VMware Cloud Foundation 4.2

Q1. What’s New with VMware Cloud Foundation 4.2?

Here are the new features in Cloud Foundation 4.2:

• **Data Persistence Platform** provides a framework for modern stateful service providers to build deep integration with the underlying virtual infrastructure leveraging the Kubernetes operator method and vSphere Pod Service, allowing customers to run their stateful applications with lower TCO and simplified operations and management.

• **VMware HCI Mesh** - Integrate disaggregated nodes to scale compute/storage independently.
  - Reduce CAPEX by sharing capacity across clusters. VMware HCI Mesh introduces the capability to share storage capacity across vSAN clusters, capturing capacity that otherwise might be stranded in clusters that run compute heavy workloads. Customers can consolidate more workloads on existing capacity and reduce the need to procure more storage in the short term.
  - Lower OPEX with VMware HCI Mesh, as customers reduce the amount of storage resources required, they also spend less time maintaining resources, which frees up employees to focus on other tasks.

• **VMware NSX-T 3.1 Federation - Common Policies, Intrinsic Security, Operational Simplicity**
  - Cloud-scale Networking: Federation enhancements for consistent networking across sites.
  - Intrinsic Security: Distributed IPS, FQDN-based Enhancements.
  - Lifecycle and monitoring: NSX-T support with VMware vSphere Lifecycle Manager, simplified installation, enhanced monitoring, search, and filtering.

• **VMware Cloud Foundation SDDC Manager security hardening** - Hardening of bring up, configuration and lifecycle management operations.
  - VMware Cloud Foundation 4.2 introduces additional flexibility to leverage static IP pools for NSX-T Host Overlay (TEP) networks as an alternative to DHCP. This applies to the management domain and VI workload domains with uniform L2 clusters.
  - Supports VMware ESXi lockdown mode to avoid unauthorized access to the platform.

• **VMware Advanced Security™ for Cloud Foundation™** v2 uses a unique, intrinsic approach to deliver unified protection for data center workloads and traffic that is easy to operationalize, while enabling customers to replace multiple legacy security solutions. This solution brings together world-class workload protection, intrusion detection and prevention, and web application firewall for public and private clouds based on VMware Cloud Foundation.
  - Advanced Security Bundles in v2 Release:
    - Advanced Security Add-on for VMware Cloud Foundation
    - Purpose built to protect modern data center and applications using VMware NSX® Advanced Threat Prevention (includes VMware NSX® Firewall, VMware NSX® Distributed IDS/IPS and VMware NSX® Intelligence) and VMware NSX® Advanced Load Balancer/WAF.
  - Advanced Security Add-on for VMware Cloud Foundation
  - Best in class workload protection, in addition to highly secure datacenter and applications using VMware Carbon Black Cloud Workload, VMware NSX® Advanced Threat Prevention (includes VMware NSX® Firewall, VMware NSX® Distributed IDS/IPS and VMware NSX® Intelligence) and VMware NSX® Advanced Load Balancer/WAF.

Q2. What is being delivered in Cloud Foundation 4.2?

VMware Cloud Foundation 4.2 includes the following components:

- vSphere 7.0 Update 1 Patch 02 with Tanzu
• vSAN 7.0 Update 1 Patch 02 supporting enhanced cloud native storage, integrated file services.

• vRealize Suite 2019 provides numerous enhancements to vRealize log insight 8.2, vRealize Operations 8.2, and vRealize Automation 8.2 Patch 1. Note: VMware Cloud Foundation 4.2 deploys vRealize Lifecycle Manager (vRSLCM) 8.2 Patch 2, then vRSLCM deploys and provides ongoing life cycle management of other vRealize Components.

• NSX-T 3.1 supporting new networking and security features including NSX-T Federation.

Q3. How can customers deploy the new vSphere with Tanzu functionality?


Q4. Will existing VMware Cloud Foundation 3.X deployments be able to upgrade to VMware Cloud Foundation 4.X?

In-place upgrades are not supported at this time, but customers running VCF 3.X may be able to redeploy VMware Cloud Foundation (non-production environments only) or perform adjacent workload migrations, in which your workload is moved between a 3x and 4x environment in a side-by-side fashion. This capability exists via our professional service organization.

Q5. Does VMware Cloud Foundation 4.2 support automated deployment of vRealize Suite?

