DELL Technologies

White Paper

Backup and Recovery for VMware Cloud Foundation 4.2 on Dell EMC VxRail with Dell EMC NetWorker 19.4

Abstract

This paper explains how Dell EMC NetWorker 19.4 software can be used to protect VMware Cloud Foundation (VCF) 4.2 Management and Workload domains running on Dell EMC VxRail 7.0.

May 2021

H18830

Revisions

Date	Description
May 2021	Initial release

Acknowledgments

Author:

Denis Twomey, Dell Technologies Customer Solution Centers

About Dell Technologies Customer Solution Centers

Dell Technologies Customer Solution Centers help customers explore and validate the Dell Technologies portfolio of hardware, software and solutions. Each of our global Customer Solution Centers is staffed by deep subject matter experts, working in state-of-the-art labs equipped with the latest technologies and showcases.

Services provided by Customer Solution Centers include technical briefings, architectural design workshops and Proofs of Concept (POCs) that allow customers to validate their chosen solution.

Customers may engage with their account team to take advantage of one of these free services.

Learn more at https://www.delltechnologies.com/csc

Table of contents

Scope

This paper arises from a Proof of Concept that was recently carried out by Dell Technologies Customer Solution Centers to support a customer engagement involving a data protection solution for VMware Cloud Foundation (VCF) 4.2 Management and Workload domains on Dell EMC VxRail using Dell EMC NetWorker 19.4. In this paper, we document the environment and procedures that were used during the Proof of Concept. It is our intention that the information contained in this document can be used by customers and partners as a reference when making implementation decisions for their particular environment.

The scope of this document is limited to:

- Dell EMC NetWorker (software) protecting VCF 4.2 on Dell EMC VxRail 7.0.132
- How to perform image-level and file-level backups and restores of the various components
- Subsequent recovery of VCF management and workloads on Dell EMC VxRail.

This paper describes which components must be backed up and how this is performed. Some components will require image-level backups while others will require file-level backups. The backup and restore strategies described in this paper could also be applied to other backup software.

Please note:

- It is assumed the reader of this paper has a working knowledge of how NetWorker, VxRail and VCF components work.
- Due diligence is required to determine the software and hardware versions and sizing of the various components to fit a customer's VCF environment.
- All details are accurate at time of writing but are subject to change in the context of product updates.

Environment overview

This section describes the environment that was used to create this white paper.
The components and versions used were:

- Dell EMC NetWorker 19.4
- Dell EMC PowerProtect Data Domain Virtual Edition 7.2
- VMware Cloud Foundation (VCF) 4.20
- Dell EMC VxRail 7.0.131-26875681

Figure 1 describes the high-level architecture of the tested environment. Figure 2 illustrates the logical VLAN network layout, including production and backup traffic flow. For full configuration details of the tested environment, please refer to the Appendix titled “Configuration details”.

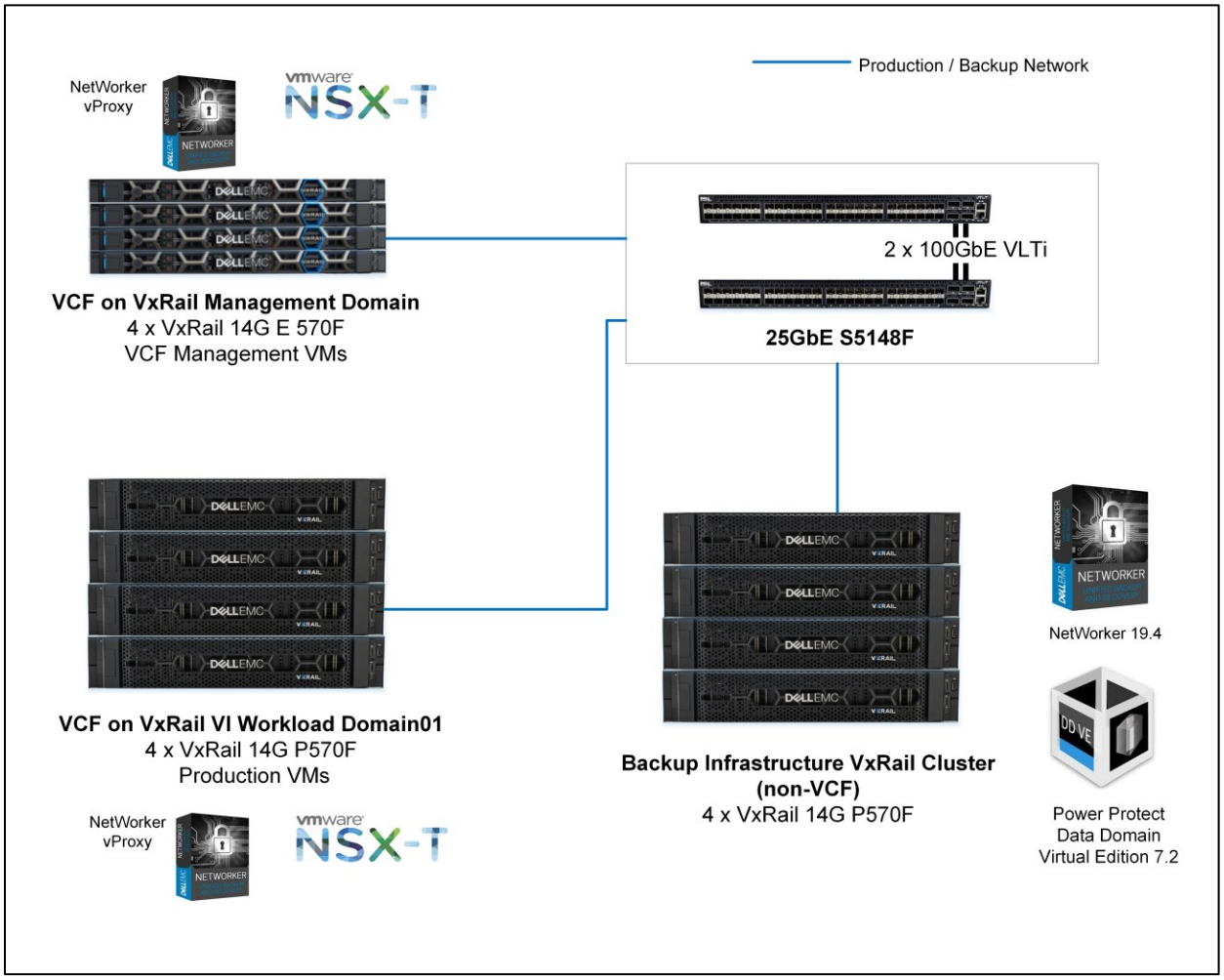

Figure 1 High-level architecture of the tested environment

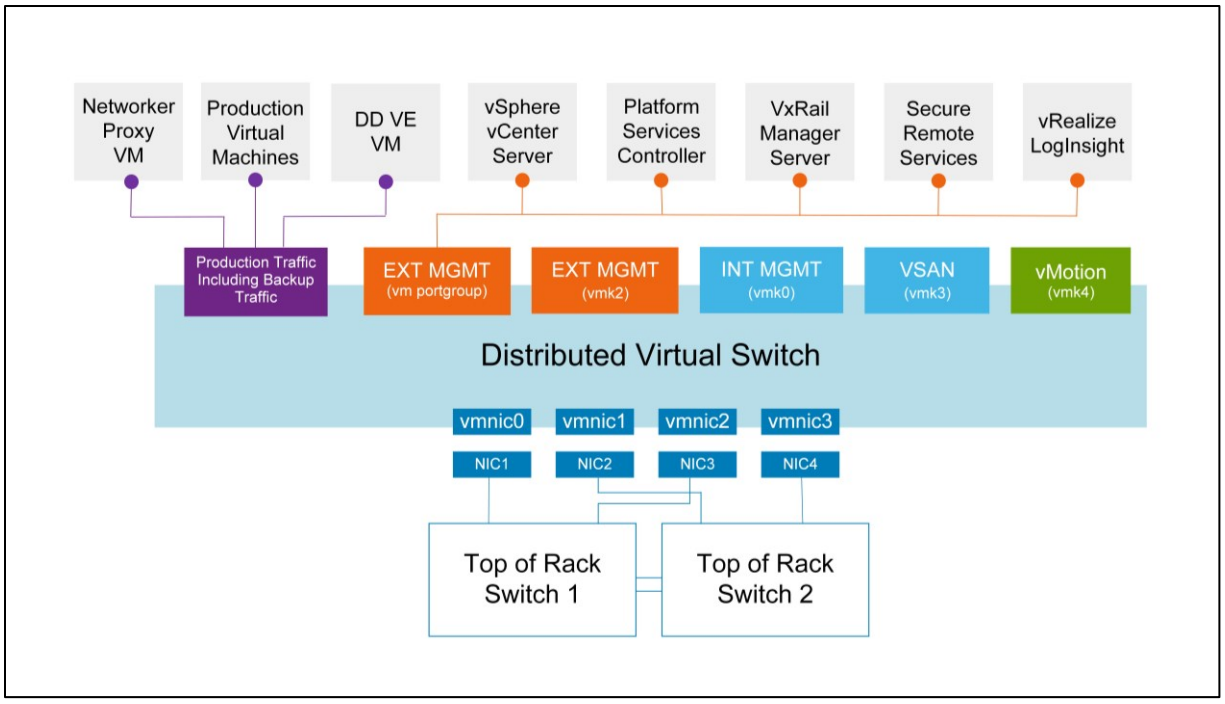

Figure 2 Dell EMC VxRail 7.0.131-26875681 VLAN Layout

VCF on VxRail reference environment build process

The following process was used to install, configure and verify VCF on VxRail.

1. Deploy and configure VxRail 7.0.131-26875681.
2. Validate the VxRail installation and verify that it is running as expected.
3. Deploy Cloud Builder 4.2.0.0-17559673
4. Use Cloud Builder to deploy and configure the VCF / SDDC 4.2 environment

The full bill of materials that was used in the VCF build is described in Table 1, and is also described in the VCF 4.2 on VxRail Release Notes.

Table 1 VMware Cloud Foundation 4.2 installation: Bill of materials

Software component	Version	Date	Build number
Cloud Builder VM	4.2	9 FEB 2021	17559673
SDDC Manager	4.2	9 FEB 2021	17559673
VMware vCenter Server Appliance	7.0 Update 1c	17 DEC 2020	17327517
VMware ESXi	7.0 Update 1d	04 FEB 2021	17551050
VMware NSX-T Data Center	3.1.0	30 OCT 2020	17107167
VMware vRealize Suite Lifecycle Manager	8.2 Patch 2	04 FEB 2021	17513665
Workspace ONE Access	3.3.4	04 FEB 2021	17498518
vRealize Automation	8.2	06 OCT 2020	16980951
vRealize Log Insight	8.2	06 OCT 2020	16957702

The following table lists the VMs that require backup.

Table 2 VCF VMs requiring backup

VM Name	Workload Domain	Backup required
Vcf-mg-lcm	Management	Required
Vcf-mg-nsx	Management	Required
Vidm-primary	Management	Required
Vcf-mg-nsxt-n1	Workload Domain1	Required
Vcf-mg-nsxt-n2	Workload Domain1	Required
Vcf-mg-nsxt-n3	Workload Domain1	Required
Vcf-mg-nsxt9-n1	Workload Domain1	Required
Vcf-mg-nsxt9-n2	Workload Domain1	Required
Vcf-mg-nsxt9-n3	Workload Domain1	Required
Vcf-w1-edge3	Workload Domain1	Required
Vcf-w1-edge4	Workload Domain1	Required
Vcf-mg-NW194-vp	Management	Required
Vcf-mg-sddc	Management	Required
Vcf-mg-vcsa	Management	Required
Vcf-mg-vrli	Management	Required
Vcf-mg-vrli-n1	Management	Required
Vcf-mg-vrli-n2	Management	Required
Vcf-mg-vxm	Management	Required
Vcf-t9-vcsa	Workload Domain1	Required
Vcf-t9-vxm	Workload Domain1	Required

Figure 3 shows the vSphere view of the environment; the Management Domain components are marked in blue, the Workload Domain components are marked in green.

