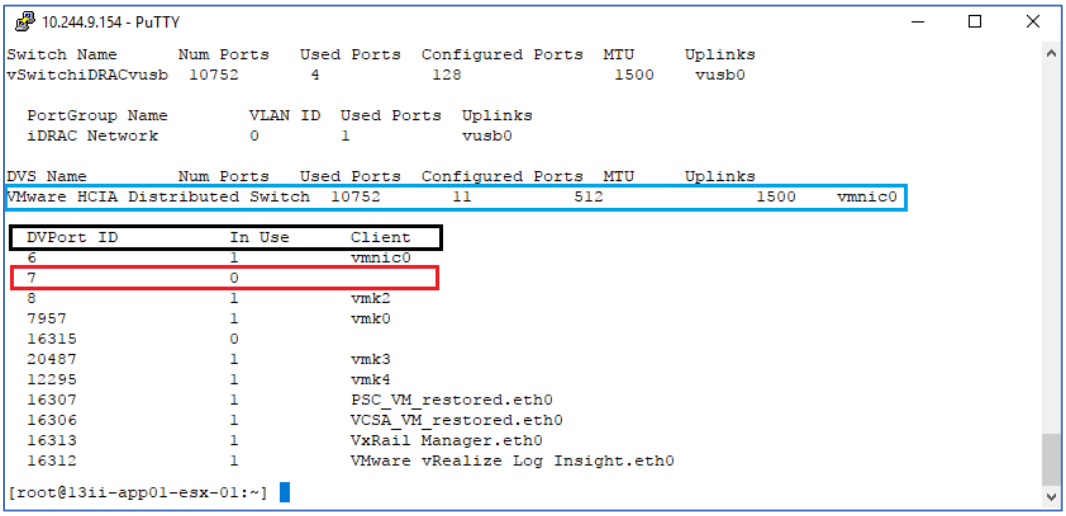


9. Monitor the progress of the migration in the **Recent Tasks** pane until it completes.



10. SSH to the primary-node.
11. Run this command to identify the free DVPort ID

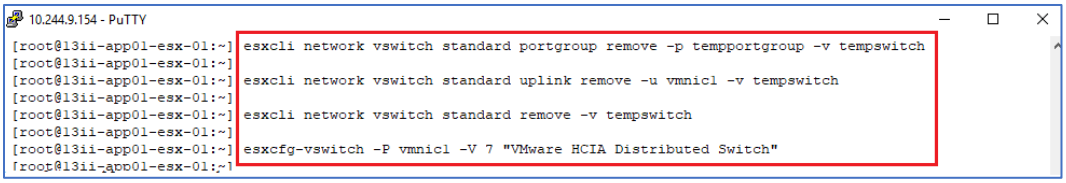
```
esxcfg-vswitch -l
```



In the preceding sample command output, {DVS name is *VMware HCIA Distributed Switch*} and {the free DVport ID is *7*}.

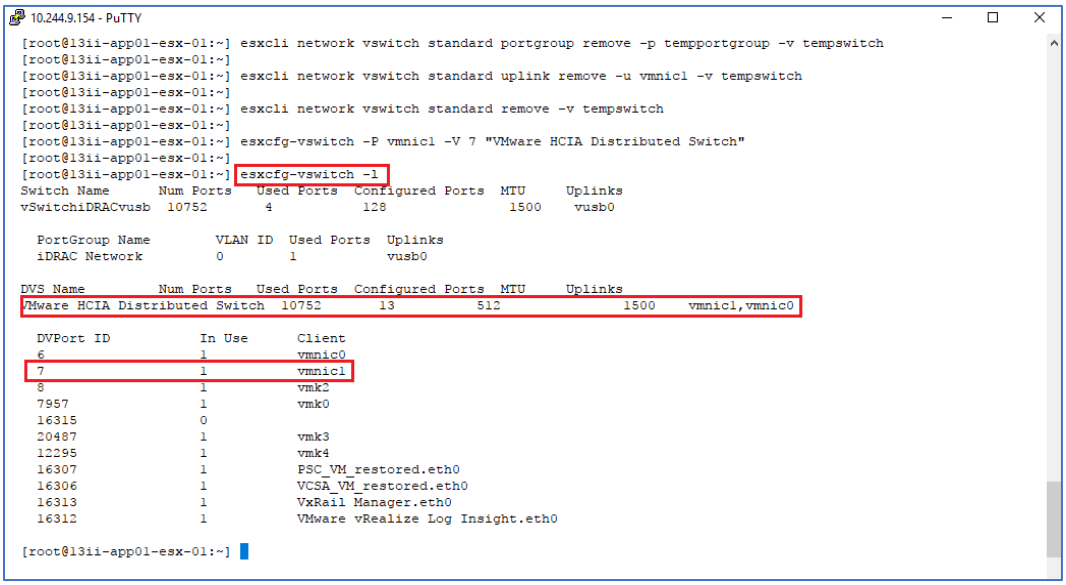
12. Having acquired the free **DVport ID**, run the following commands to **delete the tempswitch VSS** on the primary-node and to **move the vmnic1 back to the DVS**:

```
esxcli network vswitch standard portgroup remove -p tempportgroup -v tempswitch
esxcli network vswitch standard uplink remove -u vmnic1 -v tempswitch
esxcli network vswitch standard remove -v tempswitch
esxcfg-vswitch -P vmnic1 -V 7 "VMware HCIA Distributed Switch"
```



