DOCUMENTATION - **APRIL 2018**

VMware Cloud Foundation Guardrails

Guidance on Supported Customizations

VMware Cloud Foundation 2.3.1 (Doc version 1.1)

vmware®

Table of Contents

Introduction

This document explains the supported changes you can do to a VMware Cloud Foundation 2.3 environment and what you need to watch out for.

Follow the product documentation at https://docs.vmware.com/en/VMware-Cloud-Foundation/index.html. Carefully read the complete Release Notes and check all known issues.

As a rule for VMware Cloud Foundation, do not make changes to the hardware configuration manually. Examples include, switch configuration changes unless specified by user configurable options (see below), host changes, cabling, etc. unless performing maintenance guided by VMware GSS and the hardware vendor.

Certain changes to workload domain cluster configurations performed manually within vCenter Server are not allowed. Examples include adding or removing hosts, renaming or changing virtual distributed switch (vDS) configurations, renaming of hosts, datastores, or management workload domain VMs, making changes to management domain VM configurations, etc. Seek guidance from VMware GSS when in doubt.

vSAN features such as encryption, compression and erasure coding may be modified within vCenter Server if you have sufficient resources. See the vSAN and VMware Cloud Foundation documentation for additional information.

Adding and changing customer VM configuration is allowed. Allowed changes are

- advised in the VMware Cloud Foundation product documentation
- advised in public VMware Cloud Foundation KB articles
- advised by *Support (VMware Global Support Services)*

Important Note on Integrated Systems

This document applies to Ready Node based VMware Cloud Foundation installations.

Integrated Systems can have stricter rules or other specific guidance from the vendor. If you are implementing one of the Integrated Systems (Dell EMC VxRack SDDC, FUJITSU PRIMEFLEX for VMware Cloud Foundation, Hitachi Unified Compute Platform (UCP) RS, or QCT QxStack) please reach out to the respective vendor to double check recommendations in this document.

For example: Dell EMC does not support some of the network cabling options described in this document for VxRack SDDC.

Physical Switches and Networks

Switch OS and Firmware

You must install the exact switch OS and firmware on all switches as stated in the documentation. Do not do any upgrades or changes unless instructed by the product documentation (see the section "BIOS Settings"). If there are any uncertainties or you wish to upgrade your Switch OS or Firmware, contact *Support*.

Switch Configuration

SDDC Manager configures the physical switches. The product documentation explains the action you can perform on the switches directly (see the section "Replacing and Restoring Switches").

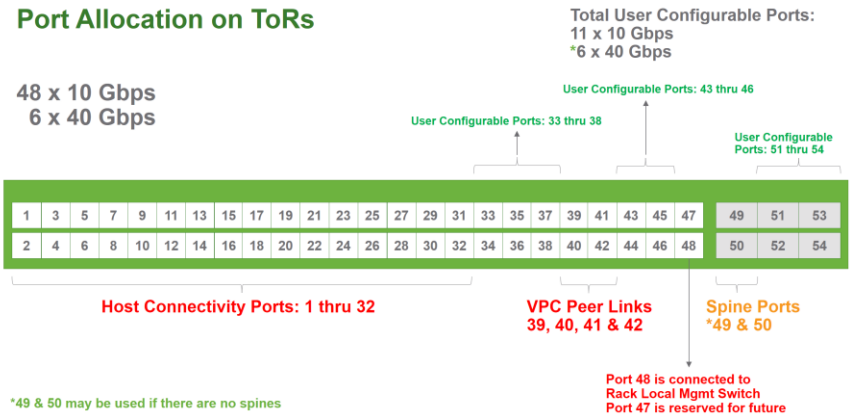
Do a backup of the switch configuration before you do any of the following manual changes. The following additional modifications are allowed:

1. Add VLANs on the free user configurable ports (see next section "Port Changes") – e.g. for backup and archiving solutions or specific use cases which are not covered by SDDC Manager's ability to create VLANs
2. Additional configuration of uplink ports (for example VPC Domains for layer 2 or SVI for layer 3)
3. Add additional users (for monitoring)

Port Changes

Follow the VIA Imaging Guide to cable all switches. You must not change cabling for any port.

