**VMO2 Baguley VCF Solution High Level Design**

Infrastructure & Network Design

Version 0.1

TABLE OF CONTENTS

[1 Requirements 7](#_Toc89178120)

[1.1 Business Requirements. 7](#_Toc89178121)

[1.2 Technical Requirements 11](#_Toc89178122)

[2 Base vmware Cloud foundation 23](#_Toc89178123)

[2.1 VMware Cloud Foundation Overview 23](#_Toc89178124)

[2.2 VMware Cloud Foundation Software Installation 23](#_Toc89178125)

[2.3 SDDC Architectures 25](#_Toc89178126)

[2.4 Physical Infrastructure Design 28](#_Toc89178127)

[2.5 Virtual Infrastructure Design 30](#_Toc89178128)

[2.6 Network Design for ESXi for the Management Domain 33](#_Toc89178129)

[2.7 vCenter Server Design for the Management Domain 35](#_Toc89178130)

[2.8 vSphere Networking Design for the Management Domain 44](#_Toc89178131)

[2.9 Software Defined Networking Design for the Management Domain 50](#_Toc89178132)

[2.10 Shared Storage Design for a Virtual Infrastructure Workload Domain 69](#_Toc89178133)

[2.11 VMware Workspace One Access 79](#_Toc89178134)

[3 Base vmware Cloud foundation 84](#_Toc89178135)

[3.1 VMware Life Cycle Architecture 84](#_Toc89178136)

[3.2 Cloud Operations Design 86](#_Toc89178137)

[3.3 Cloud Monitoring Architecture 91](#_Toc89178138)

[3.4 Logging Architecture 12](#_Toc89178139)

[4 Appendix 24](#_Toc89178140)

LISt of Tables

[Table 1 - Document Information 5](#_Toc89178141)

[Table 2 - Document Control 5](#_Toc89178142)

[Table 3 - Document Impact on DCT Delivery 5](#_Toc89178143)

[Table 4 - Compliance and Governance 5](#_Toc89178144)

[Table 5 - Document References 5](#_Toc89178145)

[Table 6 - Business Requirements 10](#_Toc89178146)

[Table 7 - Technical Requirements 22](#_Toc89178147)

[Table 8 – SDDC Availability and Zone Design Decisions 27](#_Toc89178148)

[Table 9 - Availability Zone Characteristics 29](#_Toc89178149)

[Table 10 - Physical Availability and Zone Design Decisions 29](#_Toc89178150)

[Table 11 - SDDC ESXi Design Decisions 32](#_Toc89178151)

[Table 12 - SDDC Network Design Decisions 34](#_Toc89178152)

[Table 13 - vCenter Server Compute Resource Specifications 37](#_Toc89178153)

[Table 14 - vCenter Server Storage Resource Specifications 37](#_Toc89178154)

[Table 15 - SDDC vCenter Server Design Decisions 43](#_Toc89178155)

[Table 16 - Goals of the vSphere Networking Design 44](#_Toc89178156)

[Table 17 - SDDC vSphere Network Decisions 49](#_Toc89178157)

[Table 18 - Components of NSX-T Manager 51](#_Toc89178158)

[Table 19 - NSX-T Resource Specification 55](#_Toc89178159)

[Table 20 - Resource Specifications of NSX-T Edge Nodes per Form Factor 56](#_Toc89178160)

[Table 21 - SDDC Design Decisions for SDN 68](#_Toc89178161)

[Table 22 - SDDC Storage Decisions 76](#_Toc89178162)

[Table 23 - SDDC Software Defined Storage Decisions 78](#_Toc89178163)

[Table 24 - Cross Region Workspace ONE Access Logical Components 81](#_Toc89178164)

[Table 25 - SDDC Design Decisions for Workspace ONE Access 83](#_Toc89178165)

[Table 26 - vRealize Suite Lifecycle Manager Logical Components 87](#_Toc89178166)

[Table 27 - Elements and Components in vRealize Suite Lifecycle Manager 88](#_Toc89178167)

[Table 28 - SDDC vRealize Suite Lifecycle Manager Design Decisions 90](#_Toc89178168)

[Table 29 - vRealize Operations Manager Direct Integrations 6](#_Toc89178169)

[Table 30 - SDDC Design Decisions for vRealize Operations Manager 11](#_Toc89178170)

[Table 31 - SDDC Design Decisions for vRealize Log Insight 23](#_Toc89178171)

LIST OF FIGURES

[Figure 1 - VMware Cloud Foundation Logical Architecture 24](#_Toc89178172)

[Figure 2 - Cloud Builder VM Provisioning Overview 25](#_Toc89178173)

[Figure 3 - Technology Components and Versions 25](#_Toc89178174)

[Figure 4 - SDDC Architectures 26](#_Toc89178175)

[Figure 5 - Component Location in a Single Availability Zone 28](#_Toc89178176)

[Figure 6 - Physical Infrastructure in the SDDC 29](#_Toc89178177)

[Figure 7 - Virtual Infrastructure in the SDDC 31](#_Toc89178178)

[Figure 8 - ESXi Logical Design 32](#_Toc89178179)

[Figure 9 - Logical Design of vCenter Server in the management Domain 37](#_Toc89178180)

[Figure 10 - vCenter Server Network Design 39](#_Toc89178181)

[Figure 11 - vSphere Logical Layout for the Management Domain 41](#_Toc89178182)

[Figure 12 - vSphere Distributed Switch Design for Management Domain 48](#_Toc89178183)

[Figure 13 - NSX-T Logical Design for the Management Domain 54](#_Toc89178184)

[Figure 14 - Host to ToR Connectivity 55](#_Toc89178185)

[Figure 15 - NSX-T Edge Network Configuration 58](#_Toc89178186)

[Figure 16 - Dynamic Routing in a Single Availability Zone 60](#_Toc89178187)

[Figure 17 - Dynamic Routing in Multiple Availability Zones 60](#_Toc89178188)

[Figure 18 - Transport Zone Design 63](#_Toc89178189)

[Figure 19 - Virtual Network Segments in SDDC 64](#_Toc89178190)

[Figure 20 - Logical Storage Design 71](#_Toc89178191)

[Figure 21 - vSAN Witness Network Design 77](file:///C:/Users/D7875196/OneDrive%20-%20Virgin%20Media/Projects/VMO2%20Designs/Baguley%20VCF%20Solution%20High%20Level%20Design/HLD/VMO2%20Baguley%20VCF%20Solution%20High%20Level%20Design%20v0.1.docx#_Toc89178192)

[Figure 22 - Security and Compliance Design 80](#_Toc89178193)

[Figure 23- Logical Design of the Cross Region Workspace ONE Access Deployment 81](file:///C:/Users/D7875196/OneDrive%20-%20Virgin%20Media/Projects/VMO2%20Designs/Baguley%20VCF%20Solution%20High%20Level%20Design/HLD/VMO2%20Baguley%20VCF%20Solution%20High%20Level%20Design%20v0.1.docx#_Toc89178194)

[Figure 24 - Architecture of vRealize Suite Lifecycle Manager 86](#_Toc89178195)

[Figure 25 - Operations Management in SDDC 87](#_Toc89178196)

[Figure 26 - Logical Design of vRealize Suite Lifecycle Manager 88](#_Toc89178197)

[Figure 27 - vRealize Operations Manager Architecture 92](#_Toc89178198)

[Figure 28 - Operations Management in the SDDC 0](#_Toc89178199)

[Figure 29 - Logical Design of vRealize Operations Manager 1](#_Toc89178200)

[Figure 30 - Network Design of the vRealize Operations Manager Deployment 4](#_Toc89178201)

[Figure 31 - Architecture of vRealize Log Insight 12](#_Toc89178202)

[Figure 32 - Operations Management in the SDDC 14](#_Toc89178203)

[Figure 33 - Logical Design of vRealize Log Insight 15](#_Toc89178204)

[Figure 34 - Network Design of the vRealize Log Insight Deployment 18](#_Toc89178205)

Document Information

|  |  |
| --- | --- |
|  |  |
| Author(s) | David Dawson |
| Reference |  |
| Publication date | 9th November 2021 |
| Classification | Internal |
| Valid until date | All designs are only valid for 6 months after latest version. |

Table 1 - Document Information

Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Comments |
| 0.1 | 9th Nov 2021 | David Dawson | Initial draft |
| 0.2 | 10th December 2021 | David Dawson | Updated Design |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 2 - Document Control

Document Impact on DCT delivery

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Wintel | Unix | Database | Storage | Cloud | Network | Governance |
|  |  |  |  | X | X |  |

Table 3 - Document Impact on DCT Delivery

Compliance & Governance

|  |  |  |  |
| --- | --- | --- | --- |
| ISO/CAS(T) | SOX | GDPR | PCI |
|  |  |  |  |

Table 4 - Compliance and Governance

Document References

|  |  |  |
| --- | --- | --- |
| Reference | Title | Version |
| REF001 |  |  |
| REF002 |  |  |

Table 5 - Document References

|  |  |
| --- | --- |
| ! | ***Important Note - Security***  All projects MUST engage and comply with Global Security directives.  Evidence of document approval by DCT teams *DOES NOT* imply Global Security approval. The [Global Security Engagement Board](https://sp.upc.biz/depts/GSEB/_layouts/15/start.aspx#/SitePages/Global%20Security%20Engagement%20Board.aspx) (GSEB) must be engaged by the project for advice. |

Executive Summary

Virgin Media O2 have an initiative to build a Software Defined Datacentre (SDDC) based on VMware Virtual Cloud Foundation (VCF) - the SDDC will be utilise a Cisco ACI physical network underlay combined with VMWare NSX-T providing the networking and compute virtualisation.

The SDDC will have its own physical border firewall and its own network links/routing into the various Virgin Media and O2 WAN networks.

Document Purpose

The purpose of this document is to give the Virgin Media O2 designers a High Level view with the appropriate discissions and information required to allow the creation of the Low Level Design. It will outline the Architectural decisions made.

Document Structure

Throughout the document, the following boxes will be used for special remarks.

|  |  |
| --- | --- |
| D | ***Design Decision***  A design decision based on requirements and best practice. |

|  |  |
| --- | --- |
| ! | ***Note***  This header is to make the reader aware of something specific in the document and will give some additional context to the section. |

|  |  |
| --- | --- |
| ! | ***Important Note***  This header is to ensure the reader is fully aware of the point being highlighted. The information provided should be fully considered when understanding the context of the statement. |

# Requirements

The following ore the business and technical requirements set out by both Virgin Media and O2.

## Business Requirements.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Business ID | Category | Type | Requirement Description | Business Rational / Strategy | Design Decision Ref |
| BR.001 | Service | IaaS | The scope is to provided IaaS (Automated infrastructure as a Service) - to include virtual machines, virtualised storage, virtualised network functions. (Software defined data center) | Clear business requirement | The Automation of the solution is provided in a separate design document.  \*\*INSERT DOCUMENT LINK WHEN CC SEND OVER\*\* |
| BR.002 | Service | Internet capable | The solution must be capable of providing both intranet and internet facing services. For example, we could host virginmediao2.co.uk on this cloud | Many use cases will need off-net access - possibly using MFA | The solution provides this in the framework, however additional security sign off may be required for external access. |
| BR.003 | Service | Internal use only | Users of this service are internal only (this may include 3rd party partners working on behalf of VMO2) - ie. there will be no users from other customers directly. The platform will be used to host VMO2 provided services only. | This is not designed to be a product that we resell. This is an internal tool only. | Access to the environments and infrastructure will be via Active Directory accounts and group memberships. |
| BR.004 | Technology | BSS/OSS (not NFV) | This system is fully discrete technically from the Telco Cloud. Where possible, common technology choices will be made to drive potential synergies (both technical and operational) for the future. | NFV use cases are very different. Vmware advise to keep the two use cases discrete. | The new SDDC is a separate environment in terms of the core infrastructure. There may be a requirement to share shared services. |
| BR.005 | Technology | Fully automated | System must be able to configure resources, provision workflows and execute management operations functions in a fully automated manner | There should be no mid-workflow manual steps required to provision resources |  |
| BR.006 | Technology | Multi-component blueprints | System must provide requestable high level services (blueprints) from a service catalogue with automation tools. This should include the ability to create multi-component stacks as a single catalogue item | We should have the ability to template complex deployments (eg. LAMP stacks) | The Automation of the solution is provided in a separate design document.  \*\*INSERT DOCUMENT LINK WHEN CC SEND OVER\*\* |
| BR.007 | Technology | Portal | The system will provide secure access to a portal allowing provisioning of VMO2-managed cloud services from a common single pane of glass, rather than using multiple 3rd party portals, ensuring a common security configuration baseline. | Managed IaaS should be deployed using common tools. We will not manage IaaS that has been provisioned outside the framework - eg. Using public cloud tooling | The Automation of the solution is provided in a separate design document.  \*\*INSERT DOCUMENT LINK WHEN CC SEND OVER\*\* |
| BR.008 | Service | Hybrid deployment | The solution must be capable of provisioning IaaS and CaaS to both private and public clouds (hybrid cloud) | Hybrid cloud is a clear strategic goal |  |
| BR.009 | Technology | Inventory | The solution must maintain an inventory and resource lifecycle for provisioned, VMO2-managed cloud services. | Required for CRuD functionality |  |
| BR.010 | Technology | API capable | The solution should be able to integrate with business processes and systems of record (eg. CMDB) - using open APIs | Required for support functions | The various VMware tools deployed (vROP’s, vRA etc) will be able to provide this but will need to be configured. |
| BR.011 | Service | Availability | The various components of the CMP (ie. provisioning, cost management, monitoring, etc.) should be highly available. RPO and RTO to be defined in tech requirements | Clear business requirement | The solution will be provisioned on two sites offering resiliency and the ability to failover and recover. The exception to this is the vRA infrastructure which is only available in Knowsley. |
| BR.012 | Service | Self-service & tenancy | The solution should provide a web-based IaaS provisioning portal and API layer, supporting multi-tenancy for VM business units to have self-service portals (unmanaged blueprints/ OVAs) | Tenancy is a requirement for the VMB compute cloud project as well as other plans around self-service | The Automation of the solution is provided in a separate design document.  \*\*INSERT DOCUMENT LINK WHEN CC SEND OVER\*\* |
| BR.013 | Service | DBaaS | The solution should be capable of providing Database as a Service (DBaaS) as a future capability. Database technologies available (Oracle, SQL server, MariaDB, etc.) to be defined in technical requirements and may expand during development sprints over time | Most applications require DB functionality. No DB offering severely limits the usefulness of the platform | The solution will be capable of providing DBaaS, however additional hardware and licensing will be required. |
| BR.014 | Service | JV Cloud | The solution must be fully capable and accessible for all the VMO2 business (not just exVM or exO2) | Clear business requirement | The solution will be fully accessible to all VMO2 users via Active Directory authentication. |
| BR.015 | Service | Security | The solution must adhere to current VMO2 security standards. These may vary between clusters (eg. TSR may be applicable to some but not others) | Clear business requirement | Although the current VMO2 security standards for this environment are unknown at this point the solution offers the ability to scale out into additional clusters if required. |
| BR.016 | Technology | Storage | The solution must provide block and file capability (SMB/CIFS/NFS). Object storage should be accessible from applications | Clear business requirement |  |
| BR.017 | Service | Resilience | On premise clusters should be at least n+1 resilient. This is similar in principle to a single availability zone within public clouds. Normal VMware HA will operate within each cluster providing resilience at all levels | Clear business requirement | Each of the clusters will have at least 4x nodes in them. |
| BR.018 | Service | Geo-resilience | The solution should be capable of providing geographic site resilience within the private cloud (ie. should be minimum two VMO2 owned data centres). The vision is that this solution expand to most data centres and there must be future planning for quorum requirements. | Some applications will require multi-site resiliency | The solution will currently span two VMO2 datacenters within the UK. |
| BR.019 | Service | Supportable | The platform itself should be monitored and integrated into standard VMO2 OSS tools for operations and support | Clear business requirement | The platform will provide a monitoring solution within it. The output from these can be integrated into other non-platform solutions. |
| BR.020 | Technology | Backups | The platform must provide a backup service to workloads. The backups must be able to be physically discrete from the original data. As such, whilst COW snapshot technology may be offered for business agility, it cannot be the sole backup method | Clear business requirement | Still Outstanding |
| BR.021 | Service | E2E provisioning | The platform should via an automated process provide users with credentials (if necessary elevated) to access their resources once provisioning is completed. Addition of further users/groups may be a day-2 activity | Clear business requirement |  |
| BR.022 | Service | User authentication | User authentication and authorisation for the CMP tooling (in particular, provisioning) should be linked to users' primary login IDs and therefore integrated with the Joiners/Movers/Leavers (JML) process | Operational/security requirement to avoid movers/leavers having logins to management systems | The solution will be integrated into Active Directory, however the JML process is out of scope of the solution. |