13. To confirm that the preceding commands have worked, run this command:

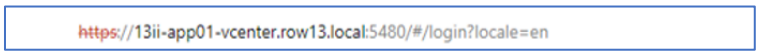
```
esxcfg-vswitch -l
```

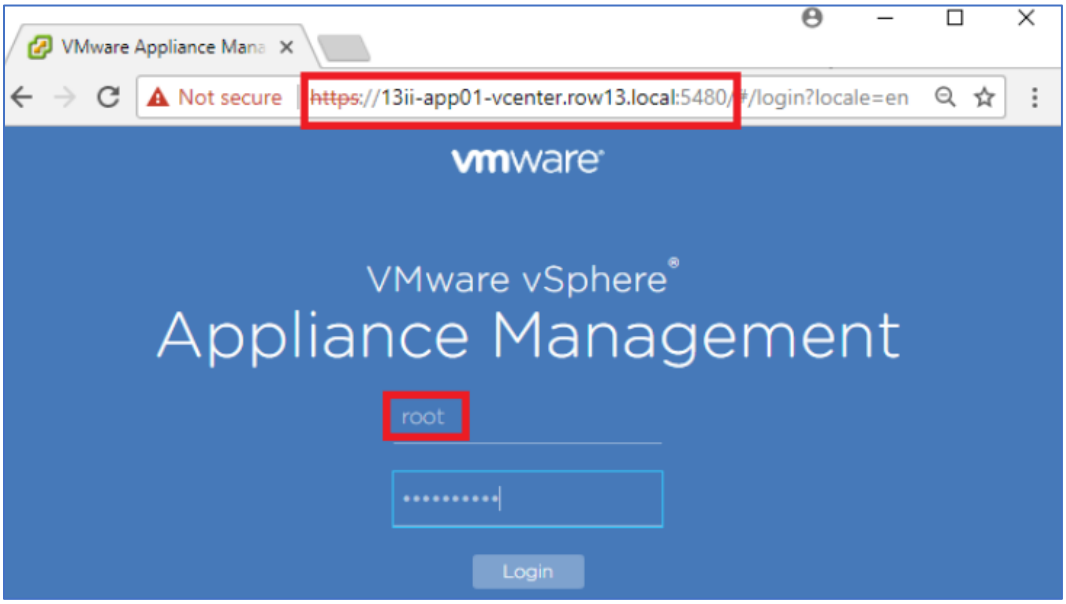


Reboot the Newly Deployed vCSA and PSC

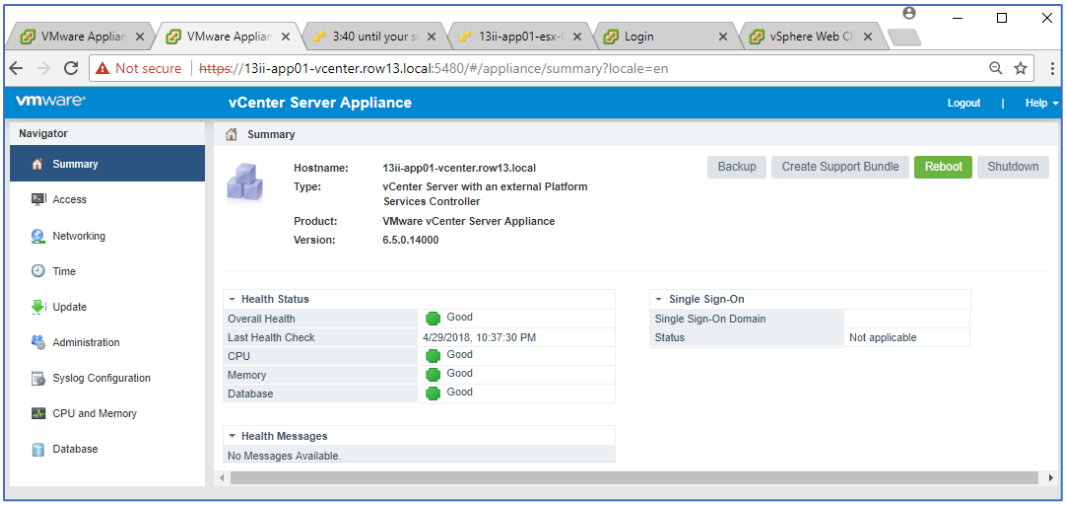
To ensure the stability of the newly deployed vCSA and PSC, they must be rebooted.

Log into VMware vSphere Appliance Management Interface (VAMI) of vCSA at port 5480.

