ICEDDE-23484 - Wootton Basset -IT Cloud 2.5 VCF/SDDC Infrastructure Design

Infrastructure & Network Design

Version 0.1

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

DOCUMENT INFORMATION

Author(s)	David Dawson
Reference	ICEDDE-23484
Publication date	16/6/2023
Classification	Internal
Valid until date	All designs are only valid for 6 months after latest version.

DOCUMENT CONTROL

Version	Date	Author	Comments
0.1	16/6/2023	David Dawson	Initial draft
1.0	25/09/2023	David Dawson	Document Approved. ICEDDE-23484 - Wootton Basset -IT Cl

DOCUMENT IMPACT ON ICED DELIVERY

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

COMPLIANCE & GOVERNANCE

ISO/CAS(T)	SOX	GDPR	PCI

DOCUMENT REFERENCES

Reference	Title	Version
REF001		
REF002		

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 (GSEB) must be engaged by the project for advice.

EXECUTIVE SUMMARY

Virgin Media O2 have an initiative to extend their Software Defined Datacentre (IT Cloud v2.5) in Knowsley and Baguley and build new Software Defined Datacentres in Wootton Basset, Marlow and Slough - the IT Cloud v2.5 will be utilise a Cisco physical network underlay combined with VMWare NSX-T providing the networking and compute virtualisation.
The IT Cloud v2.5 will have its own physical border firewall and its own network links/routing into the various Virgin Media, Virgin Media Business and O2 Corp networks.

Each of the datacentres will have it's own design specific to that site.

DOCUMENT PURPOSE

The purpose of this document is to give the Virgin Media O2 build and operational teams the information required to support the Virgin Media O2 SDDCv2.5.5 solutions in the various locations. It will also outline the Architectural decisions made.

DOCUMENT STRUCTURE

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

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.

	***Outstanding Decision*** This indicates an outstanding decision that must be made.

1 BACKGROUND

In order for Virgin Media O2 to deploy a new SDDCv2.5 in Wootton Basset they will need to deploy VMware Cloud Foundation (VCF) or the components required for this and VMware vRealize Cloud components. This new SDDCv2.5 will be built on HPe DL380 hardware and the technology will be housed in the datacentre in Wooton Basset.

Once the hardware is built VMware Virtual Cloud Foundation (VCF) will be deployed onto it, this will include the following VCF components:

- VMWare vSphere ESX
- VMware vCenter
- VMware SDDC Manger
- VMware NSX-T Datacenter
- VMWare vSAN – Management Domain Only
- VMware vRealize Lifecycle Manager
- VMware vRealize Log Insight
- VMware vRealize Operations Manager
- VMware vRealize Network Insight
- VMware Hybrid Connect (HCX) – Optional
- VMware NSX Advanced Load Balancer (AVI)

	***Design Decision*** This design will only cover the VMware VCF, Cloud components and Pure Storage, build and deployment, an additional design document may be required for the HPE hardware design.

1.1 In Scope

The following items are in scope.

In Scope items

ID	In Scope Items
IS.001	VMWare vSphere ESX
IS.002	VMware vCenter
IS.003	VMware SDDC Manger
IS.004	VMware NSX-T Datacenter
IS.005	VMWare vSAN – Management Domain Only
IS.006	VMware vRealize Lifecycle Manager
IS.007	VMware vRealize Log Insight
IS.008	VMware vRealize Operations Manager
IS.009	VMware NSX Advanced Load Balancer (AVI)
IS.010	VMware vRealize Network Insight
IS.012	VMware Hybrid Connect (HCX)
IS.013	HPE Storage Design (Pure Storage)

Table 1 - In Scope Items

*The VMware Automation and Orchestration designs will be provided by the Automation team.

A Support Model

ID	In Scope Items
IS.014	Support for User access to the new platform

Table 2 - In Scope Support Model

1.2 Out of Scope

The following items are out of scope for this design.

ID	Out of Scope Items

OS.001	HPE Hardware Design
OS.002	VMware vRealize Automation Design
OS.003	Any Required Foundation Designs for the site.
OS.004	Network Rack designs

Table 3 - Out of Scope Items

Important Note

DCT and TCS will be responsible for the support of the physical and Virtual infrastructure.

2 REQUIREMENTS AND RAID

Captured/extrapolated Non-Functional Requirements and statements of design compliance/non-compliance.

NOTE – The Business and Non Functional requirements are based on the original SDDC ones.

2.1 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, that will be provided by the automation team.
	Service	IaaS	The solution must be accessible by both Telefonica & Virgin Media.		
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 NSX-T T0 gateways will provide access to the internal via Proxy servers within the solution
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 is a requirement to use the

					automation solution that Telco cloud uses.
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, that will be provided by the automation team.
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, that will be provided by the automation team.
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	This solution from a day one point of view is for private cloud only
BR.009	Technology	Inventory	The solution must maintain / integrate an inventory and resource lifecycle for provisioned, VMO2-managed cloud services.	Required for CRuD functionality	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.
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 solution (ie. provisioning, cost management, monitoring, etc.) should be highly available. RPO and RTO to be defined in tech requirements	Clear business requirement	SDDC-MGMT-PHY-VMO2 SDDCV2.5 WOOTON BASSET-005
BR.012	Service	Self-service & tenancy	The solution should provide a web-based IaaS provisioning portal and API layer, supporting multi-tenancy for various 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	VMB isn't inscope for this initial deployment.
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, network connectivity permitting.
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	The Pure Storage solution can offer all these capabilities.
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	This solution design is for Wootton Basset only but eventually we will have SDDC infrastructure deployed in 5 VMO2 sites.
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	The solution will use the site specific backup solution for the site it is deployed onto. See section 6.2 for more details.
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	Still outstanding

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 4 - Business Requirements

2.2 Technical Requirements

Functional Requirements

Technical ID	Category	Type	Requirement Description	Design Decision Comment	Requirement Satisfied
FTR.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.	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.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	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	

			should not require manual steps to be performed prior to being "customer ready"		
FTR.003	Functional	Provisioning and Orchestration	Solution should be capable of providing multi-component catalogue items (eg. LAMP stack + NLBs)	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.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	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.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	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.006	Functional	Provisioning and Orchestration	IaaS portal should have options to select quantity of desired product (eg. 4x web servers)	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.007	Functional	Provisioning and Orchestration	Solution should have an IaaS portal to act as a central point to enable self-service	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.008	Functional	Provisioning and Orchestration	Solution should allow uptime scheduling of deployed resources to enable efficient resource utilisation (eg. Users can Start/stop	The Automation of the solution is provided in a separate design	

			virtual machines when not in use - for example test environments outside of work hours)	document, that will be provided by the automation team.	
FTR.009	Functional	Provisioning and Orchestration	Solution should be able to integrate with other future automation tools. Ie. should have an open API for integration	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.010	Functional	Provisioning and Orchestration	ESX Hosts within the same cluster will be spread across multiple racks	SDDC-MGMT-PHY-VMO2 SDDCV2.5 WOOTON BASSET-001 - 004	
FTR.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.	
FTR.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.	
FTR.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.	
FTR.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.	
FTR.015	Functional	Architecture	Solution must support a minimum of two separate NSX instances per region. One instance is tied to the Management vCenter	This will be achieved when the first compute vCenter Server is deployed.	

			Server, and the other instance is tied to the Compute vCenter Server		
FTR.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.	
FTR.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.	
FTR.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.	
FTR.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.	
FTR.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.	
FTR.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	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	

			components such as Apache, httpd or tomcat		
FTR.022	Functional	Cost management and resource optimization	Solution should have a basic cost breakdown for each area requested in the service request		
FTR.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.	
FTR.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.	
FTR.025	Functional	Feature	All ESX hosts must boot from local storage (Drives or SSD cards)	Each ESXi server will boot from local storage.	
FTR.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.	
FTR.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.	
FTR.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.	
FTR.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.	

FTR.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.	
FTR.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.	
FTR.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.	
FTR.033	Functional	Feature	Replace the vCenter Server 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.	
FTR.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.	
FTR.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.	
FTR.036	Functional	Feature	The solution must allow workloads to automatically be enrolled in to PAM as part of the provisioning process	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.037	Functional	Feature	The solution must allow workloads to automatically be added to Antivirus monitoring as part of the provisioning process	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	

FTR.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)	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.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	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
FTR.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.	
FTR.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.	
FTR.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.	
FTR.043	Functional	Networking	The solution must segment connectivity to underlay network functions using VLANs	This will be done as part of the deployment of NSX within both the management and workload Domains.	
FTR.044	Functional	Networking	Support assignment of static IP addresses to all management components in the SDDC	This will be done as part of the deployment of NSX within both	

			infrastructure except for NSX VTEPs which can be DHCP assigned	the management and workload Domains.	
FTR.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	
FTR.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.	
FTR.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.	
FTR.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.	
FTR.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.	