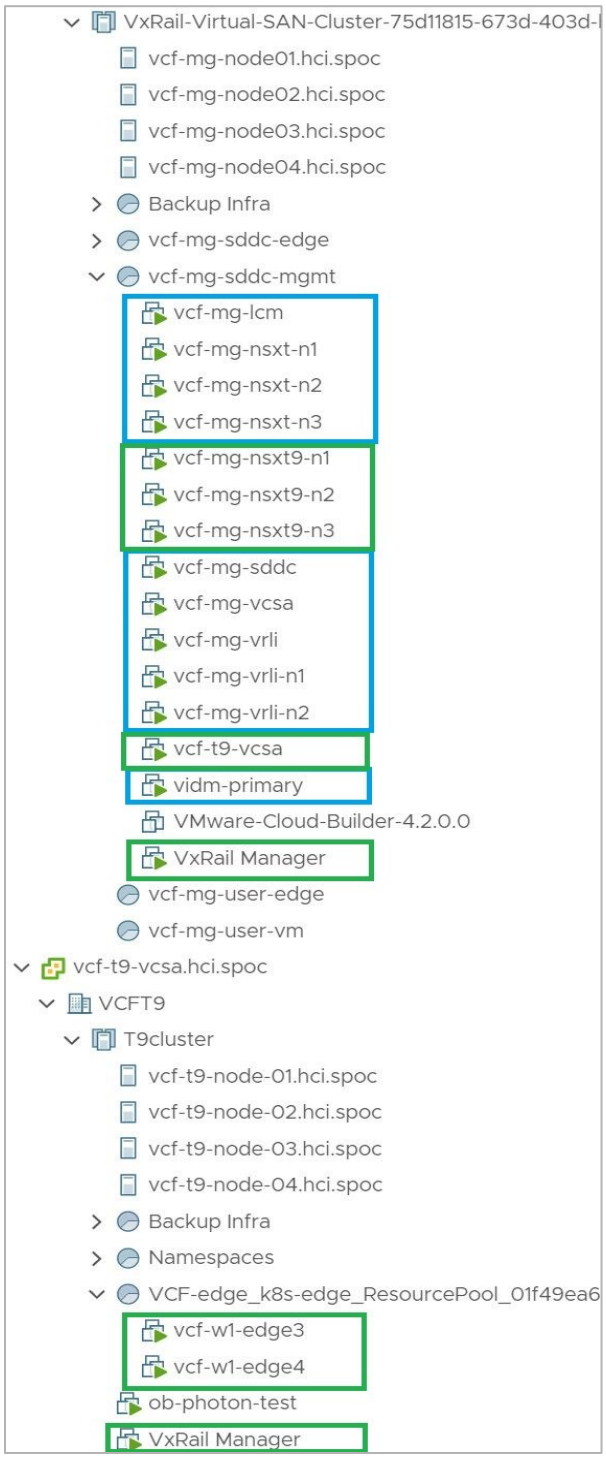

Figure 3 VCF Management and Workload Domain vCenter view

NetWorker and Data Domain

As shown in Figure 4, a separate vCenter was used to host NetWorker 19.4 and the PowerProtect Data Domain Virtual Edition (VE) 7.2. All the backup and production traffic shared the same VLAN.

NetWorker 19.4 consists of the NetWorker server and a built-in storage node. Data Domain VE was configured, licensed and then integrated with NetWorker as a target for backups.

NOTE: NetWorker and PowerProtect Data Domain VE can also be deployed on the vCenter where VCF resides if preferred.

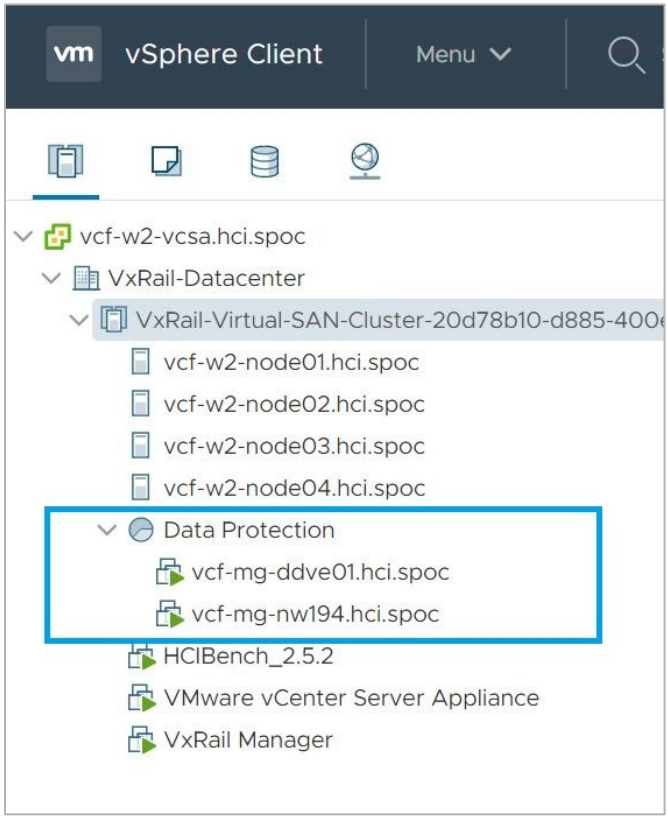

Figure 4 Data protection infrastructure – separate vCenter

The NetWorker console was then used to discover the VCF Domain and Workload Domain vCenters, as shown in Figure 5 (the Management domain is marked in blue, the Workload domain is marked in green).

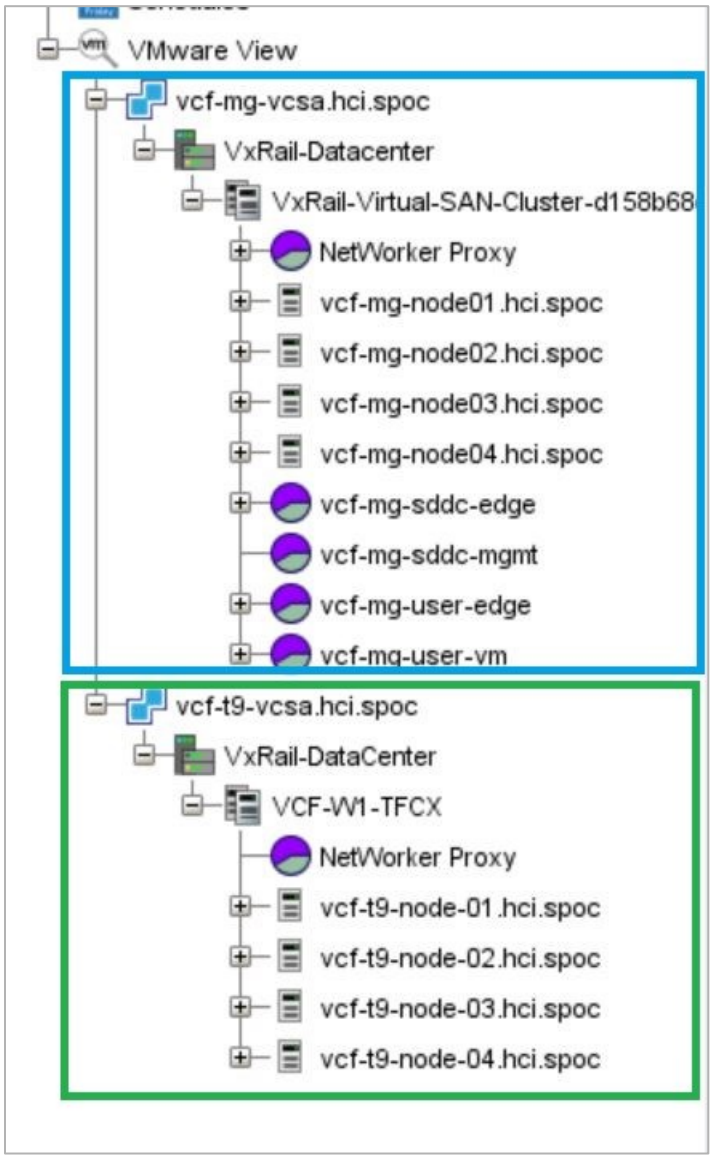

Figure 5 NetWorker console: Management and Workload vCenters

A NetWorker vProxy was deployed on the VCF Management Domain vCenter and a second NetWorker vProxy was deployed on the Workload Domain vCenter. The Networker vProxy VMs have two IP addresses; one IP address is on the management network and a second NIC is on the production network which allows the VM to communicate from the VCF environment to the Backup environment.

NOTE: For best practices on vProxy recommendations and scaling refer to the NetWorker product documentation.

Backup

In order to successfully recover a destroyed or partially destroyed VCF infrastructure, there are a number of VMs and other configuration data that must be restored from a backup. Table 3 lists the components of VCF that must be backed up and the type of backup that is required in each case.

At the time of writing this paper, the backup methods below were recommended, however, these are subject to change in the context of future releases.

Table 3 Backup methods for VCF core components

VM name (core component)	Backup method
Management vCenter Server	Image level
Workload vCenter Server	Image level
SDDC Manager	Image level
Log Insight Nodes	Image level
NSX-T Manager	File level
VxRail Manager(s)	Image and File level
VMware Workspace ONE Access (VIDM)	Image Level
Workload Edges	Image Level

There are also a number of optional VCF components that may be part of your environment and that should be backed up if they are present. Table 4 lists these optional VCF components and the type of backup method that is required in each case. The components listed in Table 4 were not in scope for this paper.

Table 4 Backup methods for VCF optional components

VM name (optional components)	Backup method
vRealize Automation Appliances	Image level
vRealize Automation Proxy Agents	Image level
vRealize Log Insight Appliance	Image level
vRealize Operations Manager	Image level
Life Cycle Manager Appliance (LCM)	Image level
Windows SQL Server	Image level / application level (NetWorker NMM module)

NetWorker initiates the image-level backups on a schedule and uses the vProxies on each vCenter to perform both the backups and the restores. The procedure for image-level backups and restores is discussed in more detail later in this chapter.

In order to carry out file-level backups of the NSX-T virtual machines, some manual configuration of their corresponding managers is required. It is a VMware best practice to back up the NSX-T configurations to an external SFTP server, this is discussed in more detail later in this chapter.

The VxRail Manager file-level backup also requires some manual configuration on the VxRail Manager VM to ensure that it is being backed up correctly. VxRail Manager backups are written to the vSAN by default, this is discussed in more detail later in this chapter.

In this paper we are also optionally recommending that NetWorker perform file-level backups of the data that is stored on the SFTP server. Backup of this data is not mandatory, however, we strongly recommend that it is performed to protect from the loss of the SFTP server.

Image-level backups

This section explains how to perform image-level backups of the associated VCF on VxRail Management components.

NOTE: The information provided in this section assumes that the reader has a working knowledge of NetWorker. Please refer to the relevant version of the NetWorker Administration Guide.

1. Create a NetWorker Group to act as a backup target for all the images of the Management Domain.

    a. For **Group Type,** select VMware.
    b. Under **VMware > vCenter**, select the VCF Management vCenter and then select each of the VMs that require backup, see Table 3 - Backup methods for VCF core components. Table 4 - Backup methods for VCF optional components, may also need to be considered depending on the environment.

