Executive Summary

This document provides certain best practices with regards to the Emergency Restore feature in vSphere Data Protection 5.5 release. It also describes the methods and processes to be used for protecting a vCenter Server and all its components as well as overall disaster recovery plan using Emergency Restore in case vCenter Server or its components are unavailable.

Emergency Restore Overview

VMware has introduced a new feature called Emergency Restore with vSphere Data Protection 5.5 release. This feature is particularly useful in scenarios where the vCenter server or the vSphere web client is unavailable due to some outage and the user is unable to access the VDP GUI via the vSphere web client. The same can also be used to restore the AD server (in case of Windows 2012) if the authentication being used by vCenter server is the AD and there is an outage of the AD server VM.

A VMware administrator can now access the VDP configure utility and use the Emergency Restore tab in order to perform restore operations even when the vCenter server or the vSphere web client is unavailable. Emergency Restore tab displays a list of virtual machines that have been backed up by the VDP appliance. They can be restored as new virtual machines onto the VSphere server where VDP is running. The progress of the restore job can be seen in the Emergency Restore tab, making it easier for the VMware administrator to monitor the restore tasks.

Benefits of using Emergency Restore for recovery of vCenter server

VDP is dependent on the vCenter Server for many of its core operations and having the vCenter running in a stable environment is critical to achieving a healthy backup environment. Having an outage of the vCenter Server not only affects the core VDP functionality but also the entire vSphere virtual environment hence it is imperative to have a disaster recovery plan for the vCenter Server.

In case of vCenter server being unavailable, VDP provides an option of restoring the vCenter server from its latest backup using Emergency Restore. There are other methods as well which can be used in order to get the vCenter and VDP operational again, such as:

- Reconfigure the existing VDP to point to an alternate vCenter server
- Deploy a fresh VDP appliance in an alternate vCenter server and attach the disks of the previous VDP.
  NOTE: In order to attach disks, the VSphere server should have access to the datastores where the previously used VDP data disks reside.

Using Emergency Restore to recover the vCenter Server has the following benefits as compared to the above methods:

- All previously created backup jobs are maintained and continue to run as per the set schedule
- All previously created replication jobs are maintained and continue to run as per the set schedule

- All previously created restore points are maintained with their original names
- All previously created restore points provide “restore to original location” option as long as the VM is part of the vCenter inventory
- Email reporting continues to run as per the set schedule

This way the user will save the trouble of having to reconfigure everything again once the vCenter and VDP is up and running.

Best practices and Recommendations for Emergency Restore:

- Ensure that VM which is being restored has a virtual hardware version which is supported by the VSphere host where VDP is running.
  TIP: It is recommended to have VDP running on latest VSphere server in order to avoid emergency restore failures due to incompatible virtual hardware version.

- Ensure that there is enough free space in the target datastore to accommodate the entire VM.
  TIP: It is recommended to have a large enough datastore attached to the VSphere host where VDP is running to accommodate your critical VMs in case of Emergency Restore

- Ensure that target datastore where VM is being restored to, is of the latest VMFS version 5.x.
  TIP: It is recommended to have VDP running on latest VSphere server in order to avoid emergency restore failures due to incompatible VMFS block size of target datastores.

- Ensure that the network connectivity is available for the restored VMs.
  TIP: It is recommended to have at least one vSphere standard switch configured on the VSphere host where VDP is running which can be used in case of Emergency Restore.
  If using vSphere distributed switch, in case of vCenter being unavailable, the restored VM would not be able to connect to the network. Hence it is advised that the host where VDP is running has at least one vSphere standard switch connected to the same network/subnet as the VM being restored.

- Ensure that there is at least one local account with administrator privilege on the VSphere host where VDP is running. If using AD credentials for managing the VSphere host where VDP is running, in case of the domain controller VM itself being unavailable due to some outage then the Emergency Restore operation would fail.
  TIP: It is recommended that the host where VDP is running has at least one local user account with administrator privilege, the credentials of which can be specified in the Emergency Restore dialog.