Table 6 - Business Requirements

## Technical Requirements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Technical ID | Category | Type | Requirement Description | Design Decision Comment | Requirement Satisfied |
| TR.001 | Functional | Provisioning and Orchestration | Solution should allow different scenarios of templated solutions based on platform, compute, storage and network configuration. Ie. Beyond the blueprint (Eg. RHEL virtual machine), there should be the ability to choose size (vCPU,RAM), network connectivity etc. | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.002 | Functional | Provisioning and Orchestration | Solution should be able to provision, and complete all automation steps to be operationally ready for on-premise private and public cloud at minimum. This may mean that the solution requires extra automation software beyond VRA8 to be able to complete requests which may be existing tooling. ie. deployed resources should not require manual steps to be performed prior to being "customer ready" | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.003 | Functional | Provisioning and Orchestration | Solution should be capable of providing multi-component catalogue items (eg. LAMP stack + NLBs) | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.004 | Functional | Provisioning and Orchestration | Solution should be accessible from both a web-based interface (management console) and an application programming interfaces (APIs) where appropriate | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.005 | Functional | Provisioning and Orchestration | Solution must be able to integrate with Ansible and PowerShell and any other DevSecOps tooling as required by VMO2 users | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.006 | Functional | Provisioning and Orchestration | IaaS portal should have options to select quantity of desired product (eg. 4x web servers) | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.007 | Functional | Provisioning and Orchestration | Solution should have an IaaS portal to act as a central point to enable self-service | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.008 | Functional | Provisioning and Orchestration | Solution should allow uptime scheduling of deployed resources to enable efficient resource utilisation (eg. Users can Start/stop virtual machines when not in use - for example test environments outside of work hours) | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.009 | Functional | Provisioning and Orchestration | Solution should be able to integrate with other future automation tools. Ie. should have an open API for integration | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.010 | Functional | Provisioning and Orchestration | ESX Hosts within the same cluster will be spread across multiple racks | *SDDC-MGMT-PHY-VMO2DC1-001 - 004* | *Will be satisfied and detailed within the Low Level Design.* |
| TR.011 | Functional | Provisioning and Orchestration | Clusters must be defined to take advantage of LG's License agreements, for example, not mix different operating system workloads on the same cluster | *Each Cluster will need to be licensed accordingly for both Windows and / or Linux.* | *Will be satisfied and detailed within the Low Level Design.* |
| TR.012 | Functional | Provisioning and Orchestration | NSX will be the default Network Load Balance solution within the environment, by exception, projects can use approved 3rd party Load Balancers for Specific to be defined use cases. Application Load Balancing may require specific 3rd Party Load Balancers | *The default Network Load balancers will be enabled as standard within NSX-T.* | *Will be satisfied and detailed within the Low Level Design.* |
| TR.013 | Functional | Provisioning and Orchestration | Compute and Edge NSX Clusters should be deployed separately to break the dependency on scaling requirements | *This can be achieved as long as the budget permits.* | *Will be satisfied and detailed within the Low Level Design.* |
| TR.014 | Functional | Architecture | The solution must use the latest supported release of the VVD product suite. | *The solution will use VCF4.2 and compatible components.* | *Will be satisfied and detailed within the Low Level Design.* |
| TR.015 | Functional | Architecture | Solution must support a minimum of two separate NSX instances per region. One instance is tied to the Management vCenter Server, and the other instance is tied to the Compute vCenter Server | *This will be achieved when the first compute vCenter Server is deployed.* | *Will be satisfied and detailed within the Low Level Design.* |
| TR.016 | Functional | Architecture | Solution should support the applying vSphere Distributed Resource Scheduler (DRS) anti-affinity rules to the NSX components in both stacks | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.017 | Functional | Architecture | One vCenter Server supporting the SDDC management components  One vCenter Server supporting the edge components and compute workloads | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.018 | Functional | Architecture | Build 4 ESXi nodes at each SDDC location for Management Cluster | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.019 | Functional | Audit | The solution must provide or integrate with an audit capability of Security Groups and Policy | *The solution will implement vRealize Log Insight that will capture logs and if required integrate with other security solutions.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.020 | Functional | Capacity | There must be a method to ensure compute resource is capacity managed. For some virtual machines VMO2 would want to ensure no oversubscription i.e. 1vCPU = 1 hyperthreaded CPU core, whereas for others we might want a 3:1 oversubscription ratio due to the low utilization of the VM | *The solution will deploy vRealize Operations Manager that will monitor the solution.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.021 | Functional | Cloud migration, backup and DR | Solution should support the configuration and deployment of applications onto cloud platforms (eg. Tomcat, MariaDB, etc.). Ie. it should be possible to create more advanced catalogue items beyond simple IaaS (IaaS+) which may include commonly used software components such as Apache, httpd or tomcat | *The solution will have connectivity to other private and public clouds and vRA for automation. Deployment of applications will be a deliverable for vRA and not this solution as this solution will be an endpoint.* |  |
| TR.022 | Functional | Cost management and resource optimization | Solution should have a basic cost breakdown for each area requested in the service request |  |  |
| TR.023 | Functional | Feature | The solution should be able to use a mix of private (rfc1918), CGN (rfc 6598) or public “floating IPs” depending on whether the service is internal only or externally facing | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.024 | Functional | Feature | The solution should support IP Address Management (IPAM) solution for NSX management and VM IP address allocation | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.025 | Functional | Feature | All ESX hosts must boot from local storage (Drives or SSD cards) | *Each ESXi server will boot from local storage.* | *SDDC-MGMT-ESXi- VMO2DC1-006 and SDDC-MGMT-ESXi- VMO2DC1-007. Additional details will be within the Low Level Design.* |
| TR.026 | Functional | Feature | For the management cluster NSX instance, Solution must support consumption only by provider staff using the vSphere Web Client and the API | *Access to the Management Cluster and VMware technologies within it will be managed via Active Directory Groups.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.027 | Functional | Feature | Solution should support configuring the Distributed Firewall to limit access to administrative interfaces in the management cluster | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.028 | Functional | Feature | Solution must support connectivity between regions that is capable of routing between each cluster | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.029 | Functional | Feature | Solution must replace the NSX Manager certificate with a certificate signed by a third-party Public Key Infrastructure | *The infrastructure and design will support this, more details will be in the LLD.* | *SDDC-MGMT-SDN- VMO2DC1-078 and SDDC-MGMT-SDN- VMO2DC1-079*  *Will be satisfied and detailed within the Low Level Design* |
| TR.030 | Functional | Feature | The solution should support IPv6 addressing for Workloads | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.031 | Functional | Feature | The solution must support OOB management for all ESXI hosts | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.032 | Functional | Feature | Set up each ESXi host in the management cluster with a minimum of 192 GB RAM | *Each of the ESXi hosts has this capacity by default.* | *SDDC-MGMT-ESXi- VMO2DC1-005, details will be in the Low Level Design.* |
| TR.033 | Functional | Feature | Replace the vCenter Server machine certificate and Platform Services Controller machine certificate with a certificate signed by a 3rd party Public Key Infrastructure | *The infrastructure and design will support this, more details will be in the LLD.* | *SDDC-MGMT-VC- VMO2DC1-038 and SDDC-MGMT-VC- VMO2DC1-039. Will be satisfied and detailed within the Low Level Design* |
| TR.034 | Functional | Feature | Use a SHA-2 or higher algorithm when signing certificates | *The infrastructure and design will support this, more details will be in the LLD.* | *SDDC-MGMT-VC- VMO2DC1-038 and SDDC-MGMT-VC- VMO2DC1-039. Will be satisfied and detailed within the Low Level Design* |
| TR.035 | Functional | Feature | The solution must enable automatic deployment of NSX based micro-segmentation, load balancer and firewall configuration via Infrastructure as Code templates or Self Service | *This will be done as part of the deployment of NSX within both the management and workload Domains.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.036 | Functional | Feature | The solution must allow workloads to automatically be enrolled in to PAM as part of the provisioning process | *Provision will be made with vRA8 to allow the integration, it won’t be part of this design.* | *Satisfied within the vRA8 CC Design* |
| TR.037 | Functional | Feature | The solution must allow workloads to automatically be added to Antivirus monitoring as part of the provisioning process | *Provision will be made with vRA8 to allow the integration, it won’t be part of this design.* | *Satisfied within the vRA8 CC Design* |
| TR.038 | Functional | Identity, security and compliance | Solution must have functionality to make certain catalogue/portfolio items available to certain business units.  This could be used for example to limit access to certain non-generalized catalogue items such as Hadoop, middleware, etc. to users or groups for which they are relevant (Multi-tenancy) | *Provision will be made with vRA8 to allow the integration, it won’t be part of this design.* | *Satisfied within the vRA8 CC Design* |
| TR.039 | Functional | Inventory and classification | Solution must allow the creation of tags to organize and classify resources and to enable FinOPS integration. Mandatory tags include.  1. Cost center | *Provision will be made with vRA8 to allow the integration, it won’t be part of this design.* | *Satisfied within the vRA8 CC Design* |
| TR.040 | Functional | Monitoring | The solution must provide comprehensive infrastructure monitoring, logging and alerting, and integrate with the existing VMO2 SIEM and Monitoring service | *The solution will deploy various monitoring solutions (vROP’s, vRLI, vRNI) and these can integrate with VMO2 solutions.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.041 | Functional | Networking | The solution should support integration with non NSX Firewalls for automation of firewall rules | *This will be done as part of the deployment of NSX within both the management and workload Domains.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.042 | Functional | Networking | The underlay Network should support BGP routing adjacency | *This will be done as part of the deployment of NSX within both the management and workload Domains.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.043 | Functional | Networking | The solution must segment connectivity to underlay network functions using VLANs (EPGs?) | *This will be done as part of the deployment of NSX within both the management and workload Domains.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.044 | Functional | Networking | Support assignment of static IP addresses to all management components in the SDDC infrastructure except for NSX VTEPs which can be DHCP assigned | *This will be done as part of the deployment of NSX within both the management and workload Domains.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.045 | Functional | Networking | Support creation of DNS records for all management nodes to enable forward, reverse, short and FQDN resolution | *This will be done into the systems.local DNS structure* | *Will be satisfied and detailed within the Low Level Design* |
| TR.046 | Functional | Networking | Solution must use a common NTP framework time source for all nodes. NB. This does not necessarily mean the same time server - servers at different strata within the same framework could be valid | *The infrastructure and design will support this, more details will be in the LLD.* | *SDDC-MGMT-ESXi- VMO2DC1-014. Will be satisfied and detailed within the Low Level Design* |
| TR.047 | Functional | Networking | Underlay network must support MTU size to at least 9000 bytes (jumbo frames) on physical switch ports and distributed switch port groups that support the following traffic types.  -  vSAN  -  vMotion  -  VXLAN  -  vSphere Replication  -  NFS | *The infrastructure and design will support this, more details will be in the LLD.* | *SDDC-MGMT-SDN- VMO2DC1-008 and SDDC-MGMT-SDN- VMO2DC1-009. Will be satisfied and detailed within the Low Level Design* |
| TR.048 | Functional | Networking | Solution must support the use of NSX for vSphere to introduce VXLANs for the use of virtual application networks and tenant networks | *This will be done as part of the deployment of NSX within both the management and workload Domains.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.049 | Functional | Networking | Solution should support the deployment of a minimum of two NSX Edge services gateways (ESGs) in an ECMP configuration for North-South routing in both management and edge and compute cluste | *This will be done as part of the deployment of NSX within both the management and workload Domains.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.050 | Functional | Performance | The environment must be capable of achieving high transfer rates. VMO2 Networks needs to achieve near 10Gbps capabilities from the virtual machines to the local physical network equipment as some servers could be involved in processing high bitrate media. For the purpose of testing this excludes contention on network uplinks and assumes the uplinks are not loaded. | *The physical servers will be patched into 25GB network switches.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.051 | Functional | Service request | Solution should have a catalogue of all targeted cloud platforms (ie. private data centres, public clouds) |  |  |
|  | | | | |  |
| TR.052 | Non Functional | Provisioning and orchestration | Guests making up the same application should be able to have anti-affinity rules applied to ensure they are not on the same node of a cluster | *Anti Affinity rules can be created on a case by case basis, but will not be detailed within the design* |  |
| TR.053 | Non Functional | Provisioning and orchestration | Storage should be resilient to SPOFs (ie. RAID) | *All hardware and software will be built with resilience in mind.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.054 | Non Functional | Access Management | The solution must allow user access to the Infrastructure or hosted workloads to be added or revoked on demand via Self Service | *The solution will provide Active Directory groups to mange user access, however the process for this is out od scope of this document.* | *Active Directory groups Will be satisfied and detailed within the Low Level Design* |
| TR.055 | Non Functional | Architecture | The architecture design of the SDDC should minimize hardware requirements as much as possible whilst complying with VVD requirements, including when the SDDC is scaled. | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.056 | Non Functional | Availability | Any component failure must not result in outage greater than N+1. ie. n+2 within a single site is the minimum level of resilience | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.057 | Non Functional | Availability | Upgrades or patching to VMWare components should be non-disruptive to running workloads. Upgrades or patching to Management and provisioning service should be within planned service maintenance windows | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.058 | Non Functional | Availability | The management plane solution must include the ability to quickly rollback problematic patches or upgrades | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.059 | Non Functional | Backup & Restore | The solution must allow a backup or restore of a business data to be initiated on demand via Self Service or Infrastructure as Code |  |  |
| TR.060 | Non Functional | Cloud migration, backup and DR | The IaaS provisioning portal and inventory of deployed systems should have a Recovery Point Objective (RPO) of less than 1 hour and a Recovery Time Objective (RTO) of less than 4 hours |  |  |
| TR.061 | Non Functional | Feature | The solution must provide an approval workflow in the Self Service Portal | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.062 | Non Functional | Feature | The solution must automatically raise pre-approved CRs as part of the provisioning process | *This decision isn’t in scope of this solution.* | *This decision isn’t in scope of this solution.* |
| TR.063 | Non Functional | Feature | The solution must allow workloads to be added automatically to a backup schedule as part of the provisioning process using tagging | *This decision isn’t in scope of this solution.* | *This decision isn’t in scope of this solution.* |
| TR.064 | Non Functional | Feature | The solution must allow workloads to be automatically added to any License Management solution as part of the provisioning process | *This decision isn’t in scope of this solution.* | *This decision isn’t in scope of this solution.* |
| TR.065 | Non Functional | Feature | The solution must allow file shares to be automatically created on SAN as part of the provisioning process | *This decision isn’t in scope of this solution.* | *This decision isn’t in scope of this solution.* |
| TR.066 | Non Functional | Feature | The solution must allow server volumes to be automatically created as part of the provisioning process | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.067 | Non Functional | Feature | The solution must allow server certificates to be automatically deployed as part of the provisioning process | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.068 | Non Functional | Feature | The solution must allow a new version of an OS template to be automatically deployed via 3rd party orchestration tools e.g. Jenkins | *This decision isn’t in scope of this solution.* | *This decision isn’t in scope of this solution.* |
| TR.070 | Non Functional | Feature | The solution must allow a snapshot or clone of a VM to be initiated on demand via Self Service or Infrastructure as Code | *This technical requirement will be address by the vRA8 solution. The design can be found here \*\*\*INSERT LINK\*\*\** | *Satisfied within the vRA8 CC Design* |
| TR.071 | Non Functional | Identity, security and compliance | Solution should contain IAM policies that defines a users permissions, ie. RBAC - some users may need admin rights to modify catalogue items, some users may simply need to provision guests | *The solution will provide Active Directory groups to manage user access, however the process for this is out od scope of this document.* | *Active Directory groups Will be satisfied and detailed within the Low Level Design* |
| TR.072 | Non Functional | Identity, security and compliance | Solution should be able to integrate with existing corporate identity providers (e.g. Active Directory) for solution access and management. Explicitly, the solution should NOT have a discrete IAM solution requiring a separate leavers/joiners process | *The solution will provide Active Directory groups to manage user access, however the process for this is out od scope of this document.* | *Active Directory groups Will be satisfied and detailed within the Low Level Design* |
| TR.073 | Non Functional | Identity, security and compliance | Solution should be managed in accordance of the VMO2 organization policies | *This decision isn’t in scope of this solution, however the design will comply with the VMO2 security policies.* | *This decision isn’t in scope of this solution, however the design will comply with the VMO2 security policies.* |
| TR.074 | Non Functional | Integration | The Management solution must integrate with VMO2's existing foundation services - Active Directory / Authentication, DNS, NTP, CA and DHCP services at the Infrastructure layer | *The solution will integrate with the foundation services, however any additional foundation components will be out of scope of this design and will have their own.* | *The solution will integrate with the foundation services, however any additional foundation components will be out of scope of this design and will have their own.* |
| TR.075 | Non Functional | Inventory and classification | Solution should be able to capture change management CR# via workflows | *This decision isn’t in scope of this solution.* | *This decision isn’t in scope of this solution.* |
| TR.076 | Non Functional | Inventory and classification | Solution should be able to integrate with existing ITSM systems (e.g. Remedy, etc.), such as change management, asset management etc. | *This decision isn’t in scope of this solution.* | *This decision isn’t in scope of this solution.* |
| TR.077 | Non Functional | Migration | SDDC solution must support migration of applications from physical to virtual servers | *The solution will provide this functionality.* | *Will be satisfied and detailed within the Low Level Design.* |
| TR.078 | Non Functional | Security | The solution must align to VMO2 security standards | *This decision isn’t in scope of this solution, however the design will comply with the VMO2 security policies.* | *This decision isn’t in scope of this solution, however the design will comply with the VMO2 security policies.* |
| TR.079 | Non Functional | Security | The solution must align to VMO2 security standards | *This decision isn’t in scope of this solution, however the design will comply with the VMO2 security policies.* | *This decision isn’t in scope of this solution, however the design will comply with the VMO2 security policies.* |
| TR.080 | Non Functional | Service Management | The solution must provide comprehensive performance, capacity and availability management tools and reports, subject to tooling availability | *The solution will deploy various monitoring solutions (vROP’s, vRLI, vRNI) and these can integrate with VMO2 solutions.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.081 | Non Functional | Service request | Solution should be able to provide post provisioning activities such as reboot / change for VMO2 managed services + (CReate, Update, Delete - CRUD) | *The infrastructure and design will support this, more details will be in the LLD.* | *Will be satisfied and detailed within the Low Level Design* |
| TR.082 | Non Functional | Testing | There should be a non-production management plane deployed for the testing of upgrades/patches/etc prior to deployment to production. | *A test / non production Management cluster will be provisioned as part of this solution.* | *Will be satisfied and detailed within the Low Level Design.* |

Table 7 - Technical Requirements

|  |  |
| --- | --- |
| ! | ***Important Note***  The Design Decision made in this high level solution overview are based on industry and VMware best practices. |

# Base vmware Cloud foundation

## VMware Cloud Foundation Overview

VMware Cloud Foundation is an integrated software stack that bundles compute virtualization (VMware vSphere), storage virtualization (VMware vSAN), network virtualization (VMware NSX-T) and cloud management (VMware vRealize Suite) into a single platform that can be deployed on premise as a private cloud or run as a service within the public cloud. Cloud foundation helps to break down the traditional administrative silos in datacenters, merging compute, storage, network provisioning and cloud management to facilitate end to end support for application deployment.

To manage the logical infrastructure in the private cloud, Cloud Foundation augments the VMware virtualization and management components with SDDC Manager. SDDC Manager automates the bring up, configuration, provisioning, and lifecycle management of the entire SDDC stack. From this interface, the IT administrator can provision new private cloud resources, monitor changes to the logical infrastructure, and manage life cycle and other operation activities. Cloud Foundation enables datacenter cloud administrators to provision an application environment in a rapid, repeatable way verses the traditional manual process.



Figure 1 - VMware Cloud Foundation Logical Architecture

## VMware Cloud Foundation Software Installation

VMware Cloud Foundation is capable of automatically deploying and configuring all the building blocks of the SDDC.

VMware Cloud Builder VM

The cloud builder VM performs all of the initial deployment steps from deploying the baseline image and then deploying the various software components. The cloud builder VM has to be attached to the management vLAN on which both the ESXi host management network is connected as well as the various software components such as SDDC Manager and vCenter Server. Once the initial deployment of VMware vCloud Foundation has been completed the Cloud Builder VM can be removed. The following figure illustrates the process of using Cloud Builder VM to deploy VMware Cloud Foundation.



Figure 2 - Cloud Builder VM Provisioning Overview

Technology Components

Within the solution the following components and version will be deployed.

|  |  |
| --- | --- |
| Technology Components | Versions |
| vRealize Operations Manager | 8.2.x |
| vRealize Automation | 8.2.x |
| VCF Base Platform Deployment | 4.2.x |
| NSX-T | 3.1.x |
| VMware Cloud Director | 10.1.x |
| vRealize Lifecycle Manager | 8.2 |
| VMware Cloud Director Availability | 4.1.x |
| VCF vRealize Log Insight | 8.2.x |
| VCF vRealize Operations Manager | 8.2.x |
| VCF VI Workload Domain Deployment | 4.2.x |
| VMware SDDC Manager | 4.2 |
| VMware vSAN | 7.0.x |
| VMware Cloud Builder VM | 4.2 |
| VMware vCenter Server | 7.0 |
| VMware ESX | 7.0 |
| VMWare HCX |  |
| VMware Network Insight | 8.2.x |

Figure 3 - Technology Components and Versions

|  |  |
| --- | --- |
| D | ***Design Decision***  Are we deploying VMware HCX as part of the deployment, it is included in VCF Enterprise. |

## SDDC Architectures

You start SDDC deployment from the management domain and extend it with more virtual infrastructure and solutions. You select a deployment architecture according to the number of tenant workloads you plan to support and the available virtual infrastructure.



Figure 4 - SDDC Architectures

Standard SDDC Architecture

In a standard deployment, the management domain consists of workloads supporting the virtual infrastructure, cloud operations, cloud automation, business continuity, and security and compliance components for the SDDC. You allocate separate workload domains to tenant or containerized workloads. Each workload domain is managed by a separate vCenter Server instance and a dedicated or shared NSX-T Manager cluster for scalability. The workload domain construct also has autonomous licensing and life cycle management. The vCenter Server and NSX-T Manager components for these workload domains are running in the management domain too.

Consolidated SDDC Architecture

In a consolidated deployment, the management domain runs both the SDDC management workloads and tenant workloads.

|  |  |
| --- | --- |
| D | ***Design Decision***  Within the VMO2DC1 deployment we will be using the Standard SDDC Architecture model. |

Management Domain Architecture

The management domain runs all management components of the SDDC for both the management domain and workload domains, except for workload NSX-T Edge nodes. You start with an initial management domain configuration which is extended with each workload domain deployment. For extending the capabilities of the SDDC, you can also deploy additional solutions in the management domain, for example, solutions for cloud operations and cloud automation.

Workload Domains

The SDDC functionality is distributed across multiple workload domains and vSphere clusters. Each workload domain is a logical abstraction of private cloud capacity and consists of one or more clusters. Each cluster can exist vertically in a single rack or be spanned horizontally across multiple racks.

SDDC Availability Zones and Regions

The SDDC design consists of one region that includes at least one management domain but can also include one or more workload domains. Clusters within a region can use two availability zones.

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 design will use a single region, with the option to use one or two availability zones in that Region. |

Additional design decisions for Availability and Zones.

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-PHY-VMO2DC1-001 | In Region VMO2DC1, that is Region A, deploy one or two availability zones to support all SDDC management components and their SLAs. | VCF |
| SDDC-MGMT-PHY-VMO2DC1-002 | Use two separate power feeds for each rack. | VCF |
| SDDC-MGMT-PHY- VMO2DC1-003 | Mount the compute resources (minimum of 4 ESXi hosts) for the first cluster in the management domain together in one rack. | VCF |
| SDDC-MGMT-PHY- VMO2DC1-004 | When using two availability zone, in each availability zone, mount the compute resources (minimum of 4 ESXi hosts) for the first cluster in the management domain together in one rack. | VCF |

Table 8 – SDDC Availability and Zone Design Decisions

Component Location in a single Availability Zone

|  |  |
| --- | --- |
|  |  |

Figure 5 - Component Location in a Single Availability Zone

## Physical Infrastructure Design

The physical infrastructure design includes deciding on the configuration of availability zones and regions, the cluster layout in data center racks.



Figure 6 - Physical Infrastructure in the SDDC

Availability Zones and Regions for the Management Domain

Availability zones and regions have different purposes. Availability zones protect against failures of individual hosts. You can consider regions to place workloads closer to your customers, comply with data privacy laws and restrictions, and support disaster recovery solutions for the entire SDDC.

Availability Zones

An availability zone is the fault domain of the SDDC. Multiple availability zones can provide continuous availability of an SDDC, minimize down time of services and improve SLAs.

|  |  |
| --- | --- |
| Availability Zone Characteristic | Description |
| Outage prevention | You avoid outages and improve SLAs. An outage that is caused by external factors, such as power supply, cooling, and physical integrity, affects only one zone. These factors do not cause outage in other zones except in the case of major disasters. |
| Reliability | Each availability zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Each zone should have independent power, cooling, network, and security. Do not share common points of failures in a physical data center, like generators and cooling equipment, across availability zones. Additionally, these zones should be physically separate so that even uncommon disasters affect only one zone.  Availability zones are either two distinct data centers in a metro distance, or two safety or fire  sectors (data halls) in the same large-scale data center. |
| Distance between zones | Multiple availability zones belong to a single region. The physical distance between availability zones is short enough to offer low, single-digit latency (less than 5 ms) and large bandwidth (10 Gbps or greater) between the zones.  You can operate workloads across multiple availability zones in the same region as if they were part of a single virtual data center. This architecture supports high availability that is suitable for mission critical applications. If the distance between two locations of equipment becomes too large, these locations can no longer function as two availability zones in the same region and  must be designed as separate regions. |

Table 9 - Availability Zone Characteristics

Regions

Regions provide disaster recovery across different SDDC instances or a location that is closer to your customers. Each region is a separate SDDC instance. The regions have a similar physical layer and virtual infrastructure designs but different naming.

Regions are geographically separate, but latency between them must be 150 ms or lower.

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 design will use a single region for SDDC Management and one availability zone. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-PHY-VMO2DC1-005 | In Region A, deploy one availability zone to support all SDDC management components and their SLAs. | VCF |

Table 10 - Physical Availability and Zone Design Decisions

## Virtual Infrastructure Design

The virtual infrastructure design includes the software components that make up the virtual infrastructure layer for providing software-defined storage, networking, and compute.

These components include the software products that provide the virtualization platform hypervisor, virtualization management, storage virtualization, and network virtualization. The VMware products in this layer are vSphere, vSAN, and NSX-T Data Center.



Figure 7 - Virtual Infrastructure in the SDDC

ESXi Design for the Management Domain

The compute layer of the virtual infrastructure layer in the SDDC is implemented by ESXi, a bare- metal hypervisor that you install directly onto your physical server. With direct access and control on underlying resources, ESXi logically partitions hardware to consolidate applications and cut costs.

Logical Design for ESXi for the Management Domain

In the logical design for ESXi, you determine the high-level integration of the ESXi hosts with the other components of the SDDC for providing virtual infrastructure to the SDDC management components.