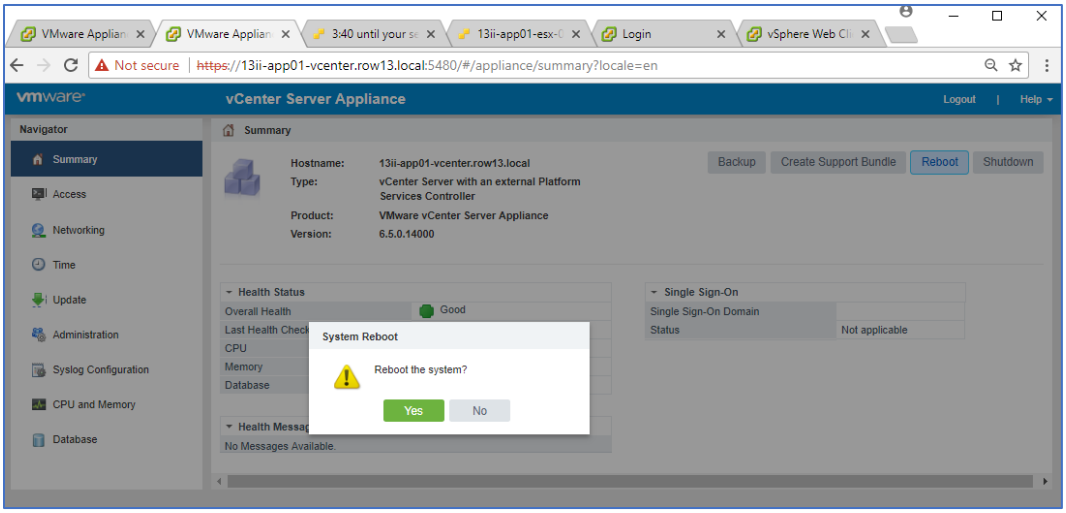




14. Click the **Summary** tab on the Navigator pane and then click the **Reboot** button on the Summary pane.

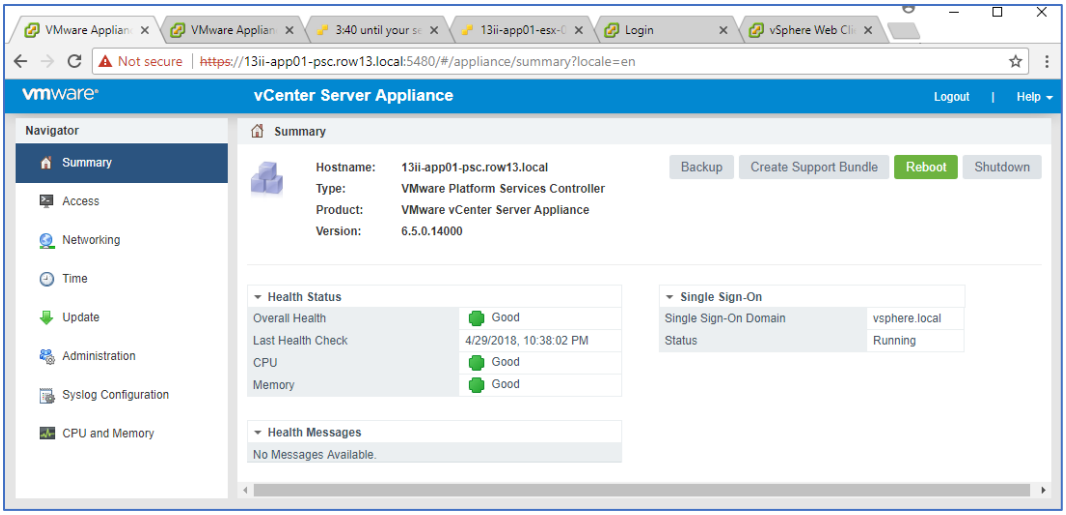


15. Click **Yes** to confirm and proceed with the reboot.

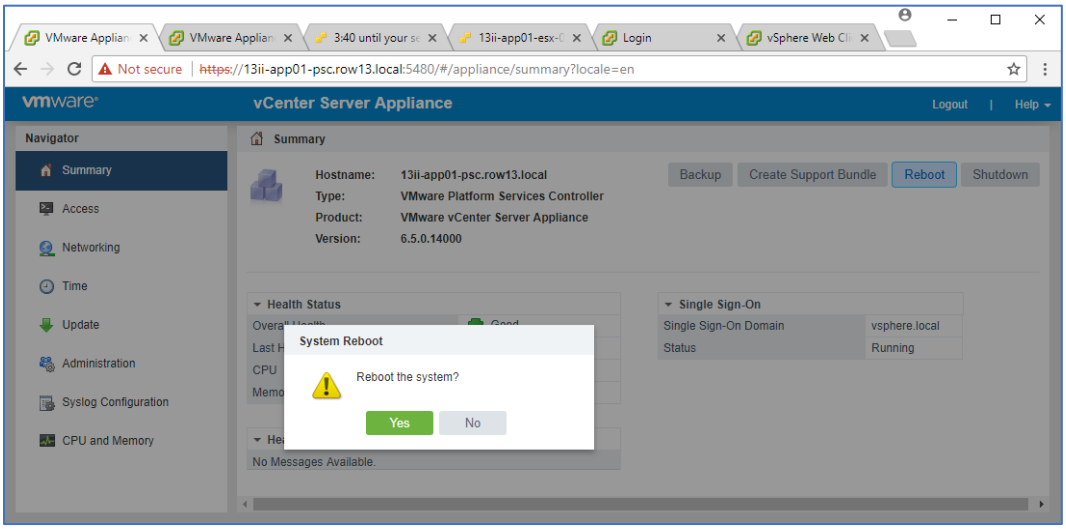


16. Log into VMware vSphere Appliance Management Interface (VAMI) of PSC at port 5480.

17. Click the **Summary** tab on the Navigator pane and then click **Reboot** on the Summary pane.



18. Click **Yes** to confirm and proceed with reboot.



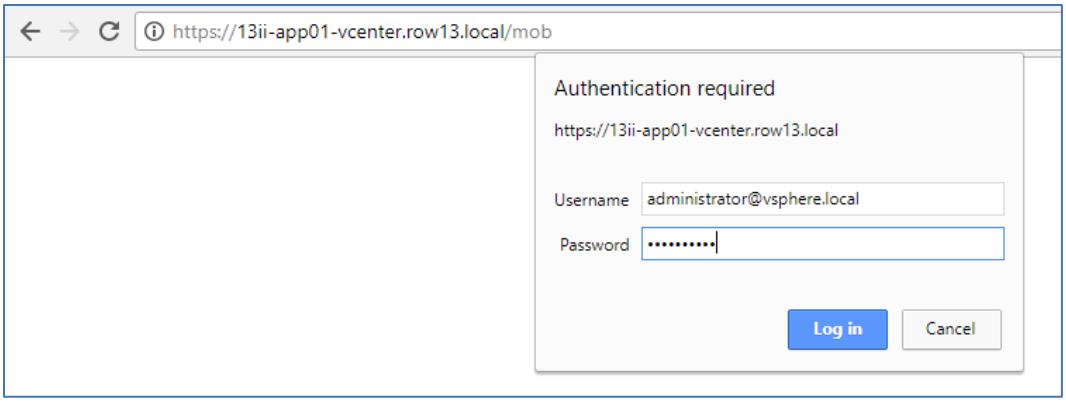
VxRail Manager Configuration for the Restored vCSA and PSC