VMware Cloud Foundation 4.2 supports automated deployment for vRealize Suite Lifecycle Manager (vRSLCM) and then vRSLCM provides deployment of the underlying vRealize components as well as ongoing life cycle management of the vRealize Suite. VMware provides manual guidance to ensure that the vRealize Suite updates are successful.

Q6. Does VMware Cloud Foundation 4.2 provide automated patching and updating for vRealize Suite?

VMware Cloud Foundation’s SDDC Manager retrieves validated vRealize Suite patches and updates from the Cloud Foundation online patch depot. Cloud Foundation administrators may then install vRealize Suite updated through the VMware Cloud Foundation SDDC Manager interface, providing a ‘single-pane’ experience for lifecycle management of the Cloud Foundation platform. VMware Cloud Foundation then leverages the automation available within vRealize Suite Lifecycle Manager (vRSLCM) to execute automated patching and updating in the background.

Q7. Does VMware Cloud Foundation 4.2 support VMware PKS (TKGi)?

Yes. VMware Cloud Foundation 4.2 will support VMware TKGi (formerly VMware PKS). For more information, see: https://docs.pivotal.io/tkgi/1-8/vsphere-vcf.html.

General

Q8. Where can I find more information and resources?

You can find additional Cloud Foundation information here:

• VMware Cloud Foundation Resource Center: http://vmware.com/go/CloudFoundationrc
• Product Page: vmware.com/go/cloudfoundation
• Documentation: vmware.com/go/cloudfoundation-docs
• Community: vmware.com/go/cloudfoundation-community
• Talk to your VMware Partner or VMware Sales team.

Q9. What is VMware Cloud Foundation?

VMware Cloud Foundation™ provides the simplest path to hybrid cloud through an integrated software platform that is the foundation for both private and public cloud environments. Cloud Foundation provides a complete set of software-defined services for compute, storage, network, and security, along with cloud management capabilities. The result is simple, secure, and agile cloud infrastructure that can be can deployed on premises and consumed as a service from public cloud.

Q10. How can I use Cloud Foundation in the public cloud?

Select service providers from the VMware Cloud Provider program offer cloud services powered by VMware Cloud Foundation, including CenturyLink, OVH and Rackspace. Reach out to the specific service providers for more information.
**VMware Cloud on AWS** is an on-demand service operated, managed, and sold by VMware. VMware Cloud on AWS is powered by VMware Cloud Foundation.

Additional solutions such as Azure VMware Solution and Google Cloud VMware Engine are also powered by VMware Cloud Foundation.

**Note:** The following questions and answers focus on Cloud Foundation for on-premises deployment.

Q11. What types of OEM integrated systems are available with Cloud Foundation from OEMs?

Integrated Systems from OEMs can be either:

- Jointly Engineered Solutions VMware Cloud Foundation on Dell EMC VxRail
- Global Partner Appliances which include Fujitsu PRIMEFLEX and the Hitachi Unified Compute Platform UCP-RS, HPE and Lenovo.
- Composable Cloud Foundation on HPE Synergy and Cloud Foundation on Dell MX
- VMware Ready Nodes available from 15 OEMs

Q12. What is the unique integration of a jointly engineered solution?

Jointly engineered systems, such as Cloud Foundation on VxRail, provide unique integration with Cloud Foundation components. VxRail integration with Cloud Foundation includes, but is not limited to, lifecycle management of the hardware and software sub-systems using native SDDC Manager orchestrated workflows integrated with VxRail Manager. Note that VxRail does require Dell professional services for installation.

Q13. Can vSAN ReadyNodes be added to Dell EMC VxRail deployments (and vice versa)?

No. It is not possible to deploy vSAN ReadyNodes and VxRail nodes within the same deployment. Refer to the **VCF on VxRail admin guide** for more information.

Q14. How does VMware Cloud Foundation integrate with composable systems?

Composable systems, such as Dell MX and HPE Synergy integrate with Cloud Foundation through the Redfish API that enables the ability to compose and decompose hardware resources under control of VMware Cloud Foundation.

Q15. Who supports Cloud Foundation software and hardware?

When purchasing an OEM Solution, the OEM partner will be the single point of contact for support of both hardware and software. When Cloud Foundation software is purchased from VMware, the support model will follow the standard practice of VMware products with VMware Technical Support delivering support for the Cloud Foundation software.

Q16. What VMware Technical Support options are available for VMware Cloud Foundation?