There is a range of free ports shown as user configurable ports in the image below which you can use to create additional physical networks. These networks would not be managed by SDDC Manager. You must maintain them manually.



Unused Ports

Some vendors recommend that unused ports should be shut down, this is not done by the SDDC manager and needs to be done manually.

As soon as you indicate to the SDDC Manager that one of those unused ports is to be used as an uplink port, it starts to manage that port (for instance by adding VLANs to it in a L2 scenario and adding an IP-address to it in a L3-scenario).

Inter-rack Switch Locations and Uplink Cabling

The documentation states that both inter-rack switches must be on the second rack.

You may distribute the inter-rack switches on different racks to increase system availability if you keep the cabling identical between all systems.

Impact on SDDC Manager functionality: none

The documentation states that uplinks into the data center network have to be from the ToR switches of the first rack.

Optional: Contact *Support* to get permission to configure the uplinks into the data center from the inter-rack switches to increase system availability. You can inter-connect VMware Cloud Foundation 2.3 racks from the Spine switches to your datacenter demarcation switch-routers.

If you modify the uplink cabling this way SDDC Manager no longer automates uplink connectivity, you must maintain it manually in that case.

Stretching vMotion, vSAN, or VXLAN Networks

vMotion, vSAN, and VXLAN networks are created inside each workload domain and are not routed by default. Contact *Support* if you want to manually route networks for specific use cases.

Two Physical Racks for a ToR Switch Pair

The documentation states that each rack has its own set of ToR switches.

You can connect servers from two physical racks to one set of ToR switches. This way you get up to 32 1U servers into a VMware Cloud Foundation rack if a physical rack can only run 24 or fewer servers due to power constraints. VMware Cloud Foundation can consist of up to 16 physical racks using 8 sets of ToR Switches. Make sure to follow the cabling guidelines on the Top of Rack switches.

The image below shows three sets of two physical racks with 16 servers each. All 2 * 16 servers share one set of Top of Rack switches. You can have up to 8 of those combinations in one VMware Cloud Foundation installation.

VLANs

Do not delete any of the default VLANs created by SDDC Manager. Do not modify any of the default VLANs manually. Do not create VLANs manually. Do not change vDS portgroup names or configuration for these networks manually. Only use the SDDC Manager UI to modify VLANs.

IPAM Address Management for Custom Servers

If you like to add your own custom management servers into the Management Workload Domain consider that the SDDC manager UI does not give the option to add servers to the management domain that can be managed by the internal SDDC IPAM solution. Exclude IP-ranges from the SDDC manager and maintain a separate IPAM solution for those addresses.

Server Hardware

The minimum server configuration is described in the product documentation (VIA Guide).

BIOS, Network Ports, and Disk Layout

Make sure you pick servers from the VMware Cloud Foundation Compatibility Guide (http://vmware.com/go/cloudfoundation-vcg). The server model must be on that list. You can vary CPU and memory if it is supported by vSAN. The memory value specified in the Compatibility Guide is the minimum value. You must not have less memory in the system as specified.

Each server must have two supported 10 G network ports. Do not add extra network ports.

You can vary vSAN disk layout according to the rules in KB 52084 (https://kb.vmware.com/s/article/52084). Take special care to check the additional minimums and maximins for disk configuration specified in the VIA Users Guide, section “Components of a Physical Rack”.

Storage Drivers, and Firmware

If the firmware/driver version is on the Compatibility Guide (specifically the vSAN Hardware Compatibility Guide for storage controllers and drives), it's okay to upgrade these manually. Contact *Support* to confirm before you upgrade.

General

Unsupported VMware Software

The following software cannot be used in current VMware Cloud Foundation installations:

- vCenter HA
- Fault Tolerance
- NSX-T

Lockdown Mode

Lockdown Mode is not supported in VMware Cloud Foundation. It stops all communications with ESXi hosts unless it comes through the vCenter Server authentication. VMware Cloud Foundation uses SSH to communicate with the ESXi hosts over a private unrouteable subnet. If you enabled lockdown mode on VMware Cloud Foundation it would break the system.

However, the ESXi hosts' management ports are on an un-routable network. And the ESXi hosts have the SSH ports firewalled to only allow access from the subnet where only ESXi hosts and SDDC Manager and vCenter Server are attached.