FTR.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.	
FTR.051	Functional	Service request	Solution should have a catalogue of all targeted cloud platforms (ie. private data centres, public clouds)		

Table 5 – Technical Functional Requirements

Non Functional Requirements

Technical ID	Category	Type	Requirement Description	Design Decision Comment	Requirement Satisfied
NFTR.001	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	
NFTR.002	Non Functional	Provisioning and orchestration	Storage should be resilient to SPOFs (ie. RAID)	All hardware and software will be built with resilience in mind.	
NFTR.003	Non Functional	Access Management	The solution must allow user access to the Infrastructure or hosted workloads to be	The solution will provide Active Directory groups to mange user access, however the process for	

			added or revoked on demand via Self Service	this is out od scope of this document.	
NFTR.004	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.	
NFTR.005	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.	
NFTR.006	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.	
NFTR.007	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.	
NFTR.008	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		
NFTR.009	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		
NFTR.010	Non Functional	Feature	The solution must provide an approval workflow in the Self Service Portal	The Automation of the solution is provided in a separate design	

				document, that will be provided by the automation team.	
NFTR.011	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.*	
NFTR.012	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.*	
NFTR.013	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.*	
NFTR.014	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.*	
NFTR.015	Non Functional	Feature	The solution must allow server volumes to be automatically created as part of the provisioning process	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
NFTR.016	Non Functional	Feature	The solution must allow server certificates to be automatically deployed as part of the provisioning process	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
NFTR.017	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.	

NFTR.018	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	The Automation of the solution is provided in a separate design document, that will be provided by the automation team.	
NFTR.019	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.	
NFTR.020	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.	
NFTR.021	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.	
NFTR.022	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.	
NFTR.023	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.	
NFTR.024	Non Functional	Inventory and classification	Solution should be able to integrate with existing ITSM systems (e.g. Remedy, etc.),	This decision isn't in scope of this solution.	

			such as change management, asset management etc.		
NFTR.025	Non Functional	Migration	SDDC solution must support migration of applications from physical to virtual servers	The solution will provide this functionality.	
NFTR.026	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.	
NFTR.027	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.	
NFTR.028	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.	
NFTR.029	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.	
NFTR.030	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.	

Table 6 – Technical Non-Functional Requirements

2.3 Risks

ID	Description	Probability (L/M/H)	Impact (L/M/H)	Mitigating actions
R.001				

Table 7 - Risks

2.4 Assumptions

ID	Assumption
A.001	The HPE servers will be installed in the datacentre in Wootton Basset
A.002	All Network connectivity will be in place before the deployment.
A.003	All Storage (HPE Purestore) and SAN fabrics will be installed in the datacentre

2.5 Issues

ID	Description	Probability (L/M/H)	Impact (L/M/H)	Mitigating actions
I.001				
I.002				

Table 8 - Issues

2.6 Dependencies

ID	Name	Description
D.001		

Table 9 - Dependencies

3 SOLUTION

The proposed solution will deliver an SDDCv2.5 VMware Cloud Foundation (VCF) platform with the VMware vRealize Suite of applications deployed onto it in Wootton Basset. The Solution will deploy an initial Management Domain into the datacentre using vSAN as it's primary storage. In addition to this we will also deploy a physical edge with local storage and two Workload Domains, production and non production using the HPE Purestore for their backend storage. The solution will be deployed on vSAN ready HPE hardware.
The VCF components are shown on the diagram below and more details on the individual components will be covered later in this design.

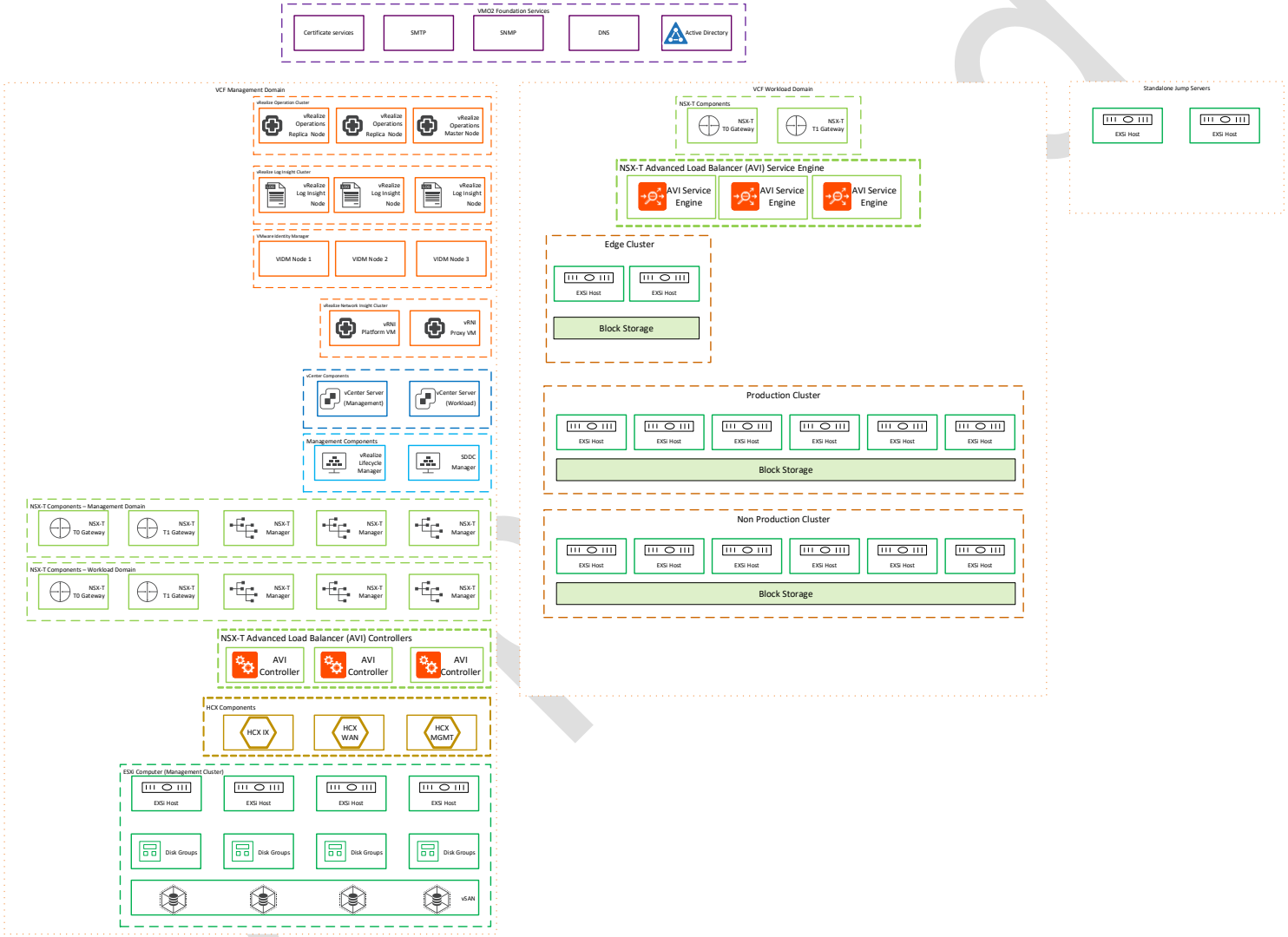


Figure 1 – Infra/Network Solution Diagram – Wootton Basset.

3.1 Location

The new Management and Workload Domains will be deployed in the following locations

Production – Wootton Basset

3.2 Environments

The following table defines all environment types and how many are required by this design.

Environment Type	Description	Required	# of instances
Production (PROD)	The principal production environment. All WOOTTON BASSET SDDCV2.5 services will be located in this environment.	Yes	1
Pre-production (ORT)	A non-production environment used for staging changes into production. Should be functionally equivalent to production though not necessarily providing the same levels of capacity/performance.	Yes	1
Performance Test	A non-production environment used for capacity and/or performance testing. May be functionally non-equivalent to prod (e.g. may have resilience), but should provide a basis for accurate performance testing.	Yes	1
User Acceptance Test (UAT)	A non-production environment used for testing new functionality with users prior to roll out to production (either directly, or via pre-prod).	Yes	1
Functional Test (JIT)	Used to test functional changes as part of the development process. May be implemented with other test systems to form an integrated test environment.	Yes	1

Table 10 - Environments Required

Environments

A production and Non Production environment will be deployed as part of this design.

Note

Although there is only a production and non production build for the platform, this solution will provide multiple environments delivered via NSX Micro segmentation.

3.3 Technical constraints & Licensing

There are no know technical constraints on the design currently. All licenses will be provided by the global ELA we have in place with VMware.

3.4 Security Considerations

The new Management and Workload Domains that will be deployed as part of this design will be centrally managed by the Cloud and TCS teams. Controls are already in place from previous designs that manage the lockdown of the virtual center servers that will manage the new clusters.

Important Note

Within the new cluster multiple environments could be deployed and access will be managed by NSX Micro Segmentation.

In addition to the NSA models Virgin Media O2 admin users will need the ability to see and manage the VCF infrastructure servers on the platform, this will be achieved by the creation of Active Directory groups in the systems.private Domain.
Below are a few examples of the groups required.

Domain	Group Name	Role

SYSTEMS.PRIVATE	TBC	Read Only Virtual Center Access
SYSTEMS.PRIVATE	TBC	Admin Access to Virtual Center
SYSTEMS.PRIVATE	TBC	Read Only NSX Access
SYSTEMS.PRIVATE	TBC	Admin Access to NSX

Table 11 - Production Environments Active Directory Groups

Logging

All user / administration tasks will be logged using vRLI, once deployed into the VCF platform.

3.5 Virgin Media O2 Foundation Services

The foundation services that will be deployed as part of this expansion into the new workload Domain will be used to support this and future solutions on the new VMO2 VCF platform in Wooton Basset.
Once the solution is completed both foundation / shared services in Knowsley, Baguley and Wooton Basset SDDC's will be available for use on the platform.

