VMware Cloud Foundation 4.0 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 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).

NOTE: VMware Cloud Foundation 4.0 must be installed as a new deployment; you cannot upgrade to VMware Cloud Foundation 4.0.

The VMware Cloud Foundation 4.0 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:** Cloud Foundation 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.
- **Firmware lifecycle management with vSphere Lifecycle Manager (vLCM):** Cloud Foundation allows users to create vSphere Lifecycle Manager (vLCM) enabled workload domains. On these workload domains, users can deploy and upgrade firmware on individual vSphere clusters. Cloud Foundation streamlines the applicability of these firmware upgrades through its ESXi bundles and performs pre-checks and validations before they are applied.

- **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.
- **NSX-T stretched cluster support:** Cloud Foundation provides a new API to perform automation of stretch cluster operations for the management and VI workload domains. Stretch clusters are only supported for VUM-based workload domains.
- **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.
- **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 for the 4.0 Release**: Updated Bill of Materials with new product versions.
- **VMware Validated Design (VVD) 6.0 alignment**: This release aligns with the VVD 6.0 release. The VMware Cloud Foundation Documentation includes links to a shared *Planning and Preparation Workbook*, as well as Solution Architecture and Design Guides and Solution Deployment Guides. The solution guides expand on Cloud Foundation capabilities and include guidance on deploying vRealize Suite 8.1 components, integrating Active Directory, and using Workspace ONE Access for Role Based Access Control (RBAC) with NSX-T Data Center.

VMware Cloud Foundation 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
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.

VMware Software Edition License Information

3

The SDDC Manager software is licensed under the Cloud Foundation license. As part of this product, the SDDC Manager software deploys specific VMware software products.

The following VMware software components deployed by SDDC Manager are licensed under the VMware Cloud Foundation license:

- VMware ESXi
- VMware vSAN
- VMware NSX-T Data Center

The following VMware software components deployed by SDDC Manager are licensed separately:

- vCenter Server

  NOTE: Only one vCenter Server license is required for all vCenter Servers deployed in a Cloud Foundation system.

For details about the specific VMware software editions that are licensed under the licenses you have purchased, see the Cloud Foundation Bill of Materials (BOM) section above.

For general information about the product, see VMware Cloud Foundation.

Supported Hardware

4

For details on vSAN Ready Nodes in Cloud Foundation, see VMware Compatibility Guide (VCG) for vSAN and the Hardware Requirements section on the Prerequisite Checklist tab in the Planning and Preparation Workbook.

Documentation

5

To access the Cloud Foundation documentation, go to the VMware Cloud Foundation product documentation.

To access the documentation for VMware software products that SDDC Manager can deploy, see the product documentation and use the drop-down menus on the page to choose the appropriate version:

- VMware vSphere product documentation, also has documentation about ESXi and vCenter Server
- VMware vSAN product documentation
- VMware NSX-T Data Center product documentation

Browser Compatibility and Screen Resolutions

6

The Cloud Foundation web-based interface supports the latest two versions of the following web browsers except Internet Explorer:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Internet Explorer: Version 11

For the Web-based user interfaces, the supported standard resolution is 1024 by 768 pixels. For best results, use a screen resolution within these tested resolutions:

- 1024 by 768 pixels (standard)
- 1366 by 768 pixels
- 1280 by 1024 pixels
- 1680 by 1050 pixels

Resolutions below 1024 by 768, such as 640 by 960 or 480 by 800, are not supported.

Installation and Upgrade Information

7

You can install VMware Cloud Foundation 4.0 as a new release. You cannot upgrade to VMware Cloud Foundation 4.0.

Installing as a New Release

The new installation process has three phases:

Phase One: Prepare the Environment

The *Planning and Preparation Workbook* provides detailed information about the software, tools, and external services that are required to implement a Software-Defined Data Center (SDDC) with VMware Cloud Foundation, using a standard architecture model.

Phase Two: Image all servers with ESXi

Image all servers with the ESXi version mentioned in the Cloud Foundation Bill of Materials (BOM) section. See the *VMware Cloud Foundation Deployment Guide* for information on installing ESXi.