The VMware Technical Support matrix lists the following support options for VMware Cloud Foundation:

- Basic
- Production
- Business Critical
- Healthcare Critical
- Mission Critical
- U.S. Federal Production

We recommend purchasing at least Production support, or better Business Critical or Mission Critical with VMware Cloud Foundation.

Q17. How can I purchase Cloud Foundation software?

There are four ways to purchase Cloud Foundation software:

1. directly from VMware, 2. from VMware channel partners (3) as part of an integrated system from OEM vendors and (4) as a subscription service from a public cloud service provider.
Q18. Can I install the Cloud Foundation software myself?

Yes. VMware provides documentation for customers to deploy the Cloud Foundation software on their own. It is highly recommended that you work with VMware Professional Services or your Solution Provider to receive assistance with your deployment. Visit the Documentation page for more information on how to deploy Cloud Foundation.

Q19. What is the difference between SDDC Manager and vRealize Automation?

SDDC Manager and vRealize Automation automate different aspects of building and running private and public clouds. SDDC Manager automates the installation and lifecycle management of the vSphere, vSAN, and NSX from bring-up and configuration to patching and upgrading, making it simple for the cloud admin to build and maintain the SDDC. For VCF 3.X, SDDC Manager also automates the installation and configuration of vRealize Log Insight, vRealize Operations, and vRealize Automation. (not supported in VCF 4.2)

On the other hand, vRealize Automation automates the delivery and management of the virtual machines and apps, enabling end users to consume these as services and at scale. vRealize Automation also has integration with SDDC Manager via QuickStart.

Q20. Does SDDC Manager replace other existing management tools, such as vCenter Server?

No. SDDC Manager complements vCenter Server by delivering new functionality that helps cloud admins build and maintain the SDDC. The cloud admin will continue to use vCenter Server as the primary management interface for the virtualized environment.

Pricing and Packaging

Q21. What Editions are available for purchase of VMware Cloud Foundation 4.2?

VMware Cloud Foundation 4.2 is available in the following SKUs: Starter, Standard, Advanced and Enterprise editions, with and without vSAN. The Standard, Advanced, and Enterprise editions include VMware Tanzu Standard, while the Starter edition does not include Tanzu Standard, but it can be purchased as an add-on.

For more information on each edition, please see https://www.vmware.com/products/cloud-foundation.html#compare.

Q22. What is Cloud Foundation with VMware Tanzu Standard?

The VMware Cloud Foundation Standard, Advanced and Enterprise editions are offered with VMware Tanzu Standard to run and manage Kubernetes across multiple clouds. The VMware Cloud Foundation Starter edition does not include Tanzu Standard, but this can be purchased as an add-on. Note that these are only available via ELA and SPF. Contact your VMware account team for more information.

Q23. What capabilities are added when Tanzu Standard is sold with VMware Cloud Foundation?

VMware Tanzu Standard includes a Kubernetes-based container management (Tanzu Kubernetes Grid), global policy management (subset of Tanzu Mission Control capabilities) and support for monitoring (via Prometheus and Grafana). This can be added to VMware Cloud Foundation Standard, Advanced and Enterprise editions. VMware Cloud Foundation with Tanzu Standard delivers consistent operations across on-premises and public clouds through a single integrated architecture that is easy to deploy with centralized control of multiple clusters across multiple teams.

Q24. Where can I go for additional information on Cloud Foundation Pricing and Packaging?

Consult with your VMware Sales Representative, channel partner or qualified OEM partner for more pricing and packaging information.

Technical

Q25. What is VMware SDDC Manager?

SDDC Manager is the centralized management software in Cloud Foundation used to automate the lifecycle of vSphere, vSAN, NSX Data Center and vRealize Suite*, from bring-up, to configuration, to
infrastructure provisioning to upgrades/patches. (* limitations noted)

Q26. Can I use the SDDC Manager with existing deployments?

No. To benefit from SDDC Manager’s automation capabilities you do a fresh install of the full SDDC software stack.

Q27. What is the Cloud Builder?

Cloud Builder is a Photon OS VM that is delivered as an OVA file and includes a virtual imaging appliance (VIA). It contains all code and product bits to automate the deployment of the full SDDC stack for the management domain for your VMware Cloud Foundation instance. The VM can be deployed on any physical device that has connectivity with the ESXi hosts, including laptops and external hosts. Follow the Cloud Builder UI on the VM to deploy the SDDC stack. Input parameters are passed in via a deployment parameters file import.