After vCSA and PSC are restored, the VxRail Manager database must be updated with the UUID, morefid and VM-name of the new vCSA and PSC. If this step is skipped, the VxRail upgrade feature will be impacted.

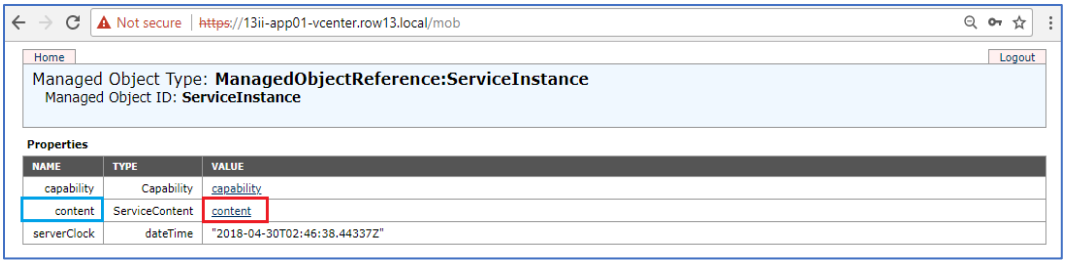
Obtain UUID, morefid, VM name for vCSA and PSC

The UUID, morefid and VM names can be obtained using the Managed Object Browser.

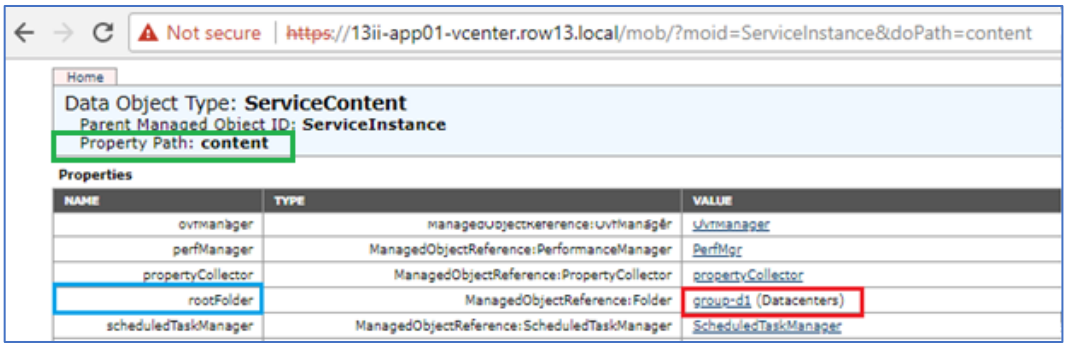
1. Log into the mob via https://vCenter-Server-IP/mob or via https://vCenter-Server-FQDN/mob and enter SSO account credentials (e.g., administrator@vsphere.local).



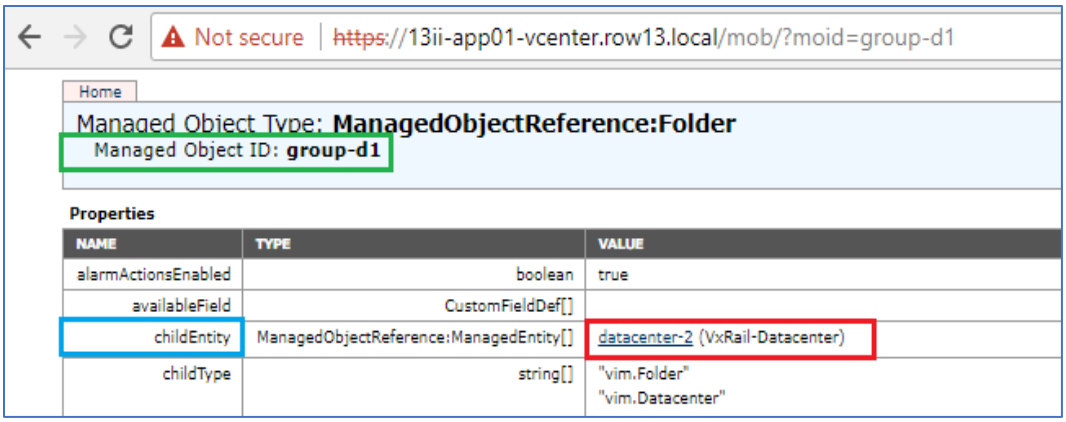
2. Click on the link in the VALUE column on the row*:* **content**