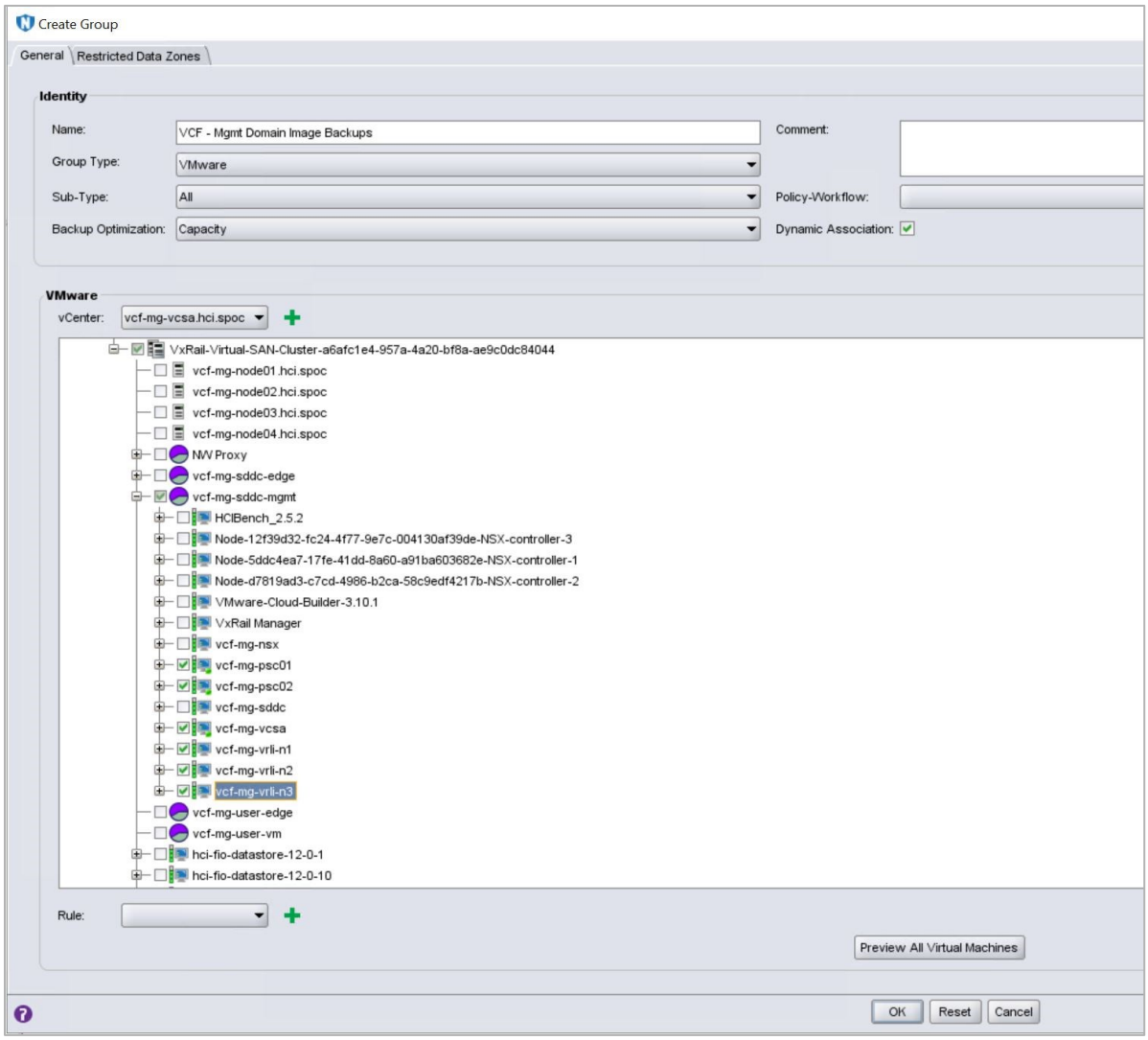

Figure 6 NetWorker: Create NetWorker Group

NOTE: The VCSA for the Workload Domain sits in the Management Domain, this means that the backup of the VCSA for the Workload Domain will be carried out by the Management Domain's Image Backup Policy.

2. Repeat step 1 for the Workload Domain.
3. Create a Policy and schedule the Image Backups for both the Management Domain and the Workload Domain.

NOTE: Although it is possible to backup all images from both domains within a single Group / Policy it is recommended that you create separate Groups / Policies for logical separation.

In the testing carried out for this paper, image-level backups were divided into 6 logical Groups, with a corresponding Policy created for each Group. These Groups / Policies were as follows:

- Management Domain – Image backups
- Management Domain – NSX file backups
- Management Domain – VxRail file backups
- Workload Domain – Image backups

- Workload Domain – NSX file backups
- Workload Domain – VxRail file backups

Figure 7 shows how this looks in NetWorker.

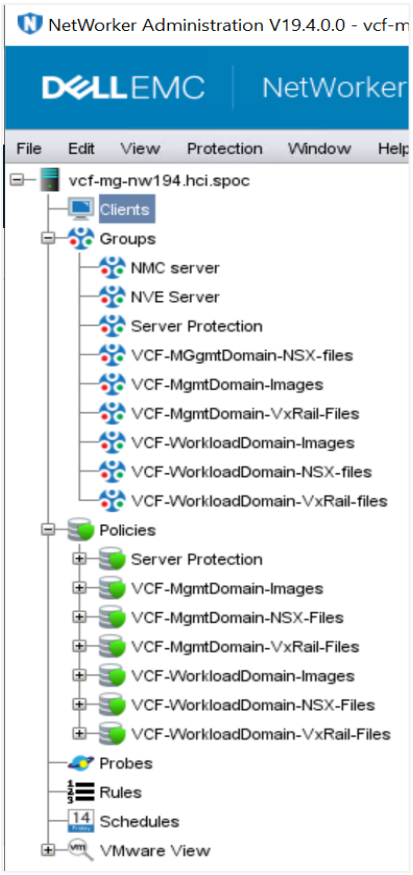

Figure 7 NetWorker: Groups and Policies view

All Groups / Policies should be scheduled to run at the same time, so that the image-level backup process captures what was taking place in the components at the same time – almost like a point-in-time snapshot.

In the testing carried out for this paper, all backups were configured to write to a PowerProtect Data Domain. Figure 8 shows the NetWorker UI while some backups are in progress and others have completed.

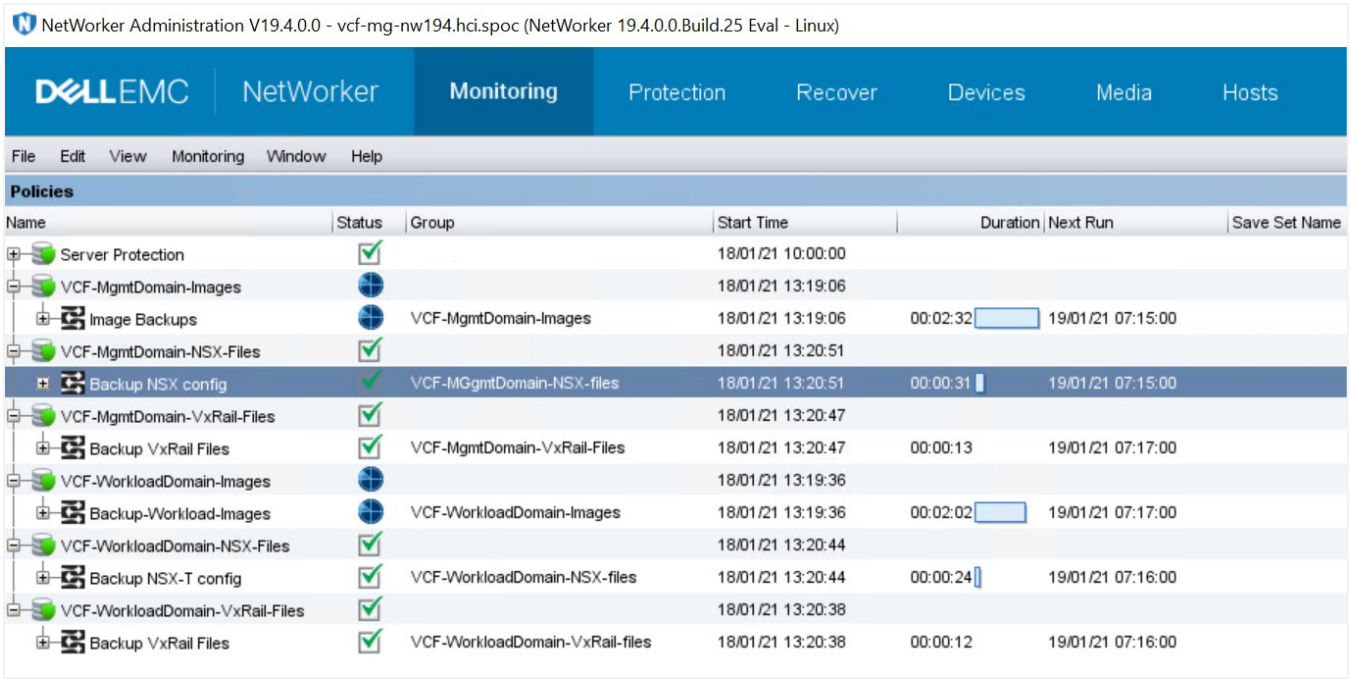

Figure 8 NetWorker: Backups in progress

File-level backups: NSX-T configuration files

As mentioned earlier, it is a VMware best practice to automatically back up the NSX-T configuration files to an external SFTP server.

To configure the backups for NSX-T use HTTPS to connect to the NSX-T Manager VM and then configure the backup server and folder. The procedure documented below describes how to do this.

Ensure that the procedure is followed for both the Management Domain and the Workload Domain NSX-T environments.

NSX-T backup configuration

This section describes how to back up the NSX-T configuration.

NOTE: It is not a requirement to back up the Edge devices in order to recover the NSX-T component.

1. Connect to the NSX-T Manager over https.
2. Navigate to the **Backup & Restore** tab under **System**.
3. It may already be configured but the screen should resemble Figure 9.

Figure 9 NSX-T: Backup configuration

4. Ensure that the **Backup** tab is selected and click **EDIT**.
5. Enter the details for the SFTP server.

IMPORTANT: Keep careful record of the **Passphrase**, it is needed for Restore.

