Backup and Restore of the vCenter Server using the Avamar VMware Image Protection Solution

December 2017

ABSTRACT

This whitepaper defines how to protect the vCenter Server Appliance (VCSA) and the Platform Services Controllers (PSC). Enterprise customers utilize the distributed model of the vCenter Server, and therefore protection of the complete vCenter Server infrastructure is of critical importance for a VMware virtual administrator. The goal is to better serve virtual administrators in their challenge of keeping the virtual infrastructure running with the business critical application of the vCenter Server.

302-004-537 Rev 01

This document is not intended for audiences in China, Hong Kong, Taiwan, and Macao.

Copyright

Contents

vCenter deployments overview

This document describes how to protect vCenter 6.5 deployments with Avamar using the VMware image backup proxy appliance. This document assumes that the vCenter (VC) and Platform Services Controller (PSC) are deployed as virtual machines.

For the restores to complete successfully, perform one of the following:

- Ensure that these virtual machines use a fully qualified domain name (FQDN) with correct DNS resolution, or
- Ensure that the host name of the machine is configured as an IP address. Note that if the host name is configured as an IP address, the IP address cannot be changed.

There are mainly two types of vCenter deployments:

- vCenter Server Appliance/Windows Virtual Machine with an embedded Platform Services Controller.
- vCenter Server (also multiple) Appliance/Windows Virtual Machine with an external Platform Services Controller. This type has two sub categories:
  - vCenter Server environment with a single external Platform Services Controller.
  - vCenter Server environment with multiple Platform Services Controller instances. This environment contains multiple vCenter Server instances registered with different external Platform Services Controller instances that replicate their data.

Best practices for backup and restore

Review the following recommendations and best practices when planning a vCenter virtual machine or its component virtual machine(s) backup.

Note: Image backups will not save Distributed switch configurations. The following VMware KB article provides steps to backup and restore the configuration of vSphere Distributed Switches: https://kb.vmware.com/s/article/2034602

- It is recommended to schedule the backup of the vCenter Server when the load on the vCenter Server is low, such as during off-hours, to minimize the impact of vCenter virtual machine snapshot creation and snapshot commit processing overhead.
- Ensure that there are no underlying storage problems that might result in long stun times.
- As a best practice, keep the vCenter virtual machine and all of its component virtual machines in one single isolated policy. The group/policy should not be shared with any other virtual machines. This is to ensure that the backup times of all vCenter Server component virtual machines are as close to each other as possible.
- If using one or more external Platform Services Controllers, it is recommended to have one dedicated proxy associated to the entire vCenter Server virtual machines

backup. This will ensure that the backup times of all vCenter Server component virtual machines are as close to each other as possible.

- Ensure that the backup start time of the vCenter Server does not overlap with any operations for other protected virtual machines being managed by this vCenter so that there is no impact on other protected virtual machines during snapshot creation and snapshot commit of the vCenter virtual machine.
- If the vCenter Server and Platform Services Controller instances fail at the same time, you must first restore the Platform Services Controller and then the vCenter Server instances.

Protecting embedded PSC (Simple)

Backup

To perform the backup:

1. Create a policy, and then add the vCenter virtual machine (VC VM) group to the policy.
2. Select the full virtual machine and not individual disks.

   Note: When selecting virtual machines and objects, ensure that you unselect the **Enable CBT** option.
3. Run the policy as scheduled or perform an ad-hoc (on-demand) policy backup.

Restore

Note: There is no post-restore operation to be performed for embedded installs.

Depending on the failure, you can perform the virtual machine recovery by using one of the following methods:

- Restore to original: Use this method when the vCenter Server Appliance (VCSA) is intact and running, but corrupted.