To provide the resources required to run the management components of the SDDC according to the design objectives, each ESXi host consists of the following elements:

|  |  |
| --- | --- |
| * CPU * Memory * Storage * Out of Band Management Interface * Network Interfaces |  |

Figure 8 - ESXi Logical Design

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 design will use the following design decisions. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-ESXi-VMO2DC1-001 | Use vSAN ReadyNodes with vSAN storage for each ESXi host in the management domain. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-002 | Allocate hosts with uniform configuration across the first cluster of the management domain. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-003 | Install each ESXi host in the first, four-node, cluster of the management domain with a minimum of 30 physical CPU cores. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-004 | When sizing CPU, do not consider multithreading technology and associated performance gains. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-005 | Install each ESXi host in the first, four-node, cluster of the management domain with a minimum of 256 GB RAM. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-006 | Install and configure all ESXi hosts in the first cluster of the management domain to boot using a 32-GB device or greater. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-007 | Use the default configuration for the scratch partition on all ESXi hosts in the first cluster of the management domain. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-008 | For workloads running in the first cluster in the management domain, save the virtual machine swap file at the default location | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-009 | Use SDDC Manager to perform the life cycle management of ESXi hosts in the management domain. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-010 | Place the ESXi hosts in the first cluster of the management domain on the VLAN-backed management network segment. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-011 | Allocate statically assigned IP addresses and host names across all ESXi hosts in the first cluster of the management domain. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-012 | Configure forward and reverse DNS records for each ESXi host in the first cluster of the management domain, assigning the records to the child domain on the region. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-013 | Configure time synchronization by using an internal NTP time source across all ESXi hosts in the management domain for the region. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-014 | Set the NTP service policy to Start and stop with host across all ESXi hosts in the first cluster of the management domain. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-015 | Configure the SSH service policy to Start and stop with host across all ESXi hosts in the management domain. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-016 | Set the advanced setting UserVars.SuppressShellWarning to 1 across all ESXi hosts in the management domain. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-017 | Join each ESXi host in the management domain to the Active Directory domain of the region in which the ESXi host resides. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-018 | Change the default ESX Admins group to an Active Directory group ug-esxi-admins. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-019 | Add ESXi administrators to the ug-esxi-admins group in Active Directory following standard access procedures. | VCF |
| SDDC-MGMT-ESXi- VMO2DC1-020 | Configure a policy for ESXi host password and account lockout according to the security best practices or industry standards with which your organization maintains compliance. | VCF |

Table 11 - SDDC ESXi Design Decisions

## Network Design for ESXi for the Management Domain

In the network design for the ESXi hosts in the management domain, you place the hosts on a VLAN for traffic segmentation. You decide on the IP addressing scheme and name resolution for connectivity to the SDDC management components and maintenance of the hosts.

Network Segments

To perform system functions in a virtual infrastructure in addition to providing network connectivity to the virtual machines, the ESXi hosts in the management domain are connected to several dedicated networks

Management Network

Carries traffic for management of the ESXi hosts and communication to and from vCenter Server. In addition, on this network, the hosts exchange heartbeat messages when vSphere HA is enabled in non-vSAN clusters. When using multiple availability zones, you use this network for vSAN witness traffic

vSphere vMotion Network

Carries traffic for relocating virtual machines between ESXi hosts with zero downtime.

vSAN Network

Carries the communication between ESXi hosts in the cluster to implement a vSAN shared storage. In addition, on this network, the hosts exchange heartbeat messages when vSphere HA is enabled in vSAN clusters.

Underlay Transport Network

Carries overlay traffic between the management components in the management domain and traffic for software-defined network services such as load balancing and dynamic routing (East-West traffic).

Uplink Networks

Carry traffic for communication between software-defined overlay networks and the external network (North-South traffic). In addition, on these networks, routing control packets are exchanged to establish required routing adjacencies and peering’s.

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 design will use the following design decisions. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-NET-VMO2DC1-001 | Use vSphere Distributed Switches. | VCF |
| SDDC-MGMT-NET- VMO2DC1-002 | Use a single vSphere Distributed Switch per cluster. | VCF |
| SDDC-MGMT-NET- VMO2DC1-003 | Configure the MTU size of the vSphere Distributed Switch to 9000 for jumbo frames | VCF |
| SDDC-MGMT-NET- VMO2DC1-004 | Use ephemeral port binding for the management port group. | VCF |
| SDDC-MGMT-NET- VMO2DC1-005 | Use static port binding for all non-management port groups. | VCF |
| SDDC-MGMT-NET- VMO2DC1-006 | Use the Route based on physical NIC load teaming algorithm for the management port group. | VCF |
| SDDC-MGMT-NET- VMO2DC1-007 | Use the Route based on physical NIC load teaming algorithm for the vMotion Port Group. | VCF |
| SDDC-MGMT-NET- VMO2DC1-008 | Use the vMotion TCP/IP stack for vSphere vMotion traffic. | VCF |
| SDDC-MGMT-NET- VMO2DC1-009 | Enable Network I/O Control on vSphere distributed switch of the management domain cluster | VCF |
| SDDC-MGMT-NET- VMO2DC1-010 | Set the share value for management traffic to Normal. | VCF |
| SDDC-MGMT-NET- VMO2DC1-011 | Set the share value for vSphere vMotion traffic to Low. | VCF |
| SDDC-MGMT-NET- VMO2DC1-012 | Set the share value for virtual machines to High. | VCF |
| SDDC-MGMT-NET- VMO2DC1-013 | Set the share value for vSAN traffic to High. | VCF |
| SDDC-MGMT-NET- VMO2DC1-014 | Set the share value for vSphere Fault Tolerance to Low. | VCF |

Table 12 - SDDC Network Design Decisions

## vCenter Server Design for the Management Domain

The vCenter Server design includes determining the number of vCenter Server instances in the management domain, their size, networking configuration, cluster layout, redundancy, and security configuration.

By using vCenter Server, you manage your vSphere infrastructure from a centralized location. It acts as a central administration point for ESXi hosts and their respective virtual machines.

Implemented within the same appliance is the Platform Services Controller which provides a set of infrastructure services including vCenter Single Sign-On, License service, Lookup Service, and VMware Certificate Authority (VMCA).

Logical Design for vCenter Server for the Management Domain

For the management domain in each region, you deploy a vCenter Server appliance that manages the ESXi hosts that are running the management components of the SDDC and supports integration with other solutions for monitoring and management of the virtual infrastructure.

A workload domain, including the management domain, consists of one vCenter Server instance with an embedded Platform Services Controller.

vCenter Server is deployed as a preconfigured virtual appliance that is running the VMware Photon™ operating system. vCenter Server is required for some advanced vSphere features, such as vSphere High Availability (vSphere HA), vSphere Fault Tolerance, vSphere Distributed Resource Scheduler (vSphere DRS), vSphere vMotion, and vSphere Storage vMotion.



Figure 9 - Logical Design of vCenter Server in the management Domain

Deployment Specification of vCenter Server for the Management Domain

You determine the size of the compute resources, high availability implementation, and patching and upgrade support for the management domain vCenter Server according to the design objectives and aggregated requirements of the management components of the SDDC.

The number of vCenter Server instances in your SDDC is determined by the number of workload domains. Each workload domain has a single vCenter Server instance. You determine the amount of compute and storage resources for the vCenter Server instance according to the scale of the environment, the plans for deployment of virtual infrastructure workload domains, and the requirements for isolation of management workloads from tenant workloads.

vCenter Server Sizing Compute and Storage Resources

When you deploy the vCenter Server appliance, you select to deploy an appliance that is suitable for the size of your environment. The option that you select determines the number of CPUs and the amount of memory for the appliance.

|  |  |  |  |
| --- | --- | --- | --- |
| vCenter Server Appliance Size | Management Capacity | Number of vCPU’s | Memory |
| X-Large environment | Up to 2,000 hosts or 35,000 virtual machines | 24 | 56 GB |
| Large environment | Up to 1,000 hosts or 10,000 virtual machines | 16 | 37 GB |
| Medium environment | Up to 400 hosts or 4,000 virtual machines | 8 | 28 GB |
| Small environment | Up to 100 hosts or 1,000 virtual machines | 4 | 19 GB |
| Tiny environment | Up to 10 hosts or 100 virtual machines | 2 | 12 GB |

Table 13 - vCenter Server Compute Resource Specifications

When you deploy the vCenter Server appliance, the ESXi host or cluster on which you deploy the appliance must meet minimum storage requirements. You determine the required storage not only according to the size of the environment and the storage size, but also according to the disk provisioning mode.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appliance Size | Management Capacity | Default Storage Size | Large Storage Size | X-Large Storage Size |
| X-Large environment | Up to 2,000 hosts or 35,000 virtual machines | 1805 GB | 1905 GB | 3665 GB |
| Large environment | Up to 1,000 hosts or 10,000 virtual machines | 1065 GB | 1765 GB | 3525 GB |
| Medium environment | Up to 400 hosts or 4,000 virtual machines | 700 GB | 1700 GB | 3460 GB |
| Small environment | Up to 100 hosts or 1,000 virtual machines | 480 GB | 1535 GB | 3295 GB |
| Tiny environment | Up to 10 hosts or 100 virtual machines | 415 GB | 1490 GB | 3245 GB |

Table 14 - vCenter Server Storage Resource Specifications

Enhanced Lined Mode Design for the Management Domain

By using Enhanced Linked Mode of vCenter Server, you can log in to all vCenter Server instances across the SDDC that are joined to the same vCenter Single Sign-on domain and access their inventories.

You can join up to 15 vCenter Server instances in to a single vCenter Single Sign-On domain.

Life Cycle Management Design of vCenter Server for the management Domain

You decide on the life cycle management of the vCenter Server appliance according to the amount of time and effort to perform a deployment, upgrade, or patch operation. You also consider the impact such an operation has on the management solutions that are connected to the management domain vCenter Server.

Life cycle management of vCenter Server includes the process of performing patch updates or upgrades to the vCenter Server appliance. In a typical vSphere environment, you perform life cycle management manually. When you implement a solution by using VMware Cloud Foundation, you use SDDC Manager for life cycle management where other management components are included as part of the life cycle management process.

Network Design for vCenter Server for the Management Domain

In the network design for the management domain vCenter Server, you place vCenter Server on a VLAN for traffic segmentation and decide on the IP addressing scheme and name resolution for optimal support for the SDDC management components and host management.



Figure 10 - vCenter Server Network Design

IP Addressing

You can assign the IP address of the management domain vCenter Server by using DHCP or statically according to the network configuration in your environment.

Name Resolution

vCenter Server systems must be connected to the following components:

* Systems running vCenter Server add-on modules
* Each ESXi host

Time Synchronization

Time synchronization provided by the Network Time Protocol (NTP) is important to ensure that all components within the SDDC are synchronized to the same time source.

vSphere Cluster Design for the Management Domain

The cluster design must consider the characteristics of the management workloads that the cluster handles in the management domain.

When you design the cluster layout in vSphere, consider the following guidelines:

* Use fewer, larger ESXi hosts, or more, smaller ESXi hosts.
* A scale-up cluster has fewer, larger ESXi hosts.
* A scale-out cluster has more, smaller ESXi hosts.
* Compare the capital costs of purchasing fewer, larger ESXi hosts with the costs of purchasing more, smaller ESXi hosts. Costs vary between vendors and models.
* Evaluate the operational costs for managing a few ESXi hosts with the costs of managing more ESXi hosts.
* Consider the purpose of the cluster.
* Consider the total number of ESXi hosts and cluster limits.



Figure 11 - vSphere Logical Layout for the Management Domain

vSphere HA Design for the Management Domain

The vSphere HA configuration protects the virtual machines of the management components of the SDDC whose operation is critical for the operation of your environment. You consider the varying and sometimes significant CPU or memory reservations for the management virtual machines and the requirements of vSAN.

vSphere DRS Design for the Management Domain

vSphere Distributed Resource Scheduling (vSphere DRS) provides load balancing in a cluster by migrating workloads from heavily loaded ESXi hosts to ESXi hosts with more available resources in the cluster. vSphere DRS supports manual and automatic modes.

vSphere EVC Design for the management Domain

If you enable vSphere Enhanced vMotion Compatibility (EVC) in the management domain, the virtual machines of the SDDC management components can be migrated between ESXi hosts containing older CPUs. You can use EVC for a rolling upgrade of all hardware with zero downtime.

vSphere HA Design for the Management Domain

The vSphere HA configuration protects the virtual machines of the management components of the SDDC whose operation is critical for the operation of your environment. You consider the varying and sometimes significant CPU or memory reservations for the management virtual machines and the requirements of vSAN.

If a ESXi host failure occurs, vSphere HA restarts virtual machines on other hosts in the cluster. A primary ESXi host communicates with the management domain vCenter Server and monitors the virtual machines and secondary ESXi hosts in the cluster. vSphere HA uses admission control to ensure that sufficient resources are reserved for virtual machine recovery when a host fails.

You configure several vSphere HA features to provide high availability for the management components of the SDDC.

Information Security and Access Control for vCenter Server for the Management Domain

You design authentication access, controls, and certificate management for the management domain vCenter Server according to industry standards and the requirements of your organization.

Identity Management

Users can log in to vCenter Server only if they are in a domain that was added as a vCenter Single Sign-On identity source. vCenter Single Sign-On administrator users can add identity sources or change the settings for identity sources that they added. An identity source can be a native Active Directory (Integrated Windows Authentication) domain or an OpenLDAP directory service. For backward compatibility, Active Directory as an LDAP server is also available.

Password Management and Account Lockout Behavior

vCenter Server enforces password requirements for access to the vCenter Server Management Interface. By default, you must include at least six characters, which should not be any of your previous five passwords. Account locking is supported for access to the vCenter Server Management Interface. By default passwords are set to expire after 90 days

Certificate management

Access to all vCenter Server interfaces must use a Secure Socket Layer (SSL) connection. By default, vCenter Server uses a certificate for the appliance which is signed by the VMware Certificate Authority (VMCA). To provide secure access to the vCenter Server appliance, replace the default certificate with a CA-signed certificate.

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 vCenter Server design will use the following design decisions. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-VC-VMO2DC1-001 | Deploy a dedicated vCenter Server instance in the first availability zone of the region for the management domain. | VCF |
| SDDC-MGMT-VC- VMO2DC1-002 | When using two availability zones in Region A, add the vCenter Server appliance to the virtual machine group for Availability Zone 1. | VCF |
| SDDC-MGMT-VC- VMO2DC1-003 | Deploy an appliance for the management domain vCenter Server of a small deployment size or larger. | VCF |
| SDDC-MGMT-VC- VMO2DC1-004 | Deploy the appliance of the management domain vCenter Server with the default storage size. | VCF |
| SDDC-MGMT-VC- VMO2DC1-005 | Join all vCenter Server instances to a single vCenter Single Sign-On domain | VCF |
| SDDC-MGMT-VC- VMO2DC1-006 | Create a ring topology for the Single Sign-On domain running in the vCenter Server instances. | VCF |
| SDDC-MGMT-VC- VMO2DC1-007 | Protect the workload domain vCenter Server appliance by using vSphere HA | VCF |
| SDDC-MGMT-VC- VMO2DC1-008 | In vSphere HA, set the restart priority policy for the vCenter Server appliance to high. | VCF |
| SDDC-MGMT-VC- VMO2DC1-009 | Use SDDC Manager to perform the life cycle management of the appliance for the management domain vCenter Server. | VCF |
| SDDC-MGMT-VC- VMO2DC1-010 | Place the appliance of the management domain vCenter Server on the management VLAN network segment of the region. | VCF |
| SDDC-MGMT-VC- VMO2DC1-011 | Allocate a statically assigned IP address and host name to the appliance of the management domain vCenter Server. | VCF |
| SDDC-MGMT-VC- VMO2DC1-012 | Configure forward and reverse DNS records for the appliance of the management domain vCenter Server, assigning the record to the child domain for the region. | VCF |
| SDDC-MGMT-VC- VMO2DC1-013 | Configure time synchronization by using an internal NTP time for the appliance of the management domain vCenter Server. | VCF |
| SDDC-MGMT-VC- VMO2DC1-014 | Create a cluster in the management domain for the initial set of ESXi hosts. | VCF |
| SDDC-MGMT-VC- VMO2DC1-015 | In Region VMO2DC1, create the first cluster in the management domain with this configuration:  - A minimum of 4 ESXi hosts for a single availability zone  - A minimum of 8 ESXi hosts for two availability zones, that is, minimum of 4 ESXi hosts in each availability zone. | VCF |
| SDDC-MGMT-VC- VMO2DC1-016 | Use vSphere HA to protect all virtual machines against failures. | VCF |
| SDDC-MGMT-VC- VMO2DC1-017 | Set host isolation to Power Off in vSphere HA. | VCF |
| SDDC-MGMT-VC- VMO2DC1-018 | When using a single availability zone, configure admission control for 1 ESXi host failure and percentage- based failover capacity. | VCF |
| SDDC-MGMT-VC- VMO2DC1-019 | When using two availability zones, configure admission control for percentage-based failover based on half of the ESXi hosts in the cluster. | VCF |
| SDDC-MGMT-VC- VMO2DC1-020 | When using a single availability zone, set the isolation address for the cluster to the gateway IP address for the vSAN network. | VCF |
| SDDC-MGMT-VC- VMO2DC1-021 | When using two availability zones, set two isolation addresses - one address for the vSAN network gateway in each availability zone. | VCF |
| SDDC-MGMT-VC- VMO2DC1-022 | Set the advanced cluster setting das.usedefaultisolationaddress to false | VCF |
| SDDC-MGMT-VC- VMO2DC1-023 | Enable VM Monitoring for each cluster. | VCF |
| SDDC-MGMT-VC- VMO2DC1-024 | Enable vSphere DRS (Distributed Resource Scheduling) on all clusters, using the default fully automated mode (medium) | VCF |
| SDDC-MGMT-VC- VMO2DC1-025 | Create virtual machine groups for use in startup rules in the first cluster in the management domain. | VCF |
| SDDC-MGMT-VC- VMO2DC1-026 | Create virtual machine rules to set the startup order of the SDDC management components. | VCF |
| SDDC-MGMT-VC- VMO2DC1-027 | When using two availability zones, create a host group and add the ESXi hosts in Availability Zone 1 in Region A to it. | VCF |
| SDDC-MGMT-VC- VMO2DC1-028 | When using two availability zones, create a host group and add the ESXi hosts in Availability Zone 2 in Region A to it. | VCF |
| SDDC-MGMT-VC- VMO2DC1-029 | When using two availability zones, create a virtual machine group and add the virtual machines in Availability Zone 1 in Region A to it. | VCF |
| SDDC-MGMT-VC- VMO2DC1-030 | When using two availability zones, create a virtual machine group and add the virtual machines in Availability Zone 2 in Region A to it. | VCF |
| SDDC-MGMT-VC- VMO2DC1-031 | When using two availability zones, create a should-run VM-Host affinity rule to run the group of virtual machines in Availability Zone 1 on the group of hosts in the same zone. | VCF |
| SDDC-MGMT-VC- VMO2DC1-032 | When using two availability zones, create a should-run VM-Host affinity rule to run the group of virtual machines in Availability Zone 2 on the group of hosts in the same zone. | VCF |
| SDDC-MGMT-VC- VMO2DC1-033 | Enable Enhanced vMotion Compatibility (EVC) on all clusters in the management domain. | VCF |
| SDDC-MGMT-VC- VMO2DC1-034 | Set the cluster EVC mode to the highest available baseline that is supported for the lowest CPU architecture on the hosts in the cluster. | VCF |
| SDDC-MGMT-VC- VMO2DC1-035 | Join the management domain vCenter Server to the Active Directory domain for the region that vCenter Server resides in | VCF |
| SDDC-MGMT-VC- VMO2DC1-036 | Assign global permissions to the vCenter Server inventory to an Active Directory group, such as ug-vc-admin, by using the Administrator role | VCF |
| SDDC-MGMT-VC- VMO2DC1-037 | Configure a password and account lockout policy for the appliance of the management domain vCenter Server according to the industry standard for security and compliance of your organization. | VCF |
| SDDC-MGMT-VC- VMO2DC1-038 | Replace the default VMCA- signed certificate of the appliance of the management domain vCenter Server with a certificate that is signed by a certificate authority. | VCF |
| SDDC-MGMT-VC- VMO2DC1-039 | Use a SHA-2 algorithm or stronger for signed certificates. | VCF |

Table 15 - SDDC vCenter Server Design Decisions

## vSphere Networking Design for the Management Domain

The network design prevents unauthorized access and provides timely access to business data. This design uses vSphere Distributed Switch and VMware NSX-T Data Center for virtual networking.

Virtual Network Design Guidelines

|  |  |
| --- | --- |
| Design Goals | Description |
| Meet diverse needs | The network must meet the diverse needs of many different entities in an organization. These entities include applications, services, storage, administrators, and users. |
| Reduce costs | Reducing costs is one of the simpler goals to achieve in the vSphere infrastructure. Server consolidation alone reduces network costs by reducing the number of required network ports and NICs, but a more efficient network design is desirable. For example, configuring two 25-GbE NICs might be more cost effective than configuring four 10-GbE NICs. |
| Improve performance | You can achieve performance improvement and decrease the time that is required to perform maintenance by providing sufficient bandwidth, which reduces contention and latency. |
| Improve availability | A well-designed network improves availability, usually by providing network redundancy. |
| Support security | A well-designed network supports an acceptable level of security through controlled access and isolation, where required. |
| Enhance infrastructure functionality | You can configure the network to support vSphere features such as vSphere vMotion, vSphere High Availability, and vSphere Fault Tolerance. |

Table 16 - Goals of the vSphere Networking Design

Follow networking best practices throughout the management environment.

* Separate network services from one another to achieve greater security and better performance.
* Use Network I/O Control and traffic shaping to guarantee bandwidth to critical virtual machines. During network contention, these critical virtual machines will receive a higher percentage of the bandwidth.
* Separate network services on a single vSphere Distributed Switch by attaching them to port groups with different VLAN IDs.
* Keep vSphere vMotion traffic on a separate network.

When a migration using vSphere vMotion occurs, the contents of the memory of the guest operating system is transmitted over the network. You can place vSphere vMotion on a separate network by using a dedicated vSphere vMotion VLAN.