Q28. What is Multi-Instance Management?

Multi-instance Management allows the ability to have multiple Cloud Foundation instances managed within a single management plane.

Q29. Can Cloud Foundation Multi-Instance Management be used in a deployment based upon a consolidated architecture?

Yes, Multi-instance Management is supported in both a consolidated and standard architecture. The management cluster within a consolidated architecture is managed using resource pools. A standard architecture can be scaled easily by adding more compute and storage.

Workload Domains

Q34. What is a workload domain?

Workload Domains are a logical abstraction of private Cloud capacity that is provisioned automatically by SDDC Manager and administered and patched independently. Workload Domains provide a unit of consumption at the SDDC level by presenting an integrated selection of compute, storage, and network resources for business workloads to run in.

Q35. Why would a user create another workload domain?

In order to scale deployments, assign unique characteristics and maintain workload isolation, it is a best practice to create additional workload domains for new workloads.

Hardware

Q30. What are the physical server requirements?

VMware Cloud Foundation is supported on vSphere-compatible server hardware which meets the minimum requirements for VMware Cloud Foundation and the desired workloads. If vSAN is used as the principal storage system, the servers must be vSAN ReadyNodes. See the vSAN Compatibility Guide and the VMware Cloud Foundation product documentation for details.

Q31. What switching hardware is supported?

You can use those Enterprise-grade network switches that meet the requirements of vSAN, and which are capable of meeting the scale demands of a highly connected set of vSAN hosts.

Q32. How does Cloud Foundation leverage Composable Infrastructure?

Composable Infrastructure allows building physical servers on the fly using an API. Cloud Foundation has a composability plug-in which uses the "RedFish API" to perform this integration. This API communicates with the composable hardware manager to request physical infrastructure on demand.

Q33. Which Composable Infrastructure systems are supported?

VMware Cloud Foundation supports Dell MX and HPE Synergy as composable infrastructure systems.

Q36. What is a management domain?

The management domain is a special purpose workload domain that is used to host the infrastructure components needed to instantiate, manage, and monitor the Cloud Foundation infrastructure. The management domain is automatically created using the Cloud Builder appliance when it is initially configured.
Q37. How many nodes are required for the management domain?

The management domain leverages vSAN for storage and requires a minimum of 4 nodes.

Q38. How many vCenter Server instances can be deployed in a workload domain?

Each workload domain has one dedicated vCenter Server instance.
(Note: Only one vCenter Server license is needed per Cloud Foundation instance or 15 workload domains)

Q39. What is the minimum number of vSphere hosts that can be in a Virtual Infrastructure Workload Domain?

Workload domains require a minimum of three hosts.

Q40. Can I extend/delete a workload domain after it has been created?

Yes, Cloud Foundation provides a fully automated process for creating, extending, and deleting workload domains using SDDC Manager. If supplemental storage has been added to the workload domain, manual processes may be required to provision or un-provision this storage accordingly.

Q41. Can I reduce the size of a workload domain?

Yes, Cloud Foundation allows removing hosts and clusters from workload domains.

Storage

Q42. What is the difference between Principal storage and Supplemental storage within VMware Cloud Foundation?

Principal storage is selected when creating a management domain, workload domain, or when creating a new cluster within a workload domain. Supplemental storage may be added to management or workload domain clusters after their creation. Principal storage is required for every cluster. Supplemental storage can be used for additional storage options. Both principal and supplemental storage can be used for primary workloads/use-cases.

Q43. Can I change the principal storage selection after creating a workload domain cluster?

No, you must create a new cluster within the workload domain or a new workload domain to change the principal storage selection. vMotion can be used to move the VMs to the newly created cluster. Supplemental storage can be manually added or removed without re-creating the cluster.

Q44. Does VMware Cloud Foundation support external Fibre Channel Storage Arrays as a principal storage within a Cloud Foundation Workload Domain?

Yes, while vSAN the preferred and most integrated storage choice for workload domain clusters, administrators have the option to provision external FC storage systems using VMFS on FC as the principal storage. In addition, vVols and NFSv3 storage systems may also be used for workload domain principal storage. vVols, VMFS on FC, NFS v3 or v4, and iSCSI may also be used as supplemental storage. vSAN is the only principal storage option for the management domain. Management domain supplemental storage can be any of the supplemental storage options available to workload domains. For all storage options, the system must appear on the vSphere SAN/NAS Compatibility Guide: http://vmw.re/storagevcg.