Use any one of the following if you have completely lost your vCenter Server Appliance (VCSA):

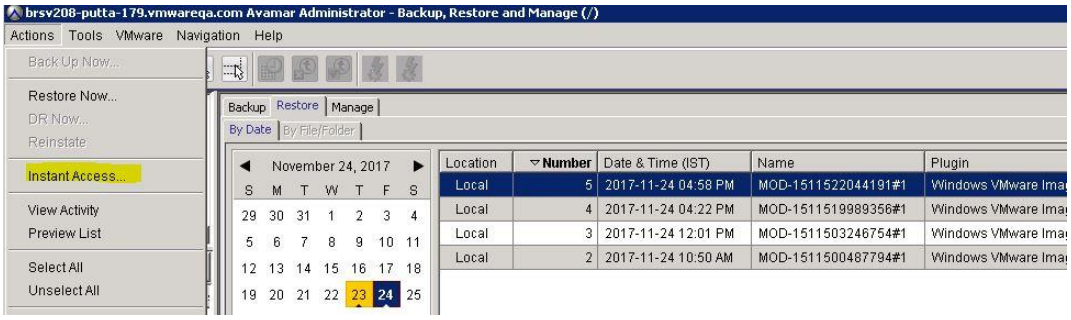
- Restore as a new virtual machine to a managed ESXi server. Note that this vCenter must be registered with the Avamar Server.

- Restore as new VM to an unmanaged ESXi. When using this method, the ESXi should be registered with the Avamar Server.

  This ESXi should be disassociated from all vCenter Servers.

Note: If all the VCs fail, ensure that there is one healthy ESXi with a proxy registered to the Avamar Server for restore operations.

- Instant access restore to an ESXi. Use this method if the backup is saved to a Data Domain system. Restores using this method will complete more quickly than the other methods.



Once the restore is complete, perform storage migration of this virtual machine to the desired datastore, and then unmount the NFS datastore from the ESXi.

For appliance restore, perform any one of the above methods depending on the failure type, and then perform the following steps.

Procedure

1. After the recovery operation, wait until the virtual machine starts up.

2. Log in to the vCenter Server Appliance shell as “root”.

3. Verify that all PSC and VC services are running.

   For an appliance, run the following command in the appliance shell:

   service-control --status –all

   For a vCenter Server installed on Windows, from the Windows Start menu, select **Control Panel > Administrative Tools > Services**.

Protecting external deployment models

Backup

Ensure that you back up all vCenter Server and PSC instances at the same time.

1. Create one group and add the VC VM and PSC VM to the group. This will ensure that snapshots are taken at the same time.
2. Ensure that you select the full virtual machine and not individual disks.
3. Run the policy as scheduled or perform an ad-hoc (on-demand) policy backup.

Restore

Note: In the event of a complete environment failure, PSC should be restored first, followed by the vCenter Server restore.

Depending on the failure, you can perform virtual machine recovery by using one of the following methods:

- Restore to original. Use this method when the vCenter Server Appliance (VCSA) is intact and running, but corrupted.

Use any of the following methods if you have completely lost your vCenter Server Appliance (VCSA):

- Restore as a new virtual machine to a managed ESXi server. Note that this vCenter Server must be registered with the Avamar Server.
- Restore as new VM to an unmanaged ESXi. When using this method, the ESXi should be registered with the Avamar Server.

  This ESXi should be disassociated from all vCenter Servers.

- Instant access restore to an ESXi. Use this method if the backup is saved to a Data Domain system.

  Restores using this method will complete more quickly than the other methods. Once the restore is complete, perform storage migration of this virtual machine to the desired datastore, and thenunmount the NFS datastore from the ESXi.

VCSA/VCSAs with one external PSC

Scenario 1: PSC fails

1. Perform an image-level recovery of the PSC by using one of the methods indicated above, and then power ON the virtual machine.
2. Verify that all Platform Services Controller services are running:
   - For a Platform Services Controller deployed as an appliance, run the **service-control --status --all** command in the appliance shell.
   - For a Platform Services Controller installed on Windows, from the Windows Start menu, select **Control Panel > Administrative Tools > Services**.
3. Log in to the vCenter Server Appliance(s) shell as **root**.

4. Verify that no vCenter services are running, or stop any vCenter services that are running by typing the following:

   service-control --stop

5. Run the **vc-restore** script to restore the vCenter virtual machines. For a vCenter Server Appliance, type:

   vcenter-restore -u *psc_administrator_username* -p *psc_administrator_password*

   For a vCenter Server installed on Windows, navigate to **C:\Program Files\VMware\vCenter Server**, and then run:

   vcenter-restore -u *psc_administrator_username* -p *psc_administrator_password*

   where *psc_administrator_username* is the vCenter Single Sign-On administrator user name, which must be in UPN format.