* When using pass-through devices with Linux kernel version 2.6.20 or an earlier guest OS, avoid MSI and MSI-X modes. These modes have significant performance impact.
* For best performance, use VMXNET3 virtual machine NICs.
* Ensure that physical network adapters that are connected to the same vSphere Standard Switch or vSphere Distributed Switch, are also connected to the same physical network.

Network Segmentation and vLAN’s

Separating different types of traffic is required to reduce contention and latency, and for access security.

High latency on any network can negatively affect performance. Some components are more sensitive to high latency than others. For example, reducing latency is important on the IP storage and the vSphere Fault Tolerance logging network because latency on these networks can negatively affect the performance of multiple virtual machines. According to the application or service, high latency on specific virtual machine networks can also negatively affect performance.

Virtual Networks

The number of networks or VLANs that are required depending on the type of traffic.

* vSphere system traffic
* Management
* vSphere vMotion
* vSAN
* NFS
* TEP
* Traffic that supports the services and applications in the organization
* NSX-T Edge uplinks

Virtual Switch Type Design for the management Domain

Virtual switches simplify the configuration process by providing a single pane of glass for performing virtual network management tasks.

vSphere supports two types of virtual switches:

* vSphere Standard Switch
* vSphere Distributed Switch

A distributed switch offers several enhancements over a standard switch such as centralized control plane and support for traffic monitoring features.

vSphere Distributed Switch Design for the Management Domain

The first cluster in the management domain uses a single vSphere Distributed Switch with two physical network cards whose design includes traffic types on the switch, the number of required NICs, and MTU configuration.

VMware Validated Design also supports up to three distributed switches and up to six physical network cards per host.

Distributed Port Group and VMKernel Adapter Design for the Management Domain

A distributed port group specifies port configuration options for each member port on a vSphere Distributed Switch. Distributed port groups define how a connection is made to a network. vSphere Distributed Switch introduces two abstractions that you use to create consistent networking configuration for physical NICs, virtual machines, and VMkernel traffic.

Uplink Port Group

An uplink port group or dvuplink port group is defined during the creation of the distributed switch and can have one or more uplinks. An uplink is a template that you use to configure physical connections of hosts as well as failover and load balancing policies. You map physical NICs of hosts to uplinks on the distributed switch. You set failover and load balancing policies over uplinks and the policies are automatically propagated to the host proxy switches, or the data plane.

Distributed Port Group

Distributed port groups provide network connectivity to virtual machines and accommodate VMkernel traffic. You identify each distributed port group by using a network label, which must be unique to the current data center. You configure NIC teaming, failover, load balancing, VLAN, security, traffic shaping , and other policies on distributed port groups. As with uplink port groups, the configuration that you set on distributed port groups on vCenter Server (the management plane) is automatically propagated to all hosts on the distributed switch through their host proxy switches (the data plane).



Figure 12 - vSphere Distributed Switch Design for Management Domain

NIC Teaming

For a predictable level of performance, use multiple network adapters in one of the following configurations.

* An active-passive configuration that uses explicit failover when connected to two separate switches.
* An active-active configuration in which two or more physical NICs in the server are assigned the active role.

vMotion TCP/IP Stack Design for the Management Domain

Use the vMotion TCP/IP stack to isolate traffic for vSphere vMotion and to assign a dedicated default gateway for vSphere vMotion traffic.

By using a separate TCP/IP stack, you can manage vSphere vMotion and cold migration traffic according to the topology of the network.

* Route the traffic for the migration of virtual machines that are powered on or powered off by using a default gateway that is different from the gateway assigned to the default stack on the ESXi host.
* Assign a separate set of buffers and sockets.
* Avoid routing table conflicts that might otherwise appear when many features are using a common TCP/IP stack.
* Isolate traffic to improve security

vSphere Network I/O Control Design for the Management Domain

You can use vSphere Network I/O Control to allocate network bandwidth to management applications and to resolve situations where several types of traffic compete for common resources.

When Network I/O Control is enabled, the distributed switch allocates bandwidth for the traffic that is related to the main vSphere features.

* Fault tolerance traffic
* iSCSI traffic
* vSphere vMotion traffic
* Management traffic
* VMware vSphere Replication traffic
* NFS traffic
* vSAN traffic
* Backup traffic
* Virtual machine traffic

The following heuristics can help with design decisions for Network I/O Control.

Shares and Limits

When you use bandwidth allocation, consider using shares instead of limits. Limits impose hard limits on the amount of bandwidth used by a traffic flow even when network bandwidth is available.

Limits on Network resource Pools

Consider imposing limits on a given network resource pool. For example, if you put a limit on vSphere vMotion traffic, you can benefit in situations where multiple vSphere vMotion data transfers, initiated on different ESXi hosts at the same time, result in oversubscription at the physical network level. By limiting the available bandwidth for vSphere vMotion at the ESXi host level, you can prevent performance degradation for other traffic.

Teaming Policy

When you use Network I/O Control, use Route based on physical NIC load teaming as a distributed switch teaming policy to maximize the networking capacity utilization. With load- based teaming, traffic might move among uplinks, and reordering of packets at the receiver can result occasionally.

Traffic Shaping

Use distributed port groups to apply configuration policies to different traffic types. Traffic shaping can help in situations where multiple vSphere vMotion migrations initiated on different ESXi hosts converge on the same destination ESXi host. The actual limit and reservation also depend on the traffic shaping policy for the distributed port group where the adapter is connected to.

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 vSphere Network design will use the following design decisions. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-NET-VMO2DC1-001 | Use vSphere Distributed Switches. | VCF |
| SDDC-MGMT-NET- VMO2DC1-002 | Use a single vSphere Distributed Switch per cluster. | VCF |
| SDDC-MGMT-NET- VMO2DC1-003 | Configure the MTU size of the vSphere Distributed Switch to 9000 for jumbo frames | VCF |
| SDDC-MGMT-NET- VMO2DC1-004 | Use ephemeral port binding for the management port group. | VCF |
| SDDC-MGMT-NET- VMO2DC1-005 | Use static port binding for all non-management port groups. | VCF |
| SDDC-MGMT-NET- VMO2DC1-006 | Use the Route based on physical NIC load teaming algorithm for the management port group. | VCF |
| SDDC-MGMT-NET- VMO2DC1-007 | Use the Route based on physical NIC load teaming algorithm for the vMotion Port Group. | VCF |
| SDDC-MGMT-NET- VMO2DC1-008 | Use the vMotion TCP/IP stack for vSphere vMotion traffic. | VCF |
| SDDC-MGMT-NET- VMO2DC1-009 | Enable Network I/O Control on vSphere distributed switch of the management domain cluster | VCF |
| SDDC-MGMT-NET- VMO2DC1-010 | Set the share value for management traffic to Normal. | VCF |
| SDDC-MGMT-NET- VMO2DC1-011 | Set the share value for vSphere vMotion traffic to Low. | VCF |
| SDDC-MGMT-NET- VMO2DC1-012 | Set the share value for virtual machines to High. | VCF |
| SDDC-MGMT-NET- VMO2DC1-013 | Set the share value for vSAN traffic to High. | VCF |
| SDDC-MGMT-NET- VMO2DC1-014 | Set the share value for vSphere Fault Tolerance to Low. | VCF |

Table 17 - SDDC vSphere Network Decisions

## Software Defined Networking Design for the Management Domain

In this design, you use NSX-T Data Center for connecting the management workloads by using virtual network segments and routing. You also create constructs for region-specific and cross- region solutions. These constructs isolate the solutions from the rest of the network, providing routing to the data center and load balancing.

NSX-T Data Center

NSX-T Data Center provides network virtualization capabilities in the management domain. With network virtualization, networking components that are usually part of the physical infrastructure, can be programmatically created and managed by using this software-defined network (SDN) platform. NSX-T Data Center provides both a declarative intent-based policy model, and an imperative based model to define and manage the SDN.

The deployment of NSX-T Data Center includes management, control plane, and services components. For the management domain, all these components run in the first cluster in the management domain to support the SDN needs of the management domain itself.

NSX-T Manager

NSX-T Manager provides the user interface and the RESTful API for creating, configuring, and monitoring NSX-T components, such as virtual network segments, and Tier-0 and Tier-1 gateways.

NSX-T Manager implements the management and control plane for the NSX-T infrastructure. NSX-T Manager is the centralized network management component of NSX-T, providing an aggregated view on all components in the NSX-T Data Center system.

|  |  |
| --- | --- |
| Component | Description |
| Services | * Logical switching and routing * Networking and edge services   Security services and distributed firewall |
| RESTful API | You can automate all configuration and monitoring operations by using any cloud automation platform, security vendor platform, or automation framework. |
| Management Plane Agent (MPA) | Available on each ESXi host. The MPA is in charge of persisting the desired state of the system and for communicating non-flow-controlling (NFC) messages such as configuration, statistics, status, and real-time data between transport nodes and the management plane. |
| NSX-T Controller | NSX-T Controllers implement the central control plane (CCP). They control the virtual networks and overlay transport tunnels. The controllers are responsible for the programmatic deployment of virtual networks across the entire NSX-T architecture.  The CCP is logically separated from all data plane traffic, that is, a failure in the control plane does not affect existing data plane operations. The controller provides configuration to other  NSX-T Data Center components, such as segment, gateway, and edge node configuration. |
| Integration with vCenter Server | NSX-T Data Center components are not assigned to a specific vCenter Server or vSphere construct. You can share them across different vSphere environments. |

Table 18 - Components of NSX-T Manager

NSX-T Edge Nodes

An NSX-T Edge node is a special type of transport node which contains service router components.

NSX-T Edge nodes provide north-south traffic connectivity between the physical data center networks and the NSX-T SDN networks. Each NSX-T Edge node has multiple interfaces where traffic flows.

You also use the NSX-T Edge nodes in east-west traffic flow between virtualized workloads. They provide stateful services such as load balancers and DHCP. In a multi-region deployment, east- west traffic between the regions flows through the NSX-T Edge nodes too.

[Logical Design for NSX-T Data Center for the Management Domain](#_bookmark30_2)

NSX-T Data Center provides networking services to SDDC management workloads such as load balancing, routing and virtual networking. NSX-T Data Center is connected to the region-specific Workspace ONE Access for central user management.

[Physical Network Infrastructure Design for NSX-T Data Center for the Management Domain](#_bookmark31_2)

Design of the physical data center network includes defining the network topology for connecting the physical switches and the ESXi hosts, determining switch port settings for VLANs and link aggregation, and designing routing.

[NSX-T Manager Deployment Specification and Network Design for the Management Domain](#_bookmark32_2)

You determine the size of the compute resources, high availability implementation, and patching and upgrade support for the NSX-T Manager instance for the management domain according to the design objectives and aggregated requirements of the management components of the SDDC.

[NSX-T Edge Deployment Specification and Network Design for the Management Domain](#_bookmark33_2)

Following the principles of this design and of each product, you deploy, configure, and connect the NSX-T Edge nodes to support networks within the software-defined networking.

[Life Cycle Management Design of NSX-T Data Center for the Management Domain](#_bookmark34_2)

You decide on the life cycle management of the NSX-T Data Center components according to the amount of time and effort to perform a deployment, upgrade, or patch operation. You also consider the impact such an operation has on the management solutions that are connected to NSX-T Data Center for the management domain.

[NSX-T Services Design for the Management Domain](#_bookmark35_2)

NSX-T Edge clusters are pools of capacity for NSX-T service router and load balancing functions.

[Overlay Design for NSX-T Data Center for the Management Domain](#_bookmark36_2)

As part of the overlay design, you determine the NSX-T Data Center configuration for handling traffic between management workloads. You determine the configuration of vSphere Distributed Switch and virtual segments on it, and of the transport zones.

[Virtual Network Segment Design for NSX-T for the Management Domain](#_bookmark37_2)

Management applications that are deployed on top of the management domain can use a pre-defined configuration of NSX-T virtual network segments.

[Information Security and Access Control Design for NSX-T Data Center for the Management](#_bookmark38_2) [Domain](#_bookmark38_2)

You design authentication access, controls, and certificate management for the NSX-T Data Center instance in the management domain according to industry standards and the requirements of your organization.

Logical Design for NSX-T Data Center for the Management Domain

NSX-T Data Center provides networking services to SDDC management workloads such as load balancing, routing and virtual networking. NSX-T Data Center is connected to the region-specific Workspace ONE Access for central user management.



Figure 13 - NSX-T Logical Design for the Management Domain

An NSX-T Data Center deployment consists of these components:

* Unified appliances that have both the NSX-T Local Manager and NSX-T Controller roles. They provide management and control plane capabilities.
* NSX-T Edge nodes that provide advanced services such as load balancing, and north-south connectivity.
* The ESXi hosts within the management domain are registered as NSX-T transport nodes to provide distributed routing and firewall services to management workloads.

Physical Network Infrastructure Design for NSX-T Data Center for the Management Domain

Design of the physical data center network includes defining the network topology for connecting the physical switches and the ESXi hosts, determining switch port settings for VLANs and link aggregation, and designing routing.

A software-defined network (SDN) both integrates with and uses components of the physical data center. SDN integrates with your physical network to support east-west transit in the data center and north-south transit to and from the SDDC networks.

Several typical data center network deployment topologies exist:

* Core-Aggregation-Access
* Leaf-Spine
* Hardware SDN

VMware Validated Design uses the leaf-spine networking topology, because in a single data center deployment, it provides predictable performance, scalable nature, and applicability across multiple vendors.

In an environment with multiple availability zones, Layer 2 networks must be stretched between the availability zones by the physical infrastructure. You also must provide a Layer 3 gateway that is highly available between availability zones. The method for stretching these Layer 2 networks and providing a highly available Layer 3 gateway is vendor-specific.

In an environment with multiple availability zones or regions, dynamic routing is needed to provide networks the ability to fail ingress and egress of traffic from availability zone to availability zone, or region to region. This design uses BGP as the dynamic routing protocol. As such, BGP must be present in the customer environment to facilitate the failover of networks from site to site. Because of the complexity of local-ingress, local-egress is not generally in use. In this design, network traffic flows in and out of a primary site.



Figure 14 - Host to ToR Connectivity

NSX-T Manager Deployment Specification and Network Design for the Management Domain

You determine the size of the compute resources, high availability implementation, and patching and upgrade support for the NSX-T Manager instance for the management domain according to the design objectives and aggregated requirements of the management components of the SDDC.

As a best practice, you must deploy a highly available NSX-T Manager instance so that the NSX-T central control place can continue propagating configuration to the transport nodes. You also select an NSX-T Manager appliance size according to the number of ESXi hosts required to run the SDDC management components.

You can deploy NSX-T Manager in a one-node configuration or as a cluster for high availability.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appliance Size | vCPU | Memory (GB) | Storage (GB) | Scale |
| Extra-Small | 2 | 8 | 300 | Cloud Service Manager only |
| Small | 4 | 16 | 300 | Proof of concept |
| Medium | 6 | 24 | 300 | Up to 64 ESXi hosts |
| Large | 12 | 48 | 300 | More than 64 ESXi hosts |

Table 19 - NSX-T Resource Specification

NSX-T Edge Deployment Specification and Network Design for the Management Domain

Following the principles of this design and of each product, you deploy, configure, and connect the NSX-T Edge nodes to support networks within the software-defined networking.

Deployment Specification of the NSX-T Edge Nodes for the Management Domain

You determine the size of the compute resources, high availability implementation, and patching and upgrade support for the NSX-T Edge appliances for the management domain according to the design objectives and aggregated requirements of the management components of the SDDC.

Deployment Model for the NSX-T Edge Nodes for the Management Domain

For NSX-T Edge nodes, you determine the form factor and the appliance number and place according to the requirements for network services in the management domain.

An NSX-T Edge node is an appliance that provides centralized networking’s services which cannot be distributed to hypervisors, such as load balancing, NAT, VPN, and physical network uplinks. Some services, such as T-0 gateways, are limited to a single instance per NSX-T Edge node. However, most services can coexist in these nodes. NSX-T Edge nodes are grouped in one or more edge clusters, representing a pool of capacity for NSX-T Data Center services

Form Factors of NSX-T Edge Nodes

An NSX-T Edge node can be deployed as a virtual appliance, or installed on bare metal hardware. The edge node on bare-metal hardware can have better performance capabilities at the expense of more difficult deployment and limited deployment topology use cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Form Factor |  | Appliance Size | CPU or vCPU | Memory (GB) | Storage (GB) |
| NSX-T Edge on bare metal hardware | Minimum requirements |  | 8 CPU | 8 | 200 |
| Recommended requirements |  | 24 CPU | 256 | 500 |
| NSX-T Edge virtual appliance |  | Small  Use for proof of concept only | 2 vCPU | 4 | 200 |
|  | Medium | 4 vCPU | 8 | 200 |
|  | Large  Use in large environments that require load balancers | 8 vCPU | 32 | 200 |
|  | Extra Large | 16 vCPU | 64 | 200 |

Table 20 - Resource Specifications of NSX-T Edge Nodes per Form Factor

High Availability Design for the NSX-T Edge Nodes for the Management Domain

The NSX-T Edge cluster runs on the first cluster in the management domain. vSphere HA and vSphere DRS protect the NSX-T Edge appliances. In an environment with multiple availability zones, to configure the first availability zone as the main location for the NSX-T Edge nodes, you use vSphere DRS.

NSX-T Edge Cluster Design

The NSX-T Edge cluster is a logical grouping of NSX-T Edge transport nodes. These NSX-T Edge appliances run on a vSphere cluster, and provide north-south routing and network services for the management workloads. You can dedicate this vSphere cluster only to edge appliance or can share it with the other management appliances.

First vSphere Cluster in the Management Domain

The first cluster in the management domain contains all components for managing the SDDC

Dedicated Edge vSphere Cluster

A dedicated vSphere Edge cluster contains only NSX-T Edge appliances.

High Availability for Multiple Availability Zones

NSX-T Edge nodes connect to top of rack switches in each data center to support northbound uplinks and route peering for SDN network advertisement. This connection is specific to the top of rack switch that you are connected to.

If an outage of an availability zone occurs, vSphere HA fails over the edge appliances to the other availability zone by using vSphere HA. Availability Zone 2 must provide an analog of the network infrastructure which the edge node is connected to in Availability Zone 1.

Network Design for the NSX-T Edge Nodes for the Management Domain

You implement an NSX-T Edge configuration with a single N-VDS. You connect the uplink network interfaces of the edge appliance to VLAN trunk port groups that are connected to particular physical NICs on the host.

The NSX-T Edge node contains an NSX-T managed virtual switch called an N-VDS. This internal N-VDS is used to define traffic flow through the interfaces of the edge node. An N-VDS can be connected to one or more interfaces. Interfaces cannot be shared between N-VDS instances.



Figure 15 - NSX-T Edge Network Configuration

Uplink Policy Design for the NSX-T Edge Nodes for the Management Domain

By using uplink profiles, you can apply consistent policy on the uplinks of the N-VDS instance on each NSX-T Edge appliance. The uplink profile for the NSX-T Edge appliances supports the VLANs for connection to physical Layer 3 devices.

A transport node can participate in an overlay and VLAN network. Uplink profiles define policies for the links from the NSX-T Edge transport nodes to top of rack switches. Uplink profiles are containers for the properties or capabilities for the network adapters. Uplink profiles are applied to the N-VDS of the edge node.

Uplink profiles can use either load balance source or failover order teaming. If using load balance source, multiple uplinks can be active. If using failover order, only a single uplink can be active.

Teaming can be configured by using the default teaming policy or a user-defined named teaming policy. You can use named teaming policies to pin traffic segments to designated edge uplinks.

Life Cycle Management Design of NSX-T Data Center for the Management Domain

You decide on the life cycle management of the NSX-T Data Center components according to the amount of time and effort to perform a deployment, upgrade, or patch operation. You also consider the impact such an operation has on the management solutions that are connected to NSX-T Data Center for the management domain.

Life cycle management of NSX-T Data Center involves the process of applying patches, updates or upgrades to the NSX-T Data Center appliances and hypervisor components. In a typical environment, you perform life cycle management by using the Upgrade Coordinator which is a service in NSX-T Manager. When you implement a solution by using VMware Cloud Foundation, you use SDDC Manager for life cycle management where additional components, such as automatic patching, upgrade, and product compatibility verification, are included as part of the life cycle management process.

NSX-T Services Design for the Management Domain

NSX-T Edge clusters are pools of capacity for NSX-T service router and load balancing functions.

North - South Routing

The routing design considers different levels of routing in the environment, such as number and type of NSX-T gateways, dynamic routing protocol, and so on. At each level, you apply a set of principles for designing a scalable routing solution.

Routing can be defined in the following directions:

* North-south traffic is traffic leaving or entering the NSX-T domain, for example, a virtual machine on an overlay network communicating with an end-user device on the corporate network.
* East-west traffic is traffic that remains in the NSX-T domain, for example, two virtual machines on the same or different segments communicating with each other.

As traffic flows north-south, edge nodes can be configured to pass traffic in an active-standby or an active-active model, where active-active can scale up to 8 active nodes. NSX-T service routers (SRs) for north-south routing are configured an active-active equal-cost multi-path (ECMP) mode that supports route failover of Tier-0 gateways in seconds.



Figure 16 - Dynamic Routing in a Single Availability Zone

Intra-SDN Routing

Gateways are needed to provide routing between logical segments created in the NSX-T based SDN. Logical segments can be connected directly to a Tier-0 or Tier-1 gateway.

Dynamic Routing in Multiple Availability Zones

In an environment with multiple availability zones, plan for failover of the NSX-T Edge nodes and configuring BGP so that traffic from the top of rack switches is directed to Availability Zone 1 unless a failure in Availability Zone 1 occurs.



Figure 17 - Dynamic Routing in Multiple Availability Zones

Load Balancers

The logical load balancer in NSX-T Data Center offers high-availability service for applications and distributes the network traffic load among multiple servers.

Because it is a stateful service, the load balancer is instantiated in a Tier-1 gateway.