Phase Three: Install Cloud Foundation 4.0

Refer to the *VMware Cloud Foundation Deployment Guide* for information on deploying Cloud Foundation.

Resolved Issues

8

The following issues have been resolved:

- vCenter upgrade operation fails on the management domain and workload domain
- Upgrade task status may be reported incorrectly in the SDDC Manager Dashboard Tasks panel
- Using the API to attempt to upgrade multiple clusters only upgrades one cluster
- APIs for managing SDDC cannot be executed from the SDDC Manager Dashboard
- Host commissioning fails if the network pool does not have sufficient free IP addresses
- NTP/DNS server is not updated for NSX-T Managers
- The certificate rotate operation on the second NSX-T domain fails
- Add cluster operation fails
- Multi Transport Zone NSX-T workload domain operations may fail

Known Issues

9

This chapter includes the following topics:

VMware Cloud Foundation Known Issues

- **VMware HCX is not supported**

  VMware Cloud Foundation 4.0 includes VMware NSX-T Data Center 3.0 on a vSphere Distributed Switch (VDS) switch, which is not compatible with VMware HCX.

  Workaround: None.

Bring-up Known Issues

- **The Cloud Foundation Builder VM remains locked after more than 15 minutes.**

  The VMware Imaging Appliance (VIA) locks out the admin user after three unsuccessful login attempts. Normally, the lockout is reset after fifteen minutes but the underlying Cloud Foundation Builder VM does not automatically reset.

  Workaround: Using SSH, log in as admin to the Cloud Foundation Builder VM, then switch to the `root` user. Unlock the account by resetting the password of the admin user with the following command:

```
pam_tally2 --user=<user> --reset
```

- **Bring-up fails during the step Configure NSX-T Transport Node Action**

  Bring-up fails and reports `Failed configuring transport node for ESXi <server hostname>.`. When logged into NSX Manager, one or more hosts will show either a failure to configure a transport node or remain in an unconfigured state.

  Workaround:

  - If the NSX Manager reports that one or more hosts failed to configure a transport node, resolve the errors on the failed host(s) in NSX Manager and then retry bring-up.
  - If the NSX Manager reports that one or more hosts do not have a transport node configured, retry bring-up.

- **Bring-up fails if Edge node FQDNs or the DNS Zone Name contain uppercase letters**

  The Edge node FQDNs and the DNS Zone Name should use only lowercase letters.

  Workaround: Once the Edge node FQDNs and DNS Zone Name are configured correctly, retry bring-up.

- **Cloud Builder appliance platform audit issues**

  When you upload an XLS or JSON file with your SDDC configuration details to the Cloud Builder appliance, the Cloud Builder platform audit does not validate the following:

  - DHCP is configured for the NSX-T Host Overlay (Host TEP) VLAN.
  - The NSX-T Host Overlay (Host TEP) VLAN and NSX-T Edge Overlay (Edge TEP) VLAN are routed to each other with the MTU specified for those networks.

  Workaround: Make sure to verify that you have entered the correct values for these items and that your infrastructure is prepared correctly before you start the bring-up process.

- **The platform audit connectivity checks for the uplink IP addresses for the NSX-T Edge nodes (for Application Virtual Networks) are executed with random IPs from the respective networks.**

  This could lead to a temporary IP overlap with existing objects in those networks.

  Please contact VMware Support for assistance if you are running critical workflows in the networks that could be affected by this issue.

- **Bring-up fails if you select "extra small" for the NSX-T Edge Node Appliance Size**

  The Deployment Parameter Workbook allows you to choose "extra small" as the NSX-T Edge Node Appliance Size. When you upload the workbook to VMware Cloud Builder, validation succeeds, but deployment fails.

  Workaround: Select a different size for the NSX-T Edge node appliance.

Upgrade Known Issues

- **Cluster level upgrade is not available if the workload domain has a faulty cluster**

  This issue occurs if any host or cluster in the workload domain is in an error state.

  Workaround: Remove the faulty host or cluster from the workload domain. The cluster level upgrade option is then available for the workload domain.