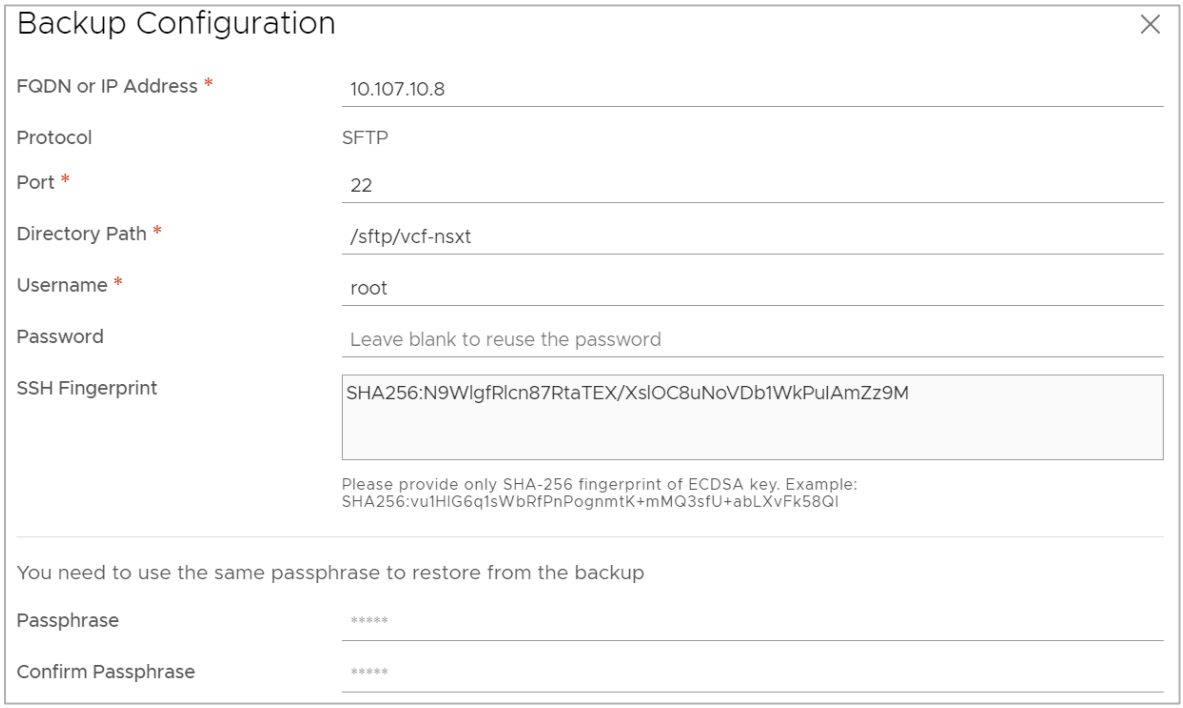

Figure 10 NSX-T: Backup Configuration

The system will now carry out periodic backups on its own schedule.

NOTE: Perform this procedure for both the Management and the Workload Domains.

Confirmation of NSX-T backups

To confirm that backups are being backed up to the SFTP server follow the procedure below. Ensure that you check for both Management Domain and Workload Domain NSX-T backups.

1. Connect over SSH to the SFTP server.
2. Navigate to the folder that was configured for the backup.
   This folder should contain files after a backup has been performed.

IMPORTANT: NSX-T backups are stored with a Node ID and IP address; this IP address is needed to carry out a Restore.

NSX-T has one important difference from NSX-V backups that must be understood; along with the timestamp, the backups are stored with a Node ID and IP address, it will always be the same IP address. As part of the Restore process you will need to re-deploy the NSX-T Manager OVA, if the OVA is not deployed with the same IP address that is listed with the backups, the NSX-T backups will not be available for restore.

We advise that you take note of the IP address when the environment is operational.

To find the IP embedded with the backups:

1. Use SSH to connect to NSX-T node 1 and execute the following commands (the output below is provided as an example):

```
cd /var/vmware/nsx/file-store
ls -l
aggsvc_poll_intervals_change_helper.py
get_backup_timestamps.shbackup_restore_helper.py
nsx_backup_cleaner.py

./get_backup_timestamps.sh
Enter file server ip: 10.107.10.8
Enter port:22
Enter username: root
Enter directory path: /sftp/vcf/new-nsxt
```

2. Enter number of latest backup or press **Enter** to list all backups:

```
The authenticity of host '10.107.10.8 (10.107.10.8)' can't be
established.
ECDSA key fingerprint is
SHA256:N9WlgfRlcn87RtaTEX/XslOC8uNoVDb1WkPuIAmZz9M.
Are you sure you want to continue connecting (yes/no)? yes
root@10.107.10.8's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2021-01-22;12:05:30    10.107.31.26    02d30a42-39c7-cbaf-4825-
64f0f0a56c96
2021-01-22;12:06:39    10.107.31.26    02d30a42-39c7-cbaf-4825-
64f0f0a56c96
2021-01-22;12:08:35    10.107.31.26    02d30a42-39c7-cbaf-4825-
64f0f0a56c96
2021-01-22;12:13:35    10.107.31.26    02d30a42-39c7-cbaf-4825-
64f0f0a56c96
```

Note the IP address. Ensure that the re-deployed OVA has the same IP address to enable recovery of the NSX-T environment.

File-level backups: VxRail Manager configuration files

In order for VxRail Backups to be successfully captured in VCF 4.2, the following points must be considered:

- Ensure that the automatic backup of the VxRail configuration files is being run by the internal cron scheduler on VxRail Manager.
- These backups are stored on the vSAN only. To get these backups off the vSAN and onto the SFTP server, and in turn onto NetWorker, a manual procedure is required, as outlined in step 6-10 below.

NOTE: We have tested image-level backups and restores of VxRail Manager successfully. It is expected that support for image backups will be included in a future VxRail release.

1. Log into the VxRail VM as the “mystic” user.
   This can be done either from the vSphere Web Console or by using SSH.
2. Type the command:
   `sudo su`
   Or
   `sudo su root`
3. Navigate through the folder structure as follows:
   `cd /mystic/vxm_backup_restore`
4. To find out if there are backups already running, type the following command to list the backups:
   `python vxm_backup_restore.py -l`
   If the backup scheduler is not set, the following message will display:

   `Backup management file is not found in datastore`

   Go to step 5.

   If backups have been scheduled, a list of backups will display similar to those shown in Figure 11.

   Go to step 6.

```
[root@vcf-mg-node01:/vmfs/volumes/vsan:52bc0f774bcdfc5f-39c5bde62fc2a8ca/92d0fd5f-904d-cb72-2108-e4434b8802b0] pwd
/vmfs/volumes/vsan:52bc0f774bcdfc5f-39c5bde62fc2a8ca/VxRail_backup_folder
[root@vcf-mg-node01:/vmfs/volumes/vsan:52bc0f774bcdfc5f-39c5bde62fc2a8ca/92d0fd5f-904d-cb72-2108-e4434b8802b0] ls -al *.tgz
-rw-------    1 root     root      58555780 Jan 12 16:38 VxRailArchive_20210112163837_16804010.tgz
-rw-------    1 root     root      90154955 Jan 13 07:00 VxRailArchive_20210113070003_16804010.tgz
-rw-------    1 root     root     121174358 Jan 14 07:00 VxRailArchive_20210114070003_16804010.tgz
-rw-------    1 root     root      10315004 Jan 14 11:15 VxRailArchive_20210114111516_16804010.tgz
-rw-------    1 root     root     155217446 Jan 15 07:00 VxRailArchive_20210115070004_16804010.tgz
-rw-------    1 root     root     166445380 Jan 16 07:00 VxRailArchive_20210116070003_16804010.tgz
-rw-------    1 root     root     171356510 Jan 17 07:00 VxRailArchive_20210117070004_16804010.tgz
-rw-------    1 root     root     177710924 Jan 18 07:00 VxRailArchive_20210118070004_16804010.tgz
[root@vcf-mg-node01:/vmfs/volumes/vsan:52bc0f774bcdfc5f-39c5bde62fc2a8ca/92d0fd5f-904d-cb72-2108-e4434b8802b0]
```

Figure 11 VxRail Manager: SFTP backups

5. Type the following command and follow the interactive prompts to setup the scheduler for the backups.
   `python vxm_backup_restore.py -c`
   The options for the scheduler are manual, daily, weekly or monthly. One of the interactive command line prompts will ask for a time to run the scheduler.
6. Manually create a backup by typing the following command:
   `python vxm_backup_restore.py -b`

Verify that there is now a backup listed on the vSAN from the one that was just performed with the previous command:
`python vxm_backup_restore.py -l`
The backup files look like this:
`VxRailArchive_20210112163837_16804010.tgz`

The backup will also create a separate file called `vmbackup.json`.

The backup command in step 6 will write backups to the vSAN datastore only. To have backups copied to the SFTP server, continue to step 7 and complete all the steps described in this procedure.

7. Create a folder on the SFTP server for VxRail Manager backups.
8. Log on to one of the ESX nodes using SSH.

NOTE: First, you may need to enable/start SSH and ESXi shell daemons on the ESXi node via services.

9. Navigate to the folder on the vSAN storage where the backups are stored. For example:.
   `cd /vmfs/volumes/vsan<your vsan cluster location>`
   `cd VxRail_backup_folder`
   There should be files in the backup folder in .tgz format, similar to what is show in Figure 11.
10. SCP the VxRail Manager configuration backups of both the Management and Workload Domains to their respective SFTP server folders.

    Management and Workload domains for our environments are shown below as an example:

```
scp *.tgz root@hci-sftp.hci.spoc:/sftp/vcf-vxm-mgmt
scp *.json root@hci-sftp.hci.spoc:/sftp/vcf-vxm-mgmt

scp *.tgz root@hci-sftp.hci.spoc:/sftp/vcf-vxm-wld
scp *.json root@hci-sftp.hci.spoc:/sftp/vcf-vxm-wld
```

    Figure 12 shows an example of SCP being performed.

```
[root@vcf-mg-node01:/vmfs/volumes/vsan:52bc0f774bcdfc5f-39c5bde62fc2a8ca/92d0fd5f-904d-cb72-2108-e4434b8802b0] pwd
/vmfs/volumes/vsan:52bc0f774bcdfc5f-39c5bde62fc2a8ca/VxRail_backup_folder
[root@vcf-mg-node01:/vmfs/volumes/vsan:52bc0f774bcdfc5f-39c5bde62fc2a8ca/92d0fd5f-904d-cb72-2108-e4434b8802b0] scp *.tgz
root@hci-sftp.hci.spoc:/sftp/vcf/vxrail-mgmtdom
root@hci-sftp.hci.spoc's password:
VxRailArchive_20210112163837_16804010.tgz                                   100%   56MB  79.8MB/s   00:00
VxRailArchive_20210113070003_16804010.tgz                                   100%   86MB  79.5MB/s   00:01
VxRailArchive_20210114070003_16804010.tgz                                   100%  116MB  77.9MB/s   00:01
VxRailArchive_20210114111516_16804010.tgz                                   100%   10MB  72.7MB/s   00:00
VxRailArchive_20210115070004_16804010.tgz                                   100%  148MB  83.9MB/s   00:01
VxRailArchive_20210116070003_16804010.tgz                                   100%  159MB  85.9MB/s   00:01
VxRailArchive_20210117070004_16804010.tgz                                   100%  163MB  83.4MB/s   00:01
VxRailArchive_20210118070004_16804010.tgz                                   100%  169MB  79.8MB/s   00:02
```

Figure 12 SCP from VxRail Manager ESX server node

On the SFTP server, output similar to that shown in Figure 13 should now be visible.

```
[root@hci-sftp vxrail-mgmtdom]# pwd
/sftp/vcf/vxrail-mgmtdom
[root@hci-sftp vxrail-mgmtdom]# ls -al
total 928668
drwxr-xr-x. 2 root     root          4096 Jan 18 11:11 .
drwxr-xr-x. 6 vcf-user vcf-user        86 Jan 15 13:31 ..
-rw-------. 1 root     root          1046 Jan 18 13:20 vxmbackup.json
-rw-------. 1 root     root      58555780 Jan 18 13:20 VxRailArchive_20210112163837_16804010.tgz
-rw-------. 1 root     root      90154955 Jan 18 13:20 VxRailArchive_20210113070003_16804010.tgz
-rw-------. 1 root     root     121174358 Jan 18 13:20 VxRailArchive_20210114070003_16804010.tgz
-rw-------. 1 root     root      10315004 Jan 18 13:20 VxRailArchive_20210114111516_16804010.tgz
-rw-------. 1 root     root     155217446 Jan 18 13:20 VxRailArchive_20210115070004_16804010.tgz
-rw-------. 1 root     root     166445380 Jan 18 13:20 VxRailArchive_20210116070003_16804010.tgz
-rw-------. 1 root     root     171356510 Jan 18 13:20 VxRailArchive_20210117070004_16804010.tgz
-rw-------. 1 root     root     177710924 Jan 18 13:20 VxRailArchive_20210118070004_16804010.tgz
[root@hci-sftp vxrail-mgmtdom]#
```

Figure 13 VxRail backups on SFTP server

11. There is one other file from each VxRail Manager that is required.

    `recoveryBundle-<VxRail-version>.zip`

    The VxRail version will depend on what is deployed, substitute in the version that is deployed. This file is copied only once, after an upgrade or the first backup.