These foundation services will include but will not be limited to the following:

VMO2 ITCLOUDv2.5 Foundation Services – DNS
VMO2 ITCLOUDv2.5 Foundation Services – Certificate Authority
VMO2 ITCLOUDv2.5 Foundation Services – Active Directory
VMO2 ITCLOUDv2.5 Foundation Services – Linux Authentication
VMO2 ITCLOUDv2.5 Foundation Services – Unix Jump Servers
VMO2 ITCLOUDv2.5 Foundation Services – Windows RDP Servers
VMO2 ITCLOUDv2.5 Foundation Services – Backups
VMO2 ITCLOUDv2.5 Foundation Services – Automation Proxy (Ansible)
VMO2 ITCLOUDv2.5 Foundation Services – Automation Proxy (Powershell)
VMO2 ITCLOUDv2.5 Foundation Services – Antivirus (CrowdStrike)
VMO2 ITCLOUDv2.5 Foundation Services – Satellite Server
VMO2 ITCLOUDv2.5 Foundation Services – KMS

VMO2 ITCLOUDv2.5 Foundation Services – SMTP Relay
VMO2 ITCLOUDv2.5 Foundation Services – Qualys
VMO2 ITCLOUDv2.5 Foundation Services – Internet Proxies
VMO2 ITCLOUDv2.5 Foundation Services – Zabbix
VMO2 ITCLOUDv2.5 Foundation Services – Splunk
VMO2 ITCLOUDv2.5 Foundation Services – SCCM
VMO2 ITCLOUDv2.5 Foundation Services – SCOM
VMO2 ITCLOUDv2.5 Foundation Services - ADDM
VMO2 ITCLOUDv2.5 Foundation Services - NTP

Separate design will be created for the above outside this document if and when required.

4 INFRASTRUCTURE – BASE VCF COMPONENTS

In order to deliver the solution, we will be deploying VMware Cloud Foundation (VCF) and the VMware vRealize Suite of applications into Wootton Basset. The only exception to this will be the vRealize Automation and Orchestration as we will be using the existing automation solution already in place within the fO2 infrastructure. The Solution will deploy an initial Management Domain into the datacentre using vSAN as it's primary storage. In addition to this we will also be deploying a Workload Domain with three clusters in it, Edge, Production and Non Production using the HPE Purestore for their backend storage. The solution will be deployed on vSAN ready HPE hardware (DL380's).
The VCF components are shown on the diagram below and more details are listed in the Points of Interest table.

We will be deploying the following components:

4.1 Compliance & Governance

The new Virgin Media CMP cluster will support the following

- CAS(T) / (TSR)
- GDPR
- SOX
- PCI

Although this solution will be compliant, any future compliance & governance requirements required by application and services deployed onto the infrastructure will be covered in those designs.

Security Vulnerability Management

Virtual machines deployed into the solution will be reachable from existing Foundation Services for security management in accordance with standard procedure.

4.2 Hardware

- HPE DL380's (Management, Compute and Edge)

- HPE PureStore Storage
- Brocade G630 (Core SAN Fabrics)
- Brocade G620 (Edge SAN Fabrics)

4.3 Software

- VMWare vSphere ESX
- VMware vCenter
- VMware SDDC Manger
- VMware NSX-T Datacenter
- VMWare vSAN – Management Domain Only
- VMware vRealize Lifecycle Manager
- VMware vRealize Log Insight
- VMware vRealize Operations Manager
- VMware vRealize Network Insight
- VMware Hybrid Connect (HCX) – Optional
- VMware NSX Advanced Load Balancer (AVI)

Important Note

The following sections will show the deployments into a single Datacentre.

4.4 Solution Summary

The main points of interest in the infrastructure are shown below.

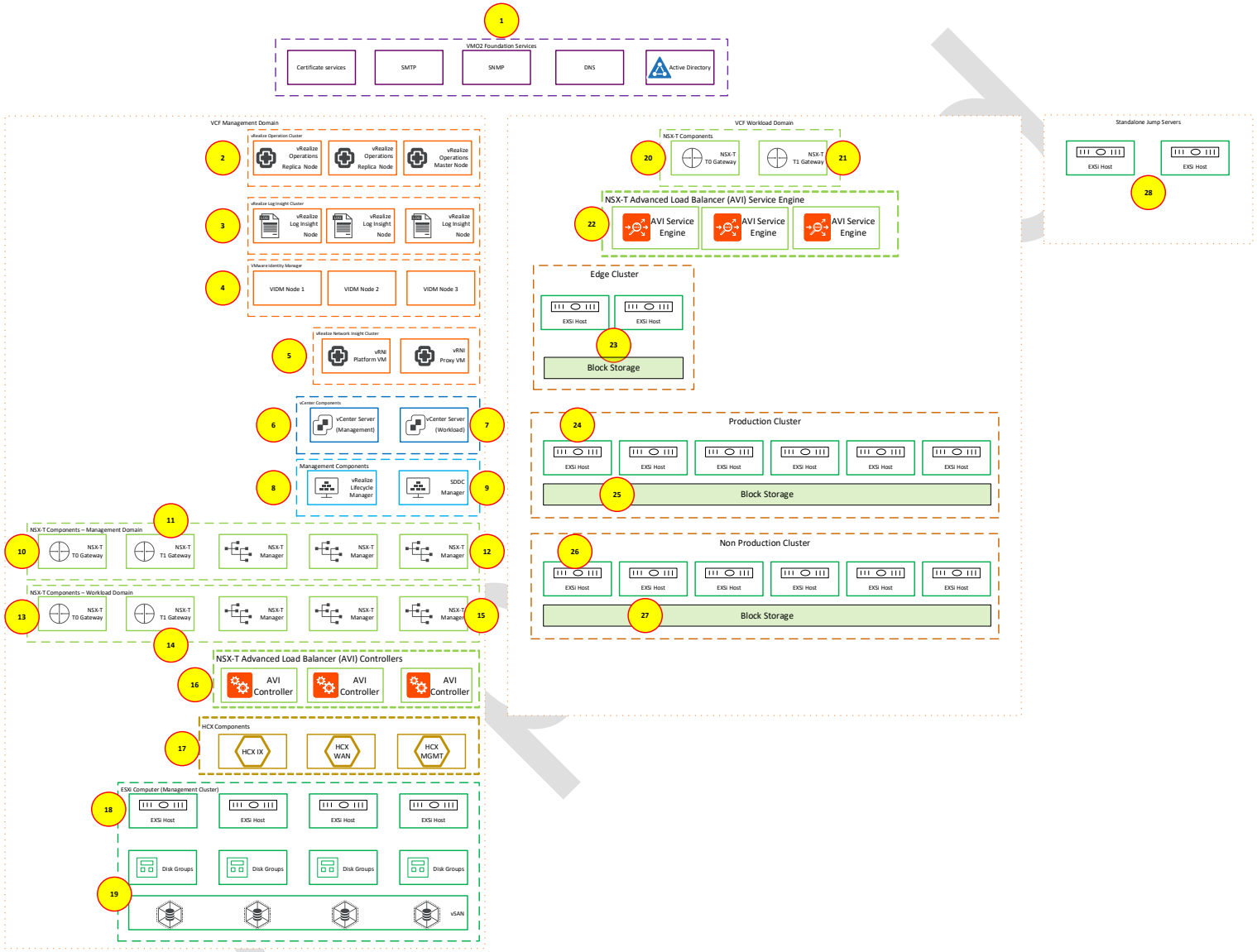


Figure 2 - Infrastructure Points of Interest

Points of Interest – Infrastructure Components

The following table highlights the main components

Number	Component	Description
1	VMO2 Foundation Services	
2	VMware vRealize Operations Manager	
3	VMware vRealize Log Insight	
4	VMware Identity Manager	
5	VMware vRealize Network Insight	
6	VMware vCenter Server (Management)	
7	VMware vCenter Server (Workload)	
8	VMware vRealize Lifecycle Manager	
9	VMware SDDC Manager	
10	VMware NSX-T T0 Gateway (Management)	
11	VMware NSX-T T1 Gateway (Management)	
12	VMware NSX-T Datacenter (Management)	
13	VMware NSX-T T0 Gateway (Workload)	
14	VMware NSX-T T1 Gateway (Workload)	
15	VMware NSX-T Datacenter (Workload)	
16	NSX-T Advanced Load Balancer Controllers	
17	VMware Hybrid Connect (HCX) – (Optional)	
18	ESXi Hosts - Management	
19	VMware vSAN	
20	VMware NSX-T T0 Gateway (Workload)	
21	VMware NSX-T T1 Gateway (Workload)	
22	NSX-T Advanced Load Balancer Service Engines	
23	ESXi Hosts - Edge	
24	ESXi Hosts – Compute (Production)	
25	Production Storage	
26	ESXi Hosts – Compute (Non Production)	
27	Non Production Storage	
28	ESXi Hosts – Stand Alone for Jump Servers	

Table 12 - Points of Interest – VCF Components

D

Operating System and Versions

We will utilise the latest version of VCF 5.0 for this deployment, this will include the following:

VMWare vSphere ESX – ver 8.0
VMware vCenter – ver 8.0
VMware SDDC Manger – ver 5.0
VMware NSX-T Datacenter – ver 4.1
VMWare vSAN – ver 8.0
VMware vRealize Lifecycle Manager – ver 8.8.2
VMware vRealize Log Insight – ver 8.8.2
VMware vRealize Operations Manager – ver 8.8.2

As the solution scales out over the next few years we will be able to add in additional HPE servers to the management cluster as well as adding in additional Workload Domains and clusters, these will all be deployed and configured using the SDDC manager.