Q45. Is vSAN required with Cloud Foundation?

vSAN is required for the Cloud Foundation management domain principal storage. It is possible to add supported storage options as supplemental storage for the management domain (see A41). The workload domains may use vSAN or a supported storage option for principal storage, with a variety of additional storage options available as supplemental storage (see A41).

Q46. Which principal storage options are supported with VMware Cloud Foundation?

VMware Cloud Foundation can consume and is validated against vSAN, vVols, NFS v3, and VMFS on FC. vSAN is the only principal storage option for the management domain. VMware recommends using vSAN as the principal storage for all workload domains to leverage the benefits of managing and maintaining a full software defined stack. vSAN is also updated and patched by SDDC Manager. Updating and patching non-vSAN
storage is a manual task and falls outside of the lifecycle management offered by SDDC Manager. To ensure supportability, the storage system will need to be validated on the vSphere SAN/NAS Compatibility Guide: [http://vmw.re/storagevcg](http://vmw.re/storagevcg).

Q47. Which supplemental storage options are supported with VMware Cloud Foundation?

VMware Cloud Foundation supports the use of NFS (v3, or v4.2), VMFS on FC, iSCSI, and vVols as supplemental storage. Supplemental storage is not integrated to or shown within SDDC Manager.

Q48. Does Cloud Foundation support all-flash vSAN storage?

Yes, Cloud Foundation supports both the Hybrid and All-Flash vSAN configurations. Note that clusters within a multi-cluster workload domain can have both Hybrid and All-Flash vSAN configurations, mixing Hybrid and All-Flash nodes within a single cluster is not supported.

Q49. Can I use Network Attached Storage (NAS) with Cloud Foundation?

VMware Cloud Foundation supports the use of NFS (v3, or v4.2), VMFS on FC, iSCSI and vVols as supplemental storage. Supplemental storage is not integrated to or shown within SDDC Manager.

Q50. Can I use any server to create a workload domain when utilizing non-vSAN storage?

Yes, any vSphere-compatible server can be used for a workload domain cluster not using vSAN. They do not need to be vSAN ReadyNodes in this case.

Q51. Does VMware Cloud Foundation 4.2 support vSAN Stretched Clusters?

vSAN stretched clusters are currently only supported on workload domains using vSphere Upgrade Manager (VUM) vs. vSphere Lifecycle Manager (VLCM).

Q52. Is stretched clustering supported for a workload domain configured for Kubernetes?

No. vSAN Stretched Clustering for workload domains that are configured for Kubernetes Workload Management is currently not supported.

Q53. What is VMware HCI Mesh?

VMware HCI Mesh is vSAN’s all new feature that provides for “Disaggregated HCI” or DHCI exclusively through software. HCI Mesh allows an administrator to easily define a relationship between two vSAN clusters, and borrow capacity from another cluster, improving the agility and efficiency in an environment. This disaggregation allows the administrator to separate compute from storage. HCI Mesh uses vSAN’s native protocols for optimal efficiency and interoperability between clusters. Complementing the inherent capability within vSAN to treat storage as an exclusive resource of the cluster, HCI Mesh delivers the flexibility in resource provisioning that many of our customers have been asking for.

Q54. Is HCI Mesh supported with VCF for remote or stretched clusters?

No, not at this time.

Networking

Q55. Can I connect the NSX-T Manager in Cloud Foundation to other non-Cloud Foundation infrastructure?

No. This is not supported. NSX-T is only aware of the corresponding Cloud Foundation Workload Domains.

Q56. Does VMware Cloud Foundation support Bare Metal Edge Servers in NSX-T?

Yes. The overwhelming majority of customers deployment use case can be fulfilled with VM form factor edge nodes. Support for Bare Metal Servers configured as NSX-T Edge Nodes is provided for customers specific use cases which cannot be supported on an VM form factor edge node.
Q57. Does VCF support Bare Metal Servers (i.e., Windows or Linux servers) or KVM as NSX-T transport nodes?

No, VCF does not support hosts which are not managed by SDDC manager to be part of the NSX-T installation. Today, SDDC manager does not support KVM or other NSX-T bare metal servers as transport nodes.

Q58. What is NSX-T Federation?