SDDC Manager Known Issues

- **Edge cluster deployment task is stuck with a "Running" status**

  If Edge cluster deployment appears stuck for more than 40 mins at the"Deploy NSX-T Data Center Edge Node VM" or "Deploy and configure multiple NSX-T edge node VM" or "Create edge uplink segments" subtask in the Tasks view of SDDC Manager UI, then deployment may have failed. Check the domain manager logs at /var/log/vmware/vcf/domainmanager/domainmanager on the SDDC Manager VM. If you see a failure related to "Deploy and configure multiple NSX-T edge node VM", "Deploy NSX-T Data Center" or "Create edge uplink segments", then the task has failed.

  Workaround:

  a SSH to the SDDC Manager VM.

  b Run the following command: `systemctl restart domainmanager.service`

  c Retry the Edge cluster deployment from the SDDC Manager UI.

- **Adding an NSX-T Edge cluster fails if the SDDC Manager reboots before the task completes**

  If the SDDC Manager VM reboots before the Edge cluster task completes, the task will fail and cannot be restarted until you restart to domain manager service.

  Workaround:

  a SSH to the SDDC Manager VM.

  b Run the following command: `systemctl restart domainmanager.service`

  c Verify that the domain manager service is running: `systemctl status domainmanager.service`

  d Retry the Edge cluster deployment from the SDDC Manager UI.

- **When you replace the certificates for NSX Manager in SDDC Manager the NSX Container Plug-in (NCP) crashes**

  You will not be able to deploy new vSphere pods, load balancers, or other NSX-T resources until you restart the workload management service.

  Workaround:

  a SSH into the vCenter Server appliance.

b Run the following command:

```
vmon-cli -r wcp
```

Workload Domain Known Issues

- **Adding host fails when host is on a different VLAN**

  A host add operation can sometimes fail if the host is on a different VLAN.

  a Before adding the host, add a new portgroup to the VDS for that cluster.

  b Tag the new portgroup with the VLAN ID of the host to be added.

  c Add the Host. This workflow fails at the "Migrate host vmknics to dvs" operation.

  d Locate the failed host in vCenter, and migrate the vmk0 of the host to the new portgroup you created in step 1. For more information, see Migrate VMkernel Adapters to a vSphere Distributed Switch in the vSphere product documentation.

  e Retry the Add Host operation.

  NOTE: If you later remove this host in the future, you must manually remove the portgroup as well if it is not being used by any other host.

- **You are not able to add a cluster or a host to a NSX-T workload domain that has a dead host**

  If one of the hosts of the workload domain goes dead and if you try to remove the host, the task fails. And then, that particular host is set to the deactive state without an option to forcefully remove it. In this condition, if you try to add a new cluster or add a host to the workload domain, the task runs for a long time and then fails eventually.

  Workaround: Bring the dead host back to normal state, after which you would be able add a cluster and a host.

- **Deploying partner services on an NSX-T workload domain displays an error**

  Deploying partner services, such as McAfee or Trend, on a workload domain enabled for vSphere Update Manager (VUM), displays the “Configure NSX at cluster level to deploy Service VM” error.

  Workaround: Attach the Transport node profile to the cluster and try deploying the partner service. After the service is deployed, detach the transport node profile from the cluster.

- **If the witness ESXi version does not match with the host ESXi version in the cluster, vSAN cluster partition may occur**

  vSAN stretch cluster workflow does not check the ESXi version of the witness host. If the witness ESXi version does not match the host version in the cluster, then vSAN cluster partition may happen.

Workaround:

a Upgrade the witness host manually with the matching ESXi version using the vCenter VUM functionality.

b Replace or deploy the witness appliance matching with the ESXi version.

- **vSAN partition and critical alerts are generated when the witness MTU is not set to 9000**

  If the MTU of the witness switch in the witness appliance is not set to 9000, the vSAN stretch cluster partition may occur.

  Workaround: Set the MTU of the witness switch in the witness appliance to 9000 MTU.