NOTE: If an upgrade is performed on the VxRail Manager VM, it is recommended that the new version of this file be recopied.

12. From either SSH or the VxRail Manager web console in vSphere, issue the following command: (As an example, the two commands below are from our environment)

    ```
    scp /data/store2/recovery/recoveryBundle-7.0.131.zip root@hci-
    sftp.hci.spoc:/sftp/vcf-vxm-mgmt

    scp /data/store2/recovery/recoveryBundle-7.0.131.zip root@hci-
    sftp.hci.spoc:/sftp/vcf-vxm-wld
    ```

13. Lastly, in the NetWorker Console create Groups and Policies for the Management and Workload Domain VxRail Manager Configuration Files to perform scheduled backups of the folders on the SFTP server.

Restore and recovery

This section discusses restore and recovery methods for VCF.

Table 5 Recovery methods for VCF core components

VM name (core component)	Restore method
Management vCenter server	Image level
Management Workload vCenter server	Image level
SDDC Manager	Image level
Log Insight Nodes	Image level
VMware Workspace ONE Access (VIDM)	Image level
Workload Edges	Image level
NSX-T Manager	Deploy OVA – Restore the configuration from SFTP
VxRail Manager	Deploy OVA – Restore the configuration from SFTP

NOTE: The OVAs for restore of NSX-T Manager and VxRail Manager must be the same as the original.

If the environment has the components shown in Table 6, this is what is required:

Table 6 Restore methods for VCF optional components

VM name (Optional components)	Backup restore
vRealize Automation Appliances	Image level
vRealize Automation Proxy Agents	Image level
vRealize Log Insight Appliance	Image level
Life Cycle Manage Appliance (LCM)	Image level
vRealize Operations Manager	Image level
Windows SQL Server	Image level / application level (NMM module)

Restore methods

There are many Restore methods available from NetWorker. This paper documents the methods that are required for each component of the VCF environment.

For file-level restores of NSX-T Manager and VxRail Manager, the same version of OVA that is used in the backups up must be deployed first and then the configuration files must be restored from the SFTP server.

As mentioned earlier, the SFTP server should also be backed up by NetWorker, this gives some extra protection in case of the SFTP server being lost.

After a Restore, it is recommended to follow the power on sequence mentioned in the VCF Administration Guide: https://docs.vmware.com/en/VMware-Validated-Design/6.2/sddc-shutdown-and-startup/GUID-1AC4B8D0-DB2A-475C-BE59-4D19C76969B0.html

Restore scenarios

There are multiple scenarios where a restore may be necessary. A restore may be partial or a complete recovery. The scope of this paper covers Full Disaster Recovery of VCF Components only.

NOTE: Since the scope of this paper is VCF recovery, the scenarios described in this paper assume that vSAN and the vCenter are intact and not compromised. Backups of the VCSA and PSC are performed in any case for safety. It is possible to restore and recover the VCSA but a discussion of this is outside the scope of this paper.

Full Disaster Recovery of VCF components

This section describes how to restore and recover VCF following a disaster. In our test environment we simulated a disaster, and then performed each of the restore and recovery steps necessary to restore VCF:

1. Image restores
2. VxRail Manager restore
3. NSX-T Manager restore

Disaster simulation

To simulate a disaster:

1. A clean shutdown of the VCF environment was performed.
2. The VCSA was left intact as it is part of the VxRail environment that was in place before VCF was deployed.
3. The SDDC, VxRail Manager, NSX-T and Log Insight VMs were all powered down and deleted.
4. The NetWorker Console was then opened on the **Recovery** tab.

Image restores

The first backups to restore are the VM images.

1. Open the NetWorker Management Console, select the **Recovery** tab, right-click and select **New Recover**.
2. Select the **Recovery Type**.
   Under **Recovery Type**, select **Virtual Machine Recovery** and then select the **Source vCenter server**, as shown in Figure 14.

NOTE: The vCenter may be the Management Domain or Workload Domain vCenter depending on what is being restored.

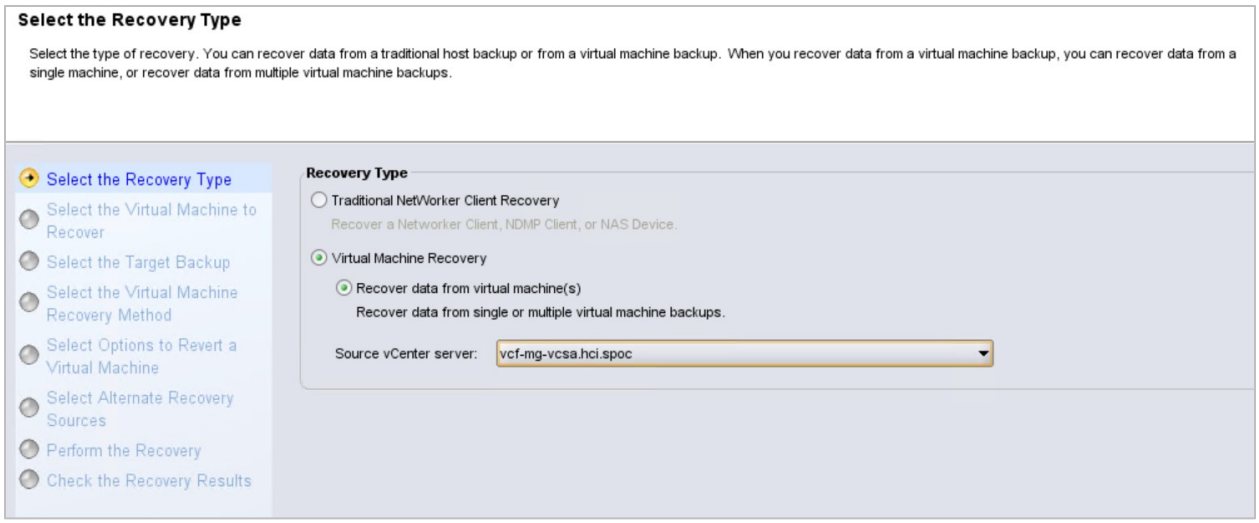

Figure 14 NetWorker: Select Recovery Type

3. **Select the Virtual Machine to Recover**.
   Select the VM to recover by typing its name. It is recommended that only one VM Image at a time is restored.

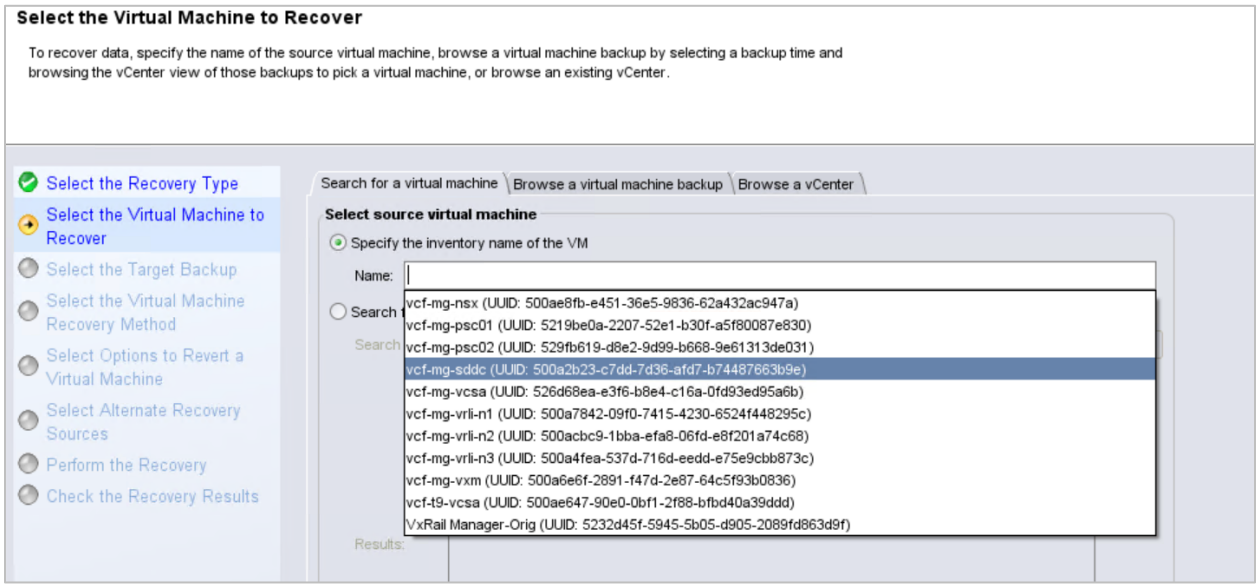

Figure 15 NetWorker: Select the Virtual Machine to Recover

4. **Select the Target Backup**
   It is important that for each image that is being restored, the backup with the same timestamp is selected.

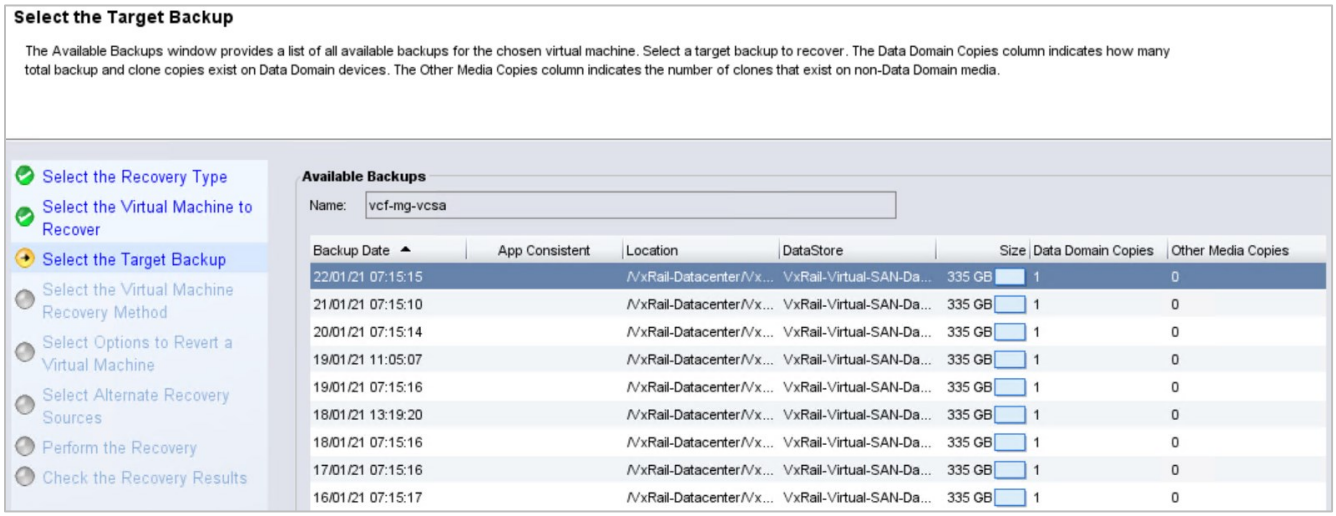

Figure 16 VM Backup sets

5. **Select the Virtual Machine Recovery Method**
   Select **Virtual Machine Recovery** to restore the full VM.

NOTE: In some Restore scenarios it may only be necessary to restore/overwrite a VM in place, in which case the **Revert a Virtual Machine** option can be selected.