6. Verify that all vCenter services are running and the vCenter Server is started, as specified in step two.

7. Perform a log in test to the vCenter Server. If the restore was successful, the login completes successfully.

Scenario 2: VCSA lost, PSC remains

1. Perform an image-level recovery of the lost vCenter Server by using one of the methods mentioned above, and then power ON the vCenter Server.

2. After successfully starting the vCenter Server, verify that all vCenter services are started.

3. Perform a log in test.

VCSA/VCSAs with multiple PSCs

Scenario 1: One PSC fails and other VCSA/PSC remains

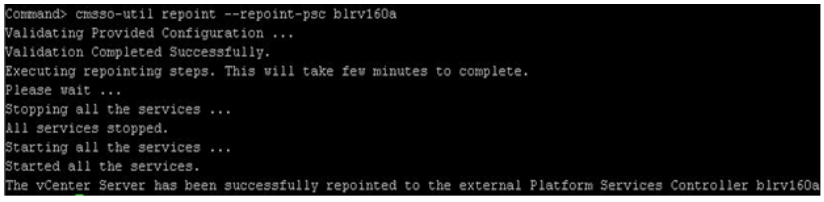
1. Repoint the VC instance to one of the functional PSCs in the same SSO domain.

Note: Log in to all vCenter Servers one by one to determine which vCenter log in fails. This will be the vCenter Server that requires the repoint steps.

2. Run the following command on the VCSA:

   cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]

   Where the square brackets **[ ]** enclose the command options.



3. Perform a log in test on the vCenter Server.
4. Deploy the new PSC and join to an active node in the same SSO and site, replacing lost ones.
5. Repoint the vCenter Server back to the new PSC.

Scenario 2: All PSCs fail and VCSA remains

Note: In this scenario, none of the vCenter logins (SSO user) have been successful.

1. Restore the most recent PSC backup and wait for the vCenter services to start.
2. Log in to the vCenter Server Appliance's shell as **root**.
3. Verify that no vCenter services are running, or stop vCenter services.
4. Run the **vc-restore** script to restore the VCSA . The procedure in the previous section provides detailed steps.

Note: If the log in test for any VCSA fails, then the restored PSC is not the PSC that the VCSA is pointing to, in which case you may be required to perform a repoint, as described in the previous section.

5. Deploy the new PSC and join to an active node in the same SSO domain and site.
6. Repoint vCenter connections as required.

Scenario 3: Multiple PSCs fail and VCSA remains

1. Perform an image-level restore of one PSC.
2. Test the VCSA login. If the login fails, repoint the VCSA to an active PSC.
3. Deploy the new PSC and join to an active node in the same SSO domain and site.

Scenario 4: VCSA fails

1. Perform an image-level restore of the lost vCenter Server by using one of the methods mentioned above, and then power ON the vCenter Server.
2. After successfully starting the vCenter Server, verify that all vCenter services have started.
3. Perform a log in test.
4. If the log in test fails, then this VCSA is pointing to an inactive PSC. Repoint the VCSA to an active node.

Note: If a total failure has occurred (all PSCs and all VSCAs failed), restore one PSC first before restoring the VCSA.

Additional considerations

Backing up the vCenter Server will not save the Distributed switch configuration as this configuration is stored on the hosts. As a best practice, back up the vDS configuration by perform the steps in the following VMware KB article. The same steps can then be used to perform a restore of the configuration after restoring the vCenter Server.

https://kb.vmware.com/s/article/2034602

After restoring the PSC, verify that replication has been performed as designed by using the following commands to display the current replication status of a PSC and any of the replication partners of the PSC:

For VCSA, go to **/usr/lib/vmware-vmdir/bin** and type the following command:

./vdcrepadmin -f showpartnerstatus -h localhost -u administrator -w Administrator_Password

For Windows, open a command prompt and type **cd "%VMWARE_CIS_HOME%"\vmdird**.