4.5 Datacentre Layout

The following diagram shows the positioning of the racks required for the solution in the Wootton Basset site.

Wootton Basset Room 1

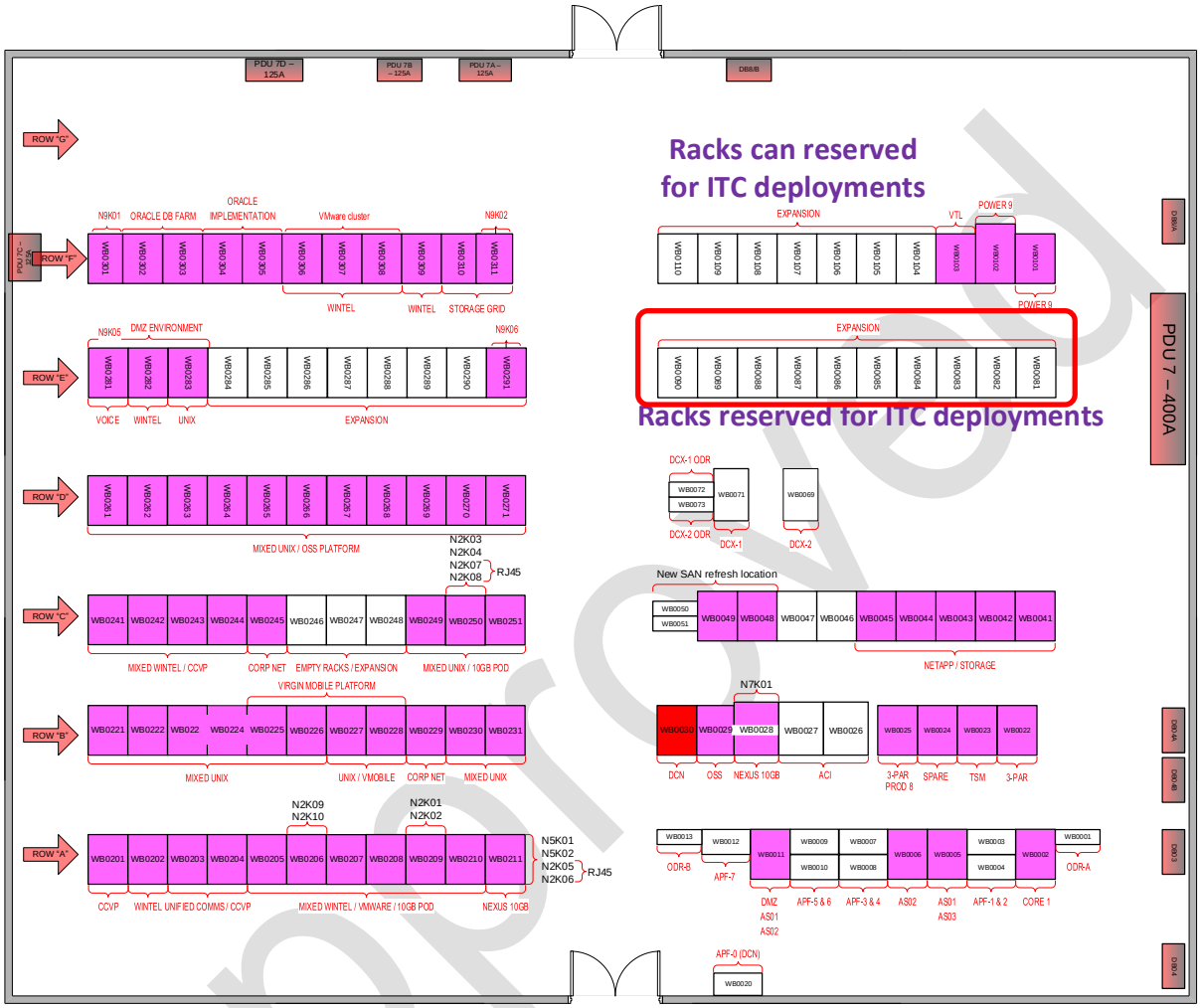


Figure 3 - Wootton Basset Room 1

Rack Layouts

The following diagram shows the suggested layout of the racks required for the solution and the positioning of the hardware.

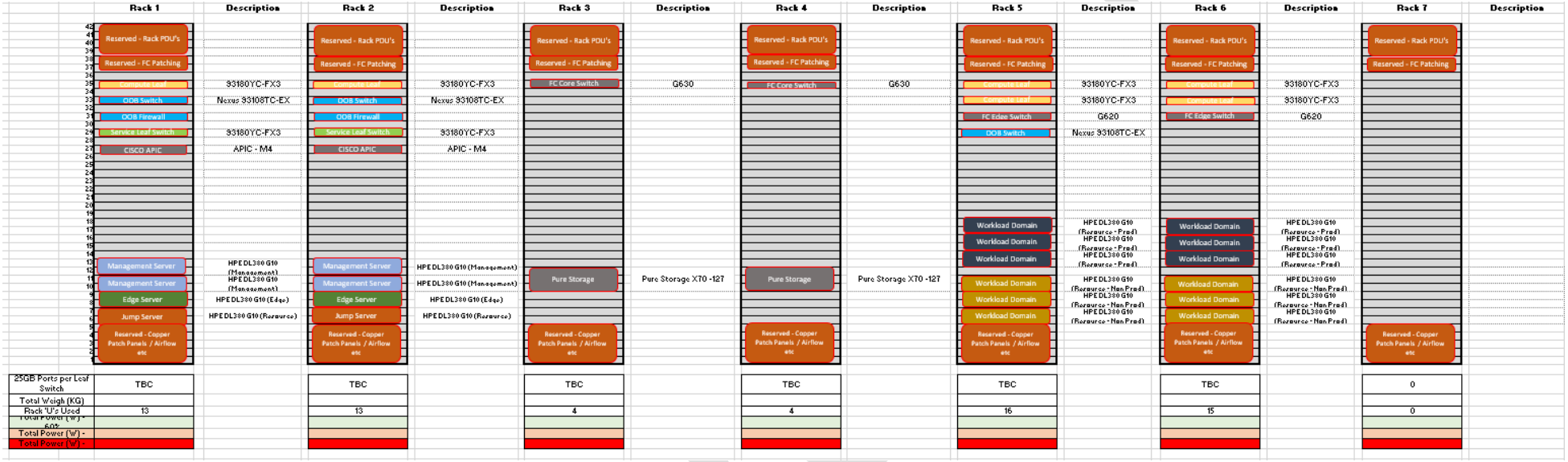


Figure 4 - Wootton Basset Rack Layout (ITC Racks Only)

The following shows the Network equipment in their network racks, however these racks and their positioning are out of scope for this design and are shown for illustration only.