- **Operations on NSX-T workload domains fails if their host FQDNs include uppercase letters**

  If the FQDNs of ESXi hosts in an NSX-T workload domain include uppercase letters, then the following operations may fail for the workload domain:

  - Add a host
  - Remove a host
  - Add a cluster
  - Remove a cluster
  - Delete the workload domain

  Workaround: See KB 76553.

- **VI workload domain creation or expansion operations fail**

  If there is a mismatch between the letter case (upper or lower) of an ESXi host's FQDN and the FQDN used when the host was commissioned, then workload domain creation and expansion may fail.

  Workaround: ESXi hosts should have lower case FQDNs and should be commissioned using lower case FQDNs.

- **Adding a host to a vLCM-enabled workload domain configured with the Dell Hardware Support Manager (OMIVV) fails**

  When you try to add a host to a vSphere cluster for a workload domain enabled with vSphere Lifecycle Manager (vLCM), the task fails and the domain manager log reports "The host (host-name) is currently not managed by OMIVV." The domain manager logs are located at /var/log/vmware/vcf/domainmanager on the SDDC Manager VM.

  Workaround: Update the hosts inventory in OMIVV and retry the add host task in the SDDC Manager UI. See the Dell documentation for information about updating the hosts inventory in OMIVV.

- **VMware Cloud Foundation does not support Service VMs (SVMs) on vLCM-enabled workload domains**

  You cannot deploy a Service VM to an NSX Manager that is associated with a workload domain that is using vSphere Lifecycle Manager (vLCM).

Workaround: None.

- **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 7-9 for each `partial success` node.

  When all host issues are resolved, transport node creation starts for the failed nodes. When all hosts are successfully created as transport nodes, retry the failed add vSphere cluster or add host task from the SDDC Manager UI.

- **The vSAN Performance Service is not enabled for vSAN clusters when CEIP is not enabled**

  If you do not enable the VMware Customer Experience Improvement Program (CEIP) in SDDC Manager, when you create a workload domain or add a vSphere cluster to a workload domain, the vSAN Performance Service is not enabled for vSAN clusters. When CEIP is enabled, data from the vSAN Performance Service is provided to VMware and this data is used to aid VMware Support with troubleshooting and for products such as VMware Skyline, a proactive cloud monitoring service. See Customer Experience Improvement Program for more information on the data collected by CEIP.

  Enable CEIP in SDDC Manager. See the VMware Cloud Foundation Documentation. After CEIP is enabled, a scheduled task that enables the vSAN Performance Service on existing clusters in workload domains runs every three hours. The service is also enabled for new workload domains and clusters. To enable the vSAN Performance Service immediately, see the VMware vSphere Documentation.

- **vSAN File Services cannot be enabled on vLCM-enabled workload domains**

In vSphere 7.0, vSphere Lifecycle Manager (vLCM) and vSAN File Services cannot be simultaneously be enabled on a vSAN cluster. See the VMware vSphere 7.0 Release Notes for more details on this limitation.

Workaround: None.

Multi-Instance Management Known Issues

- **Federation creation information not displayed if you leave the Multi-Instance Management Dashboard**

  Federation creation progress is displayed on the Multi-Instance Management Dashboard. If you navigate to another screen and then return to the Multi-Instance Management Dashboard, progress messages are not displayed. Instead, an empty map with no Cloud Foundation instances are displayed until the federation is created.

  Workaround: Stay on the Multi-Instance Dashboard till the task is complete. If you have navigated away, wait for around 20 minutes and then return to the dashboard by which time the operation should have completed.

- **Multi-Instance Management Dashboard operation fails**

  After a controller joins or leaves a federation, Kafka is restarted on all controllers in the federation. It can take up to 20 minutes for the federation to stabilize. Any operations performed on the dashboard during this time may fail.

  Workaround: Re-try the operation.

API Known Issues

- **The /v1/sso-domains APIs are not supported**

  This release does not support the SSO domain APIs:

  - `/v1/sso-domains`
  - `/v1/sso-domains/{sso-domain}/entities`

  Workaround: You can view the Cloud Foundation domains, users, and groups under **Administration > Users** in the SDDC Manager UI.