Limitations and unsupported features:

Before you start using the Emergency Restore feature, review the following limitations:

- Emergency Restore allows restore only to the root of the VSphere level in the inventory

- Emergency Restore requires that DNS server used by VDP is available and can fully resolve the hostname of the VSphere server where VDP is running. Also ensure that the both the VSphere server and the VDP appliance point to the same DNS server.
- Emergency Restore restores the VM in powered off state, user will have to manually login to VSphere host and power on the restored VM
- Emergency Restore restores the VM as a new VM, user will have to ensure that the name provided for the VM is not a duplicate of a VM that already exists
- Emergency Restore requires the VSphere host where VDP is running to be disassociated from the vCenter. Please refer to the section "How to disassociate an VSphere host from vCenter" for instructions.

Process steps for protecting vCenter Server:

The vCenter Server is a virtualization management solution from VMware that provides centralized control of the entire virtual infrastructure. The vCenter Server offers core services related to resource management and high availability for VSphere hosts and VMs, VM and template management, VM deployment, scheduled tasks and alarms, event management, statistics, and logging.

For small vSphere deployments one can have the vCenter Single Sign-On, Inventory Service, vCenter Server, and vSphere Web Client on the same virtual machine. Alternatively, one can install each of the above components separately in a different virtual machine.

NOTE: It is recommended to schedule the backup of the vCenter server when the load on the server is low such as during off hours, this is to minimize the impact of snapshot creation and snapshot commit processing overhead.

Steps for performing a backup of vCenter Server depends on the type of deployment of vCenter Server. Follow the appropriate backup mechanism as described next:

In case of vCenter Server having all its components installed on the same virtual machine:

- Ensure the VSphere host where vCenter Server VM is running is also part of the vCenter inventory.
- Create a backup job containing the standalone vCenter Server VM.
- Ensure that the job is scheduled appropriately i.e. daily or weekly or monthly.

In case of vCenter Server having a few or all components running on separate virtual machines:

- Ensure the VSphere host where each component VM is running is also part of the vCenter inventory
- Create separate backup jobs as per following grouping:
    - Job1- vCenter database VM
    - Job2- vCenter Server VM
    - Job3- Inventory Service VM
    - Job4- vSphere Web Client VM
    - Job5- Single Sign-On VM

  Having each component VM associated with a separate backup job helps in scheduling the backups to occur one after the other and minimize the stun/unstun effect of snapshot operations.

- Ensure that the backup jobs start in the same sequence as shown above and there is enough time gap of around 5 to 10 minutes between the start time of each job in order to minimize the snapshot creation overhead and stun/unstun operations.
- Ensure that all the above jobs follow the same schedule and choose appropriately i.e. daily or weekly or monthly.
- In case of having more than one component running on same VM, follow the same order of backup as shown above albeit combining the required components into one.

NOTE: It is recommended that, in addition to the image level backup of the VM running the vCenter database, database backup is done using recommended method as per the database vendor to ensure complete application level consistency. Image level backups only provided crash-consistent backups of the database.

<u>Process steps for recovering vCenter Server and its components:</u>

In case of vCenter Server having all its components installed on the same virtual machine:

- Perform emergency restore of the vCenter Server VM using the latest restore point
- Login to VSphere host using vSphere client
- Ensure that the restored VM has appropriate network label assigned
- Power on the vCenter Server VM
- Once powered on, login to the VM and ensure all the required services are up and running
- Login to the vSphere web client and ensure the VSphere hosts are in connected state
- Check that VDP is accessible via the web client

In case of vCenter Server having few or all its components running separately in different virtual machines:

- Perform emergency restore of each of the component VMs using the latest restore points
- Login to VSphere host using vSphere client
- Ensure that each of the restored VMs have appropriate network label assigned
- Power on the VMs in the following order and in each VM verify that the required service is up and running before attempting to power on the subsequent VM:
    - Single Sign-on – VMware Directory Service
    - vSphere Web Client – VMware vSphere Web Client service
    - Inventory Service – VMware vCenter Inventory Service
    - SQL server VM – SQL server service
    - vCenter Server VM – VMware VirtualCenter Server service
- Once all VMs are powered on and verified to be running, login to the vSphere web client and ensure the VSphere hosts are in connected state.
- Check that VDP is accessible via the web client

<u>Process steps for protecting Domain Controller VM:</u>

Starting from Windows 2012 onwards, Microsoft has introduced capability of performing image based restores safely in the case of virtualized domain controllers.
VDP can be used to protect the domain controllers using image backup and this will come handy in case of any outage of the domain controller VM. This is particularly useful in cases where vCenter authentication is handled by a virtualized domain controller. Any outage of the Domain Controller VM

will also end up preventing access to vCenter Server due to Active Directory being down. Hence it is imperative that the Domain Controller VM is also being protected by VDP appliance.