Overlay Design for NSX-T Data Center for the Management Domain

As part of the overlay design, you determine the NSX-T Data Center configuration for handling traffic between management workloads. You determine the configuration of vSphere Distributed Switch and virtual segments on it, and of the transport zones.

This conceptual design for NSX-T provides the network virtualization design of the logical components that handle the data to and from tenant workloads in the environment.

ESXi Host Transport Nodes

An NSX-T transport node is a node that is capable of participating in an NSX-T data plane. The management domain contains multiple ESXi hosts in a vSphere cluster to support management workloads. You register these ESXi hosts as NSX-T transport nodes so that networks and workloads on that host can use the capabilities of NSX-T Data Center. During the preparation process, the native vSphere Distributed Switch for the management domain is extended with NSX-T capabilities.

Virtual Switches

NSX-T segments are logically abstracted segments to which you can connect tenant workloads. A single segment is mapped to a unique Geneve segment that is distributed across the ESXi hosts in a transport zone. The segment supports line-rate switching in the ESXi host without the constraints of VLAN sprawl or spanning tree issues.

Consider the following limitations of distributed switches:

* Distributed switches are manageable only when the vCenter Server instance is available. You can consider vCenter Server a Tier-1 application.
* Distributed switches with NSX-T capabilities are manageable only when the vCenter Server instance and NSX-T Manager cluster is available. You can consider vCenter Server and NSX-T Manager as Tier-1 applications.
* N-VDS instances are manageable only when the NSX-T Manager cluster is available. You can consider the NSX-T Manager cluster as a Tier-1 application.

Configuration of the vSphere Distributed Switch with NSX-T

The first cluster in the management domain uses a single vSphere Distributed Switch with a configuration for system traffic types, NIC teaming, and MTU size.

To support traffic uplink and overlay traffic for the NSX-T Edge nodes for the management domain, you must create several port groups on the vSphere Distributed Switch for the management domain. The VMkernel adapter for the Host TEP is connected to the host overlay VLAN but does not require a dedicated port group on the distributed switch. The VMkernel network adapter for Host TEP is automatically created when you configure the ESXi host as a transport node.

NSX-T Edge appliances and the VMkernel adapter for the Host TEP be connected to different VLANs and subnets. The VLAN IDs for the NSX-T Edge nodes are mapped to the VLAN trunk port groups

Virtual Segments

Geneve provides the overlay capability in NSX-T to create isolated, multi-tenant broadcast domains across data center fabrics, and enables customers to create elastic, logical networks that span physical network boundaries.

The first step in creating these logical networks is to isolate and pool the networking resources. By using the Geneve overlay, NSX-T isolates the network into a pool of capacity and separates the consumption of these services from the underlying physical infrastructure. This model is similar to the model vSphere uses to abstract compute capacity from the server hardware to create virtual pools of resources that can be consumed as a service. You can then organize the pool of network capacity in logical networks that are directly attached to specific applications.

Geneve is a tunneling mechanism which provides extensibility while still using the offload capabilities of NICs for performance improvement.

Geneve works by creating Layer 2 logical networks that are encapsulated in UDP packets. A Segment ID in every frame identifies the Geneve logical networks without the need for VLAN tags. As a result, many isolated Layer 2 networks can coexist on a common Layer 3 infrastructure using the same VLAN ID.

In the vSphere architecture, the encapsulation is performed at the TEP VMkernel adapter of the ESXi host and before being sent on the physical network, making the Geneve overlay transparent to both the guest virtual machines and the underlying Layer 3 network. The Tier-0 Gateway performs gateway services between overlay and non-overlay hosts, for example, a physical server or the Internet router. The NSX-T Edge node translates overlay segment IDs to VLAN IDs, so that non-overlay hosts can communicate with virtual machines on an overlay network.

The edge cluster hosts all NSX-T Edge node instances that connect to the corporate network for secure and centralized network administration.

Transport Zones

Transport zones determine which hosts can participate in the use of a particular network. A transport zone identifies the type of traffic, VLAN or overlay, and the vSphere Distributed Switch name. You can configure one or more VLAN transport zones and a single overlay transport zone per virtual switch. A transport zone does not represent a security boundary.



Figure 18 - Transport Zone Design

Uplink Policy for ESXi Host Transport Nodes

Uplink profiles define policies for the links from ESXi hosts to NSX-T segments or from NSX-T Edge appliances to top of rack switches. By using uplink profiles, you can apply consistent configuration of capabilities for network adapters across multiple ESXi hosts or NSX-T Edge nodes.

Uplink profiles can use either load balance source or failover order teaming. If using load balance source, multiple uplinks can be active. If using failover order, only a single uplink can be active

Replication Mode of Segments

The control plane decouples NSX-T Data Center from the physical network. The control plane handles the broadcast, unknown unicast, and multicast (BUM) traffic in the virtual segments.

Virtual Network Segment Design for NSX-T for the Management Domain

Management applications that are deployed on top of the management domain can use a pre- defined configuration of NSX-T virtual network segments.

NSX-T segments provide flexibility for workload placement by removing the dependence on traditional physical data center networks. This approach also improves security and mobility of the management applications, and reduces the integration effort with existing customer network.



Figure 19 - Virtual Network Segments in SDDC

Information Security and Access Control Design for NSX-T Data Center for the Management Domain

You design authentication access, controls, and certificate management for the NSX-T Data Center instance in the management domain according to industry standards and the requirements of your organization.

Identity Management

Users can authenticate to NSX-T Manager from several sources. Role-based access control is not available with local user accounts.

* Local user accounts
* Active Directory by using LDAP
* Active Directory by using Workspace ONE Access
* Principal identity

Password Management and Account Lockout Behavior for NSX-T Manager and NSX-T Edge Nodes

By default you must include at least eight characters and passwords to expire after 90 days. You configure access to the NSX-T command line interface (CLI) and lockout behavior for the NSX-T Manager user interface and RESTful API separately.

Certificate Management

Access to all NSX-T Manager interfaces must use an Secure Sockets Layer (SSL) connection. By default, NSX-T Manager uses a self-signed SSL certificate. This certificate is not trusted by end- user devices or Web browsers.

As a best practice, replace self-signed certificates with certificates that are signed by a third- party or enterprise Certificate Authority (CA).

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 SDN design will use the following design decisions. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-SDN-VMO2DC1-001 | Use two ToR switches for each rack. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-002 | Implement the following physical network architecture: One 25 GbE (10 GbE minimum) port on each ToR switch for ESXi host uplinks. Layer 3 device that supports BGP. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-003 | Do not use EtherChannel (LAG, LACP, or vPC) configuration for ESXi host uplinks | VCF |
| SDDC-MGMT-SDN- VMO2DC1-004 | Use a physical network that is configured for BGP routing adjacency | VCF |
| SDDC-MGMT-SDN- VMO2DC1-005 | Assign static IP addresses to all management components in the SDDC infrastructure except for NSX-T tunnel endpoints (TEPs). | VCF |
| SDDC-MGMT-SDN- VMO2DC1-006 | Set the lease duration for the TEP DHCP scope to at least 7 days. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-007 | Use VLANs to separate physical network functions. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-008 | Set the MTU size to at least 1700 bytes (recommended 9000 bytes for jumbo frames) on the physical switch ports, vSphere Distributed Switches, vSphere Distributed Switch port groups, and N-VDS switches that support the following traffic types: Host Overlay (Geneve), vSAN, vSphere vMotion, NFS | VCF |
| SDDC-MGMT-SDN- VMO2DC1-009 | Set the MTU size to at least 1,700 bytes (recommended 9000 bytes for jumbo frames) on physical inter- availability zone networking components which are part of the networking path between availability zones for the following traffic types: Host Overlay (Geneve), vSAN, vSphere vMotion, and NFS | VCF |
| SDDC-MGMT-SDN- VMO2DC1-010 | Configure VRRP, HSRP, or another Layer 3 gateway availability method for these networks: Management, Edge Overlay | VCF |
| SDDC-MGMT-SDN- VMO2DC1-011 | Deploy three NSX-T Manager nodes for the management domain in the first cluster in the domain for configuring and managing the network services for SDDC management components. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-012 | Deploy each node in the NSX-T Manager cluster for the management domain as a medium- size appliance or larger with a min of 3 controllers. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-013 | Create a virtual IP (VIP) address for the NSX-T Manager cluster for the management domain. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-014 | Apply VM-VM anti-affinity rules in vSphere Distributed Resource Scheduler (vSphere DRS) to the NSX-T Manager appliances. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-015 | In vSphere HA, set the restart priority policy for each NSX-T Manager appliance to high. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-016 | When using two availability zones, create a virtual machine group for the NSX-T Manager appliances. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-017 | Place the appliances of the NSX- T Manager cluster on the management VLAN network. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-018 | Allocate a statically assigned IP address and host name to the nodes of the NSX-T Manager cluster. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-019 | Configure forward and reverse DNS records for the nodes of the NSX-T Manager cluster for the management domain, assigning the record to the child domain in the region. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-020 | Configure NTP on each NSX-T Manager appliance. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-021 | Use medium-size NSX-T Edge virtual appliances. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-022 | Deploy the NSX-T Edge virtual appliances. Do not configure a dedicated vSphere cluster for edge nodes. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-023 | Deploy two NSX-T Edge appliances in an edge cluster in the first cluster in the management domain. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-024 | Apply VM-VM anti-affinity rules for vSphere DRS to the virtual machines of the NSX-T Edge cluster. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-025 | In vSphere HA, set the restart priority policy for each NSX-T Edge appliance to high. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-026 | Configure all edge nodes as transport nodes. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-027 | Create an NSX-T Edge cluster with the default Bidirectional Forwarding Detection (BFD) configuration between the NSX-T Edge nodes in the cluster. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-028 | When using two availability zones, create a should-run VM-Host affinity rule to run the group of NSX-T Edge appliances on the group of hosts in Availability Zone 1. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-029 | Connect the management interface eth0 of each NSX-T Edge node to the management VLAN. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-030 | Connect the fp-eth0 interface of each NSX-T Edge appliance to a VLAN trunk port group pinned to physical NIC 0 of the host. Connect the fp-eth1 interface of each NSX-T Edge appliance to a VLAN trunk port group pinned to physical NIC 1 of the host. Leave the fp-eth2 interface of each NSX-T Edge appliance unused. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-031 | Use a single N-VDS in the NSX-T Edge nodes. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-032 | Create one uplink profile for the edge node with three teaming policies. 1. Default teaming policy of load balance source both active uplinks uplink-1 and uplink-2. 2. Named teaming policy of failover order with a single active uplink uplink-1 without standby uplinks.3. Named teaming policy of failover order with a single active uplink uplink-2 without standby uplinks. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-033 | Use a dedicated VLAN for edge overlay that is different from the host overlay VLAN | VCF |
| SDDC-MGMT-SDN- VMO2DC1-034 | Use SDDC Manager to perform the life cycle management of NSX-T Manager and related components in the management domain. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-035 | Deploy an active-active Tier-0 gateway. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-036 | To enable ECMP between the Tier-0 gateway and the Layer 3 devices (ToR switches or upstream devices), create two VLANs. The ToR switches or upstream Layer 3 devices have an SVI on one of the two VLANS and each Edge node in the cluster has an interface on each VLAN. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-037 | Assign a named teaming policy to the VLAN segments to the Layer 3 device pair. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-038 | Create a VLAN transport zone for Edge uplink traffic. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-039 | Use BGP as the dynamic routing protocol | VCF |
| SDDC-MGMT-SDN- VMO2DC1-040 | Configure the BGP Keep Alive Timer to 4 and Hold Down Timer to 12 between the top of tack switches and the Tier-0 gateway. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-041 | Do not enable Graceful Restart between BGP neighbors. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-042 | Enable helper mode for Graceful Restart mode between BGP neighbors | VCF |
| SDDC-MGMT-SDN- VMO2DC1-043 | Enable Inter-SR iBGP routing. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-044 | Deploy a Tier-1 gateway and connect it to the Tier-0 gateway. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-045 | Deploy a Tier-1 gateway to the NSX-T Edge cluster | VCF |
| SDDC-MGMT-SDN- VMO2DC1-046 | Deploy a Tier-1 gateway in non-preemptive failover mode. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-047 | When you have two availability zones, extend the uplink VLANs to the top of rack switches so that the VLANs are stretched between both availability zones. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-048 | When you have two availability zones, provide this SVI configuration on the top of the rack switches or upstream Layer 3 devices. In Availability Zone 2, configure the top of rack switches or upstream Layer 3 devices with an SVI on each of the two uplink VLANs. Make the top of rack switch SVI in both availability zones part of a common stretched Layer 2 network between the availability zones. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-049 | When you have two availability zones, provide this VLAN configuration. Use two VLANs to enable ECMP between the Tier-0 gateway and the Layer 3 devices (top of rack switches or upstream devices). The ToR switches or upstream Layer 3 devices have an SVI to one of the two VLANS and each NSX-T Edge node has an interface to each VLAN. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-050 | Create an IP prefix list that permits access to route advertisement by any network instead of using the default IP prefix list. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-051 | Create a route map-out that contains the custom IP prefix list and an AS-path prepend value set to the Tier-0 local AS added twice | VCF |
| SDDC-MGMT-SDN- VMO2DC1-052 | Create an IP prefix list that permits access to route advertisement by network 0.0.0.0/0 instead of using the default IP prefix list. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-053 | Apply a route map-in that contains the IP prefix list for the default route 0.0.0.0/0 and assign a lower local- preference, for example, 80, to the learned default route and a lower local-preference, for example, 90 any routes learned. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-054 | Configure Availability Zone 2 neighbors to use the route maps as In and Out filters respectively. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-055 | Deploy a standalone Tier-1 gateway to support advanced stateful services such as load balancing for other management components. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-056 | Connect the standalone Tier-1 gateway to the cross- region virtual network. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-057 | Configure the standalone Tier-1 gateway with static routes to the gateways of the networks it is connected to. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-058 | Enable all ESXi hosts in the management domain as NSX-T transport nodes. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-059 | Configure each ESXi host as a transport node without using transport node profiles | VCF |
| SDDC-MGMT-SDN- VMO2DC1-060 | Use a vSphere Distributed Switch for the first cluster in the management domain that is enabled for NSX-T Data Center. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-061 | To provide virtualized network capabilities to management workloads, use overlay networks with NSX-T Edge nodes and distributed routing. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-062 | Create a single overlay transport zone for all overlay traffic across the management domain and NSX-T Edge nodes. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-063 | Create a single VLAN transport zone for uplink VLAN traffic that is applied only to NSX-T Edge nodes. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-064 | Create an uplink profile with the load balance source teaming policy with two active uplinks for ESXi hosts. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-065 | Use hierarchical two-tier replication on all segments. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-066 | Create one or more cross- region NSX-T virtual network segments for management application components which require mobility between regions. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-067 | Create one or more region- specific NSX-T virtual network segments for management application components that are assigned to a specific region. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-068 | Limit the use of local accounts. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-069 | Enable NSX-T Manager integration with your corporate identity source by using the region-specific Workspace ONE Access instance. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-070 | Use Active Directory groups to grant privileges to roles in NSX-T Data Center. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-071 | Create an NSX-T Enterprise Admin group rainpole.io\ug- nsx-enterprise-admins in Active Directory and map it to the Enterprise Administrator role in NSX-T Data Center. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-072 | Create an NSX-T Auditor group rainpole.io\ug-nsx- auditors in Active Directory and map it to the Auditor role in NSX-T Data Center. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-073 | Create more Active Directory groups and map them to roles in NSX-T Data Center according to the business and security requirements of your organization | VCF |
| SDDC-MGMT-SDN- VMO2DC1-074 | Restrict end-user access to both NSX-T Manager user interface and its RESTful API endpoint. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-075 | Configure the passwords for CLI access to NSX-T Manager for the root, admin, and audit users, and account lockout behavior for CLI according to the industry standard for security and compliance of your organization. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-076 | Configure the passwords for access to the NSX-T Edge nodes for the root, admin, and audit users, and account lockout behavior for CLI according to the industry standard for security and compliance of your organization. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-077 | Configure the passwords for access to the NSX-T Manager user interface and RESTful API or the root, admin, and audit users, and account lockout behavior for CLI according to the industry standard for security and compliance of your organization. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-078 | Replace the default self- signed certificate of the NSX- T Manager instance for the management domain with a certificate that is signed by a third-party certificate authority. | VCF |
| SDDC-MGMT-SDN- VMO2DC1-079 | Use a SHA-2 algorithm or stronger when signing certificates. | VCF |

Table 21 - SDDC Design Decisions for SDN

## Shared Storage Design for a Virtual Infrastructure Workload Domain

The shared storage design includes the design for VMware vSAN storage.

* Optimize the storage design to meet the diverse needs of applications, services, administrators, and users.
* Strategically align business applications and the storage infrastructure to reduce costs, boost performance, improve availability, provide security, and enhance functionality.
* Provide multiple tiers of storage to match application data access to application requirements.
* Design each tier of storage with different performance, capacity, and availability characteristics. Because not every application requires expensive, high-performance, highly available storage, designing different storage tiers reduces cost.

[Logical Design for Shared Storage for a Virtual Infrastructure Workload Domain](#_bookmark52_3)

Either dedicated edge clusters or shared edge and workload clusters can use vSAN, NFS, VMware vSphere® Virtual Volumes™, or Fibre Channel storage as principal storage. No specific guidance is given as user workloads and other factors determine storage type and SLA for user workloads.

[Deployment Specification for Shared Storage for a Virtual Infrastructure Workload Domain](#_bookmark53_3)

The shared storage design includes determining the physical storage infrastructure required for using VMware vSAN and the policy configuration for delivering reliable storage service to the SDDC tenant workloads.

[Network Design for Shared Storage for a Virtual Infrastructure Workload Domain](#_bookmark58_3)

In the network design for shared storage in the workload domain, you determine the network configuration for vSAN traffic.

Logical Design for Shared Storage for a Virtual Infrastructure Workload Domain

Either dedicated edge clusters or shared edge and workload clusters can use vSAN, NFS, VMware vSphere® Virtual Volumes™, or Fibre Channel storage as principle storage. No specific guidance is given as user workloads and other factors determine storage type and SLA for user workloads.



Figure 20 - Logical Storage Design

Deployment Specification for Shared Storage for a Virtual Infrastructure Workload Domain

The shared storage design includes determining the physical storage infrastructure required for using VMware vSAN and the policy configuration for delivering reliable storage service to the SDDC tenant workloads.

[Shared Storage Platform for a Virtual Infrastructure Workload Domain](#_bookmark54_3)

For principal storage, you can select between traditional storage, VMware vSphere Virtual Volumes, and VMware vSAN.

[vSAN Physical Design for a Virtual Infrastructure Workload Domain](#_bookmark55_3)

This design uses VMware vSAN to implement software-defined storage as the primary storage type for the shared edge and workload cluster. By using vSAN, you have a high level of control over the storage subsystem.

[vSAN Deployment Specification for a Virtual Infrastructure Workload Domain](#_bookmark57_3)

When determining the vSAN deployment specification, you decide on the datastore size, number of ESXi hosts per vSphere Cluster, number of disk groups per ESXi host, and the vSAN policy.

Shared Storage Platform for a Virtual Infrastructure Workload Domain

For principal storage, you can select between traditional storage, VMware vSphere Virtual Volumes, and VMware vSAN.

Traditional Storage

Fibre Channel and NFS are applicable options for virtual machines, however they are not used in this design. iSCSI storage is currently not supported as an option for principal storage for workload domains.

VMware vSAN Storage

vSAN is a software-based distributed storage platform that combines the compute and storage resources of VMware ESXi hosts. When you design and size a vSAN cluster, host hardware choices can be more limited compared to traditional storage.

vSphere Virtual Volumes

vSphere Virtual Volumes is an applicable option when using storage arrays which support the vSphere Virtual Volume feature.

Traditional Storage and vSAN Storage

Fibre Channel and NFS are mature and applicable options to support workload needs.

Your decision to implement one technology or another can be based on performance and functionality.

|  |  |
| --- | --- |
| D | ***Design Decision***  We are going to use vSAN storage for the VMO2DC1 solution. |

vSAN is a software-based distributed storage platform that combines the compute and storage resources of ESXi hosts. It provides a simple storage management experience for the user.

However, you must carefully consider supported hardware options when sizing and designing a vSAN cluster.

Logical Design for Shared Storage

This vSAN design is limited to the shared edge and workload cluster in the workload domain. The design uses the default storage policy to achieve redundancy and performance within the vSAN Cluster.

vSAN Physical Design for a Virtual Infrastructure Workload Domain

This design uses VMware vSAN to implement software-defined storage as the primary storage type for the shared edge and workload cluster. By using vSAN, you have a high level of control over the storage subsystem.

All functional testing and validation of the design is on vSAN. Although VMware Validated Design uses vSAN, in particular for the clusters running tenant workloads, you can use any supported storage solution. If you select a storage solution other than vSAN, consider that all the design, deployment, and Day-2 guidance in VMware Validated Design applies under the context of vSAN and adjust appropriately. Your storage design must match or exceed the capacity and performance capabilities of the vSAN configuration in the design. For multiple availability zones, the vSAN configuration includes vSAN stretched clusters.

vSAN is a hyper-converged storage software that is fully integrated with the hypervisor. vSAN creates a cluster of local ESXi host hard disk drives and solid-state drives, and presents a flash- optimized, highly resilient, shared storage datastore to ESXi hosts. By using vSAN storage policies, you can control capacity, performance, and availability on a per virtual machine basis.

I/O Controllers for vSAN

The I/O controllers are as important to a vSAN configuration as the selection of disk drives. vSAN supports SAS, SATA, and SCSI adapters in either pass-through or RAID 0 mode. vSAN supports multiple controllers per ESXi host.

* You select between single- and multi-controller configuration in the following way: Multiple controllers can improve performance and mitigate a controller or SSD failure to a smaller number of drives or vSAN disk groups.
* With a single controller, all disks are controlled by one device. A controller failure impacts all storage, including the boot media (if configured).

Controller queue depth is possibly the most important aspect for performance. All I/O controllers in the [VMware vSAN Hardware Compatibility Guide](https://www.vmware.com/resources/compatibility/search.php?deviceCategory=vsan) have a minimum queue depth of 256.