ROBO Use Cases

ROBO use cases are supported. The minimum configuration is 4x VSAN Ready Nodes, 2x supported ToR switches, and a supported management switch. While you can deploy VMware Cloud Foundation on four Servers using the Consolidated Architecture it might not always be a good match for ROBO use cases, because you need supported Top-of-Rack switches and a management switch dedicated for the four servers which might impact your CapEx calculation.

Cloud Native Apps (Container) Workloads

Yes, you can set up and run Cloud Native Apps (Container) workloads on VMware Cloud Foundation. An example of how to deploy VMware Integrated Containers on VMware Cloud Foundation is described here: https://builders.intel.com/docs/cloudbuilders/a-secure-unified-cloud-platform-to-host-both-vm-based-and-container-based-applications.pdf.

Horizon View VDI Enterprise

Horizon View VDI solution is fully automated from SDDC Manager. Here is an example: https://www.youtube.com/watch?v=4qBleltnIaA&feature=youtu.be

vRealize Automation

vRealize Suite Enterprise including – vRA 7.3, vROps 6.6 and Log Insight are all available for automated deploy and configuration from SDDC Manager. See the manual and checkout the examples: https://docs.vmware.com/en/VMware-Cloud-Foundation/2.3/com.vmware.vcf.admin.doc_23/GUID-1112AEAD-9A6A-41F7-8C83-27F279CC8517.html.

Single UI for multiple VMware Cloud Foundation Instances

VMware Cloud Foundation is a single site, single location tool. It does not provide a joint UI for multiple installations.

For visibility (telemetry) across VMware Cloud Foundation instances it is possible for the customer or PSO to create vRealize Operations operational dashboards in a single console view of multiple VMware Cloud Foundation deployments. Customers can enable vROps Federation Services (https://marketplace.vmware.com/vsx/solutions/vrops-federation-management-pack-1-0) to have a single consolidated operations console across multiple SDDC instances.

In addition, depending on the use cases – please introduce your customers to a CMP "Cloud management portal" approach to managing virtualized SDDC resources. From the SDDC Manager, your customers can deploy vRealize Automation to manage VM and logical networking, security constructs across multiple VMware Cloud Foundation instances.

Using AD and DNS with multiple VMware Cloud Foundation Instances

Every VMware Cloud Foundation instance has the same naming scheme. You must use a dedicated sub-domain in Active Directory and DNS per Cloud Foundation System to avoid naming conflicts. The documentation explains how to set up a delegation from your root DNS to the SDDC Manager.

Upgrades and Patching

Only use SDDC Manager for any upgrades and patches. Never apply security fixes, patches and upgrades manually for the systems handled by SDDC Manager which are: vSphere (PSC, vCenter Server, ESXi), vSAN, and NSX.

You patch and upgrade all other components (vRealize LI, vROps, vRA, Horizon) the same way as you would normally. Do check the product interoperability matrix.

Shutdown/Restart Procedure

Follow the shutdown procedure in the documentation. In addition, it is critical to follow vSAN guidance for all Workload Domains. This is especially important for the Management Workload Domain as this is where the vCenters reside (KB 2142676: "Shutting down and powering on a vSAN 6.x Cluster when vCenter Server is running on top of vSAN"). Run a vSAN health check from the UI and fix any vSAN issues before shutting down VMware Cloud Foundation. Follow the documentation for proper restart procedure.

IP Addresses, Object Names, and Passwords

Never manually change any IP addresses of any components deployed by SDDC Manager. Always use the SDDC Manager UI. IP addresses must not be changed in other ways.

Never manually change any object names like host names, network names, cluster names, port group names, etc. created by SDDC Manager.

Only use the SDDC Manager UI Rotate password utility to change passwords. Never change passwords directly on any component.

Do not change ESXi SSH host keys.

Storage and vSAN

Storage Policies

During Bring Up the SDDC Manager sets the default vSAN policies for all Workload Domains. Do not change the default vSAN storage policy. You can create additional vSAN storage policies using the vSphere Web Client as you need.

Impact on SDDC Manager functionality: none

Stretched vSAN Cluster

It is not possible to stretch vSAN across Workload Domains or sites in VMware Cloud Foundation. Contact your VMware sales contact if you have a need for this functionality.