For example:

Use the following command to start or stop services in the vCenter server/PSC, or obtain the status:

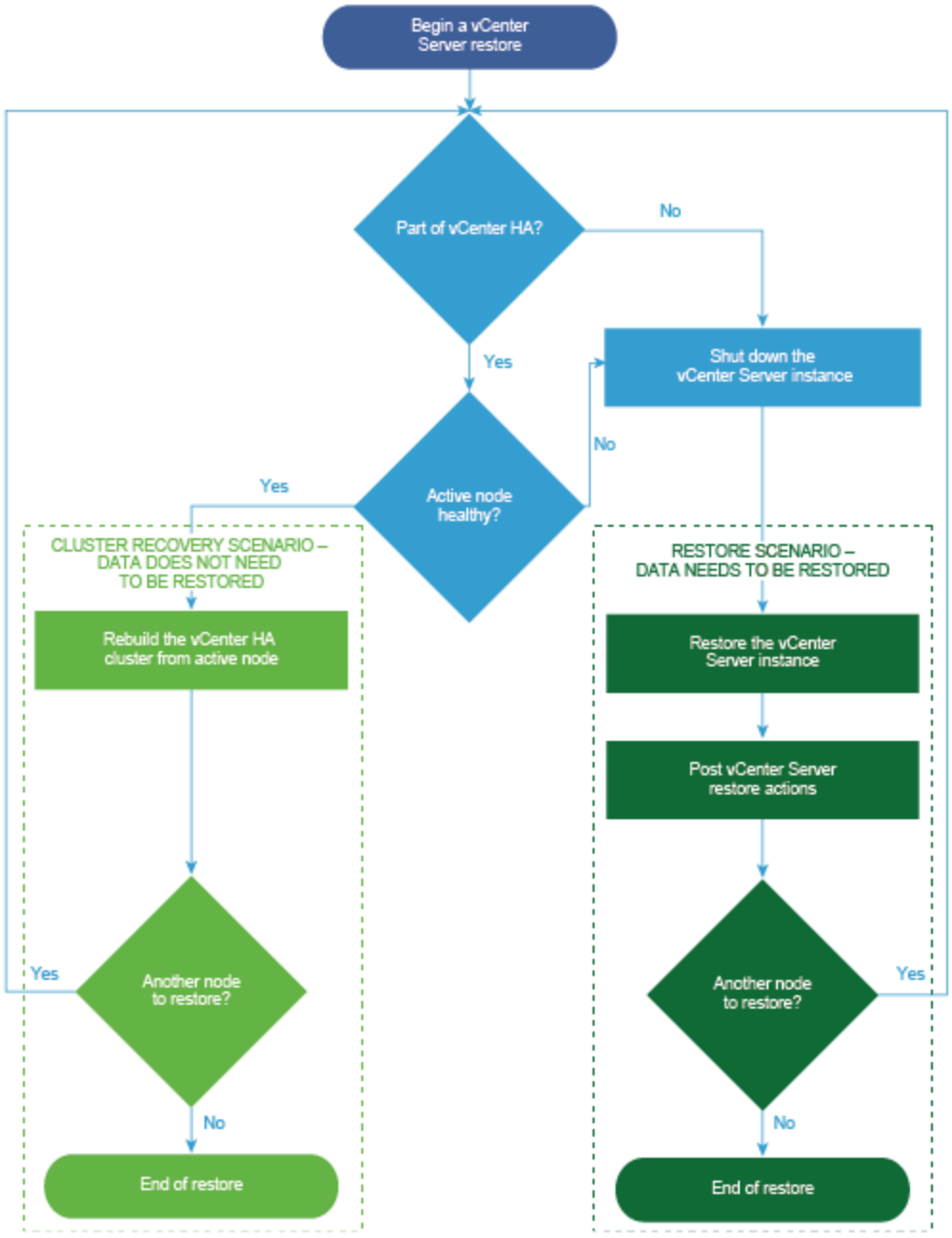
service-control –status/start/stop –all

You can use other Replication topology commands, as in the following example:

