DOCUMENTATION - **NOVEMBER 2018**

VMware Cloud Foundation Guardrails

Guidance on Supported Customizations

VMware Cloud Foundation 3.0 (Doc version 1.0)

vmware®

Table of Contents

Introduction

This document explains the supported changes you can do to a VMware Cloud Foundation 3.0 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.

Certain changes to workload domain cluster configurations performed manually within vCenter Server are not allowed. Examples include adding or removing hosts or clusters, 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 for VxRack SDDC as described in this document.

General

Unsupported VMware Software

The following software cannot be used in current VMware Cloud Foundation 3.0 installations:

- vCenter HA
- 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.

Certificates

Use the SDDC Manager’s Cert Helper to modify certificates. Do not use any other tools. If you use any other tool but the official Cert Helper you will break the trust between SDDC Manager and the environment which will break the Cloud Foundation system.

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. You can deploy VMware Cloud Foundation on four Servers using the Consolidated Architecture.

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 can be manually installed in a VI workload domain.

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.

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

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.

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.

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 1.0

- Initial version

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