VMware Cloud Foundation 4.0 on Dell EMC VxRail Release Notes

VMware Cloud Foundation 4.0

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

What's New

1

The VMware Cloud Foundation (VCF) 4.0 on Dell EMC VxRail release has been determined to be impacted by CVE-2020-4006. Fixes and Workarounds are available to address this vulnerability. For more information, see VMSA-2020-0027.

VMware Response to Apache Log4j Remote Code Execution Vulnerability: VMware Cloud Foundation is impacted by CVE-2021-44228, and CVE-2021-45046 as described in VMSA-2021-0028. To remediate these issues, see Workaround instructions to address CVE-2021-44228 & CVE-2021-45046 in VMware Cloud Foundation (KB 87095).

The VMware Cloud Foundation (VCF) 4.0 on Dell EMC VxRail release includes the following:

- **Kubernetes - Workload Management:** With Kubernetes - Workload Management, you can deploy and operate the compute, networking, and storage infrastructure required by vSphere with Kubernetes. vSphere with Kubernetes transforms vSphere to a platform for running Kubernetes workloads natively on the hypervisor layer. When enabled on a vSphere cluster, vSphere with Kubernetes provides the capability to run Kubernetes workloads directly on ESXi hosts and to create upstream Kubernetes clusters within dedicated resource pools.

- **NSX-T Data Center everywhere:** The management domain and VI workload domains now use NSX-T Data Center exclusively. This consolidated NSX-T architecture improves operational efficiency and brings Cloud Native App support to Cloud Foundation deployments.

- **vRealize Suite 8.1 support:** This release automates the deployment of vRealize Suite Lifecycle Manager 8.1. Follow the VMware Validated Design guidance to use vRealize Suite Lifecycle Manager to deploy vRealize Automation 8.1, vRealize Operations Manager 8.1, and vRealize Log Insight 8.1.

- **NSX-T Data Center flexible deployment options:** Cloud Foundation now provides additional flexibility in NSX-T deployment. The management domain now includes a dedicated NSX-T Manager cluster. VI workload domains can get a dedicated NSX-T Manager cluster, or share an existing NSX-T Manager cluster. When you create a VI workload domain, you can choose to either deploy a new NSX-T Manager cluster for the workload domain, or to share an existing NSX-T Manager cluster that was previously created for another VI workload domain.

- **Automate NSX-T tasks beyond initial deployment:** You can now use SDDC Manager to create an NSX Edge cluster to support the management domain and VI workload domains. This automation replaces the manual deployment of Edge clusters that was required in previous versions of Cloud Foundation.

- **Cloud Foundation APIs for day N operations:** See the VMware Cloud Foundation on Dell EMC VxRail API Reference Guide for more information.

- **Developer Center:** Enables you to access Cloud Foundation APIs and code samples from SDDC Manager.

- **NSX-T stretched cluster API support:** This release provides a new API to perform automation of stretch cluster operations for the management and VI workload domains. VMware Cloud Foundation on VxRail recommends stretching workload domain clusters over L3. The management network must be L2-stretched.

- **RBAC improvements:** This release introduces a new user role, called the OPERATOR role, in addition to the existing ADMIN role. The OPERATOR role can be assigned to users and groups and provides access to all SDDC Manager functionality except user management, password management, and backup configuration settings. Usage of these two roles eliminates the need for using the dual authentication mechanism to control access to administrator tasks.

- **Support for consolidated architecture:** Standard architecture is recommended for most deployments, but for smaller system requirements the consolidated architecture is now supported.

- **Option to deactivate Application Virtual Networks (AVNs) during Bring-up:** AVNs deploy vRealize Suite components on NSX overlay networks and it is recommended you use this option during bring-up. If you deactivate AVN during bring-up, vRealize Suite components are deployed to a VLAN-backed distributed port group.

- **BOM Updates:** Updated Bill of Materials with new product versions.

VMware Cloud Foundation on Dell EMC VxRail Bill of Materials (BOM)

2

The VMware Cloud Foundation software product is comprised of the following software Bill-of-Materials (BOM). The components in the BOM are interoperable and compatible.