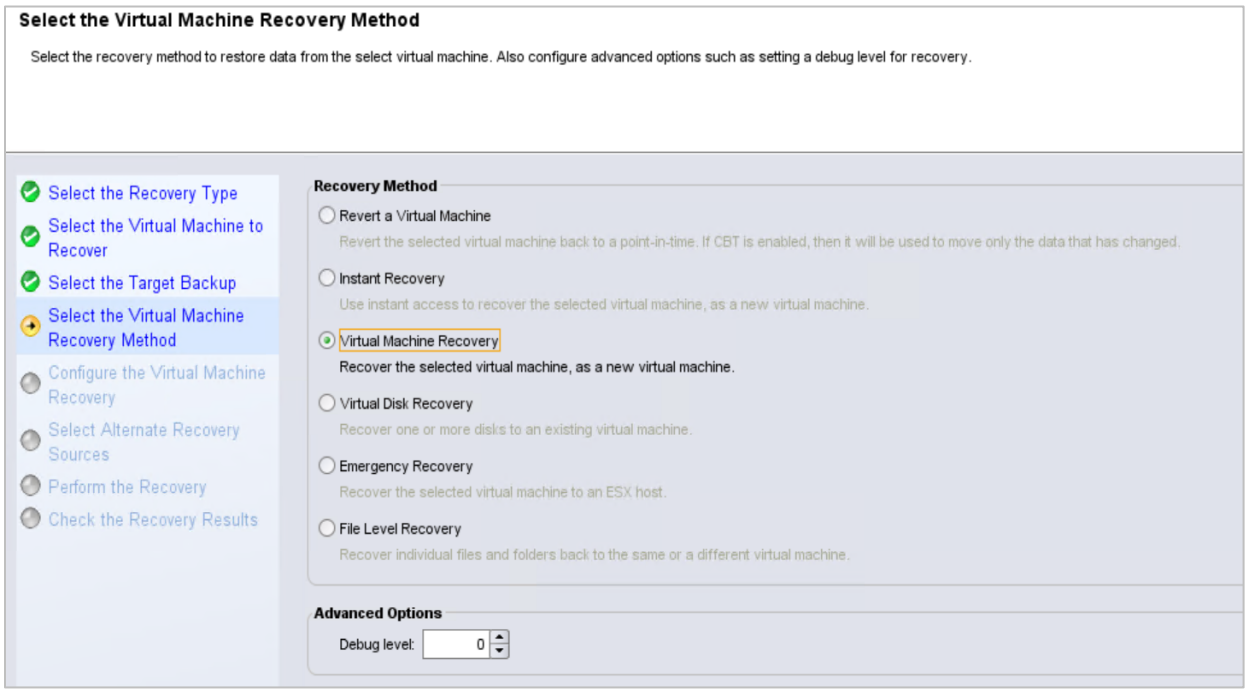

Figure 17 NetWorker: Select VM Recovery Method

6. **Configure the Virtual Machine Recovery**

   a. Ensure that the correct vProxy is selected
   b. Ensure that the **Power on virtual machine** checkbox is NOT ticked.
   c. Continue your progress through the wizard and give the recovery a name.

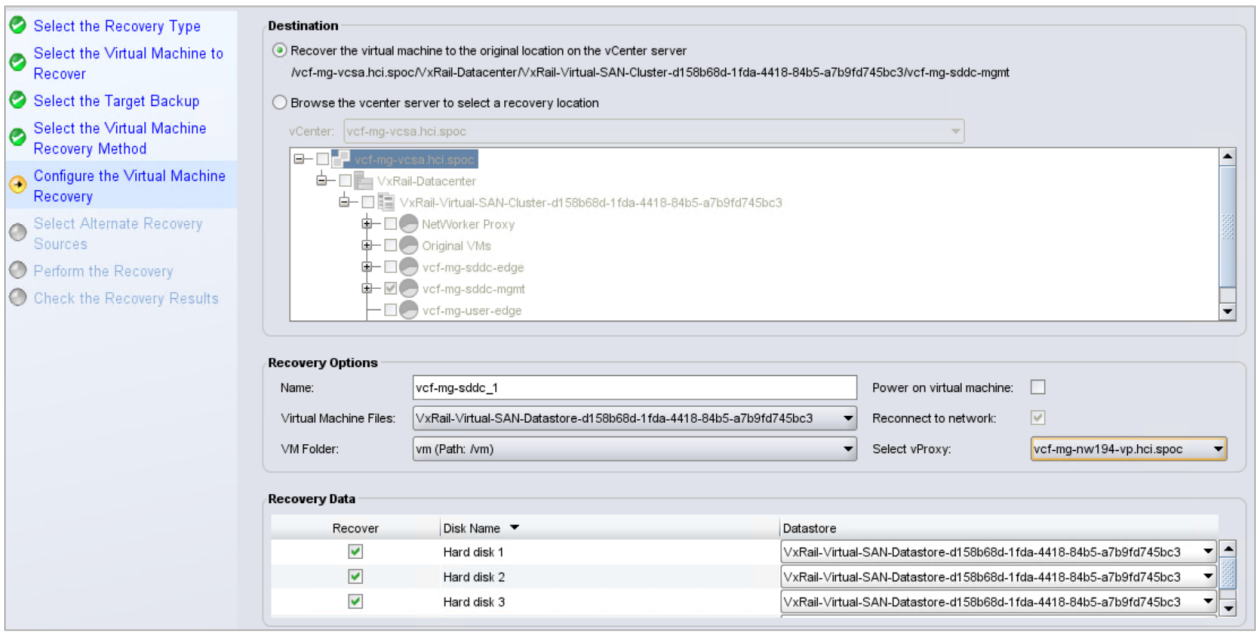

Figure 18 Destination and Recovery Options

7. Edit the VM settings to ensure that the correct networks are attached, then power on the VM.
8. Repeat the procedure for all other images that must be restored.

Once all the VMs have been restored, the next recoveries to perform are file-level recoveries of VxRail Manager and the NSX-T Management and Workload VMs.

VxRail Manager restore

NOTE: We have tested image backups and restores of VxRail Manager successfully. It is expected that image backups will be supported in a future release, if that is the case then all these steps are not required.

Ensure that the following procedure is carried out for both the Management Domain and the Workload Domain.

1. Re-deploy the VxRail Manager OVA, the exact same version as the original, back onto the vCenter.
   a. Ensure the IP supplied for deployment is different to the original VxRail Manager VM and is NOT known in DNS.
   b. Ensure the original VxRail Manager VM, if it still exists, is powered off.
   c. Ensure the VM being deployed is attached to the correct Network.
   d. Ensure the backup files are available on the vSAN in the VxRail_backup_folder.
2. The python scripts that were used earlier are also used to perform the restore from the archive on the vSAN, back to the new VxRail Manager.
   a. Connect to the new VxRail Manager Bash shell via the vSphere Web Console or SSH.
   b. The 'mystic' user is used to log into it. Ensure that the credentials are known in advance.
   c. Once at the bash prompt, navigate to the script folder:

      ```
      cd /mystic/vxm_backup_restore
      ```

      Then type the command:

      ```
      sudo su
      ```

      Or

      ```
      sudo su root
      ```

   d. Issue the command below to restore the VxRail Manager configuration.

      Ensure that the vCenter credentials are known before beginning.

      ```
      python vxm_backup_restore.py -r --vcenter 10.107.31.10
      ```

      This will be an interactive process initially but it will then automatically run.

      Here is a sample output of a restore that was performed (user input is in bold):

      ```
      python vxm_backup_restore.py -r --vcenter 10.107.31.10

      Current user is root. We can do current job.
      Input vCenter account. Default is [administrator@vsphere.local] :
      administrator@vsphere.local

      Input administrator@vsphere.local password:

      Connecting to vCenter [10.107.31.10]
      Found 1 cluster item(s), select the one you want to use.

      1)[/VxRail-Datacenter/host/VxRail-Virtual-SAN-Cluster-d158b68d-1fda-
      4418-84b5-a7b9fd745bc3]
      ```

```
2) Exit

Select an option[0-1]:1
Start to Restore VxRail Manger.

Download vxmbackup.json from VSAN datastore.

datacenter path is /VxRail-Datacenter

download file http_url:
https://192.168.104.87/folder/VxRail_backup_folder/vxmbackup.json?dcPat
h=%2FVxRail-
Datacenter&dsName=VxRail-Virtual-SAN-Datastore-8db07da6-0871-4e34-90f0-
4b2ccc512d3b



Found 2 VxRail backup item(s), select the one you want to use
1) VxRailArchive_20170907082805_6557030.tgz(OK)
2) VxRailArchive_20170907082815_6557030.tgz(OK)
0) Exit

Select an option[0-2]:1

      version is compatible with current VxM. Restore continue.

Downloading archived file to local......

datacenter path is /VxRail-Datacenter

download file http_url:
https://192.168.104.87/folder/VxRail_backup_folder/VxRailArchive_201709
07082805_6557030.tgz?dc
Path=%2FVxRail-Datacenter&dsName=VxRail-Virtual-SAN-Datastore-8db07da6-
0871-4e34-90f0-
4b2ccc512d3b

Downloading succeeded:

/tmp/VxRailRestore/VxRailArchive_20170907082805_6557030.tgz

Restoring system files......
Restoring database......

/usr/bin/systemctl stop vmware-marvin
run command: [/usr/bin/systemctl stop vmware-marvin]. Ret: [0]

/usr/bin/systemctl stop runjars
run command: [/usr/bin/systemctl stop runjars]. Ret: [0]
```

```
/usr/bin/systemctl stop vmware-loudmouth
run command: [/usr/bin/systemctl stop vmware-loudmouth]. Ret: [0]

/usr/bin/systemctl restart postgresql
run command: [/usr/bin/systemctl restart postgresql]. Ret: [0]

/usr/bin/psql -U postgres -c 'DROP DATABASE IF EXISTS marvin'
run command: [/usr/bin/psql -U postgres -c 'DROP DATABASE IF EXISTS
marvin']. Ret: [0]

/usr/bin/psql -U postgres -c 'DROP DATABASE IF EXISTS mysticmanager'
run command: [/usr/bin/psql -U postgres -c 'DROP DATABASE IF EXISTS
mysticmanager']. Ret: [0]

/usr/bin/psql -U postgres -c 'DROP DATABASE IF EXISTS spring_batch'
run command: [/usr/bin/psql -U postgres -c 'DROP DATABASE IF EXISTS
spring_batch']. Ret: [0]

/usr/bin/psql -U postgres -f /var/lib/vmware-marvin/VxRailDBAll.dump
postgres
run command: [/usr/bin/psql -U postgres -f /var/lib/vmware-
marvin/VxRailDBAll.dump postgres]. Ret: [0]

Restoring database succeeded.
Restoring system files succeeded.

42175e6e-4582-cc6e-0404-9c6a597392f3 vm-35 VxRail Manager Restore
/usr/bin/psql -U postgres marvin -c "update virtual_machine set uuid =
'42175e6e-4582-cc6e-0404-
9c6a597392f3', morefid = 'vm-35', vm_name = 'VxRail Manager Restore'
where system_vm_type =
'VXRAIL_MANAGER'"


System is restarting. Ensure that original VxRail Manager is powered
off.
Do you want to continue? (yes/no)(y/n): y
```

3. After the VxRail Manager restarts, disable the vApp option in settings:
   a. Log in to vSphere Web Client.
   b. Select the VxRail Manager VM.
   c. Go to **Configure** Tab **> Settings > vApp** Option.
   d. Clear the **Enable vApp options** and click **OK**.
   e. Select **VxRail Manager > Shut Down Guest OS*** and wait for it to power down.
   f. Select **Power On**.

*IMPORTANT: Please ensure to use **Shut Down** and then **Power On**. Do not use restart or reset.

After powering on, the VxRail Manager should be available in approximately 5 minutes.

It can now be renamed to the name of the original VM.