NSX-T Federation capabilities provide a cloud-like operating model for network administrators by simplifying the consumption of networking and security constructs. This includes centralized management, consistent networking and policy configuration with enforcement and synchronized operational state across large scale federated NSX-T deployments.

Q59. What value does NSX-T Federation provide?

With NSX-T Federation, VCF customers can leverage stretched networks and unified security policies that span multi-region VCF deployments providing workload mobility and simplifying disaster recovery.

Q60. How does NSX-T Federation work in VMware Cloud Foundation 4.2?

VCF customers can now leverage NSX-T Federation capabilities to federate and manage multiple NSX-T domains through a single pane of glass, using Global Manager (GM). GM provides a graphical user interface and an intent-based REST API endpoint. Through the GM, you can configure consistent security policies across multiple locations and stretched networking objects: Tier0 and Tier1 gateways.

Q61. For which use cases is NSX-T Federation support in VMware Cloud Foundation targeted?

NSX-T Federation can support a variety of use cases based on business demands and preferred architectures. NSX-T is well-suited for hybrid cloud connectivity, workload mobility, and disaster recovery across cloud environments.

Q62. Is NSX-T Federation automatically implemented by SDDC Manager?

NSX-T Federation in 4.2 is implemented and supported through manual guidance, including architecture and design documentation, on the VMware Docs site here (link).

Q63. Are there limitations with NSX-T Federation in VMware Cloud Foundation 4.2?

SDDC Manager is not integrated with NSX-T Global Manager in this release. As such, SDDC Manager functions (like password rotation, certificate replacement, and LCM) do not interact with NSX-T Global Manager. Further, vRealize Operations cannot collect data from the Global Managers, and vRealize Automation cannot provision workloads with Global Managers.

Q64. Are there any limitations with NSX-T Federation working with 2nd/3rd party products?

NSX-T Federation moves the management plane from Local Manager to Global Manager. Any products that integrate with NSX-T or consume NSX-T APIs should evaluate their compatibility with NSX-T Federation.

Q65. Can I upgrade to VMware Cloud Foundation 4.2 and adopt NSX-T Federation?

NSX-T Federation in VCF 4.2 is targeted for greenfield deployments. Please work with GSS and your account team to evaluate if your existing production deployment can be upgraded to VCF 4.2 to adopt NSX-T Federation.

Q66. Is NSX-T Federation supported between VCF and non-VCF deployments?

No. NSX-T Federation in VCF 4.2 is targeted between VCF deployments only.

Q67. Is NSX-T Federation supported between VCF Ready Node and VCF on VxRail deployments?

No. NSX-T Federation in VCF 4.2 is targeted for Federation between homogeneous VCF deployments only.
Q68. Do I need to federate the Management Domain in order to federate the VI Workload domain?

No. You can choose to federate VI Workload domains without federating the management domain. If you need availability of the management components such as vRA, vROps deployed in the management domain, then you need to federate the management domain.

Q69. Can I federate between the Management domain and VI Workload domain?

No. This is not supported.

VCF Remote Clusters

Q70. Is there a hard requirement of 3-4 nodes per VCF Remote Cluster site?

VCF only supports a minimum of 3 nodes and a maximum of 4 nodes per VCF Remote Cluster.

Q71. What is the license requirement for VCF Remote Clusters?

VCF standard pricing applies to VCF Remote Clusters, no special pricing or licensing is required.

Q72. Are there any hardware specific requirements for VCF Remote Clusters?

No, any vSAN Ready Nodes or Dell VX Rail system will support VCF Remote Clusters.

Q73. Why is the requirement to have two active WAN links from the remote sites to the central site?

VCF Remote Cluster is designed to optimize for cost in the remote sites. The SDDC Manager & NSX Manager is in the central, so if the WAN link between the central site and remote sites fails when a node in the remote site reboots, resulting in a dual failure state, the VMs running on the node at the remote site will not be operational until the WAN link becomes active. This can cause application instability in the remote sites. To avoid, it is strongly recommended to use dual active WAN links across sites.

Patching and Upgrades

Q74. What software components can be patched/upgraded using SDDC Manager?

VMware vSphere, vSAN, NSX, vCenter Server and SDDC Manager components are patched/upgraded.

Q75. How am I notified when patches/upgrades become available?

Users are automatically notified from the SDDC Manager user interface when patches and upgrades become available.