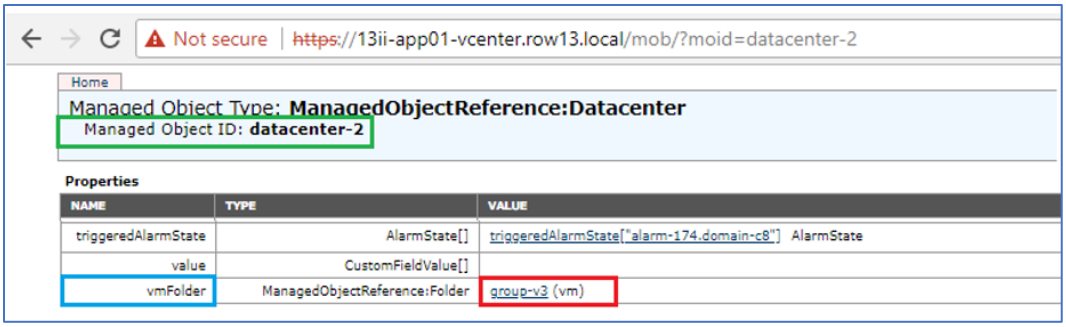
3. Click on the link in the VALUE column on the row*:* **rootFolder**



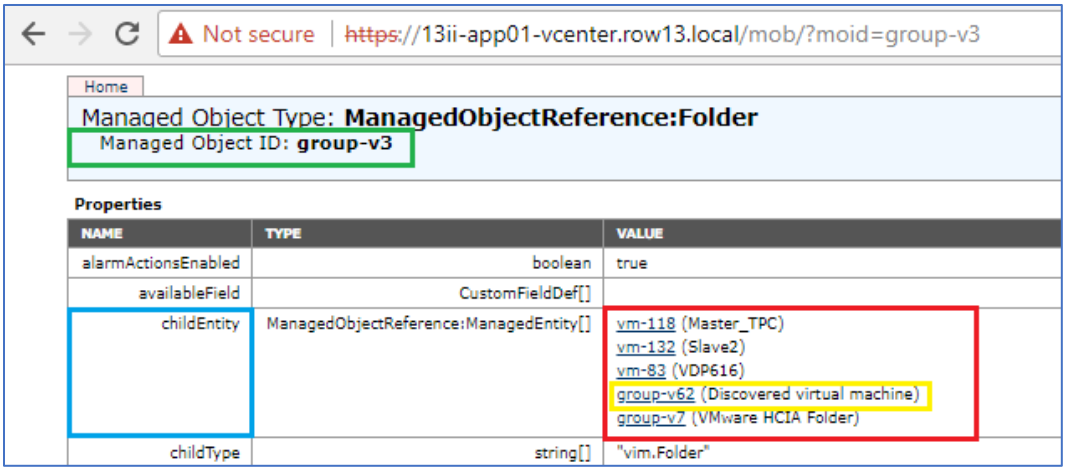
4. Click on the link in the VALUE column on the row*:* **childEntity**



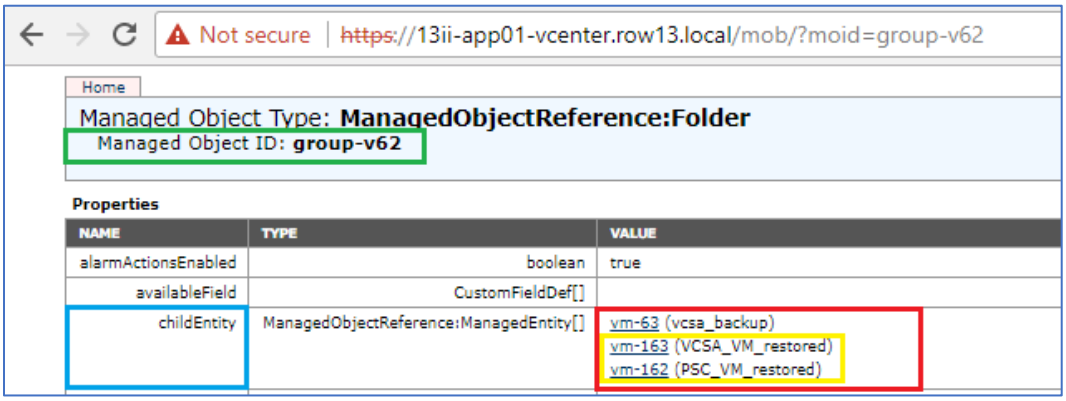
5. Click on the link in the VALUE column on the row*:* **vmFolder**