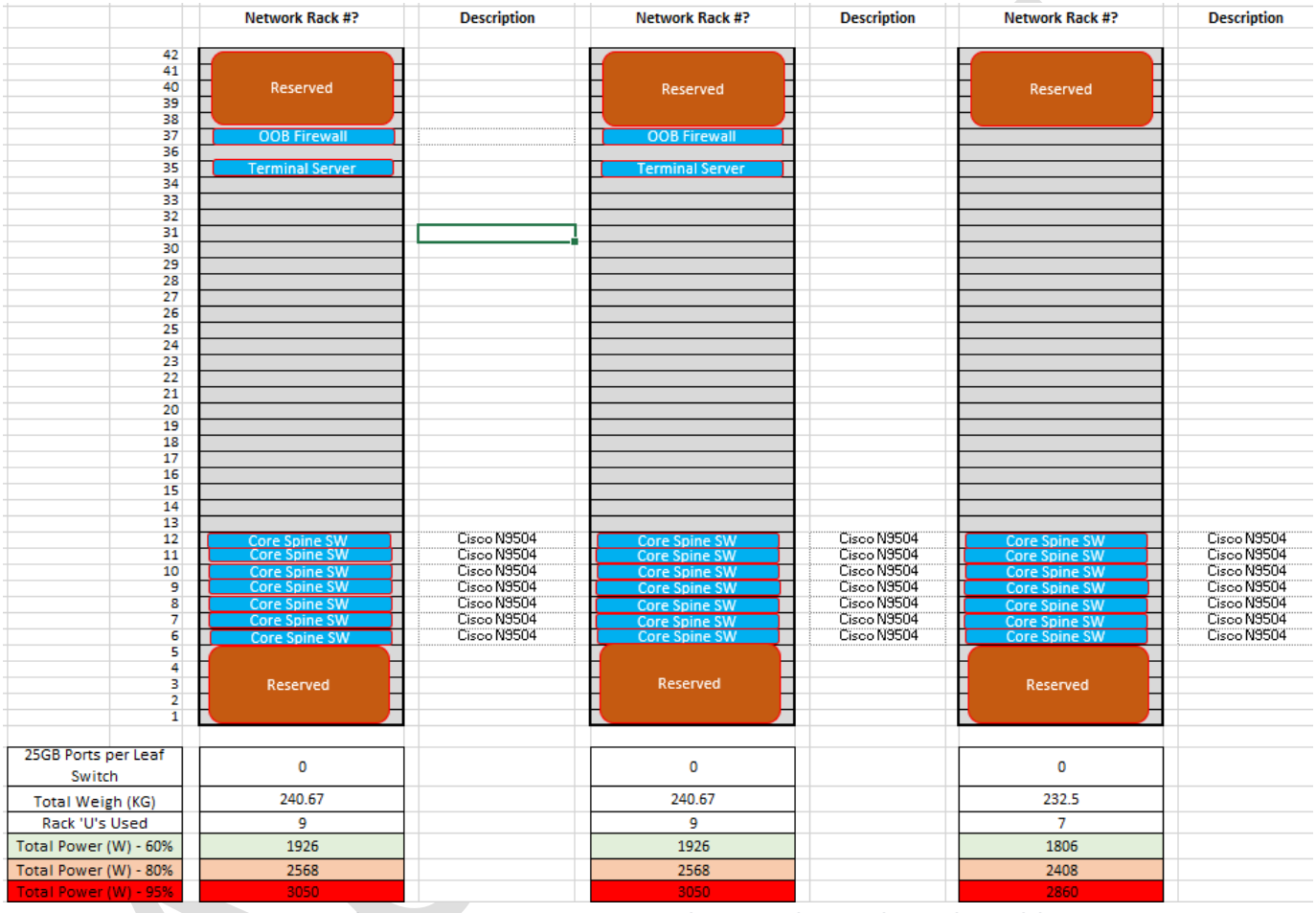
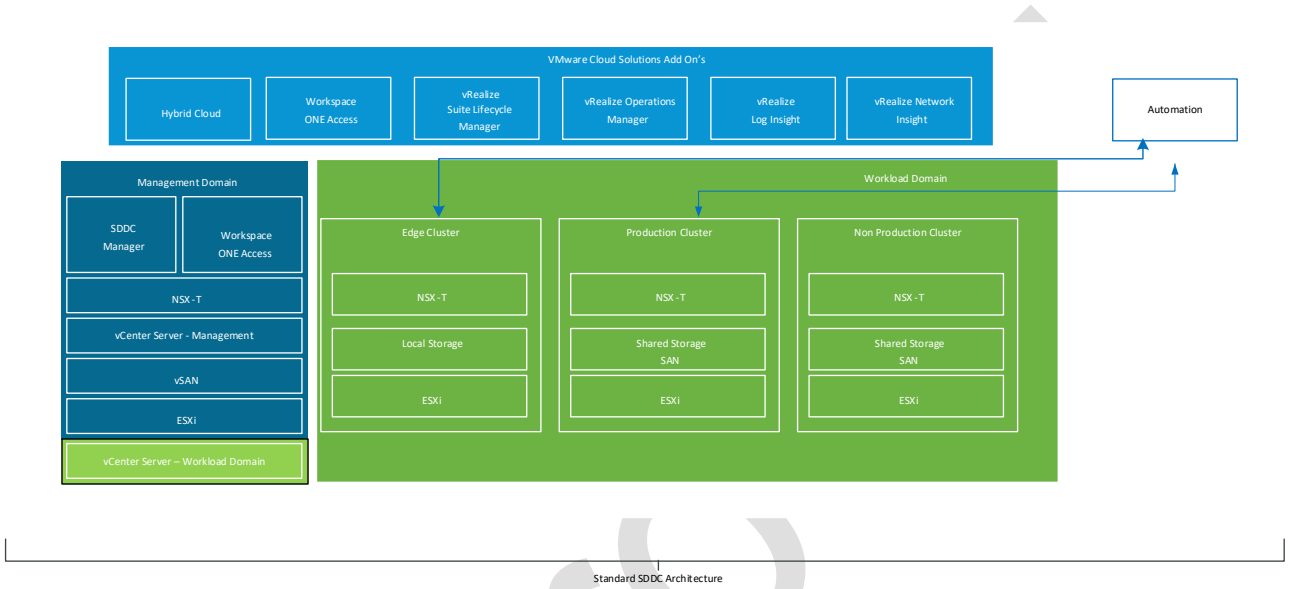


Figure 5 - Wootton Basset Rack Layout (Network Racks Only)

4.6 SDDC Architecture

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.



Standard SDDC Architecture

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.

Design Decision

Within the VMO2 SDDCV2.5 WOOTON BASSET 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.

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET design will use a single region, with the option to use one or two availability zones in that Region.

SDDC Architecture Design Decisions

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-PHY-VMO2 SDDCV2.5 WOOTON BASSET-001	In Region VMO2 SDDCV2.5 WOOTON BASSET, that is Region A, deploy one or two availability zones to support all SDDC management and workload components and their SLAs.	VCF	
SDDC-MGMT-PHY-VMO2 SDDCV2.5 WOOTON BASSET-002	Use two separate power feeds for each rack.	VCF	
SDDC-MGMT-PHY-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5	When using two availability zone, in each availability zone, mount the compute resources	VCF	

WOOTON BASSET-004	(minimum of 4 ESXi hosts) for the first cluster in the management domain together in one rack.		

Table 13 - SDDC Architecture Design Decisions

4.7 ESXi Host Specifications

The new Management, Edge and Workload Domains will be provisioned on 18 HPE DL380 G10 servers that will be located in the Wootton Basset datacenter. The network overlay will be provided by Cisco ACI.

Management Domain ESXi Host Specifications

The below table details the specification for the hosts

Attribute	Specification
Vendor and Model	HPE DL380 G10
Processor Speed	2x 6258R
Total number of Cores	56 (2x28) – (112 with Hyperthreading)
System Memory	1536GB
NIC Ports and Speed	6x 25GB
Boot Disks	2x480GB SSD's
Capacity Disks (vSAN)	6x6.4TB SSD's

Table 14 - ESXi Host Specification - Management

Edge ESXi Host Specifications

The below table details the specification for the hosts

Attribute	Specification
Vendor and Model	HPE DL380 G10
Processor Speed	2x 6226R
Total number of Cores	32 (2x16) – (64 with Hyperthreading)
System Memory	768GB
NIC Ports and Speed	6x 25GB
Boot Disks	2x480GB SSD's

Table 15 - ESXi Host Specification – Edge

Workload ESXi Host Specifications

The below table details the specification for the hosts

Attribute	Specification
Vendor and Model	HPE DL380 G10
Processor Speed	2x 6258R
Total number of Cores	56 (2x28) – (112 with Hyperthreading)
System Memory	1536GB
NIC Ports and Speed	6x 25GB
HBA Cards	2x 32GB SFP's
Boot Disks	2x 480GB SSD's
Capacity Disks (vSAN)	None (Pure Storage)

Table 16 - ESXi Host Specification – Workload

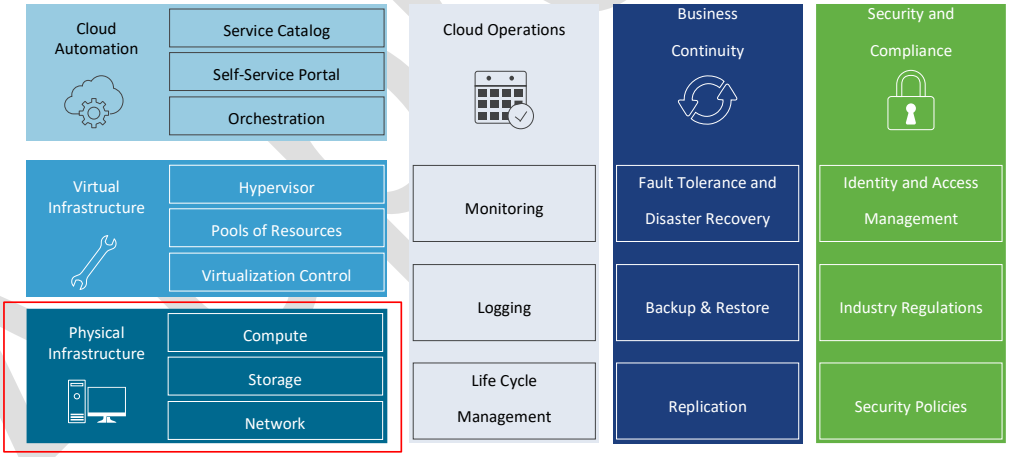


Figure 6 - Physical Infrastructure in the SDDC

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.

Regions

Regions provide disaster recovery across different SDDC instances or a locations.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.

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET design will use a single region for SDDC Management and one availability zone.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-PHY-VMO2 SDDCV2.5 WOOTON BASSET-005	In Region A, deploy one availability zone to support all SDDC management components and their SLAs.	VCF	

Table 17 - Physical Availability and Zone Design Decisions

4.8 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.