NSX-T Manager restore

This section describes the restore process for the NSX-T Manager. The same procedure is used to restore both the NSX-T Management Domain and the NSX-T Workload Domain.

1. Redeploy the OVA of the exact same version of NSX-T Manager.
   a. Ensure that the IP supplied during the deployment of the OVA is that of the 1st node, not the cluster IP. For more information see “Confirmation of NSX-T backups”.
   b. Ensure the re-deployed VM is connected to the correct network.
2. Power on the VM.
   a. Connect to the NSX-T Manager using https.
   b. Go to the **System** tab and select **Backup & Restore**.
   c. Select the **Restore** tab.
   d. Click **EDIT** and fill in the fields exactly as was done for configuring the backup.

IMPORTANT: Ensure that the same Passphrase that was used for the backup is entered here. Failure to use the correct Passphrase will hide the available restore options.

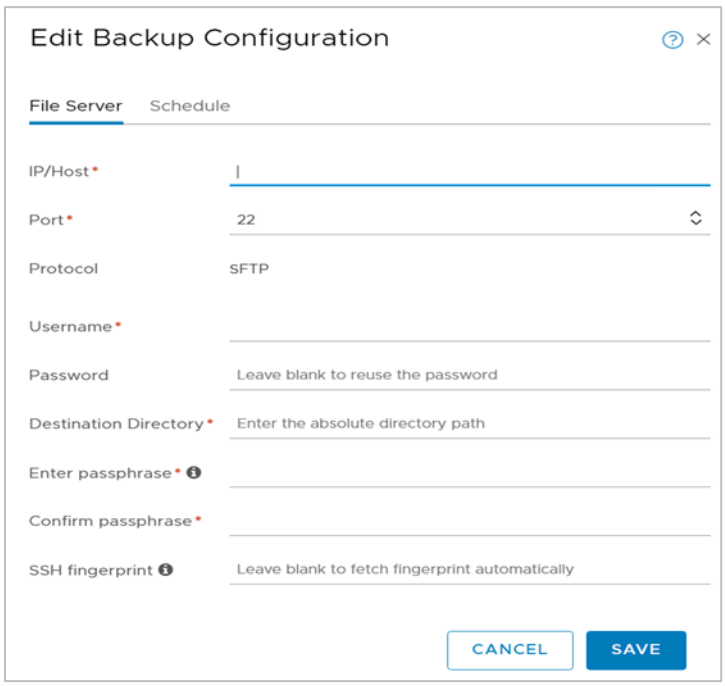

Figure 19 NSX-T Manager Restore configuration

   e. The available backups for restore should now be made visible, as shown in Figure 20.

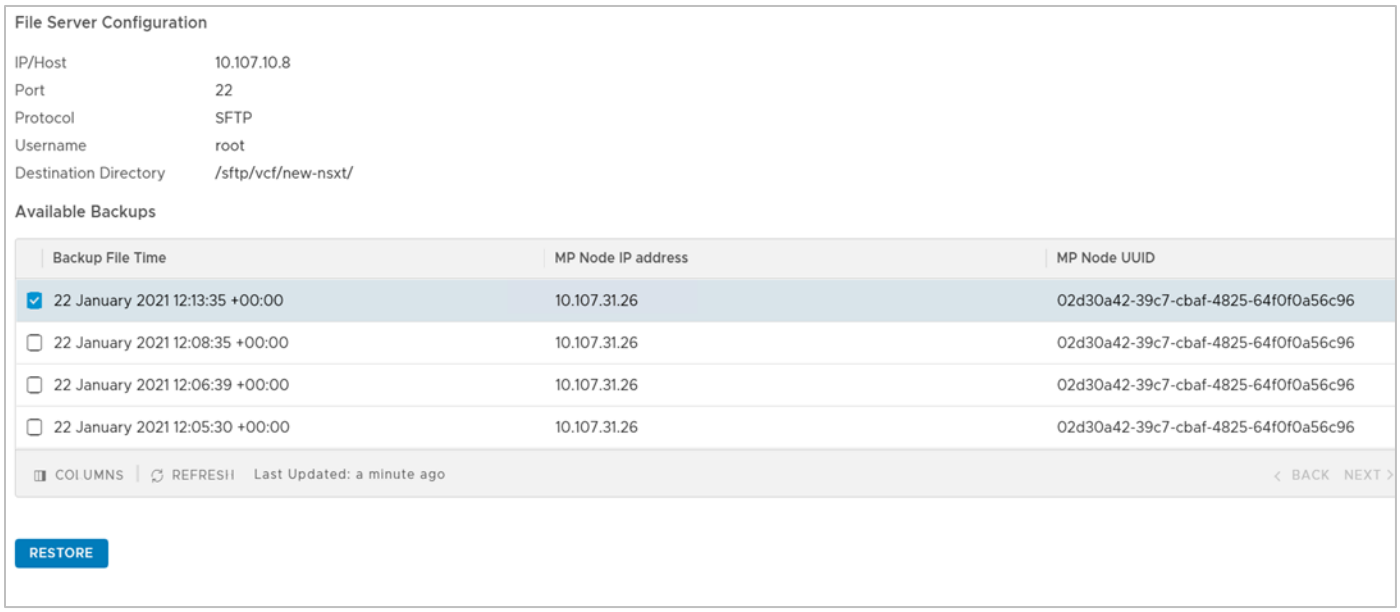

Figure 20 NSX-T Manager restore options

3. Select the backup that is as close in time as possible to the image restore.

   a. Click **Restore** and wait a few minutes.

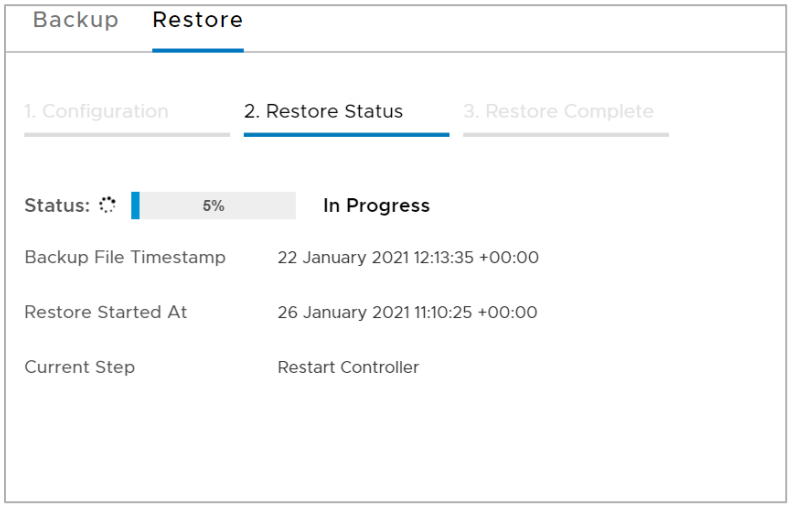

Figure 21 Restore in progress

   b. You may be logged out of the NSX-T Manager at this point; wait a few minutes and then re-connect to the NSX-T Manager.
   c. Navigate back to **System** > **Backup & Restore**.
   d. The message shown in will display, this is as expected.

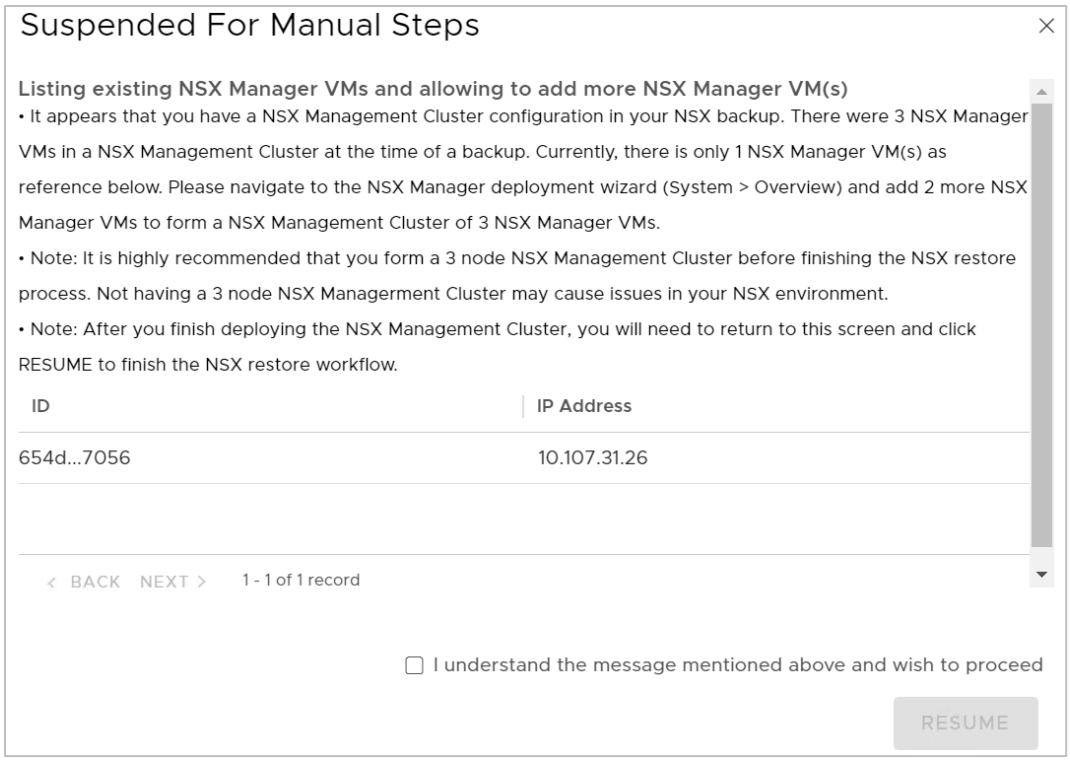

Figure 22 NSX-T Restore: Manual required steps

4. Redeploy the Cluster nodes.

   a. Navigate to the Home page of the NSX-T Manager.

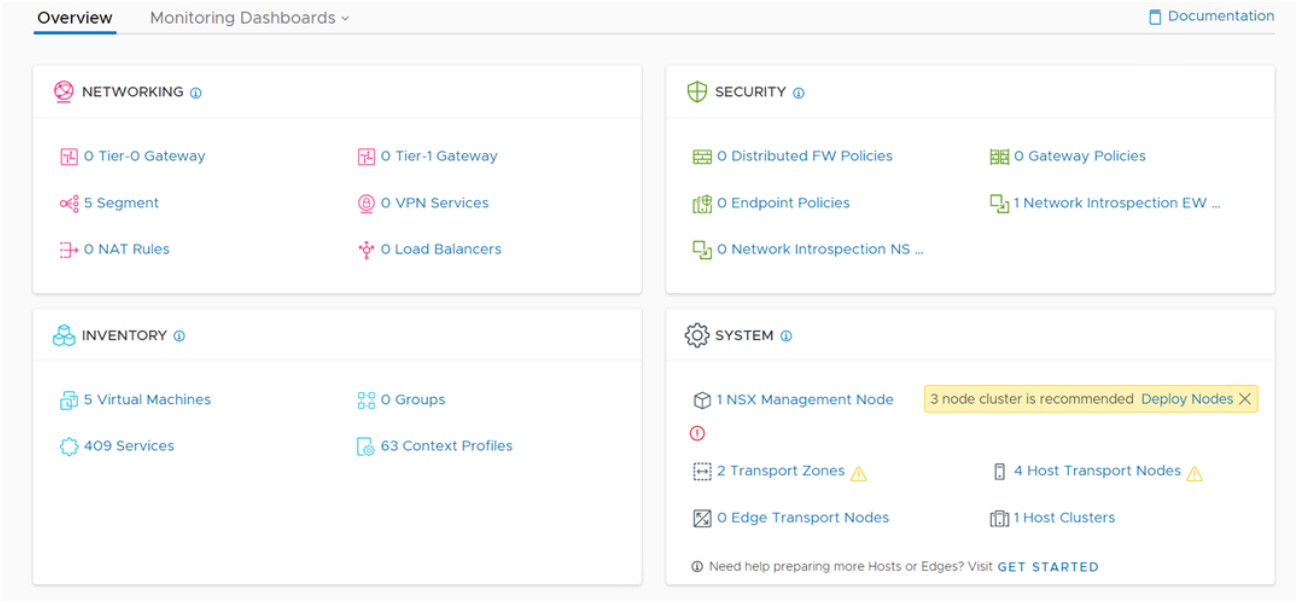

Figure 23 NSX-T Restore: Overview tab > SYSTEM

   b. Ensure that you have the details of the FQDN and IPs of the original NSX-T nodes.
   c. Redeploy the Cluster nodes as shown in Figure 24.