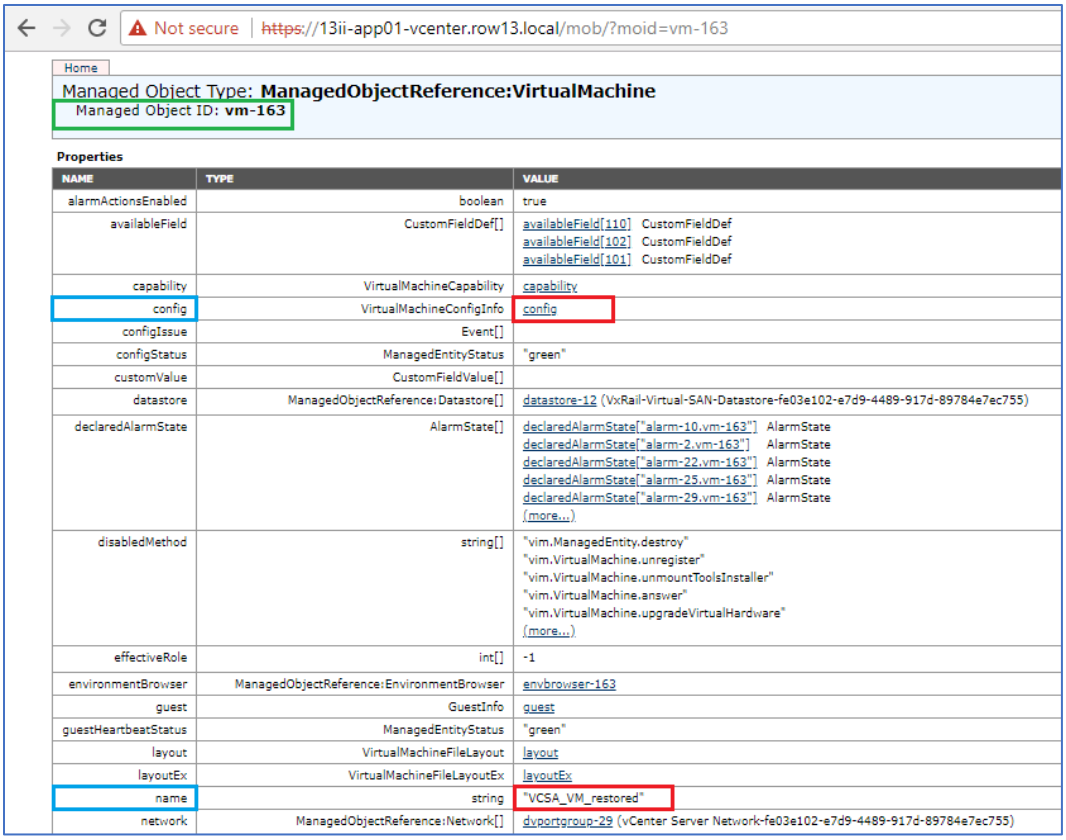
6. Click on the link described as **Discovered virtual machine** in the VALUE column on the row*:* **childEntity**



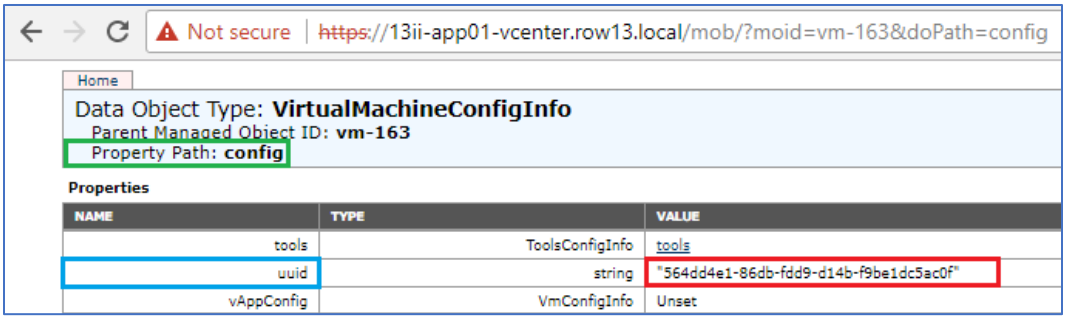
7. Managed Object Reference IDs (morefid) for the newly deployed vCSA and PSC VMs are displayed in the VALUE column on the row*:* **childEntity**. In this example, {morefid for vCSA is 163}, and {morefid for PSC is 162}. Next, follow each link (vm-163 and vm-162) separately to obtain the UUID and the name of each VM. First click on the link for vCSA.



8. On the page displayed, the VM-name is in the VALUE column on the row*:* **name**. To obtain the UUID, click the config link in the VALUE column on the row*:* **config** on the same page.



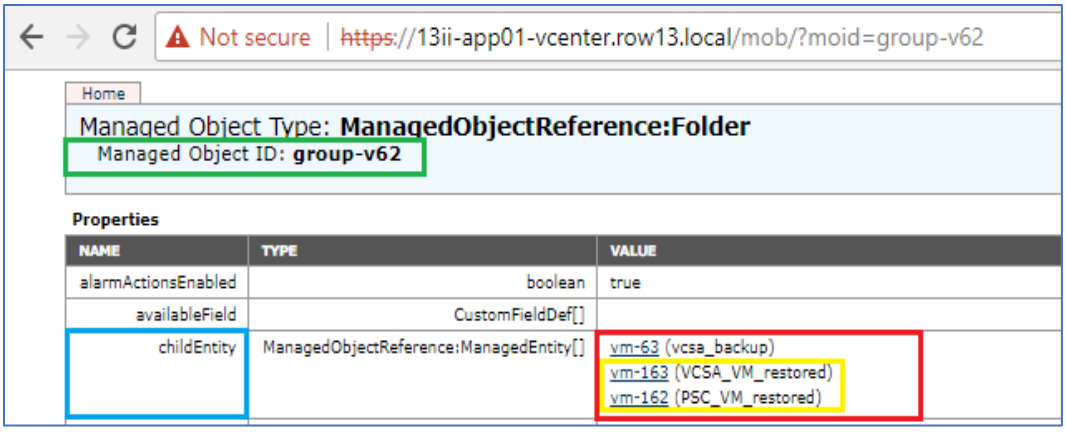
The UUID is displayed in the VALUE column on the row: **uuid**.