NFS Configuration

Do not change the NFS data store created by SDDC Manager.

Connect External Storage

You can integrate VMware Cloud Foundation with your existing IP-based Storage devices. In that case carefully check any switch over commitment to avoid performance issues. FC SAN storage cannot be connected. To connect iSCSI or NFS storage review the white paper VMW-VCF-ISCSI-USLET-101-HI-RES.pdf (https://communities.vmware.com/docs/DOC-37092) and contact *Support* to check the guidance for your case.

vCenter Server

3rd Party Plug-Ins

You can install 3rd party vCenter Server plug-ins in any of the vCenter Servers deployed by the SDDC Manager.

SDDC Manager is not aware of any 3rd party vCenter Server plugins. You are responsible for manually checking compatibility, backup/restore and upgrading. Use a file or VM level backup solution outside of VMware Cloud Foundation. Then you can restore 3rd party vCenter Server plugins if needed.

Multiple Clusters

The vCenter Servers created by SDDC Manager as part of Workload Domains have one ESXi host cluster. Do not create additional clusters in the vCenter Servers. In VMware Cloud Foundation each vCenter Server must only have one cluster.

Hybrid Cloud Use Cases

IBM Cloud

It is possible to build a hybrid cloud between your data center and the IBM Cloud with VMware Cloud Foundation. To learn how to connect VMware Cloud Foundation in your data center with VMware Cloud Foundation in the IBM Cloud contact your IBM Cloud sales representative or SE.

VMware Cloud on AWS

Contact *Support* for guidance on how to connect VMware Cloud Foundation private cloud instances with your VPC on VMware Cloud on AWS.

Operational Aspects

Workload Migration

Contact *Support* for workload migration guidelines from your brownfield vSphere to VCF WLDs. You can move vSphere workloads from existing infrastructure (SAN, vSphere 5.x, 6.x) to VMware Cloud Foundation using several different methods, like PowerCLI move-vm and an API call to the vSphere API. There are two special methods to help move workloads into VMware Cloud Foundation: Cross vCenter Workload Migration Utility and VMware HCX – Hybrid Cloud Manager.

The Cross vCenter Workload Migration Utility (https://labs.vmware.com/flings/cross-vcenter-workload-migration-utility) is a newly release Fling that can be used via GUI or RESTAPI to bulk migrate workloads from vCenter 6.0+ environments into VMware Cloud Foundation. There are some baselines requirements such as the vMotion VLAN in your VMware Cloud Foundations instances must be routable etc. Please note that the use of this Fling is not supported by *Support*.

Hybrid Cloud Manager – if you plan to use this without the help from PSO then please contact *Support* to plan migration use cases where your source vSphere environments are running on vCenter server 5.1, 5.5, 6.0 or 6.5.

We strongly encourage all migrations to be scoped and delivered by VMware PSO or qualified partners.

Disaster Recovery

Contact *Support* for DR guidelines for your VCF deployments. There are various levels of disaster recovery that's built-in to SDDC Manager today. See the VMware Cloud Foundation documentation.

For site level DR, VCF cross vCenter NSX and SRM guidance, contact your VMware sales team to involve VMware PSO.

Monitoring

All vCenter Server, Horizon, vSAN, NSX, and VMware Cloud Foundation alerts and events are collected in vRealize Log Insight for monitoring and troubleshooting purposes. VMware Cloud Foundation supports your existing monitoring tools such as Splunk, Network Insight, Zabbix, etc. All systems and network monitoring tools are supported.

Change Log

Doc version 1.1

- Added "Doc version" tag on the title page
  VMware Cloud Foundation 2.3.1 (Doc version 1.1)

- Added new Section:
  Important Note on Integrated Systems

- Server Hardware / BIOS, Network Ports, and Disk Layout

  - Edited
    Removed "Network Cards" and replaced it with "Network Ports" everywhere

  - Added
    The memory value specified in the Compatibility Guide is the minimum value. You must not have less memory in the system as specified.

  - Added
    Take special care to check the additional minimums and maximins for disk configuration specified in the VIA Users Guide, section "Components of a Physical Rack".

- General

  - Added new section
    Lockdown Mode

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com