- **Add host operations using the Cloud Foundation API fail if no ESXi license is specified**

  If an API operation that involves adding a host (creating a VI workload domain, adding a host to a vSphere cluster, adding a vSphere cluster to a workload domain) does not include an ESXi license key in the host specification (`hostSpecs`), the operation will fail. This is true even in cases where the ESXi host has already been licensed outside of the VMware Cloud Foundation system.

Workaround: Make sure that the host specification (`hostSpec`) includes a valid license key (`licenseKey`).

- **You cannot execute APIs that require scheduledTimeStamp as an input from the API Explorer**

  APIs that require `scheduledTimeStamp`, such as `/v1/upgrades` and `/v1/bundles`, will fail if you execute them using the API Explorer in the SDDC Manager UI.

  Workaround: Use a REST API client to execute these APIs.

- **Configuring a backup schedule for the SDDC Manager VM fails**

  Before you can use the VMware Cloud Foundation API to configure a backup schedule for the SDDC Manager VM, you must enable the feature.

  Workaround:

  a SSH in to the SDDC Manager VM using the `vcf` user account.

  b Enter `su` to switch to the `root` user.

  c Create a properties file (`feature.properties`) in the `/home/vcf` directory:

  ```
  vi /home/vcf/feature.properties
  ```

  d Add the following text to the file and save it:

  ```
  feature.vcf.public.api.backups.schedule=true
  ```

  e Change the file permissions to readable, writable, and executable:

  ```
  chmod -R 777 feature.properties
  ```

  f Restart the operations manager service:

  ```
  systemctl restart operationsmanager.service
  ```

  g Use the Cloud Foundation API to set the SDDC Manager VM backup schedule.

- **Adding hosts from different network pools to NSX-T workload domain clusters is only supported for hosts using vSAN storage**

  The Cloud Foundation API supports adding hosts from different network pools to NSX-T workload domain clusters, as long as those network pools have the same VLAN ID and MTU settings. In this release, this functionality is only available for hosts using vSAN storage. For clusters containing hosts using NFS or VMFS on FC storage, all hosts in the cluster must be associated with the same network pool.

  Workaround: None.

- **Stretch cluster operation fails**

  If the cluster that you are stretching does not include a powered-on VM with an operating system installed, the operation fails at the "Validate Cluster for Zero VMs" task.

Make sure the cluster has a powered-on VM with an operating system installed before stretching the cluster.

Networking Known Issues

- **VMware Cloud Foundation does not enable StandBy Relocation on Tier-1 gateways**

  If you create an NSX-T Edge cluster with more than 2 Edge nodes, you should enable StandBy Relocation. Standby relocation means that if the Edge node where the active or standby logical router is running fails, a new standby logical router is created on another Edge node to maintain high availability. If the Edge node that fails is running the active logical router, the original standby logical router becomes the active logical router and a new standby logical router is created. If the Edge node that fails is running the standby logical router, the new standby logical router replaces it.

  Workaround: Use the NSX Manager UI to enable StandBy Relocation for any Tier-1 gateway that is part of an NSX-T Edge cluster with more than 2 Edge nodes.

- **VMware Cloud Foundation supports only one NSX-T Edge Cluster residing on a vSphere Cluster.**

  This is a known limitation. When selecting the vSphere cluster during Edge cluster deployment, choose a vSphere cluster that does not host any Edge nodes for another Edge cluster.

  Workaround: Upgrade to VMware Cloud Foundation 4.0.0.1.

- **Edge nodes are not configured with DNS or NTP settings after Edge cluster creation**

  You must manually configure DNS and NTP settings for Edge nodes after you create an Edge cluster. You can use the VMware Cloud Foundation API to get the current DNS (`/v1/system/dns-configuration`) and NTP (`/v1/system/ntp-configuration`) configurations to use in the workaround.

  Workaround:

  a Log in to the NSX Manager UI for the domain (management or VI workload) in which you created the Edge cluster.

  b Browse to **System > Fabric > Nodes > Edge Transport Nodes**.

  c Select the first Edge node, click the Settings cog, and select **Change Node Settings**.

  d Add the search domain names, NTP Servers, and DNS servers.

  e Click **Save**.

  f Repeat this process for all Edge nodes in the Edge cluster.