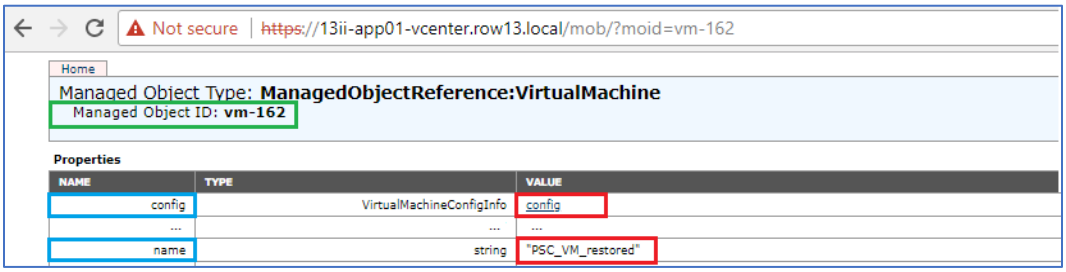
vCSA information obtained

morefid	163
name	VCSA_VM_restored
uuid	564dd4e1-86db-fdd9-d14b-f9be1dc5ac0f

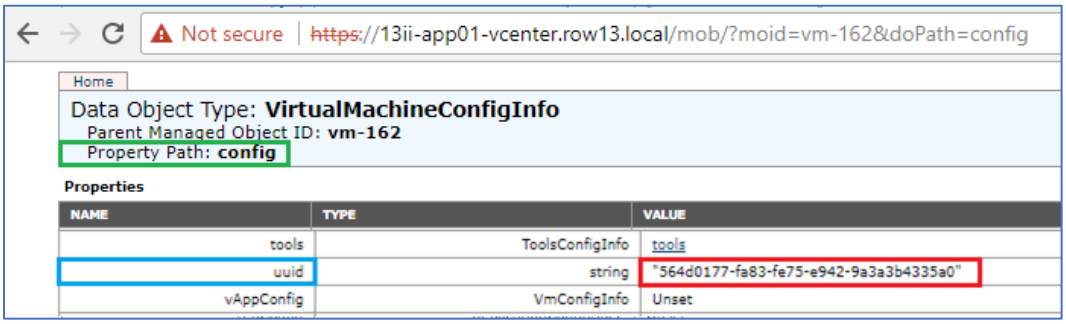
9. Go back and click on the link for PSC to obtain its UUID and VM-name.



10. On the page displayed, the VM-name is in the VALUE column on the row: **name**. To obtain the UUID, click the config link in the VALUE column on the *row:***config** on the same page.



The UUID is displayed in the VALUE column on the row:**uuid**.



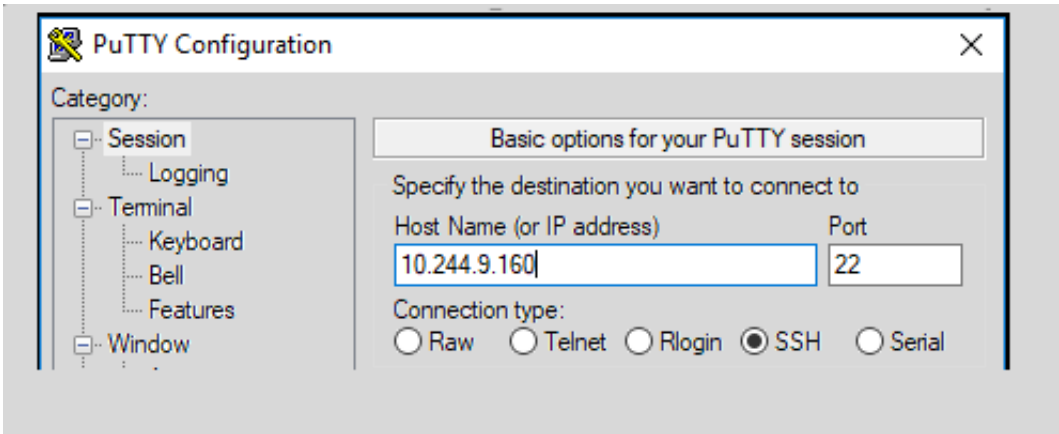
PSC information obtained

morefid	162
name	PSC_VM_restored
uuid	564d0177-fa83-fe75-e942-9a3a3b4335a0

vCSA and PSC information obtained in this step will be used to update the VxRail Manager database in the next step.