Consider regular day-to-day operations and increase of I/O because of virtual machine deployment operations, or re-sync I/O activity as a result of automatic or manual fault remediation.

vSAN Flash Options

vSAN has two configuration options: all-flash and hybrid.

Hybrid Mode

In a hybrid storage architecture, vSAN pools server-attached capacity devices (in this case magnetic devices) and flash-based caching devices, typically SSDs, or PCI-e devices, to create a distributed shared datastore.

All-Flash Mode

All-flash storage uses flash-based devices (SSD or PCI-e) as a write cache while other flash- based devices provide high endurance for capacity and data persistence.

vSAN Hardware Considerations

While VMware supports building your own vSAN cluster from compatible components, vSAN ReadyNodes are selected for this VMware Validated Design.

vSAN Deployment Specification for a Virtual Infrastructure Workload Domain

When determining the vSAN deployment specification, you decide on the datastore size, number of ESXi hosts per vSphere Cluster, number of disk groups per ESXi host, and the vSAN policy.

vSAN Datastore Size

The size of the vSAN datastore depends on the requirements for the datastore. Consider cost against availability to provide the appropriate sizing.

As per the calculations in [Sizing Storage](#_bookmark56_3), a minimum size is required to run the workloads and infrastructure. If you plan to add more solutions or additions to this environment, you must increase this size.

Number of vSAN-enabled ESXi Hosts Per Cluster

The number of ESXi hosts in the cluster depends on these factors:

* Amount of available space on the vSAN datastore
* Number of failures you can tolerate in the cluster

For example, if the vSAN cluster has only 3 ESXi hosts, only a single failure is supported. If a higher level of availability is required, you must add more hosts.

Number of Disk Groups Per ESXi Host

Disk group sizing is an important factor during volume design. The number of disk groups can affect availability and performance. If more ESXi hosts are available in the cluster, more failures are tolerated in the cluster. This capability adds cost because additional hardware for the disk groups is required. More available disk groups can increase the recoverability of vSAN during a failure. Consider these data points when deciding on the number of disk groups per ESXi host:

* Amount of available space on the vSAN datastore.
* Number of failures you can tolerate in the cluster.
* Performance required when recovering vSAN objects.

The optimal number of disk groups is a balance between hardware and space requirements for the vSAN datastore. More disk groups increase space and provide higher availability. However, adding disk groups can be cost-prohibitive.

vSAN Policy Design

After you enable and configure VMware vSAN, you can create storage policies that define the virtual machine storage characteristics. Storage characteristics specify different levels of service for different virtual machines.

The default storage policy tolerates a single failure and has a single disk stripe. Use the default policy. If you configure a custom policy, vSAN should guarantee its application. However, if vSAN cannot guarantee a policy, you cannot provision a virtual machine that uses the policy unless you enable force provisioning.

Policy design starts with assessment of business needs and application requirements. Use cases for VMware vSAN must be assessed to determine the necessary policies. Start by assessing the following application requirements:

* I/O performance and profile of your workloads on a per-virtual-disk basis
* Working sets of your workloads
* Hot-add of additional cache (requires repopulation of cache)
* Specific application best practice (such as block size)

After assessment, configure the software-defined storage module policies for availability and performance in a conservative manner so that space consumed and recoverability properties are balanced. In many cases the default system policy is adequate and no additional policies are required unless specific requirements for performance or availability exist.

A storage policy includes several attributes. You can use them alone or combine them to provide different service levels. By using policies, you can customize any configuration according to the business requirements of the consuming application.

Before making design decisions, understand the policies and the objects to which they can be applied.

If you do not specify a user-configured policy, vSAN uses a default system policy of 1 failure to tolerate and 1 disk stripe for virtual disks and virtual disk snapshots. To ensure protection for these critical virtual machine components, policy defaults for the VM namespace and swap are set statically and are not configurable. Configure policies according to the business requirements of the application. By using policies, vSAN can adjust the performance of a disk on the fly.

vSAN Witness

When using vSAN in a stretched cluster configuration, you must deploy a witness ESXi host on a physical server or as a virtual appliance. The vSAN witness appliance contains a special ESXi installation that provides quorum and tiebreaker services for stretched clusters. This appliance must be deployed in a third location that is not local to the ESXi hosts on either side of the stretched cluster.

Network Design for Shared Storage for a Virtual Infrastructure Workload Domain

In the network design for shared storage in the workload domain, you determine the network configuration for vSAN traffic.

When determining the network configuration, you must consider the overall traffic bandwidth and decide how to isolate storage traffic.

* Consider how much replication and communication traffic is running between ESXi hosts and storage arrays.
* The amount of storage traffic depends on the number of VMs that are running in the cluster, and on how write- intensive the I/O is for the applications running in the VMs.

vSAN Witness Network Design

When using two availability zones, to be able to communicate to the vCenter Server instance, connect the vSAN witness appliance for the workload domain to the management network of the management domain in Availability Zone 1.

VMware Validated Design uses vSAN witness traffic separation where you can use a VMkernel adapter for vSAN witness traffic that is different from the adapter for vSAN data traffic. In this design, you configure vSAN witness traffic in the following way:

* On each management ESXi host in both availability zones, place the vSAN witness traffic on the management VMkernel adapter.
* On the vSAN witness appliance, use the same VMkernel adapter for both management and witness traffic.

Management Network

Routed to the management networks of the management domain and the workload domain in both availability zones. Connect the first VMkernel adapter of the vSAN witness appliance to this network. The second VMkernel adapter on the vSAN witness appliance is not used.

Place the following traffic on this network:

* + Management traffic

To be able to communicate to the vCenter Server instance, the vSAN witness appliance for the workload domain must access the management network in Availability Zone 1.

* + vSAN witness traffic

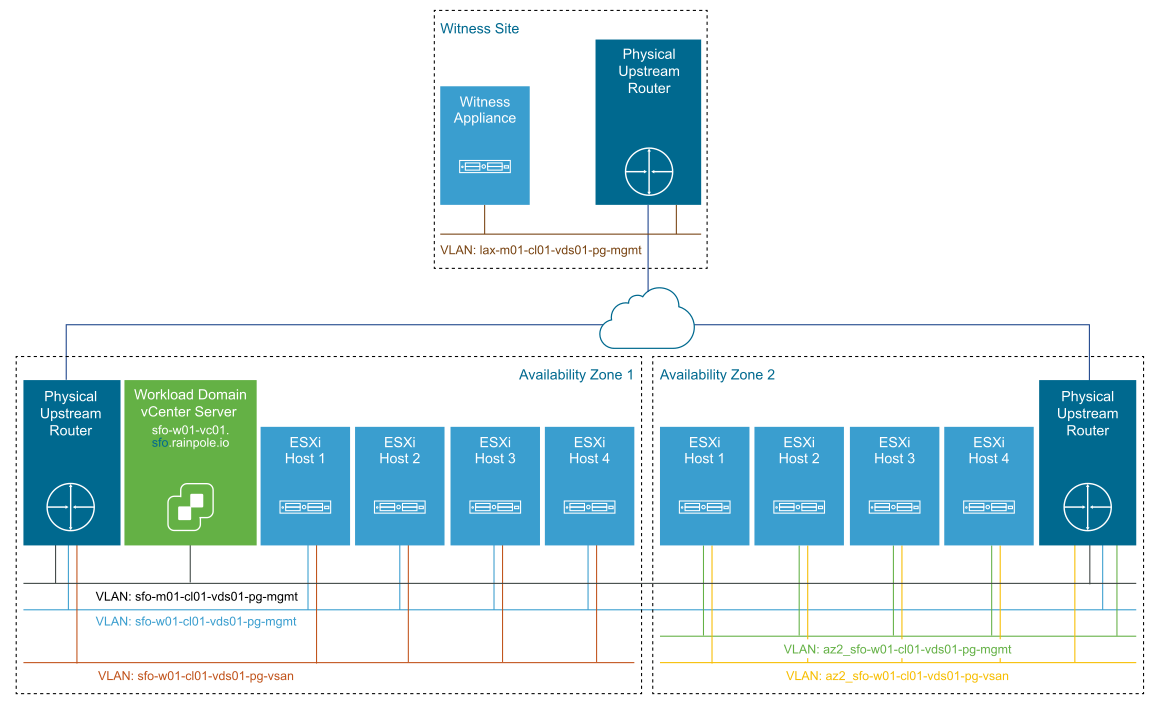


Figure 21 - vSAN Witness Network Design

|  |  |
| --- | --- |
| D | ***Design Decision***  The following design decisions have been made for the VMO2DC1 solution. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-STO-VMO2DC1-001 | When using a single availability zone in the first cluster of the management cluster, use vSAN and NFS shared storage:  - Use vSAN as the primary shared storage platform. | VCF |
| SDDC-MGMT-STO- VMO2DC1-002 | In all clusters, ensure that at least 20% of free space is always available on all non-vSAN datastores. | VCF |
| SDDC-MGMT-STO- VMO2DC1-003 | Enable Storage I/O Control with the default values on all non-vSAN datastores. | VCF |

Table 22 - SDDC Storage Decisions

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-SDS- VMO2DC1-001 | Ensure that the I/O Controller that is running the vSAN disk group(s) is capable and has a minimum queue depth of 256 set. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-002 | I/O Controllers that are running vSAN disk group(s) should not be used for an other purpose. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-003 | Configure vSAN in all-flash mode in the first cluster of the management domain. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-004 | Use a 600 GB or greater flash-based drive for the cache tier in each disk group | VCF |
| SDDC-MGMT-SDS- VMO2DC1-005 | Have at least 5TB of flash-based drives for the capacity tier in each disk group. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-006 | Provide the first cluster in the management with a minimum of 37 TB of raw capacity for vSAN. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-007 | On all vSAN datastores, ensure that at least 30% of free space is always available | VCF |
| SDDC-MGMT-SDS- VMO2DC1-008 | When using a single availability zone, the first cluster in the management domain requires a minimum of 4 ESXi hosts to support vSAN. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-009 | When using two availability zones, the first cluster in the management domain, requires a minimum of 8 ESXi hosts (4 in each availability zone) to support a stretched vSAN configuration. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-010 | Configure vSAN with a minimum of two disk groups per ESXi host. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-011 | When using two availability zones, deploy a vSAN witness appliance in a location that is not local to the ESXi hosts in any of the availability zones. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-012 | Deploy a medium-size witness appliance. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-013 | When using a single availability zone, use the default VMware vSAN storage policy | VCF |
| SDDC-MGMT-SDS- VMO2DC1-014 | When using two availability zones, add the following setting to the default vSAN storage policy: Secondary Failures to Tolerate = 1 | VCF |
| SDDC-MGMT-SDS- VMO2DC1-015 | When using two availability zones, configure two fault domains, one for each availability zone. Assign each host to their respective availability zone fault domain. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-016 | Leave the default virtual machine swap file as a sparse object on VMware vSAN. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-017 | Use the existing vSphere Distributed Switch instances in the first cluster in the management domain. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-018 | Configure jumbo frames on the VLAN dedicated to vSAN traffic. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-019 | Connect the first VMkernel adapter of the vSAN witness appliance to the management network in the witness site. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-020 | Configure the vSAN witness appliance to use the first VMkernel adapter, that is the management Interface, for vSAN witness traffic. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-021 | Place witness traffic on the management VMkernel adapter of all the ESXi hosts in the management domain. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-022 | Allocate a statically assigned IP address and host name to the management adapter of the vSAN witness appliance. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-023 | Configure forward and reverse DNS records for the vSAN witness appliance assigning the record to the child domain for the region. | VCF |
| SDDC-MGMT-SDS- VMO2DC1-024 | Configure time synchronization by using an internal NTP time for the vSAN witness appliance. | VCF |

Table 23 - SDDC Software Defined Storage Decisions

## VMware Workspace One Access

VMware Workspace ONE Access, formerly VMware Identity Manager™, is the product of the Security and Compliance layer that provides identity and access management to end users.

Workspace ONE Access implements the Zero Trust Access Control model by providing users continuous access to their applications and data based on many factors like their device, location, how they are authenticated, intelligence, and risk signals. Workspace ONE Access ensures that users do not have access to applications that they must not access. Workspace ONE Access provides a common experience for accessing on-premises or SaaS applications, while also providing administrators visibility into user application accessibility, who uses what or when, and the frequency of access. Workspace ONE Access works together with your primary identity providers while acting as a broker into the Software- Defined Data Center.

In the context of SDDC, Workspace ONE Access is the broker between existing authentication providers in your data center, for example, Active Directory and LDAP directory, and SDDC solutions, such as NSX- T Data Center and the vRealize Suite products. Workspace ONE Access provides identity and access management services to each SDDC solution and ensures that the SAML is valid across solutions and regions in the SDDC.

Security and Compliance Design

The Security and Compliance layer contains the Identity and Access Management component, which is required to control access to the SDDC solutions. In this design, the identity and access management function is provided by VMware Workspace ONE Access. To control access to the cross-region SDDC components, you add a cross-region Workspace ONE Access deployment.



Figure 22 - Security and Compliance Design

Cross-Region Workspace ONE Access Design

VMware Workspace ONE Access provides identity and access management services to several cross- region components within the Software-Defined Data Center. The design aligns with the design objectives, constraints, and use cases of these components – in terms of the number of users, availability requirements, and so on.

Logical Design for Cross-Region Workspace ONE Access

To provide identity and access management services to cross-region SDDC solutions, such as vRealize Operations Management, vRealize Automation, and vRealize Suite Lifecycle Manager, this design uses a Workspace ONE Access cluster that is deployed on the cross-region virtual network in Region A.

Workspace ONE Access provides:

* Directory integration to authenticate users against existing directories such as Active Directory or LDAP.
* Addition of two-factor authentication through integration with third-party software such as RSA SecurID, Entrust, and others.

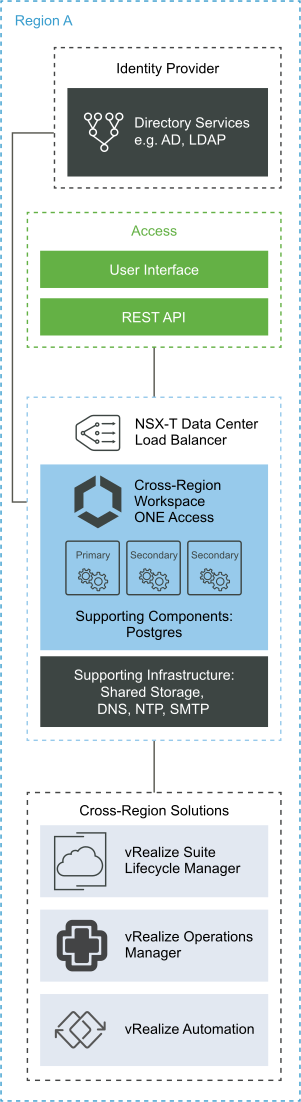


Figure 23- Logical Design of the Cross Region Workspace ONE Access Deployment

|  |  |
| --- | --- |
| Single Availability Zone | Multiple Availability Zones |
| A three-node Workspace ONE Access cluster with a load balancer deployed on the cross-region network segment. | A three-node Workspace ONE Access cluster with a load balancer deployed on the cross-region network segment. |
| All Workspace ONE Access services and databases are configured for high availability using the underlying cluster configuration. Portable, cross-region SDDC solutions are integrated with this Workspace ONE Access cluster. | All Workspace ONE Access services and databases are configured for high availability using the underlying cluster configuration. Portable, cross-region SDDC solutions are integrated with this Workspace ONE Access cluster. |
| vSphere HA protects the Workspace ONE Access cluster nodes. | vSphere HA protects the Workspace ONE Access cluster nodes. |
| DRS anti-affinity rules ensure that the Workspace ONE Access cluster nodes are not running on the same ESXi host. | DRS anti-affinity rules ensure that the Workspace ONE Access cluster nodes are not running on the same ESXi host. |
|  | A DRS rule specifies that the Workspace ONE Access cluster nodes run on ESXi hosts in Availability Zone 1. |

Table 24 - Cross Region Workspace ONE Access Logical Components

The cross-region Workspace ONE Access cluster provides an authentication source for vRealize Automation, vRealize Operations Manager, and vRealize Suite Lifecycle Manager, which provides authentication services to the enterprise directory or directories.

Supporting Infrastructure

All instances of Workspace ONE Access in this design integrate with the following supporting infrastructure:

* NTP for time synchronization
* DNS for name resolution
* Active Directory (or LDAP)

Deployment Specification for Cross-Region Workspace ONE Access

The deployment specification details the design decisions covering physical design and sizing for Workspace ONE Access.

Deployment Model for Cross-Region Workspace ONE Access

Workspace ONE Access is distributed as a virtual appliance in OVA format. The Workspace ONE Access appliance includes identity and access management services.

Deployment Type

You consider the deployment type - standard or cluster - according to the design objectives for the availability and number of users that the system and integrated SDDC solutions must support. Workspace ONE Access is deployed on the first cluster in the management domain.

In this design, you deploy a cluster topology of Workspace ONE Access for cross-region SDDC solutions.

|  |  |
| --- | --- |
| D | ***Design Decision***  The following design decisions have been made for the VMO2DC1 solution. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
|  |  |  |
| SDDC-MGMT-IAM-VMO2DC1-001 | Deploy a standalone Workspace ONE Access instance on the first cluster in the management domain in the region. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-002 | Use the OVA file to deploy the standalone Workspace ONE Access instance in each region, using the standard deployment type to provide identity and access management services to regional SDDC solutions. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-003 | Protect each Workspace ONE Access node by using vSphere High Availability. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-004 | When using two availability zones, add the Workspace ONE Access appliance to the primary availability zone VM group | VCF |
| SDDC-MGMT-IAM- VMO2DC1-005 | Place each region-specific Workspace ONE Access node in a dedicated VM folder for its region | VCF |
| SDDC-MGMT-IAM- VMO2DC1-006 | Configure a directory service connection, rainpole.io, for the Workspace ONE Access instance in each region. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-007 | Use Active Directory with Integrated Windows Authentication as the Directory Service connection option. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-008 | Use an account with the Account Operators role in Active Directory, VMO2DC1.rainpole\svc-domain-join, to perform domain join operations for the Workspace ONE Access connectors. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-009 | Use an account with the Domain Users role in Active Directory, to perform domain bind operations. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-010 | Configure the directory to synchronize only groups required for the integrated SDDC solutions. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-011 | Enable the synchronization of group members to the directory when a group is added to the Workspace ONE Access directory. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-012 | Enable Workspace ONE Access to synchronize nested group members by default. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-013 | Add a filter to the directory settings to exclude users from the directory replication | VCF |
| SDDC-MGMT-IAM- VMO2DC1-014 | Configure the mapped attributes included when a user is added to the Workspace ONE Access directory. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-015 | Configure the directory synchronization frequency to a reoccurring schedule, for example, 15 minutes. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-016 | Apply branding customizations for the Workspace ONE Access user interface that is presented to users when logging to the integrated SDDC solutions. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-017 | Place the Workspace ONE Access nodes for regional SDDC solutions on the existing region-specific virtual network segments, for Region A. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-018 | Allocate a statically assigned IP address and host name to the regional Workspace ONE Access appliance in the management domain. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-019 | Configure forward and reverse DNS records for each Workspace ONE Access appliance IP address for each regional instance. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-020 | Configure NTP for each Workspace ONE Access appliance. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-021 | Configure the region-specific Workspace ONE Access instance as the authentication provider for the NSX-T Managers in the region. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-022 | Assign roles to groups, synchronized from your corporate identity source for Workspace ONE Access. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-023 | Create a security group in your organization directory services for the Super Admin role, and synchronize the group in the Workspace ONE Access configuration. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-024 | Assign the enterprise group for super administrators, the Super Admins Workspace ONE Access role. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-025 | Create a security group in your organization directory services for the Directory Admin role, rainpole.io\ug- wsa-directory-admins, and synchronize the group in the Workspace ONE Access configuration. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-026 | Assign the enterprise group for directory administrator users,the Directory Admins Workspace ONE Access role. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-027 | Create a security group in your organization directory services for the ReadOnly Admin role, and synchronize the group in the Workspace ONE Access configuration. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-028 | Assign the enterprise group for read-only users, the ReadOnly Admin Workspace ONE Access role. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-029 | Rotate the appliance root user password on a schedule post deployment. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-030 | Rotate the appliance sshuser user password on a schedule post deployment. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-031 | Rotate the admin application user password on a schedule post deployment. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-032 | Configure a password policy for the Workspace ONE Access local directory admin user. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-033 | Replace the default self- signed certificates with a Certificate Authority-signed certificate during the deployment. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-034 | Import the certificate for the Root Certificate Authority to each Workspace ONE Access instance. | VCF |
| SDDC-MGMT-IAM- VMO2DC1-035 | Use a SHA-2 or higher algorithm when signing certificates. | VCF |

Table 25 - SDDC Design Decisions for Workspace ONE Access

# Base vmware Cloud operations

Cloud Operations

The architecture of the products of the cloud operations layer supports centralized monitoring of and logging data about the other solutions in the SDDC. You use this architecture to deliver core operational procedures in the data center.

In the operations management layer, the physical infrastructure, virtual infrastructure, and tenant workloads are monitored in real time, collecting the following information for intelligent and dynamic operational management:

Monitoring data, such as structured (metrics) and unstructured (logs) data

Topology data, such as physical and virtual compute, networking, and storage objects

## VMware Life Cycle Architecture

VMware vRealize Suite Lifecycle Manager is used to automate the deployment, upgrade, and patching of the VMware vRealize products in this design.

Overview

In this design, the vRealize Suite Lifecycle Manager solution supports the deployment, upgrade, and patching of the following vRealize products:

* Workspace ONE Access
* vRealize Log Insight
* vRealize Operations
* vRealize Automation

vRealize Suite Lifecycle Manager is a preconfigured appliance distributed in Open Virtual Appliance (OVA) format. After the appliance deployment, you can access the vRealize Suite Lifecycle Manager services by using both the browser application user interface and the API.

After you deploy vRealize Suite Lifecycle Manager, you register one or more Management domain vCenter Server instances with it.