Software Component	Version	Date	Build Number
Cloud Builder VM	4.0.0.0	14 APR 2020	16008466
SDDC Manager	4.0	14 APR 2020	16008466
VxRail Manager	7.0.000	12 MAY 2020	n/a
VMware vCenter Server Appliance	7.0.0	02 APR 2020	15952498
VMware ESXi	7.0.0	02 APR 2020	15843807
VMware vSAN	7.0.0	02 APR 2020	15843807
VMware NSX-T Data Center	3.0	07 APR 2020	15946738
VMware vRealize Suite Lifecycle Manager	8.1	14 APR 2020	15995660

- Cloud Foundation supports, but does not automate, the deployment of VMware Horizon 7 version 7.12. You can deploy Horizon 7.12 on a workload domain using the Horizon 7.12 documentation.

- You can use vRealize Suite Lifecycle Manager to deploy vRealize Automation 8.1, vRealize Operations Manager 8.1, and vRealize Log Insight 8.1 using the VMware Validated Design 6.0 documentation.

- VMware Enterprise PKS is not supported with this release of Cloud Foundation.

Documentation

3

The following documentation is available:

- VMware Cloud Foundation on Dell EMC VxRail Admin Guide

- VMware Cloud Foundation 4.0 Release Notes

- Support Matrix of VMware Cloud Foundation on Dell EMC VxRail

Limitations

4

The following limitations apply to this release:

- vSphere Lifecycle Manager (vLCM) is not supported on VMware Cloud Foundation on Dell EMC VxRail.

- VMware Cloud Foundation on VxRail automates overlay traffic to utilize the distributed virtual switch (for system traffic) that is created by the VxRail first run process. System and overlay traffic isolation through a separate distributed virtual switch is not supported

Known Issues

<div style="text-align: right; font-size: 3em; color: #999;">5</div>

For VMware Cloud Foundation 4.0 known issues, see VMware Cloud Foundation 4.0 Known Issues.

VMware Cloud Foundation 4.0 on Dell EMC VxRail known issues and limitations appear below:

- **Adding hosts with incorrect credentials locks out the ESXi account**

  If you provide an incorrect user name or password for a host when stretching a cluster or adding a host to a cluster, the task fails and the ESXi account is locked out.

  Workaround: Wait 15 minutes (the default lockout time) and retry the task.

- **Unable to reuse an existing NSX Manager cluster when creating a new VxRail VI workload domain**

  When creating a new VxRail VI workload domain, you may not be able to reuse an NSX Manager cluster created for an existing VxRail VI workload domain. This can happen if you create the second VxRail VI workload domain immediately after the first one.

  Workaround: Check the Tasks panel to make sure the original workload domain task has completed successfully. Once it has, refresh your browser to reuse the existing NSX Manager cluster with your new VxRail VI workload domain.

- **Validation APIs for domain, cluster, and host operations fail if you provide incorrect host credentials**

  When creating a new VxRail VI workload domain, you may not be able to reuse an NSX Manager cluster created for an existing VxRail VI workload domain. This can happen if you create the second VxRail VI workload domain immediately after the first one.

  Workaround: Check the Tasks panel to make sure the original workload domain task has completed successfully. Once it has, refresh your browser to reuse the existing NSX Manager cluster with your new VxRail VI workload domain.

- **Adding a host to a vSphere cluster fails at the `Create NSX-T Data Center Transport Nodes from Discovered Nodes` subtask**

  In this situation, check the NSX Manager UI. If it shows the error `Failed to uninstall the software on host. MPA not working. Host is disconnected.` for the host you are trying to add, use the following workaround.

Workaround:

a   SSH to the failed host.

b   Execute the following commands:

```
/etc/init.d/hostd restart

/etc/init.d/vpxa restart
```

c   In the SDDC Manager UI, retry the add host task.

- **You cannot delete a workload domain with a stretched cluster**

   The method for deleting a workload domain described in the *VMware Cloud Foundation on Dell EMC VxRail Administration Guide* does not work if the workload domain has a stretched cluster.

   Workaround:

   a   In the SDDC Manager UI, select **Inventory > Workload Domains**.

   b   Click the workload domain that you want to delete.

   c   Select **Actions > Delete VxRail Domain**.

- **Adding a VxRail cluster to a workload domain fails**

   If you add hosts that span racks (use different VLANs for management, vSAN, and vMotion) to a VxRail cluster after you perform the VxRail first run, but before you add the VxRail cluster to a workload domain in SDDC Manager, the task fails.