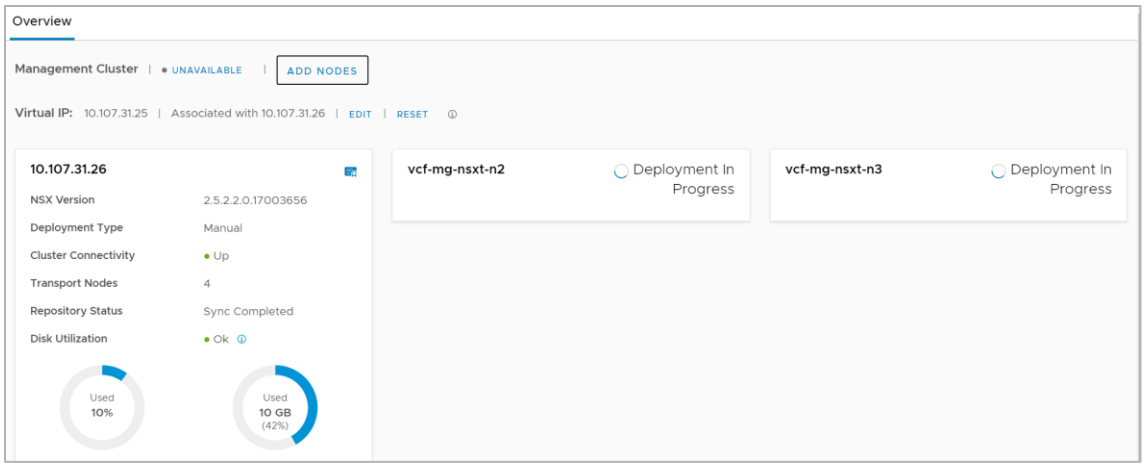

Figure 24 Redeploy NSX-T Cluster nodes

If the re-deployment of the nodes was successful, the output should resemble Figure 25.

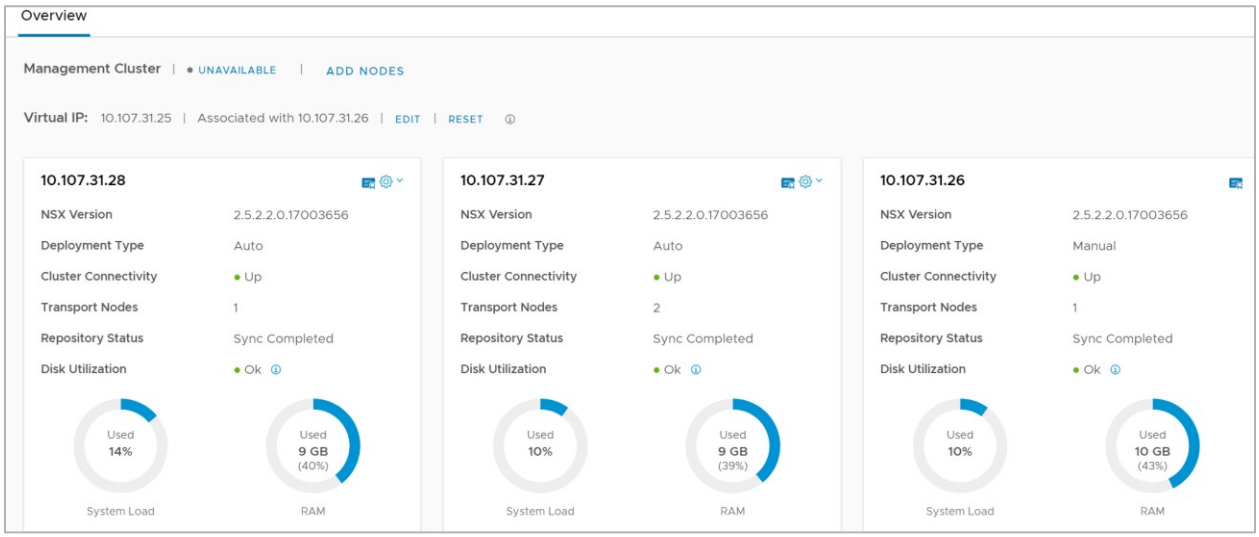

Figure 25 NSX-T: Nodes deployed

5. Navigate back to **System** > **Backup & Restore**.

   a. The onscreen message shown in Figure 26 should still be visible.

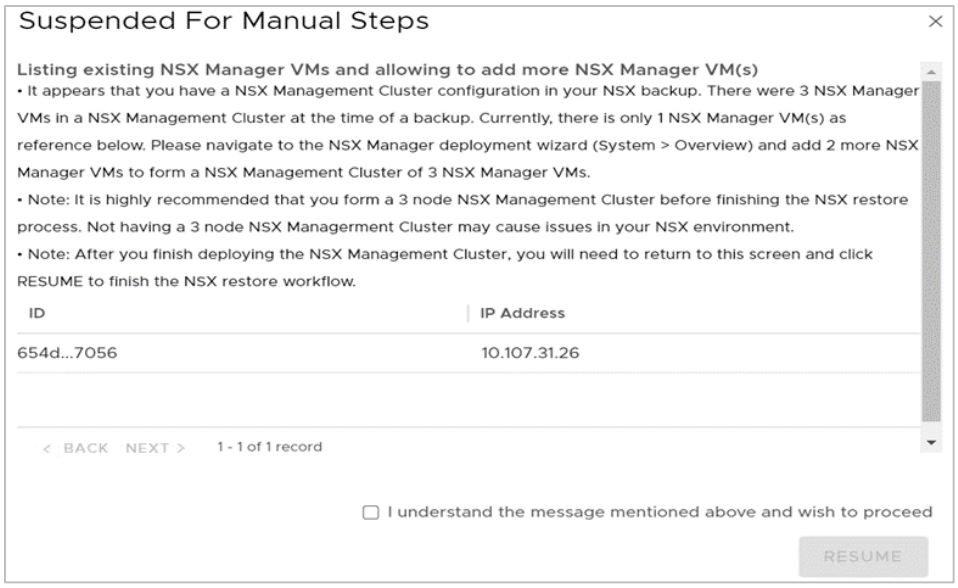

Figure 26 Resume manual step

b. Select the checkbox and click **RESUME**.
c. The restore will progress as shown in Figure 27, this will take several minutes.

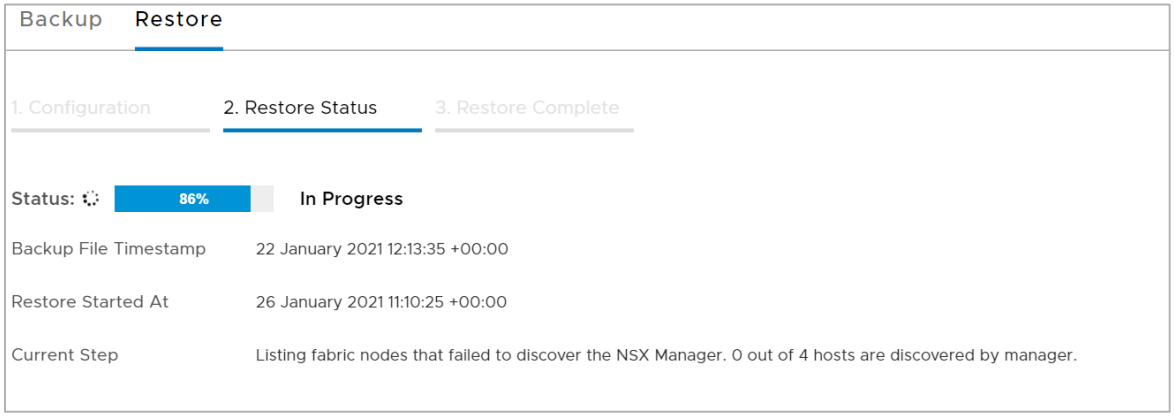

Figure 27 NSX-T Restore in progress

d. After several minutes the restore should complete successfully as shown in Figure 28.

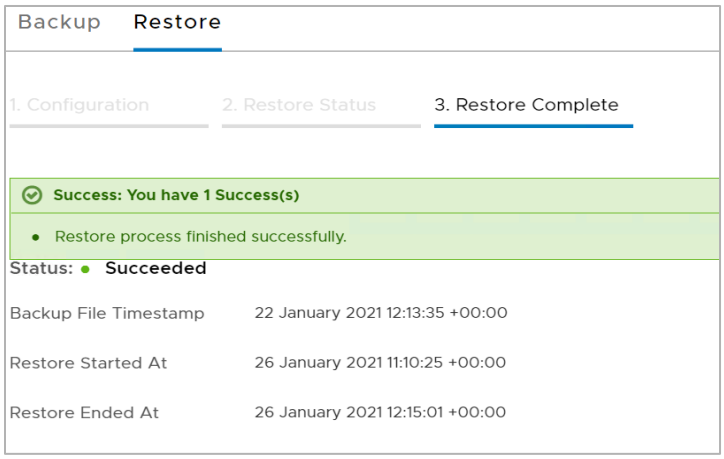

Figure 28 NSX-T Restore Complete

6. Check the status of the VCF environment, it should now be again functioning normally.

Configuration details

Table 7 Dell EMC VxRail management domain hardware

Component	Details
VxRail version	7.0.131-26875681
Nodes	4 * 14G PowerEdge E570F Intel Xeon Gold 6140 – 2.30 GHz, 384 GB RAM
Cache disks	4 * 800 GB SSD
Capacity disks	16 * 1.92 TB SSD
Disk groups	4 * disk groups (1 x cache disk + 4 x capacity disks per group)
Networking	4 * 10 Gbe QP ports Ports 1 and 3 to top of rack switch 1 Ports 2 and 4 to top of rack switch 2

Table 8 Dell EMC VxRail workload domain hardware

Component	Details
VxRail version	7.0.131-26875681
Nodes	4 * 14G PowerEdge P570F Intel Xeon Gold 6140 - 2.30 GHz, 320 GB RAM
Cache disks	800 GB SSD
Capacity disks	20 * 1.92 TB SSD
Disk groups	4 * Disk Groups (1 x cache disk + 5 x capacity disks per group)
Networking	4 * 10 Gbe QP ports Ports 1 and 3 to top of rack switch 1 Ports 2 and 4 to top of rack switch 2

Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Related resources

VMware Cloud Foundation 4.2 on Dell EMC VxRail Release Notes:

https://docs.vmware.com/en/VMware-Cloud-Foundation/4.2/rn/vmware-cloud-foundation-on-dell-emc-vxrail-22-release-notes.html

VMware Cloud Foundation documentation:

https://docs.vmware.com/en/VMware-Cloud-Foundation/index.html

VMware Cloud Foundation on Dell EMC VxRail architecture guide:

http://vxrail.is/vcfarchguide