An administrator can automate life cycle operations for vRealize products. vRealize Suite Lifecycle Manager provides the following features for management of vRealize Suite products:

* Manage a product install, upgrade, and patch repository.
* Deploy products using supported topologies.
* Patch and upgrade product deployments.
* Scale-out product deployments.
* Support the import of existing product deployments.
* Organize product deployments in logical environments.
* Manage product certificates, licenses, and passwords.
* Manage and deploy Marketplace content across vRealize solutions.

Architecture

vRealize Suite Lifecycle Manager contains the functional elements that collaborate to orchestrate the life cycle management operations of the vRealize Suite products in this validated design.



Figure 24 - Architecture of vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager contains modules for installation, upgrade and patching of vRealize Suite products in a vSphere environment. vRealize Suite Lifecycle Manager manages product binaries, downloads product content from VMware Marketplace, and integrates with Workspace ONE Access for a centralized identity and access management.

Authentication Models

You can configure vRealize Suite Lifecycle Manager user authentication to use the following authentication models:

* Local administrator account
* Workspace ONE Access

Marketplace Integration

By using vRealize Suite Lifecycle Manager, you can deploy additional vRealize Operations management packs, vRealize Log Insight content packs, and vRealize Automation blueprints and OVA files directly from the VMware Marketplace.

## Cloud Operations Design

The operations management design includes the software components that make up the operations management layer. The design provides guidance on the main elements of a product design such as deployment, sizing, networking, diagnostics, security, and integration with management solutions.



Figure 25 - Operations Management in SDDC

* Features of vRealize Suite Lifecycle Manager support initial installation and configuration of vRealize Suite products. Additional features support the life cycle management capabilities and configuration drift analysis for the vRealize Suite products.
* Monitoring operations support in vRealize Operations Manager and vRealize Log Insight provides performance, capacity management, and real-time logging of related physical and virtual infrastructure and cloud management components.

vRealize Suite Lifecycle Manager Design

vRealize Suite Lifecycle Manager provides life cycle management capabilities for vRealize components including automated deployment, configuration, patching, and upgrade as well as content management across vRealize Suite products

Logical Design for vRealize Suite Lifecycle Manager

vRealize Suite Lifecycle Manager provides life cycle management capabilities for vRealize Suite components and Workspace ONE Access. The life cycle management includes automated deployment, configuration, patching, and upgrade as well as content management across vRealize products.

You deploy vRealize Suite Lifecycle Manager as a cross-region appliance in Region A.

Logical Design

To orchestrate the deployment, patching, and upgrade of the vRealize products in the SDDC, vRealize Suite Lifecycle Manager communicates with the Management domain vCenter Server instance in the SDDC.



Figure 26 - Logical Design of vRealize Suite Lifecycle Manager

|  |  |
| --- | --- |
| Single Availability Zone | Multiple Availability Zones |
| * A single vRealize Suite Lifecycle Manager appliance deployed on the cross-region network segment. | * A single vRealize Suite Lifecycle Manager appliance deployed on the cross-region network segment. |
| * vSphere HA protects the vRealize Suite Lifecycle Manager appliance. | * vSphere HA protects the cross-region vRealize Suite Lifecycle Manager appliance. |
|  | * A DRS rule specifies that the vRealize Suite Lifecycle Manager appliance runs on an ESXi host in Availability Zone 1. |
| Life cycle management for:   * vRealize Log Insight * Cross-region Workspace ONE Access * vRealize Automation * vRealize Operations Manager analytics cluster * vRealize Operations Manager remote collectors | Life cycle management for:   * vRealize Log Insight * Cross-region Workspace ONE Access * vRealize Automation * vRealize Operations Manager analytics cluster * vRealize Operations Manager remote collectors |

Table 26 - vRealize Suite Lifecycle Manager Logical Components

vRealize Suite Lifecycle Manager operates with the following elements and components:

|  |  |
| --- | --- |
| Element | Components |
| Locker | * Passwords * Certificates * Licenses |
| Product Support | * Product binaries for install and upgrade (.ova, .pak, .iso) * Patch binaries * Product supports packs (.pspak) |
| Data Center | * Geographic location (optional) * vCenter Server instances |
| Environment | * Product deployments * Product import * Product operations, such as, scaling out, adding a license, and so on * Product health |
| My VMware | * Product entitlement * Product downloads * Product licensing |
| Marketplace | * My VMware account * Marketplace content download and compatibility * vRealize Log Insight content packs * vRealize Operations Manager management packs * vRealize Automation blueprints * vRealize Orchestrator workflow packages |

Table 27 - Elements and Components in vRealize Suite Lifecycle Manager

|  |  |
| --- | --- |
| D | ***Design Decision***  The following design decisions have been made for the VMO2DC1 solution. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-LCM-VCF-VMO2DC1-001 | In Region A, deploy a single vRealize Suite Lifecycle Manager instance on the first cluster in the management domain to manage the following management components: Cross-region vRealize Suite products, Cross-region Workspace ONE Access cluster, Regional vRealize Log Insight cluster. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-002 | Protect vRealize Suite Lifecycle Manager by using vSphere High Availability. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-003 | Deploy vRealize Suite Lifecycle Manager by using SDDC Manager. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-004 | When using two availability zones in Region A, add the vRealize Suite Lifecycle Manager appliance to the primary availability zone VM group | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-005 | Place the cross-region vRealize Suite Lifecycle Manager appliance in a dedicated virtual machine folder. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-006 | Increase the initial storage of the vRealize Suite Lifecycle Manager appliance by 100 GB. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-007 | Use SDDC Manager to perform the life cycle management of vRealize Suite Lifecycle Manager. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-008 | Configure the cross-region vRealize Suite Lifecycle Manager to send logs to the vRealize Log Insight cluster in Region A. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-009 | Communicate with vRealize Log Insight using the default Ingestion API (cfapi) port 9000 with ssl=no. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-010 | In Region A, place the vRealize Suite Lifecycle Manager appliance on the cross-region virtual network segment. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-011 | Allocate a statically assigned IP address and host name to the vRealize Suite Lifecycle Manager virtual appliance in the management domain. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-012 | Configure forward and reverse DNS records for the vRealize Suite Lifecycle Manager appliance. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-013 | Configure NTP on the vRealize Suite Lifecycle Manager appliance. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-014 | Upload and discover the vRealize Suite product binaries for install, patch, and upgrade binaries. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-015 | Create a data center object in vRealize Suite Lifecycle Manager for the cross-region SDDC solutions. Assign the Management domain vCenter Server instance to the data center. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-016 | Create a global environment in vRealize Suite Lifecycle Manager to support the deployment of Workspace ONE Access. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-017 | Create a cross-region environment in vRealize Suite Lifecycle Manager to support the deployment of: vRealize Operations Manager analytics cluster nodes, vRealize Operations remote collectors, vRealize Automation cluster nodes | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-018 | Create a region-specific environment in vRealize Suite Lifecycle Manager to support the deployment of: vRealize Log Insight cluster nodes | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-019 | Enable integration between vRealize Suite Lifecycle Manager in Region A and your corporate identity source by using the cross-region Workspace ONE Access instance. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-020 | Create a security group in your corporate directory services for the vRealize Suite Lifecycle Manager administrators, and synchronize the group in the Workspace ONE Access configuration for vRealize Suite Lifecycle Manager. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-021 | Assign the enterprise group for vRealize Suite Lifecycle Manager administrators, the LCM Cloud Admin role. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-022 | Create a security group in your corporate directory services for the vRealize Suite Lifecycle Manager content managers, and synchronize the group in the Workspace ONE Access configuration for vRealize Suite Lifecycle Manager. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-023 | Assign the enterprise group for vRealize Suite Lifecycle Manager content managers, the Content Release Manager role. The content management feature is out of scope for this design. However, this design accounts for the identity and access management controls for the feature. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-024 | Create a security group in your corporate directory services for the vRealize Suite Lifecycle Manager content developers, and synchronize the group in the Workspace ONE Access configuration for vRealize Suite Lifecycle Manager. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-025 | Assign the enterprise group for vRealize Suite Lifecycle Manager content developers, the Content Developer role. The content management feature is out of scope for this design. However, this design accounts for the identity and access management controls for the feature. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-026 | Define a custom vCenter Server role,vRealize Suite Lifecycle Manager to vSphere Integration, for vRealize Suite Lifecycle Manager that has the minimum privileges required to support the deployment and upgrade of vRealize Suite products in the design. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-027 | Configure a service account, in vCenter Server for application-to-application communication from vRealize Suite Lifecycle Manager to vSphere. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-028 | Assign global permissions for the vRealize Suite Lifecycle Manager to vSphere service account, in vCenter Server using the custom role, vRealize Suite Lifecycle Manager to vSphere Integration. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-029 | Use a dedicated My VMware account for vRealize Suite Lifecycle Manager instead of a named user account for the Marketplace integration. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-030 | Rotate the root password on or before 365 days post-deployment. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-031 | Use SDDC Manager to replace the default self-signed certificate of the virtual appliance of each vRealize Suite Lifecycle Manager instance with a CA-signed certificate. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-032 | Use a SHA-2 or higher algorithm when signing certificates | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-033 | Replace the default store passwords in the locker repository for use by life cycle operations. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-034 | Import Certificate Authority-signed certificates to the locker repository for product life cycle operations. | VCF |
| SDDC-MGMT-LCM-VCF- VMO2DC1-035 | Import vRealize Suite product licenses to the locker repository for product life cycle operations. | VCF |

Table 28 - SDDC vRealize Suite Lifecycle Manager Design Decisions

## Cloud Monitoring Architecture

vRealize Operations Manager tracks and analyzes the operation of multiple data sources in the SDDC by using specialized analytic algorithms. These algorithms help vRealize Operations Manager learn and predict the behavior of every object it monitors. Users access this information by using views, reports, and dashboards.

Architecture Overview

vRealize Operations Manager contains functional elements that collaborate for data analysis and storage, and support creating clusters of nodes with different roles.



Figure 27 - vRealize Operations Manager Architecture

Types of Nodes

For high availability and scalability, you can deploy several vRealize Operations Manager instances in a cluster to track, analyze, and predict the operation of monitored systems. Cluster nodes can have either of the following roles:

Master Node

Required initial node in the cluster. In large-scale environments, manages all other nodes. In small- scale environments, the master node is the single standalone vRealize Operations Manager node.

Master Replica Node

Optional. Enables high availability of the master node.

Data Node

Optional. Enables scale-out of vRealize Operations Manager in larger environments. Data nodes have adapters installed to perform data collection and analysis. Data nodes also host vRealize Operations Manager management packs.

Remote Collector Node

Overcomes data collection issues across the enterprise network, such as limited network performance. Remote collector nodes gather statistics about inventory objects and forward collected data to the data nodes. Remote collector nodes do not store data or perform analysis.

Types of Node Groups

Analytics Cluster

Tracks, analyzes, and predicts the operation of monitored systems. Consists of a master node, data nodes, and optionally of a master replica node.

Remote Collector Group

Consists of remote collector nodes. Only collects diagnostics data without storage or analysis. A vRealize Operations Manager deployment can contain several collector groups.

Use collector groups to achieve adapter resiliency in cases where the collector experiences network interruption or becomes unavailable.

Cloud Operations Design

The operations management design includes the software components that make up the operations management layer. The design provides guidance on the main elements of a product design such as deployment, sizing, networking, diagnostics, security, and integration with management solutions



Figure 28 - Operations Management in the SDDC

* Features of vRealize Suite Lifecycle Manager support initial installation and configuration of vRealize Suite products. Additional features support the life cycle management capabilities and configuration drift analysis for the vRealize Suite products.
* Monitoring operations support in vRealize Operations Manager and vRealize Log Insight provides performance, capacity management, and real-time logging of related physical and virtual infrastructure and cloud management components.

vRealize Operations Manager Design

The initial deployment of vRealize Operations Manager is a three-node analytics cluster, and a two-node remote collector group in the first region of the SDDC. The components run in the management domain.

Logical Design of vRealize Operations Manager

vRealize Operations Manager communicates with management components of the SDDC to collect metrics which are presented through various dashboards and views.



Figure 29 - Logical Design of vRealize Operations Manager

The vRealize Operations Manager logical components include an analytics cluster, remote collectors groups, and metric adapters.

The remote collectors ease scalability by performing the data collection from the region-specific applications, and periodically sending collected data to the analytics cluster. The remote collectors communicate directly with the data nodes in the vRealize Operations Manager analytics cluster.

Deployment Specification of vRealize Operations Manager

The deployment specification details the design decisions covering physical design and sizing for vRealize Operations Manager.

Deployment Model of vRealize Operations Manager

The analytics cluster of the vRealize Operations Manager deployment contains the nodes that analyze and store data from the monitored components. You deploy a configuration of the analytics cluster that satisfies the requirements for monitoring the number of virtual machines in the design objectives of this design.

Deployment Type

Deploy a three-node vRealize Operations Manager analytics cluster in the cross-region application virtual network. The analytics cluster consists of one master node, one master replica node, and one data node to enable scale out and high availability.

In the design, you deploy the vRealize Operations Manager analytics cluster nodes on the first vSphere cluster in the management domain in Region A. You deploy the vRealize Operations Manager remote collector nodes on the first vSphere cluster in the management domain in the region. With this configuration, you can centrally manage monitoring across the entire SDDC.

You place the vRealize Operations Manager instance in Region A, on a specific virtual network segment. This provides a consistent deployment model for management applications, and supports growth to a dual-region design.

vRealize Operations Manager is distributed as a virtual appliance in OVA format.

To accomplish this design objective, you deploy or reuse the following components to deploy this operations management solution for the SDDC:

* Cross-region vRealize Suite Lifecycle Manager
* NSX-T Load Balancer for vRealize Operations Manager
* Cross-region Workspace ONE Access cluster
* Supporting infrastructure services, such as Active Directory, DNS, and NTP.

Sizing Compute and Storage Resources

You size resources for vRealize Operations Manager to provide enough resources to accommodate the analytics operations for monitoring the SDDC and the expected number of virtual machines in the SDDC.

You allocate storage capacity for analytics data collected from the management products and from the number of tenant virtual machines that are defined in the objectives of this SDDC design.

Life Cycle Management Design for vRealize Operations Manager

Life cycle management design details the design decisions covering the life cycle management of vRealize Operations Manager.

Life cycle management of vRealize Operations Manager involves the process of performing patch updates or upgrades to the vRealize Operations Manager analytics cluster and remote collector nodes.

In this design, life cycle management is performed by using vRealize Suite Lifecycle Manager.

Logging Design for vRealize Operations Manager

You integrate vRealize Operations Manager with vRealize Log Insight to provide operational visibility.

The native integration to vRealize Log Insight from vRealize Operations provides the ability to send logs for aggregation and analysis, as needed.

Logging to a vRealize Log Insight instance through the ingestion API is established by updated in the appliance settings in the vRealize Operations Manager user interface or by updating the vRealize Log Insight

Notifications Design for vRealize Operations Manager

You configure notifications in vRealize Operations Manager to send event messages to the user. You configure a Standard Email Plug-In to deliver outbound SMTP messages to users about system events.

Data Protection and Backup Design for vRealize Operations Manager

To preserve the cloud operations services functionality when data or system loss occurs, the design supports the use of data protection. vRealize Operations Manager supports data protection through the creation of consistent image-level backups by using backup software that is based on the vSphere Storage APIs - Data Protection (VADP).

Network Design for vRealize Operations Manager

For secure access to the UI and API of vRealize Operations Manager, you place the appliance on the shared cross-region virtual network segment. This network design also supports public access to the analytics cluster nodes.

Virtual Network Segments

For secure access, load balancing, and to support future growth to a dual-region design, you deploy the vRealize Operations Manager analytics cluster on the shared cross-region virtual network segment, and you place the remote collector groups on the region-specific virtual network segments.

This network design has the following features:

* The vRealize Operations Manager analytics cluster is deployed on the same network as the cross- region Workspace ONE Access, vRealize Automation, and vRealize Suite Lifecycle Manager to provide a consistent deployment model for management applications.
* The vRealize Operations Manager remote collector groups are deployed together on the same network in each region. This configuration ensures collection of metrics locally per region if there is a cross-region network outage. Using the region-specific virtual network segment co-locates metric collection with the region-specific applications.
* vRealize Operations Manager has routed access to the VLAN-backed management network through the NSX-T Data Center Tier-0 Gateway.
* Routing to the VLAN-management network, virtual network segments, and external networks is dynamic and is based on the Border Gateway Protocol (BGP).



Figure 30 - Network Design of the vRealize Operations Manager Deployment

IP Addressing

Allocate a statically assigned IP address and host name from the cross-region network segment to the vRealize Operations Manager analytics cluster virtual appliances, and a statically assigned IP address and host name from the region-specific network segment to the vRealize Operations Manager remote collector virtual appliances.

Name Resolution

The FQDNs of the vRealize Operations Manager nodes follow a certain domain name resolution:

* The IP addresses of the analytics cluster nodes and a load balancer virtual IP address (VIP) are associated with names whose suffix is set to the root domain.

From the public network, users access vRealize Operations Manager by using the VIP address, the traffic to which is handled by an NSX-T Data Center Tier-0 gateway providing the load balancer services.

Load Balancing

A vRealize Operations Manager cluster deployment requires a load balancer to manage connections to vRealize Operations Manager. The design uses load-balancing services provided by NSX-T Data Center in the management domain.

Time Synchronization

Time synchronization provided by the Network Time Protocol (NTP) is important to ensure that all components within the SDDC are synchronized to the same time source. Configure the vRealize Operations Manager nodes with time synchronization using an internal NTP time source.

Monitoring and Alerting Design in vRealize Operations Manager

You use vRealize Operations Manager to monitor the state of the management components in the SDDC by using dashboards. You can use the self-monitoring capability of vRealize Operations Manager to receive alerts about issues that are related to its operational state. You connect vRealize Operations Manager with the management components in the SDDC by using cloud accounts, management pack adapters, and direct integrations.

In this design, vRealize Operations Manager monitors the following components:

* vCenter Server
* vSAN
* NSX-T Data Center
* Storage devices
* Workspace ONE Access (region-specific and cross-region)
* vRealize Log Insight
* vRealize Automation

Cloud Accounts

You use cloud accounts to add cloud endpoints as adapter instances to enable vRealize Operations Manager to communicate with them. vRealize Operations Manager can collect data from the following private and public cloud accounts:

Direct Integrations

vRealize Operations Manager includes direct integration with vRealize Automation and vRealize Log Insight. These integrations provide the following functionality:

|  |  |
| --- | --- |
| Integration | Description |
| vRealize Automation | * Ability to share common constructs such as cloud accounts, cloud zones, and projects across vRealize Operations Manager and vRealize Automation. * Ability to understand deployment cost: * Evaluate upfront costs on vRealize Automation. * Monitor ongoing costs per virtual machine, deployment, or project. |
| vRealize Log Insight | * Enables Logs tab in vRealize Operations Manager * Enables Troubleshoot with Logs dashboard * Enables vRealize Log Insight launch in context from vRealize Operations Manager |

Table 29 - vRealize Operations Manager Direct Integrations

Management Packs

You install and activate management packs for vRealize Operations Manager to enable collecting data from or sending data to the target system.

Information Security and Access Control Design for vRealize Operations Manager

You protect the vRealize Operations Manager deployment by configuring authentication and secure communication with the other components in the SDDC. A dedicated service account is assigned a custom role for communication between vRealize Operations Manager and the management solutions in the data center.

Identity Management Design for vRealize Operations Manager

You manage access to vRealize Operations Manager by assigning users and groups, synchronized to Workspace ONE Access, to vRealize Operations Manager roles.

Service Accounts Design for vRealize Operations Manager

You add and configure accounts associated with other solutions for activating the vRealize Operations Manager cloud accounts, management packs, and direct integrations.

Password Management Design for vRealize Operations Management

To ensure continued access to the vRealize Operations Manager appliances you must rotate the appliance root password on or before 365 days post deployment.

Certificate Management Design for vRealize Operations Manager

Access to all vRealize Operations Manager Web interfaces requires an SSL connection. By default, vRealize Operations Manager uses a self-signed certificate. To provide secure access to the vRealize Operations Manager user interface, replace the default self-signed certificate with a CA-signed certificate.