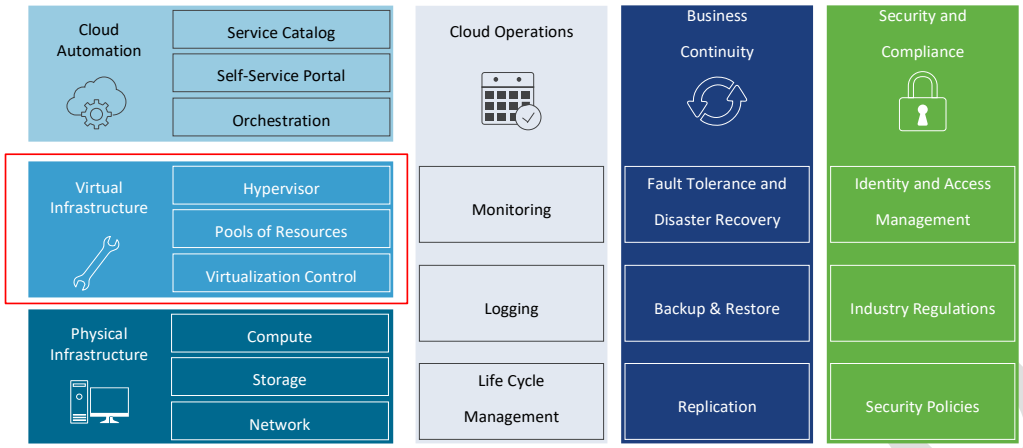


Figure 7 - Virtual Infrastructure in the SDDC

ESXi Design for the Management and Workload Domains

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 and Workload Domains

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:

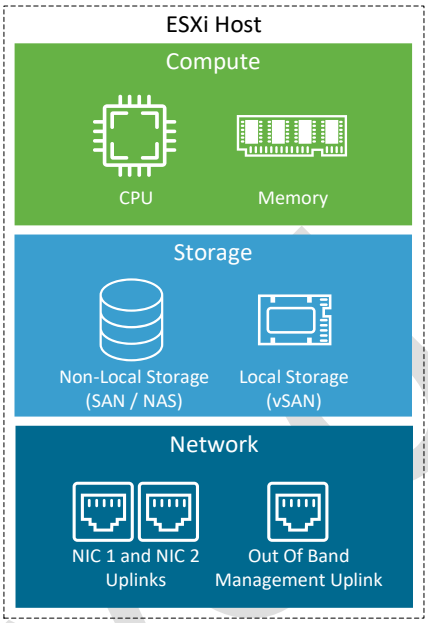
▪ CPU ▪ Memory ▪ Storage ▪ Out of Band Management Interface ▪ Network Interfaces	

Figure 8 - ESXi Logical Design

All the ESXi hosts will use the same configuration to allow consistency across the platform, the specific settings are listed below and linked back to the Business and Technical requirements where applicable.

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET design will use the following design decisions to meet our Business and Technical requirements as well as VMware Best Practices.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-001	Use vSAN ReadyNodes with vSAN storage for each ESXi host in the management domain.	VCF	
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-002	Allocate hosts with uniform configuration across the first cluster of the management domain.	VCF	

SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-004	When sizing CPU, do not consider multithreading technology and associated performance gains.	VCF	
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-009	Use SDDC Manager to perform the life cycle management of ESXi hosts in the management domain.	VCF	
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-010	Place the ESXi hosts in the first cluster of the management domain on the VLAN-backed management network segment.	VCF	
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-015	Configure the SSH service policy to Start and stop with host across all ESXi hosts in the management domain.	VCF	
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-016	Set the advanced setting UserVars.SuppressShellWarning to 1 across all ESXi hosts in the management domain.	VCF	
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-018	Change the default ESX Admins group to an Active Directory group ug-esxi-admins.	VCF	
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-019	Add ESXi administrators to the ug-esxi-admins group in Active Directory following standard access procedures.	VCF	
SDDC-MGMT-ESXi-VMO2 SDDCV2.5 WOOTON BASSET-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	

4.9 Network Design for ESXi Servers

In the network design for the ESXi hosts in the management and workload domains, you place the hosts on a VLAN for traffic segmentation. Once this is decided then you add the hosts names to DNS so the other SDDC components can resolve their names.

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 Servers. In addition, on this network, the hosts exchange heartbeat messages when vSphere HA.

vSphere vMotion Network

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

vSAN Network (Management Only)

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.

SAN Network (Workload Only)

Carries the communication between ESXi hosts in the cluster to implement a SAN shared storage.

Underlay Transport Network

Carries overlay traffic between the management and workload components in the Management and Workload 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.

ESXi Connectivity

Each of the HPe servers will have x1 iLo network port that will be connected to the OOB network switches. Two of the 25GB network ports will have a trunked port to them and this will carry the underlay networks for vMKernal, vMotion and vSAN, each of these will have it's own vLAN allocated to it. The remaining two 25Gb network card will be presented to NSX-T and these will carry the other network traffic, NSX segments will need to be presented, but these will be detailed in the VCF Network Design.

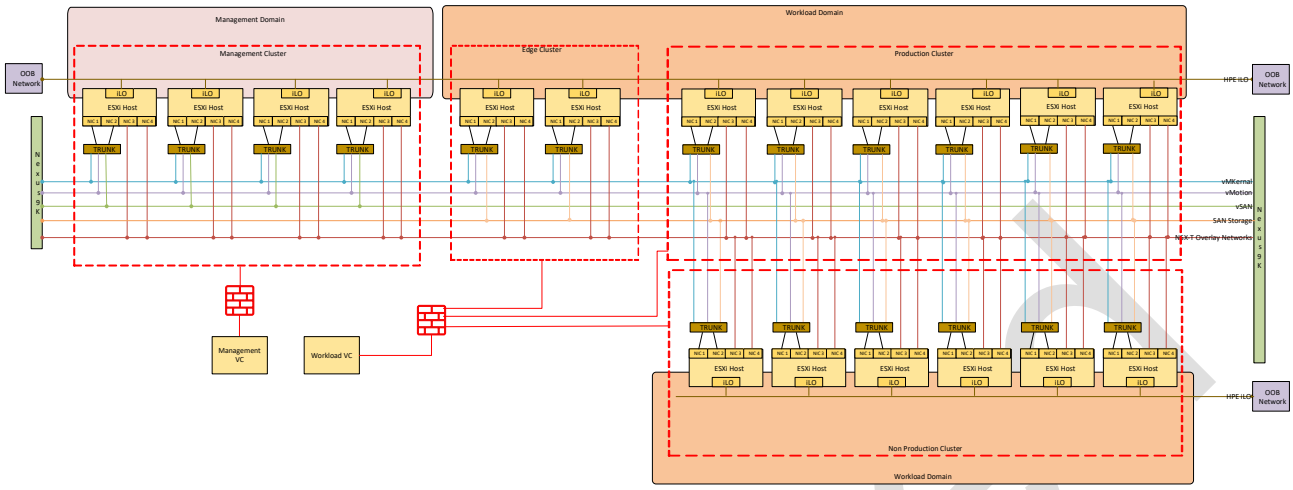


Figure 9 - ESXi Connectivity Overview

4.10 vCenter Server Design for the Management and Workload 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. This deployment type will be repeated for the workload domain to manage the clusters within that.
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.

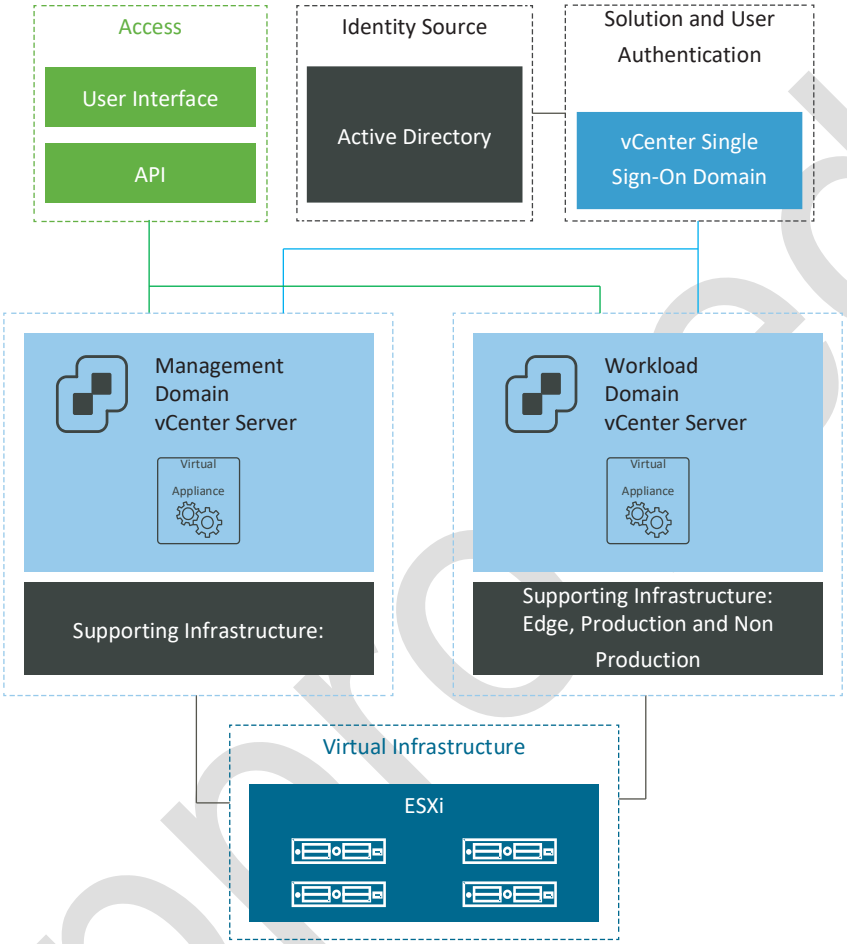


Figure 10 - Logical Design of vCenter Servers

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET design will deploy a management vCenter server as well as a workload vCenter server in the Management Domain.

Deployment Specification of vCenter Server

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.