   Workaround:

   a   Create a VxRail cluster containing hosts from a single rack and perform the VxRail first run.

   b   Add the VxRail cluster to a workload domain in SDDC Manager.

   c   Add hosts from another rack to the VxRail cluster in the vCenter Server for VxRail.

   d   Add the VxRail hosts to the VxRail cluster in SDDC Manager.

- **Adding a vSphere cluster or adding a host to a workload domain fails**

   Under certain circumstances, adding a host or vSphere cluster to a workload domain fails at the `Configure NSX-T Transport Node or Create Transport Node Collection` subtask.

   Workaround:

   a   Enable SSH for the NSX Manager VMs.

   b   SSH into the NSX Manager VMs as **admin** and then log in as `root`.

   c   Run the following command on each NSX Manager VM:

   ```
   sysctl -w net.ipv4.tcp_en=0
   ```

   d   Login to NSX Manager UI for the workload domain.

   e   Navigate to **System > Fabric > Nodes > Host Transport Nodes**.

f   Select the vCenter server for the workload domain from the **Managed by** drop-down menu.

g   Expand the vSphere cluster and navigate to the transport nodes that are in a `partial success` state.

h   Select the check box next to a `partial success` node, click **Configure NSX.**

i   Click `Next` and then click`Apply`.

j   Repeat steps 7 and 8 for each `partial success` node.

- **You cannot access VxRail Manager in vCenter Server after replacing its certificate**

  In some cases, you may not be able to access a VxRail Manager in vCenter Server after you replace the VxRail Manager's certificate using the SDDC Manager UI. The SDDC Manager Tasks panel reports the task as **Successful**.

  Workaround:

  a   SSH to the VxRail Manager as `mystic`.

  b   Change to the `root` user.

  c   Run the following command:

  ```
  ls -l /etc/vmware-marvin/ssl
  ```

  d   If the output does not show **server.pfx**, run the following command:

  ```
  cp -rf server.pfx.backup server.pfx
  ```

  e   Restart the **vmware-marvin** service and make sure it is running.

  ```
  service vmware-marvin restart

  service vmware-marvin status
  ```

  f   Wait for 5 minutes.

  g   Get the current fingerprint of the VxRail Manager:

  ```
  openssl s_client -connect localhost:443 | openssl x509 -fingerprint
  ```

  For example: BA:AD:05:1E:00:06:E9:0F:EF:54:AF:F4:2C:3E:7F:C7:26:C5:8F:5C

  h   Use the vSphere Client to connect to the VxRail Manager's vCenter Server.

  i   Select the cluster hosting the VxRail Manager.

  j   Select **Summary > Custom Attributes**.

  k   Update the VxRail SSL Thumbprint with the value you retrieved in step 7.

- **Bring-up fails with a password error**

  Bring-up fails with the error `password must contain only alphanumerics and special characters`. The error is the result of different password requirements for VxRail and VMware Cloud Foundation.

Workaround: Make sure that VxRail clusters use passwords that meet the Cloud Foundation requirements for the following users:

- Default Single-Sign On Domain User (administrator@vsphere.local): 8-20 characters. At least 1 uppercase, 1 lowercase, 1 number, and 1 special character (@, !, #, $, %, ?, ^).

- vCenter Server and Platform Services Controller Virtual Appliances root account: 8-12 characters. At least 1 uppercase, 1 lowercase, 1 number, and 1 special character (@, !, #, $, %, ?, ^).

- **If you use the special character underscore (_) in the vCenter host name for the workload domain create operation, the vCenter deployment fails.**

  The vCenter deployment fails with the "`ERROR > Section 'new_vcsa', subsection 'network', property 'system_name' validation`" error message.

  Workaround: None. This is an issue in the vCenter product installer where the installer pre-validation fails. You should create the workload domain by providing valid vCenter host names.

- **The VxRail vCenter Plugin UI options may disappear after the OpenSSL/Microsoft certificate replace operations of all the components or just VxRail Manager**

  The certificate replace operation involves changes in VxRail Manager and the vCenter VMs. Sometimes the vCenter plugin download might fail as the communication can happen with invalid thumbprint and the VxRail plugin UI option might disappear from vCenter. As a result, the user cannot invoke the add hosts and the remove hosts operations from vCenter.

  Workaround: Reload the plugin by opening the VxRail Manager page which redirects to vCenter and make sure the VxRail UI options are visible in the vCenter UI.