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 VROP’s design will use the following design decisions. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-VROP-VCF-VMO2DC1-001 | Deploy vRealize Operations Manager as a cluster of three nodes - one master, one master replica, and one data node, on the first cluster in the management domain in Region A. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-002 | Deploy two remote collector nodes on the first cluster in the management domain in the region. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-003 | Use vRealize Suite Lifecycle Manager to deploy vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-004 | Protect all vRealize Operations Manager nodes by using vSphere High Availability. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-005 | Apply vSphere Distributed Resource Scheduler (DRS) anti-affinity rules to the vRealize Operations Manager analytics cluster. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-006 | Apply vSphere Distributed Resource Scheduler (DRS) anti-affinity rules to the vRealize Operations Manager remote collector group. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-007 | When using two availability zones in Region A, add the vRealize Operations Manager nodes to the primary availability zone VM group. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-008 | Place the cross-region vRealize Operations Manager nodes in a dedicated virtual machine folder in Region A | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-009 | Place the region-specific vRealize Operations Manager Remote Collector nodes in a dedicated virtual machine folder in Region A, | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-010 | Deploy each node in the analytics cluster as a medium-size appliance. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-011 | If the number of SDDC objects exceeds 12,500, add more medium-size nodes to the analytics cluster. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-012 | Increase the initial storage of each vRealize Operations Manager analytics cluster node by 1 TB. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-013 | Deploy each remote collector node as a standard-size appliance. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-014 | Use vRealize Suite Lifecycle Manager to perform the life cycle management of vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-015 | Configure vRealize Operations Manager to send logs to the vRealize Log Insight cluster in Region A. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-016 | Communicate with the vRealize Log Insight using the default Ingestion API (cfapi) port 9000 and ssl=no. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-017 | Configure vRealize Operations Manager to use an outbound SMTP mail server to route notifications for system events. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-018 | Configure the correct currency in the vRealize Operations Manager global options. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-019 | Place the vRealize Operations Manager analytics nodes on the cross-region virtual network segment | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-020 | Place the vRealize Operations Manager remote collector nodes on the region-specific virtual network segment | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-021 | Allocate a statically assigned IP address and host name from the cross-region network segment to the vRealize Operations Manager analytics cluster nodes in the management domain. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-022 | Allocate a statically assigned IP address and host name from the region-specific network segment to the vRealize Operations Manager remote collector nodes in the management domain. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-023 | Configure forward and reverse DNS records for all vRealize Operations Manager nodes and the VIP address. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-024 | Configure the small-size load balancer, that is created in NSX-T Data Center on a dedicated Tier-1 gateway in the management domain to load balance the cross-region Workspace ONE Access cluster, to load balance also the connections across the vRealize Operations Manager analytics cluster members. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-025 | Add an NSX-T load balancer monitor, vrops-https-monitor, for vRealize Operations Manager with an active HTTPS monitor on monitoring port 443. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-026 | Add an NSX-T Data Center load balancer server pool, vrops-server-pool, for vRealize Operations Manager to use the LEAST\_CONNECTION algorithm. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-027 | Add an NSX-T Data Center load balancer fast TCP application profile for vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-028 | Add an NSX-T Data Center load balancer source IP persistence profile for vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-029 | Add an NSX-T Data Center load balancer virtual server, vrops-https, for vRealize Operations Manager to use the L4 TCP type and port 443. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-030 | Add an NSX-T Data Center load balancer HTTP application profile, for vRealize Operations Manager to redirect HTTP to HTTPS. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-031 | Add another NSX-T Data Center load balancer virtual server, vrops-http-redirect, for vRealize Operations Manager HTTP to HTTPS redirection to use the L7 HTTP type and port 80 | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-032 | Do not use a load balancer for the vRealize Operations Manager remote collector nodes. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-033 | Configure NTP on each vRealize Operations Manager appliance. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-034 | Configure the timezone of vRealize Operations Manager to use UTC. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-035 | Configure a vCenter Server cloud account for each vCenter Server instance in the SDDC. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-036 | Configure each vCenter Server cloud account to use the remote collector group for its region. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-037 | Enable the vSAN integration in the vCenter Server cloud accounts. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-038 | Configure the vRealize Automation integration in vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-039 | Configure the vRealize Automation integration to use the default collector group. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-040 | Configure the vRealize Log Insight integration in vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-041 | Configure the vRealize Log Insight integration to use the remote collector group. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-042 | Install the Storage Devices management pack for vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-043 | Install the Workspace ONE Access management pack for vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-044 | Configure the following management pack adapter instances to use the remote collector group: NSX-T Data Center, Storage Devices, vSAN, Region-specific Workspace ONE Access | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-045 | Configure the cross-region Workspace ONE Access integration to use the default collector group. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-046 | Enable vRealize Operations Manager integration with your corporate identity source by using Workspace ONE Access. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-047 | Create a security group in your corporate directory services for the vRealize Operations Manager Administrator role, and synchronize the group in the Workspace ONE Access configuration for vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-048 | Assign the enterprise group for vRealize Operations Manager administrators, the Administrator role. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-049 | Create a security group in your corporate directory services for the vRealize Operations Manager ContentAdmin role synchronize the group in the Workspace ONE Access configuration for vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-050 | Assign the enterprise group for vRealize Operations Manager content administrators the ContentAdmin role. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-051 | Create a security group in your corporate directory services for the vRealize Operations Manager ReadOnly role, and synchronize the group in the Workspace ONE Access configuration for vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-052 | Assign the enterprise group for vRealize Operations Manager read-only users, the ReadOnly role. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-053 | Define a custom vCenter Server role for vRealize Operations Manager that has the minimum privileges required to support collecting metrics and performing actions against vSphere endpoints across the SDDC, vRealize Operations to vSphere Integration – Actions. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-054 | Configure a service account in vCenter Server with global permissions, for application-to-application communication from vRealize Operations Manager to vSphere and assign the actions custom role, vRealize Operations to vSphere Integration – Actions. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-055 | Configure each vCenter Server cloud account to use the vCenter Server service account | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-056 | Define a custom vCenter Server role for vRealize Operations Manager that has the minimum privileges required to support collecting metrics from vSphere endpoints across the SDDC,vRealize Operations to vSphere Integration – Metrics | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-057 | Configure a service account in vCenter Server with global permissions, for application-to-application communication from the vSAN adapters in vRealize Operations Manager to vSphere, assign the metrics custom role, vRealize Operations to vSphere Integration – Metrics. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-058 | Configure the vSAN integration in the vCenter Server cloud account to use the vSAN service account | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-059 | Create a service in the directory services and ensure it is synchronized in Workspace ONE Access. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-060 | Assign the service account, Organization Owner organization role and Cloud Assembly Administrator service role for the application-to-application communication from vRealize Operations to vRealize Automation. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-061 | Create a service in the directory services and ensure it is synchronized in Workspace ONE Access. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-062 | Configure a service account in NSX-T Data Center for application-to-application communication from vRealize Operations Manager to NSX-T Data Center using the default NSX-T Data Center Enterprise Admins role. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-063 | Configure the endpoint of the NSX-T management pack for vRealize Operations Manager | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-064 | Configure a service account in vCenter Server with global permissions, for application-to-application communication from the storage devices adapters in vRealize Operations Manager to vSphere and assign the metrics custom role, vRealize Operations to vSphere Integration – Metrics. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-065 | Configure the endpoint of the Storage Devices management pack for vRealize Operations Manager to use the Storage Devices service account | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-066 | Configure a Workspace ONE Access management pack adapter instance for each Workspace ONE Access instance using the local system domain admin account. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-067 | Rotate the root password on or before 365 days post deployment | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-068 | Rotate the admin password on or before 60 days post deployment | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-069 | Use a CA-signed certificate containing the analytics and remote collector nodes in the SAN attributes, when deploying vRealize Operations Manager. | VCF |
| SDDC-MGMT-VROP-VCF- VMO2DC1-070 | Use a SHA-2 or higher algorithm when signing certificates. | VCF |

Table 30 - SDDC Design Decisions for vRealize Operations Manager

## Logging Architecture

vRealize Log Insight provides real-time log management and log analysis with machine learning-based intelligent grouping, high-performance searching, and troubleshooting across physical, virtual, and cloud environments.

Overview

vRealize Log Insight collects data from ESXi hosts by using the syslog protocol. vRealize Log Insight has the following capabilities:

* Connects to other VMware products, such as vCenter Server, to collect events, tasks, and alarm data.
* Integrates with vRealize Operations Manager to send notification events and enable launch in context.
* Functions as a collection and analysis point for any system that is capable of sending syslog data.

To collect additional logs, you can install an ingestion agent on Linux or Windows servers, or you can use the preinstalled agent on certain VMware products. Preinstalled agents are useful for custom application logs and operating systems that do not natively support the syslog protocol, such as Windows.

Architecture

The architecture of vRealize Log Insight in the SDDC enables several channels for the collection of log messages.



Figure 31 - Architecture of vRealize Log Insight

vRealize Log Insight clients connect to the Load Balancer (ILB) FQDN, and use the syslog or the Ingestion API via the vRealize Log Insight agent to send logs to vRealize Log Insight. Users and administrators interact with the ingested logs by using the user interface or the API.

By default, vRealize Log Insight collects data from vCenter Server systems and ESXi hosts. For analyzing forwarded logs from other components, such as NSX Data Center, use content packs. Content packs contain extensions or provide integration with other systems in the SDDC.

Types of Nodes

For functionality, high availability, and scalability, vRealize Log Insight supports the following types of nodes which have inherent roles:

Master Node

Required initial node in the cluster. In standalone mode, the master node is responsible for all activities, including queries and log ingestion. The master node also handles operations that are related to the life cycle of a cluster, such as performing upgrades and addition or removal of worker nodes. In a scaled-out and highly available environment, the master node still performs life cycle operations, such as addition or removal of worker nodes. However, it functions as a generic worker about queries and log ingestion activities.

The master node stores logs locally. If the master node is down, the logs stored on it become unavailable.

Worker Node

Optional. This component enables a scale-out growth in larger environments. As you add and configure more worker nodes in a vRealize Log Insight cluster for high availability (HA), queries and log ingestion activities are delegated to all available nodes. You must have at least two worker nodes to form a cluster with the master node. The worker node stores logs locally. If any of the worker nodes is down, the logs on the worker become unavailable.

Integrated Load Balancer (ILB)

In cluster mode, the ILB is the centralized entry point which ensures that vRealize Log Insight accepts incoming ingestion traffic. As nodes are added to the vRealize Log Insight instance to form a cluster, the ILB feature simplifies the configuration for high availability. The ILB balances the incoming traffic fairly among the available vRealize Log Insight nodes.

The ILB runs on one of the cluster nodes at all times. In environments that contain several nodes, an election process determines the leader of the cluster. Periodically, the ILB performs a health check to determine whether re-election is required. If the node that hosts the ILB Virtual IP (VIP) address stops responding, the VIP address is failed over to another node in the cluster using an election process.

All queries against data are directed to the ILB. The ILB delegates queries to a query master for the duration of the query. The query master queries all nodes, both master and worker nodes, for data and then sends the aggregated data back to the client.

Use the ILB for administrative activities unless you are performing administrative activities on individual nodes. The Web user interface of the ILB presents data from the master and from the worker nodes in a scaled-out cluster in a unified display (single pane of glass).

Cloud Operations Design

The operations management design includes the software components that make up the operations management layer. The design provides guidance on the main elements of a product design such as deployment, sizing, networking, diagnostics, security, and integration with management solutions.



Figure 32 - Operations Management in the SDDC

* Features of vRealize Suite Lifecycle Manager support initial installation and configuration of vRealize Suite products. Additional features support the life cycle management capabilities and configuration drift analysis for the vRealize Suite products.
* Monitoring operations support in vRealize Operations Manager and vRealize Log Insight provides performance, capacity management, and real-time logging of related physical and virtual infrastructure and cloud management components.

vRealize Log Insight Design

vRealize Log Insight design enables real-time logging for all components that build up the management capabilities of the SDDC.

Logical Design of vRealize Log Insight

Deploy a vRealize Log Insight cluster that consists of three nodes, in the first vSphere cluster of the management domain in the region. This configuration provides continued availability and increased log ingestion rates.

vRealize Log Insight collects logs to provide monitoring information about the SDDC from a central location.



Figure 33 - Logical Design of vRealize Log Insight

Deployment Specification of vRealize Log Insight

The deployment specification details the design decisions covering physical design and sizing for vRealize Log Insight.

Deployment Model of vRealize Log Insight

The vRealize Log Insight cluster consists of one master node and two worker nodes behind a load balancer.

Deployment Type

You enable the integrated load balancer (ILB) on the three-node cluster so that all log sources can access the cluster by its ILB. When using the ILB, if there is a scale-out, it is not necessary to reconfigure all log sources with a new destination address. Using the ILB also guarantees that vRealize Log Insight accepts all incoming ingestion traffic.

vRealize Log Insight users accessing the Web user interface or API, and clients ingesting logs using syslog or the Ingestion API, connect to vRealize Log Insight by using the ILB address.

For isolation, you place the vRealize Log Insight on a specific virtual network segment.

In the design, you deploy the vRealize Log Insight nodes on the first vSphere cluster in the management domain in each region.

To accomplish the design objective of this design, you deploy or reuse the following components to deploy this operations management solution for the SDDC:

* Cross-region vRealize Suite Lifecycle Manager
* Region-specific Workspace ONE Access
* Supporting infrastructure services, such as Active Directory, DNS, and NTP.

Sizing Compute and Storage Resources

To provide enough resources to accommodate the logging operations of the management components of the SDDC, you size resources for vRealize Log Insight .

To accommodate log data from the products in the SDDC, you must correctly size the compute resources and storage for the Log Insight nodes.

By default, the vRealize Log Insight appliance uses the predefined values for medium configurations.

To collect and store log data from the SDDC management components and tenant workloads according to the objectives of this design, select the appropriate size for the vRealize Log Insight nodes.

Life Cycle Management Design for vRealize Log Insight

Life cycle management design details the design decisions covering the life cycle management of vRealize Log Insight.

Life cycle management of vRealize Log Insight involves the process of performing patch updates or upgrades to the vRealize Log Insight cluster.

Retention and Archiving Design for vRealize Log Insight

Configure archive and retention parameters of vRealize Log Insight according to the company policy for compliance and governance.

Each vRealize Log Insight appliance has three default virtual disks and can use more virtual disks for storage.

Alert Notifications Design for vRealize Log Insight

vRealize Log Insight supports alerts that trigger notifications about its health and about the health of monitored solutions.

Integration of vRealize Log Insight with vRealize Operations Manager

vRealize Log Insight supports integration with vRealize Operations Manager to provide a central location for monitoring and diagnostics.

Data Protection and Backup Design for vRealize Log Insight

To preserve the cloud operations services functionality when data or system loss occurs, the design supports the use of data protection.

vRealize Log Insight supports data protection through the creation of consistent image-level backups, using backup software that is based on the vSphere Storage APIs - Data Protection (VADP).

Network Design of vRealize Log Insight

In each region, for isolation and colocation with logging sources, the vRealize Log Insight nodes are connected to the region-specific virtual network segments. The network design also supports public access to the vRealize Log Insight cluster.

Virtual Network Segments

For collection of logs locally in the region, the vRealize Log Insight nodes are connected to the region- specific virtual network segment.

This network design has the following features:

* The vRealize Log Insight cluster nodes are deployed together on the same network in the region. It also co-locates log collection with the region-specific applications using the region-specific virtual network segment.
* vRealize Log Insight has routed access to the VLAN-backed management network through the NSX- T Data Center Tier-0 gateway.
* Routing to the VLAN management network, virtual network segments, and external networks are dynamic and are based on the Border Gateway Protocol (BGP).



Figure 34 - Network Design of the vRealize Log Insight Deployment

IP Addressing Scheme

Allocate a statically assigned IP address and host name from the region-specific network segment to the vRealize Log Insight virtual appliances.

Name Resolution

vRealize Log Insight node name resolution, including the integrated load balancer virtual IP addresses (VIP), use a region-specific suffix

Load Balancing

A vRealize Log Insight cluster deployment requires a load balancer to manage connections to vRealize Log Insight. The design uses the vRealize Log Insight integrated load balancer (ILB).

Time Synchronization

Time synchronization provided by the Network Time Protocol (NTP) is important to ensure that all components within the SDDC are synchronized to the same time source. Configure time synchronization using an internal NTP time source across all vRealize Log Insight nodes.

Logging Design for vRealize Log Insight

Use content packs to have the logs generated from the management components in the SDDC retrieved, extracted, and parsed into a human-readable format. vRealize Log Insight saves log queries and alerts, and you can use dashboards for efficient monitoring. On the logging clients, you configure syslog and vRealize Log Insight agents.

Logging Sources

Client applications can send logs to vRealize Log Insight in one of the following ways:

* Directly to vRealize Log Insight using the syslog TCP, syslog TCP over TLS/SSL, or syslog UDP protocols
* By using a vRealize Log Insight agent
* By using vRealize Log Insight to query directly the vSphere Web Server APIs
* By using a vRealize Log Insight user interface.

Information Security and Access Control Design for vRealize Log Insight

You protect the vRealize Log Insight deployment by configuring the authentication and secure communication with the other components in the SDDC. A dedicated service account is assigned a custom role for communication between vRealize Log Insight and the management solutions in the data center.

Identity Management Design for vRealize Log Insight

You enable authentication using Workspace ONE Access to ensure accountability on user access. You can grant both users and groups access to vRealize Log Insight to perform tasks, such as analyzing logs and viewing dashboards.

Service Accounts for vRealize Log Insight

You add and configure an account associated with vRealize Operations Manager for integration with vRealize Log Insight. You add and configure an account associated with vCenter Server for ingestion by vRealize Log Insight.

Password Management for vRealize Log Insight

To ensure continued access to the vRealize Log Insight appliances you must rotate the appliance root password on or before 365 days post deployment.

Certificate Design for vRealize Log Insight

Access to the vRealize Log Insight user interface and API require an SSL connection. By default, vRealize Log Insight uses a self-signed certificate. To provide secure access to the vRealize Log Insight user interface, replace the default self-signed certificate with a CA-signed certificate.

|  |  |
| --- | --- |
| D | ***Design Decision***  The VMO2DC1 VRLI design will use the following design decisions. |

|  |  |  |
| --- | --- | --- |
| Design Decision ID | Design Decision Description | Applicable to Architecture Model |
| SDDC-MGMT-VRLI-VCF-VMO2DC1-001 | Deploy vRealize Log Insight in a cluster configuration of three nodes with an integrated load balancer: one master and two worker nodes, on the first cluster in the management domain. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-002 | Deploy vRealize Log Insight by using vRealize Suite Lifecycle Manager. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-003 | Protect all vRealize Log Insight nodes by using vSphere High Availability. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-004 | Apply vSphere Distributed Resource Scheduler (DRS) anti-affinity rules to the vRealize Log Insight cluster nodes. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-005 | When using two availability zones in Region A, add the vRealize Log Insight nodes to the primary availability zone VM group | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-006 | Place the region-specific vRealize Log Insight nodes in a dedicated virtual machine folder in Region A, | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-007 | Deploy each node in the vRealize Log Insight cluster as a medium-size appliance. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-008 | Use vRealize Suite Lifecycle Manager to perform the lifecycle management of vRealize Log Insight. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-009 | Configure a retention period of 7 days for the medium-size vRealize Log Insight appliance. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-010 | Provide a minimum of 400 GB of NFS version 3 shared storage to the vRealize Log Insight cluster in each region. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-011 | Enable alert notifications. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-012 | Forward alerts to vRealize Operations Manager. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-013 | Support launch in context with vRealize Operation Manager. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-014 | Enable embedded vRealize Log Insight user interface in vRealize Operations Manager. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-015 | Place the vRealize Log Insight nodes on the region-specific virtual network segment | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-016 | Allocate statically assigned IP addresses and host names to the vRealize Log Insight nodes in the management domain. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-017 | Configure forward and reverse DNS records for all vRealize Log Insight nodes and the ILB VIP address. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-018 | Enable the vRealize Log Insight Integrated Load Balancer (ILB) for balancing incoming. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-019 | Configure NTP on each vRealize Log Insight appliance | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-020 | Install the following content packs: VMware – Linux, VMware - Linux Systemd, NSX-T Data Center | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-021 | Configure the following agent groups that are related to content packs: SDDC - Linux OS, SDDC - Photon OS | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-022 | Install and configure the vRealize Log Insight agent on each Workspace ONE Access node to send logs to a vRealize Log Insight cluster. For the region-specific Workspace ONE Access instance, use the vRealize Log Insight agent from the corresponding regional vRealize Log Insight cluster. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-023 | Configure the SDDC - Linux OS agent group in each vRealize Log Insight cluster to include all Workspace ONE Access nodes. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-024 | Configure syslog sources and vRealize Log Insight agents to send log data directly to the virtual IP (VIP) address of the vRealize Log Insight integrated load balancer (ILB). | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-025 | Configure all vCenter Server instances as direct syslog sources to send log data directly to vRealize Log Insight. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-026 | Configure the vRealize Log Insight agent on the SDDC Manager appliance. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-027 | Configure the vRealize Log Insight agent on the vRealize Suite Lifecycle Manager appliance. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-028 | Configure the Fluentd vRealize Log Insight plugin on the vRealize Automation appliance instances. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-029 | Configure the vRealize Log Insight agent for the vRealize Operations Manager appliances including: Analytics nodes, Remote Collector instances | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-030 | Configure the NSX-T Data Center components as direct syslog sources for vRealize Log Insight including: NSX-T Manager instances, NSX Edge Cluster Instances | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-031 | Communicate with the syslog clients, such as ESXi, vCenter Server, NSX-T Data Center, using the TCP protocol. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-032 | Do not configure vRealize Log Insight to update automatically all deployed agents. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-033 | Enable vRealize Log Insight integration with your corporate identity source by using the region-specific Workspace ONE Access instances. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-034 | Create a security group in your corporate directory services for the vRealize Log Insight administrators and synchronize the group in the Workspace ONE Access configuration for vRealize Log Insight. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-035 | Assign the enterprise group for vRealize Log Insight administrators the Super Admin role. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-036 | Create a security group in your corporate directory services for the vRealize Log Insight users synchronize the group in the Workspace ONE Access configuration for vRealize Log Insight. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-037 | Assign the enterprise group for vRealize Log Insight users the User role. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-038 | Create a security group in your corporate directory services for the vRealize Log Insight viewers and synchronize the group in the Workspace ONE Access configuration for vRealize Log Insight. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-039 | Assign the enterprise group for vRealize Log Insight viewers the View Only Admin role. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-040 | In vRealize Operations Manager, add an application-to-application service account from Workspace ONE Access, for vRealize Log Insight Integration. Assign this user the default Administrator role | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-041 | Enable vRealize Operations Manager integration in vRealize Log Insight using the vRealize Operations Manager service account | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-042 | Define a custom vCenter Server role for vRealize Log Insight that has the minimum privileges required to support collecting logs from vSphere endpoints across the SDDC, vRealize Log Insight to vSphere Integration. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-043 | Configure a service account in vCenter Server with global permissions, for application-to-application communication from vRealize Log Insight to vSphere and assign the custom role, vRealize Log Insight to vSphere Integration. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-044 | Configure vRealize Log Insight to ingest events, tasks, and alarms from the Management domain vCenter Server and from the Workload domain vCenter Server by using the vRealize Log Insight service account | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-045 | Rotate the root password on or before 365 days post deployment. | VCF |
| SDDC-MGMT-VRLI-VCF- VMO2DC1-046 | Use a CA-signed certificate containing the vRealize Log Insight cluster node FQDNs, and the ILB FQDN in the SAN attributes, when deploying vRealize Log Insight. | VCF |
| SDDC-MGMT-VRLI-VCF-BAG-047 | Use a SHA-2 or higher algorithm when signing certificates. | VCF |

Table 31 - SDDC Design Decisions for vRealize Log Insight

# Appendix