The following will be implemented in the solution for both the management and workload domain vCenter servers.

vCenter Server Appliance Size	Management Capacity	Number of vCPU's	Memory
Medium environment	Up to 400 hosts or 4,000 virtual machines	8	28 GB

Table 18 - vCenter Server Sizing

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. This will give the operations team a single view of the SDDC.

Life Cycle Management Design of vCenter Server for the management Domain

Life cycle management of vCenter Servers includes the process of performing patch updates or upgrades to the vCenter Server appliances. When we implement the solution using VMware Cloud Foundation, we will 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 Servers in the Management Domain

In the network design for the management and workload domain vCenter Servers, we will place the vCenter Servers on a VLAN for traffic segmentation.

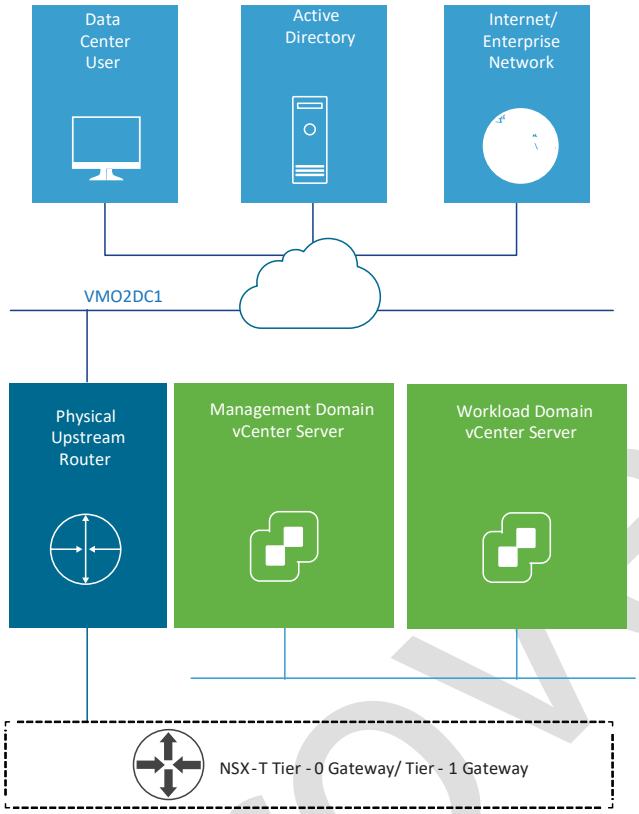


Figure 11 - vCenter Server Network Design

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.

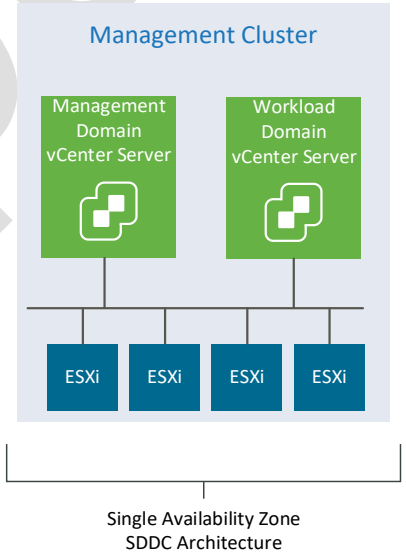


Figure 12 - vSphere Logical Layout

vSphere HA Design for the Management and Workload Domain

The vSphere HA configuration protects the virtual machines in the management and workload components of the SDDC whose operation is critical for the operation of the environment.

vSphere DRS Design for the Management and Workload 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 and Workload Domain

We will enable vSphere Enhanced vMotion Compatibility (EVC) in the management and workload domains, Virtual machines in the SDDC can be migrated between ESXi hosts containing older CPUs.

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

We will implement authentication access, control and certificate managements as per VMware and VMO2 best practices.

Identity Management

Users will 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. The identity source we will use is Active Directory.

Password Management and Account Lockout Behavior

The vCenter Servers will enforce 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). This certificate will be replaced by a VMO2 issued certificate before the environment goes into Production.

Virtual Center Design Settings

In the VMware Cloud Foundation deployment, the following will need to be implemented.

Component	Justification	Implication
vMotion will be enabled and configured automatically on the Management and Workload Domains	vMotion enables live migration of virtual machines.	vMotion will be automatically configured by SDDC Manager.
The Management and Workload Domains will utilise HA with admission control enabled	This setting provides a high level of availability for management workloads in the event of host failure	If HA determines that there are not enough resources additional virtual machines will not be powered on.
Two vCenter server systems will be automatically deployed in the management domain.	These vCenter instances will be used to manage the resources in the management and workload domains.	Two vCenter license required.
vCenter Single Sign-On will be configured to integrate with the systems.private Active Directory	Integrating with Active Directory allows users to login and be assigned permissions with their Active Directory credentials.	None
An Administrator AD group will be imported into vCenter	Allows specific domain users to administer vCenter server	vCenter needs to be integrated with Active Directory
A Read Only AD group will be imported into vCenter	Allows specific domain users to login to vCenter server and traverse the interface, while providing auditability and ease of management.	vCenter needs to be integrated with Active Directory
vSphere DRS will be enabled on the management and workload clusters in fully automatic mode and set to default threshold setting of medium	Provides best trade off between load balancing and excessive vMotion events and activity	None
HA Admission control will be enabled as default.	vSphere HA uses admission control to ensure that sufficient resources	Admission control imposes constraints on resource usage. Any action that

	are reserved for virtual machine recovery in the event of host failure.	might violate these constraints is not permitted.

Table 19 - Virtual Center Design Settings

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET design will use the following design decisions to meet our Business and Technical requirements as well as VMware Best Practices.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-001	Deploy a dedicated vCenter Server instance in the first availability zone of the region for the management domain.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-002	When using one availability zone in Region A, add the vCenter Server appliance to the virtual machine group for Availability Zone 1.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-003	Deploy an appliance for the management domain vCenter Server of a medium deployment size or larger.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-004	Deploy the appliance of the management domain vCenter Server with the default storage size.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-005	Join all vCenter Server instances to a single vCenter Single Sign-On domain	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-006	Create a ring topology for the Single Sign-On domain running in the vCenter Server instances.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-007	Protect the workload domain vCenter Server appliance by using vSphere HA	VCF	

SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-008	In vSphere HA, set the restart priority policy for the vCenter Server appliance to high.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-009	Use SDDC Manager to perform the life cycle management of the appliance for the management domain vCenter Server.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-010	Place the appliance of the management domain vCenter Server on the management VLAN network segment of the region.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-011	Allocate a statically assigned IP address and host name to the appliance of the management domain vCenter Server.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-013	Configure time synchronization by using an internal NTP time for the appliance of the management domain vCenter Server.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-014	Create a cluster in the management domain for the initial set of ESXi hosts.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-015	In Region VMO2 SDDCV2.5 WOOTON BASSET, create the first cluster in the management domain with this configuration: - A minimum of 4 ESXi hosts for a single availability zone	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-016	Use vSphere HA to protect all virtual machines against failures.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-017	Set host isolation to Power Off in vSphere HA.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5	When using a single availability zone, configure admission control for 1 ESXi host failure and percentage- based failover capacity.	VCF	

WOOTON BASSET-018			
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-022	Set the advanced cluster setting das.usedefaultisolationaddress to false	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-023	Enable VM Monitoring for each cluster.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-024	Enable vSphere DRS (Distributed Resource Scheduling) on all clusters, using the default fully automated mode (medium)	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-025	Create virtual machine groups for use in startup rules in the first cluster in the management domain.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-026	Create virtual machine rules to set the startup order of the SDDC management components.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-027	Enable Enhanced vMotion Compatibility (EVC) on all clusters in the management domain.	VCF	
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-028	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-VMO2 SDDCV2.5	Join the management domain vCenter Server to the Active Directory domain for the region that vCenter Server resides in	VCF	

WOOTON BASSET-029			
SDDC-MGMT-VC-VMO2 SDDCV2.5 WOOTON BASSET-030	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-VMO2 SDDCV2.5 WOOTON BASSET-031	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-VMO2 SDDCV2.5 WOOTON BASSET-032	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-VMO2 SDDCV2.5 WOOTON BASSET-033	Use a SHA-2 algorithm or stronger for signed certificates.	VCF	

Table 20 - SDDC vCenter Server Design Decisions

4.11 vSphere Networking Design for Management and Workload Domains

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.

In order to maintain VMware and industry best practices we will adopt the following:

- 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.

- 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 and Workload Domains

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 and Workload Domains

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.

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).

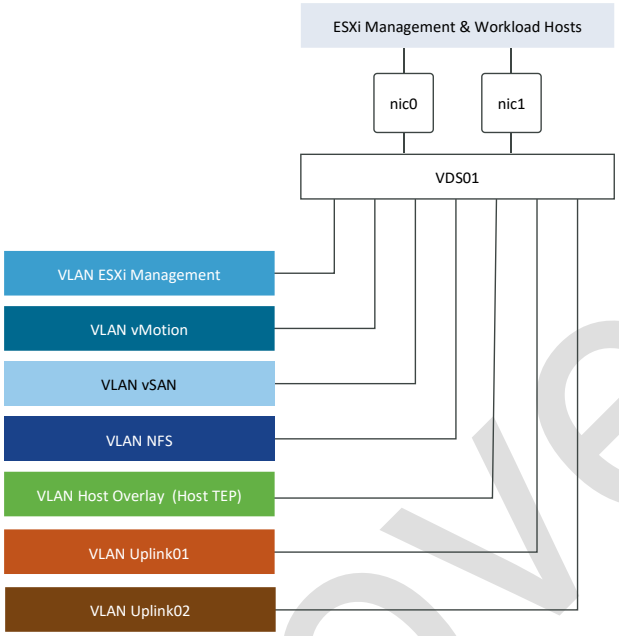


Figure 13 - vSphere Distributed Switch

Each ESXi server will utilize the four 25GB NIC's in them as well as the iLO NIC for HPE Server management.