NOTE: It is recommended that in addition to image level backups of domain controller VM, the Active Directory backup is done using the AD-aware backup methodology. The process discussed in this paper is in no way a replacement for the AD-aware backup as the DC is restored in a non-authoritative way when image level restores are performed.

In case of standalone domain controller installed in a Windows 2012 virtual machine:

- Ensure the VSphere host where the domain controller VM is running is also part of the vCenter inventory
- Create a backup job containing the standalone domain controller VM
- Ensure that this is scheduled appropriately i.e. daily or weekly or monthly

<u>Process steps for recovering Domain Controller VM:</u>

In case of standalone Domain Controller installed in a virtual machine:

- Emergency Restore has a dependency on having the hostname of VSphere where VDP is running to be fully resolvable from the VDP appliance.
  In case of an outage of the DNS server, it is recommended that you perform the following steps first
  - Login to the VDP appliance as root user via SSH
  - Edit the /etc/hosts file using vi editor and add the entry, in the last line of the file, for the VSphere where VDP is running as shown below:

    ```
    root@vdp-250-107:~/#: vi /etc/hosts
    # Generated by av_boot.rb
    192.168.250.107     vdp-250-107.privhr01.com vdp-250-107
    127.0.0.1  localhost.localdomain localhost
    ::1       localhost.localdomain localhost
    192.168.6.200   esx01.privHR01.com esx01
    ```

  - Save the /etc/hosts file
  - Login to the VDP configure utility
  - Stop and Start the Management Services for the hosts file entry to take effect
- Perform emergency restore of the domain controller VM using the latest restore point
- Login to VSphere host using vSphere client
- Ensure that the restored VM has appropriate network label assigned
- Power on the Domain Controller VM
- Verify the Directory Service event log to confirm that AD realizes there has been a rollback to previous snapshot and it has automatically initiated the safe restore of the AD. You will see messages such as these:

  ```
  The invocationID attribute for this directory server has been changed. The highest update sequence number
  at the time the backup was created is as follows:
   InvocationID attribute (old value):
  7cd58864-7088-46a7-90b6-ece0a32582cd
  InvocationID attribute (new value):
  ebbdb10c-430a-47c9-b571-b66d4cfa1b87
  Update sequence number:
  ```

70784

- Once powered on, login to vSphere web client with the required AD credentials
- Check that VDP is accessible via the web client
- Finally log back into the VDP appliance as root user via SSH and remove the added entry of the hosts file
- Stop and Start both the Management and the Backup scheduler service, this brings VDP appliance back to the state as it was before performing Emergency Restore.

How to disassociate an VSphere host from vCenter:

Before performing Emergency Restore, the VSphere host where VDP is running should be disassociated from the vCenter. Do note that you do not need to place the host in Maintenance Mode.
The steps to disassociate a host of version 5.0 or above are as follows:

- Using the vSphere Client, connect directly to the VSphere host system.
- In the left (inventory) panel, click the host.
- In the right-hand panel, click Summary.
- From the section named Host Management at the bottom right, click Disassociate host from vCenter Server.

If using VSphere host version 4.1 or lower, the disassociation has to be done as follows:

- Using the vSphere Client, connect directly to the VSphere host system as user having administrator privilege on the host, such as the root user.
- In the left (inventory) panel, click the host.
- In the right-hand panel, click Local Users & Groups.
- Right click the user vpxuser, click Remove.
- Click Yes to remove the user.
- Restart the Management agents on the VSphere host. Refer to the below kb article for instructions
  http://kb.vmware.com/kb/1003490

NOTE: After the restore of the vCenter Server is complete, ensure that the host running the VDP is connected back again to the vCenter Server.

Conclusion:

In this paper we have looked at the Emergency Restore feature that is available with version 5.5 of vSphere Data Protection. Emergency Restore feature removes the dependency of vCenter server for performing the VM restores and it provides the much needed option of restoring any VM even in case of an outage of the vCenter server or its components. The information in this paper provides VM admins the best practices needed to use this feature and also guidance interms of protecting the vCenter server and its components using VDP.