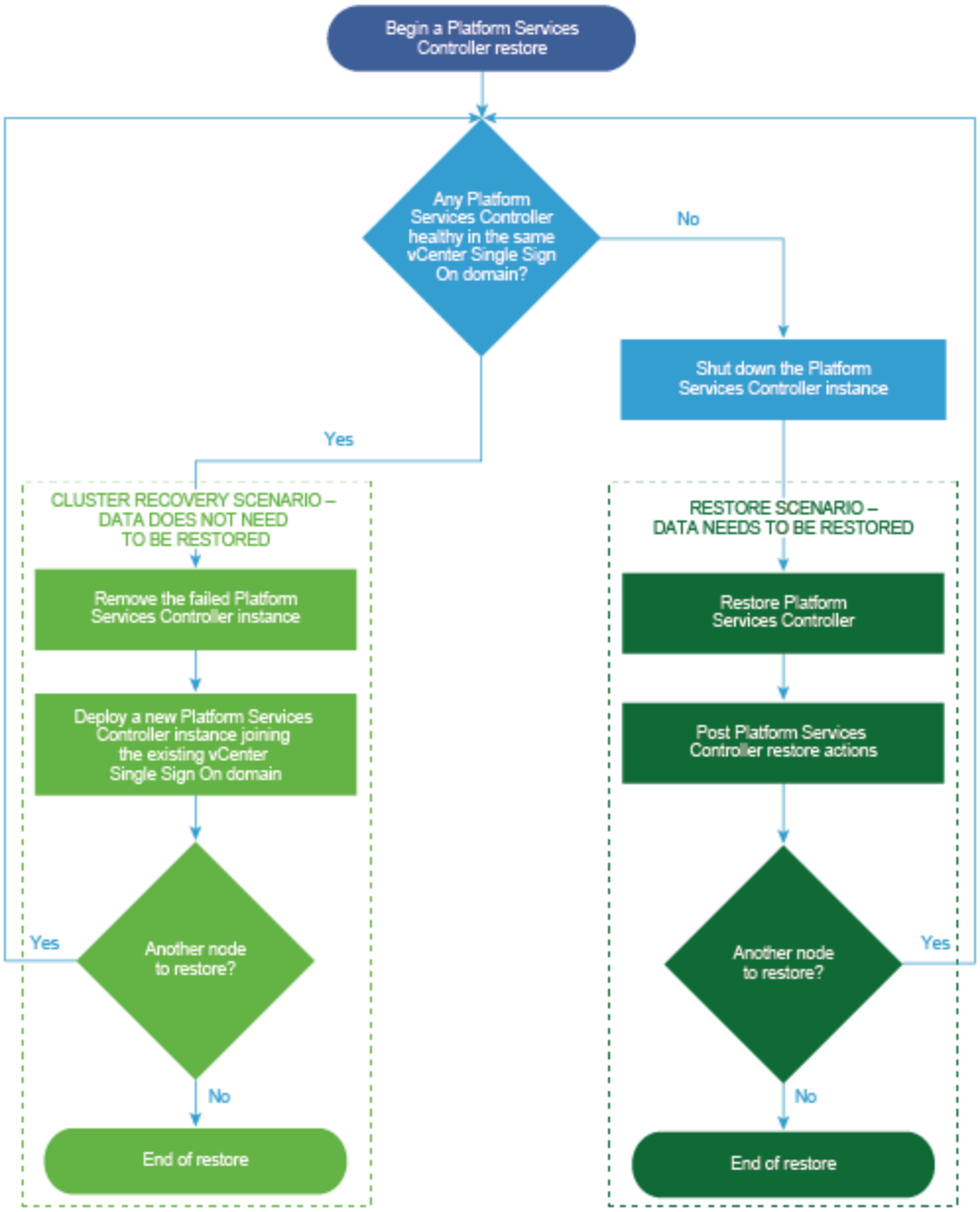
/usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h localhost -u PSC_Administrator -w password

You can replace ‘localhost’ with another PSC FQDN to obtain all of the partnerships in the current vSphere domain.

vCenter Server restore workflow



Platform Services Controller restore workflow



We value your feedback

Dell EMC and the authors of this document welcome your feedback on the solution and the solution documentation. Contact EMC.Solution.Feedback@emc.com with your comments.

References

The following additional resources provide more information.

Dell EMC documentation

The following documentation on EMC.com or EMC Online Support provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell EMC representative.

- Avamar VMware Integration Guide

VMware documentation

The following documentation on the VMware website provides additional and relevant information:

- *VMware vCenter Server documentation*