Q76. Can I schedule when patches and upgrades are applied?

Yes, SDDC Manager allows patches and upgrades to be scheduled to coincide with regular maintenance windows.

Q77. Can I patch/upgrade workload domains independent of each other?

Yes, patches and upgrades are scheduled on a per-workload domain basis allowing updates to be “rolled-in” over time.

With VMware Cloud Foundation 3.9, you can apply cluster level upgrades for ESXi.

With VMware Cloud Foundation 3.10, you can apply cluster level upgrades and parallel cluster upgrades for both ESXi and NSX-T.

With VMware Cloud Foundation 4.1, you can apply cluster level upgrades and parallel cluster upgrades for ESXi and NSX-T on VUM enabled domains. This feature is not available for NSX-T on vLCM enabled domains yet. Customers are given an option to choose vSphere Update Manager (VUM) or vSphere Lifecycle Manager (vLCM) when creating a workload domain.

Q78. When should I use VUM vs. vLCM?

VUM is the preferred solution when your hardware is not yet supported by vLCM. Note that VUM is required for the Management Domain and when running vSphere with Tanzu. Use vLCM when supported by your hardware platform. vLCM supports firmware updates with more vendors to follow in coming releases. NSX-T Instances cannot be shared between VUM and vLCM.
Configuration Minimums and Maximums

Q79. What is the minimum size of a Cloud Foundation environment with a consolidated deployment?

You need at least 4 servers to run Cloud Foundation in a consolidated architecture. Workload VMs are placed in dedicated resource pools in the Management Domain.

Q80. What is the minimum size of a Cloud Foundation environment to use VI workload domains?

With a standard architecture, you need at least 7 servers to run Cloud Foundation with a VI workload domain. What is the maximum size of a Cloud Foundation environment? Cloud Foundation inherits configuration maximums from the component products. For information on sizing VMware Cloud Foundation refer to https://configmax.vmware.com

Q81. What is the maximum size of a workload domain?

Each workload domain has its own vCenter Server and it can have as many hosts and clusters as a single vCenter Server can handle. Within Cloud Foundation 4.2, you may also size the vCenter Server instance during VI WLD creation via the API or change the vCenter size after deployment. vCenter Server limits apply, see https://configmax.vmware.com for more information.

Q82. How many workload domains can a Cloud Foundation instance have?

Cloud Foundation always has 1 management domain and up to 14 VI workload domains. Each workload domain can contain multiple ESXi host clusters. This limit is imposed by the max number of vCenter Server instances that can be configured in enhanced linked mode which supports up to 15 vCenter Servers, and each workload domain has its own vCenter Server. See https://configmax.vmware.com for more information.

Advanced Security for VMware Cloud Foundation Addon

Q83. What is VMware Advanced Security for Cloud Foundation?

VMware Advanced Security for Cloud Foundation brings together world-class workload protection, intrusion detection and prevention, advanced load balancing, and web application firewall for public and private clouds based on VMware Cloud Foundation.

Q84. How is VMware Advanced Security for Cloud Foundation sold?

VMware Advanced Security for Cloud Foundation is sold as an add-on to VMware Cloud Foundation. Two bundles are now available: Network and App Security Add-on for Cloud Foundation, and Advanced Security Add-on for Cloud Foundation.

Q85. What is included with the Network and App Security Add-on for Cloud Foundation?


Q86. Can the security bundle be added to previous versions of Cloud Foundation?

The Network and App Security Add-On for Cloud Foundation is available on Cloud Foundation 4.2 and above.

Q87. Will Network and Security Add-On for Cloud Foundation work in a vSphere environment?

Only as part of a VMware Cloud Foundation environment running NSX-T 3.1 or later.
Miscellaneous

Q88. Does SDDC Manager automate the deployment of other management components, such as vRealize Network Insight (vRNI)?

vRNI can be manually deployed and externally integrated with VMware Cloud Foundation.

Q89. What logs are sent to the vRealize Log Insight in the Cloud Foundation management cluster?

Cloud Foundation can be configured to send event logs for vSphere, vSAN, NSX, SDDC Manager, vCenter and Horizon into vRealize Log Insight.

Q90. How can SDDC Manager be protected by backup?

In Cloud Foundation 4.2, SDDC Manager backup and recovery capabilities have been enhanced, allowing VMware backup solution provider partners to easily protect and restore SDDC Manager.