- **An outage of a top of rack switch in the data center might cause lack of availability of segments and services that are provided by NSX-T Data Center**

During the failover of a top of rack switch, the TEP communication between the NSX-T components is disrupted causing some segments and services to become unavailable.

Workaround: To ensure that NSX-T Edge TEP communication fails over to the second top of rack switch in the management or workload domain, modify the teaming policy of the port groups for the uplink traffic of the NSX-T Edge nodes.

a In a Web browser, log in to vCenter Server by using the vSphere Client.

b In the **Networking** inventory, expand the tree and browse to the vSphere Distributed Switch for the management domain.

c In the navigation pane, right-click the port group for the first uplink and select **Edit Settings**.

d In the **Edit Settings** dialog box, select **Teaming and failover**.

e Move the uplink from **Unused uplinks** to **Standby uplinks** and click **OK**

f Repeat Step 5 and Step 6 for the other port group for edge uplink traffic in the management domain.

g Repeat the procedure for the port groups for edge uplink traffic in the workload domain.

vRealize Suite Known Issues

- **vRealize Operations Manager: VMware Security Advisory VMSA-2021-0018**

  VMSA-2021-0018 describes security vulnerabilities that affect VMware Cloud Foundation.

  - The vRealize Operations Manager API contains an arbitrary file read vulnerability. A malicious actor with administrative access to vRealize Operations Manager API can read any arbitrary file on server leading to information disclosure.The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned identifier CVE-2021-22022 to this issue.
  - The vRealize Operations Manager API has insecure object reference vulnerability. A malicious actor with administrative access to vRealize Operations Manager API may be able to modify other users information leading to an account takeover.The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned identifier CVE-2021-22023 to this issue.
  - The vRealize Operations Manager API contains an arbitrary log-file read vulnerability. An unauthenticated malicious actor with network access to the vRealize Operations Manager API can read any log file resulting in sensitive information disclosure. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned identifier CVE-2021-22024 to this issue.

- The vRealize Operations Manager API contains a broken access control vulnerability leading to unauthenticated API access. An unauthenticated malicious actor with network access to the vRealize Operations Manager API can add new nodes to existing vROps cluster. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned identifier CVE-2021-22025 to this issue.
- The vRealize Operations Manager API contains a Server Side Request Forgery in multiple end points. An unauthenticated malicious actor with network access to the vRealize Operations Manager API can perform a Server Side Request Forgery attack leading to information disclosure. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned identifiers CVE-2021-22026 and CVE-2021-22027 to this issue.

Workaround: See KB 85452 for information about applying vRealize Operations Security Patches that resolve the issues.

- **vRealize Log Insight: VMSA-2021-0019**

  VMSA-2021-0019 describes security vulnerabilities that affect VMware Cloud Foundation.

  VMware vRealize Log Insight contains a Cross Site Scripting (XSS) vulnerability due to improper user input validation. An attacker with user privileges may be able to inject a malicious payload via the Log Insight UI which would be executed when the victim accesses the shared dashboard link. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned identifier CVE-2021-22021 to this issue.

  Workaround: See KB 85405 for information about applying a vRealize Log Insight Security Patch that resolves the issue.

- **Connecting vRealize Operations Manager to a workload domain fails at the "Create vCenter Server Adapter in vRealize Operations Manager for the Workload Domain" step**

  When you connect vRealize Operations Manager to a workload domain, it fails at the `Create vCenter Server Adapter in vRealize Operations Manager for the Workload Domain` step with a message similar to `Failed to configure vCenter <vcenter-hostname> in vROps <vrops-hostname>, because Failed to manage vROps adapter`. This issue can occur when the vRealize Operations cluster is offline.

  Workaround: Make sure that the vRealize Operations cluster is online.

  a Log in to the vRealize Operations Manager administration interface.

  b Click **Administration > Cluster Management** and check the cluster status.

  c If the vRealize Operations cluster is offline, bring the cluster online.

  d When the cluster status displays as online, retry connecting vRealize Operations Manager to a workload domain