Update VxRail Manager Database

1. Log in to the VxRail Manager using Putty or the VM console on the vSphere Web Client.

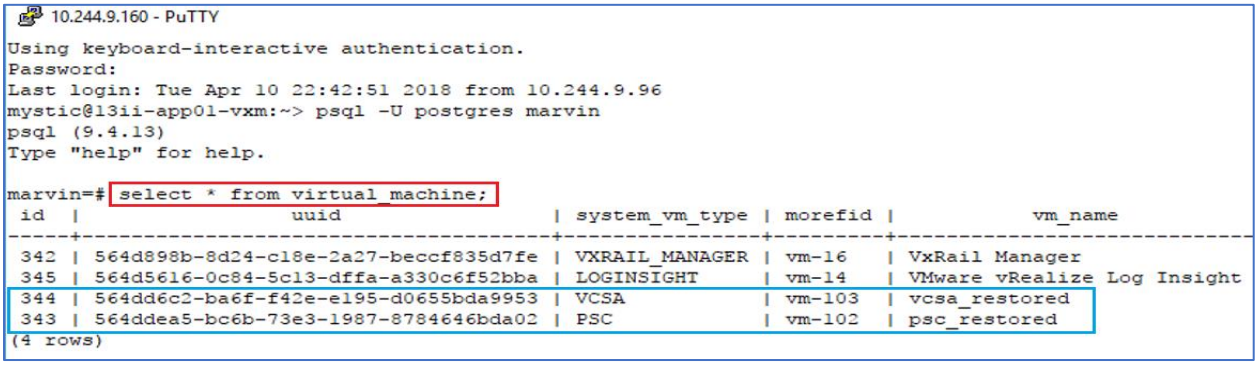


2. Run this command to enter the database shell

```
psql -U postgres marvin
```

3. In the database shell, run this query to collect the current information for old vCSA and PSC.

```
select * from virtual_machine;
```



4. Update the database table with the information obtained in the previous step for the new vCSA and PSC.

```
update virtual_machine set uuid='564dd4e1-86db-fdd9-d14b-f9be1dc5ac0f',
morefid='vm-163', vm_name='VCSA_VM_restored' where system_vm_type='VCSA';
```

```
update virtual_machine set uuid='564d0177-fa83-fe75-e942-9a3a3b4335a0',
morefid='vm-162', vm_name='PSC_VM_restored' where system_vm_type='PSC';
```

```
marvin=# update virtual_machine set uuid='564dd4e1-86db-fdd9-d14b-f9be1dc5ac0f', morefid='vm-163', vm_name='VCSA_VM_restored' where system_vm_type='VCSA';
UPDATE 1
marvin=#
marvin=# update virtual_machine set uuid='564d0177-fa83-fe75-e942-9a3a3b4335a0', morefid='vm-162', vm_name='PSC_VM_restored' where system_vm_type='PSC';
UPDATE 1
marvin=#
```

5. Run this query to verify the database is updated with the new data.

```
select * from virtual_machine;
```

```
marvin=#
marvin=# select * from virtual_machine;
 id  |                  uuid                  | system_vm_type | morefid |           vm_name
-----+----------------------------------------+----------------+---------+-----------------------------
 342 | 564d898b-8d24-c18e-2a27-beccf835d7fe | VXRAIL_MANAGER | vm-16   | VxRail Manager
 345 | 564d5616-0c84-5c13-dffa-a330c6f52bba | LOGINSIGHT     | vm-14   | VMware vRealize Log Insight
 344 | 564dd4e1-86db-fdd9-d14b-f9beldc5ac0f | VCSA           | vm-163  | VCSA_VM_restored
 343 | 564d0177-fa83-fe75-e942-9a3a3b4335a0 | PSC            | vm-162  | PSC_VM_restored
(4 rows)
```

6. Run this command to quit the database session.

```
\q
```

```
marvin=# \q
mystic@l3ii-app01-vxm:~>
```

7. Elevate to root account and restart the VxRail Manager's **vmware-marvin** and **runjars** services.

```
sudo -i
```

```
service vmware-marvin restart
```

```
service runjars restart
```

```
mystic@l3ii-app01-vxm:~> sudo -i
root's password:
l3ii-app01-vxm:~ #
l3ii-app01-vxm:~ # service vmware-marvin restart
l3ii-app01-vxm:~ #
l3ii-app01-vxm:~ # service runjars restart
```

Conclusion

The file-based backup and restore operation provides a simple and reliable way to rebuild the vCSA and PSC, which are the two of VxRail's core system VMs. Image level backup and restore operations can be arduous, time-consuming, and restored images might not be reliable. Moreover, fundamental VxRail features and functionality such as cluster shutdown, upgrade, hardware replacement, etc. are not impacted by this type of restore operation. VxRail 4.5 takes advantage of this native data protection feature provided by vSphere 6.5.

References

VMware File-based Backup and Restore

For more information on the native file-based backup and restore feature of vSphere 6.5, see this VMware document: https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.install.doc/GUID-3EAED005-B0A3-40CF-B40D-85AD247D7EA4.html

SolVe Procedures for Changing the IP of vCSA and PSC

Do not make changes to the network configuration during the restore operation. If a different IP address than the original address of the vCSA or PSC is used anyway, the VxRail Manager configuration will have to be fixed after the restore. Refer to ***Change the Internal vCSA Virtual Machine IP Address*** and ***Change the Internal PSC Virtual Machine IP Address*** procedures in SolVe at https://solveonline.emc.com. These two procedures can be accessed by navigating through this selection path: **VxRail > How To Procedures > How To Change VxRail IP Addresses**.