These will be configured as per the diagram below. The system/management vDS will carry all the ESXi Infrastructure traffic (vMKernal, vMotion, vSAN (Management Only) and SAN etc) and the other vDS will carry all data network traffic.

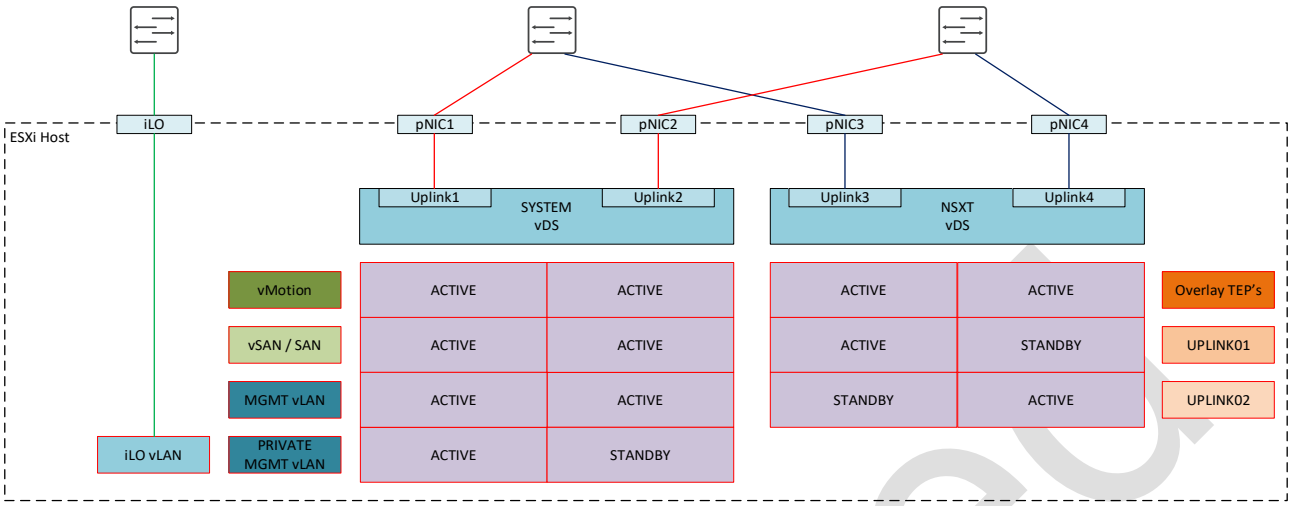


Figure 14 - vDS Connectivity

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 and Workload Domains

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

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.

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET vSphere Network design will use the following design decisions to meet our Business and Technical requirements as well as VMware Best Practices.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-001	Use vSphere Distributed Switches.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-002	Use a single vSphere Distributed Switch per cluster.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-003	Configure the MTU size of the vSphere Distributed Switch to 9000 for jumbo frames	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-004	Use ephemeral port binding for the management port group.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-005	Use static port binding for all non-management port groups.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-006	Use the Route based on physical NIC load teaming algorithm for the management port group.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5	Use the Route based on physical NIC load teaming algorithm for the vMotion Port Group.	VCF	

WOOTON BASSET-007			
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-008	Use the vMotion TCP/IP stack for vSphere vMotion traffic.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-009	Enable Network I/O Control on vSphere distributed switch of the management domain cluster	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-010	Set the share value for management traffic to Normal.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-011	Set the share value for vSphere vMotion traffic to Low.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-012	Set the share value for virtual machines to High.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-013	Set the share value for vSAN traffic to High.	VCF	
SDDC-MGMT-NET-VMO2 SDDCV2.5 WOOTON BASSET-014	Set the share value for vSphere Fault Tolerance to Low.	VCF	

Table 21 - vSphere Network Design Decisions

4.12 Shared Storage Design for Virtual Infrastructure in Management and Workload Domains

There will be two types of capacity storage deployed within the solution, vSAN and Block Storage provided by the HPE Pure Storage.

	***Design Decision*** We are going to use vSAN storage for the VMO2 SDDCV2.5 WOOTON BASSET solution in the Management Domain and SAN storage in the Workload Domain.

vSAN

The underlying storage for the Management Domain will be provided by vSAN, this will be presented via the Hyperconverged Infrastructure. Within the Management Domain we will be using Raid 1 (Mirroring) for additional resilience.
Each of the ESXi host will have all flash disks and the compute will be presented by a disk group on each of the ESXi hosts.

The breakdown of the disks is as follows:

2x 480GB Disks for the O/S
2x 750GB Disks for the vSAN Cache
6x 6.4TB Capacity Disks

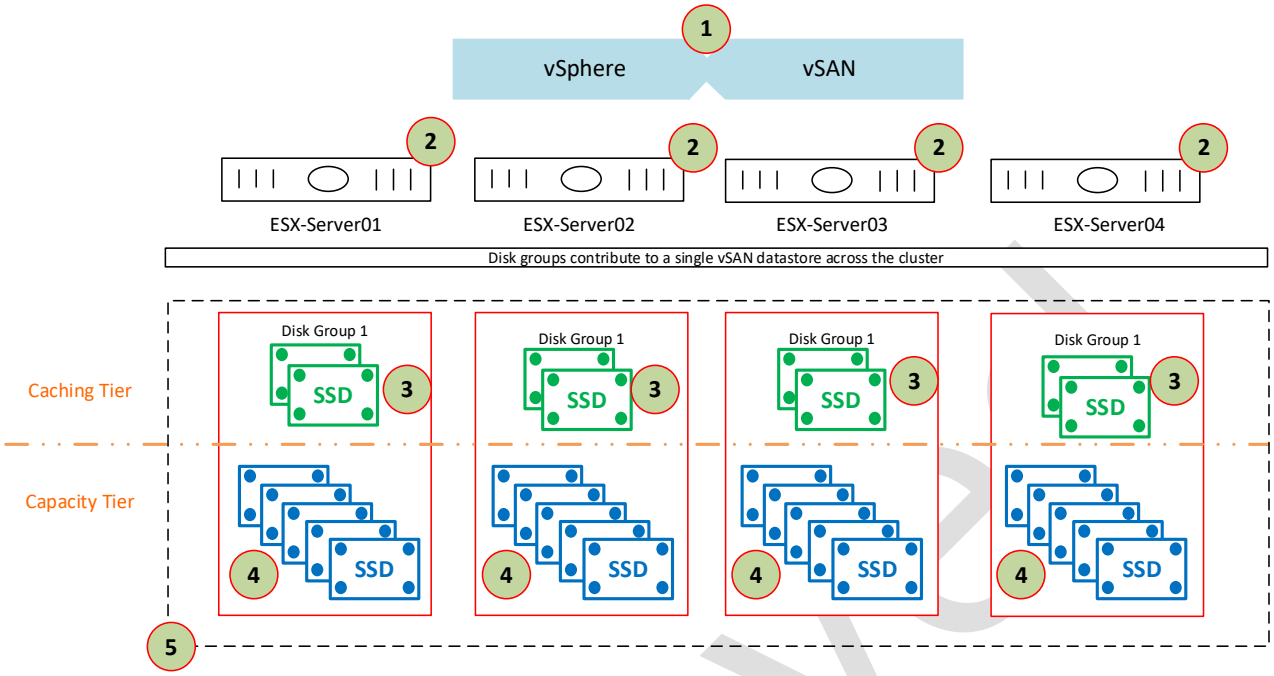


Figure 15 - vSAN Overview

vSAN Points of Interest

The table below details the points of interest for the SDDC solution.

Number	Component	Description
1	vSphere vCenter server	vCenter Server manages the vSAN components.
2	ESXi Hosts	Disks from these host are used to create the total storage.
3	X2 Mirrored SSD Disks	Used for the vSAN Caching disks
4	X6 SSD Capacity disks	Used for the Capacity presented to vSAN and vCenter for Virtual Machine storage
5	VMware Cluster	VMware Cluster

Table 22 - vSAN Points of Interest

vSAN Configuration

The following table list the vSAN requirements.

Production vSAN Configuration – Wooton Basset							
Component	**vSAN Datastore Name**	**vSAN Policy Name**	**vCenter**	**vSAN FTT**	**Number of Failures to Tolerate**	**Number of Disk Stripes per Object**	**vSAN Isolation IP**
vSAN Management Domain	WB1-MGMT-CLU01-PRD-DS01 WB1-MGMT-CLU01-PRD-DS02	WB1-xxx	WB1-xxx	RAID 1	1	1	xxx

Table 23 - vSAN Configuration Information – Wootton Basset

Pure Storage

The Pure Storage will be presented via two PureStore X70 Arrays, one will provide storage for the Production environment and the other the Non Production environment. These will be housed in the racks in Wootton Basset.
Each of the X70 arrays will have 127TB of storage that can be used for the provision of VM's on the environment.

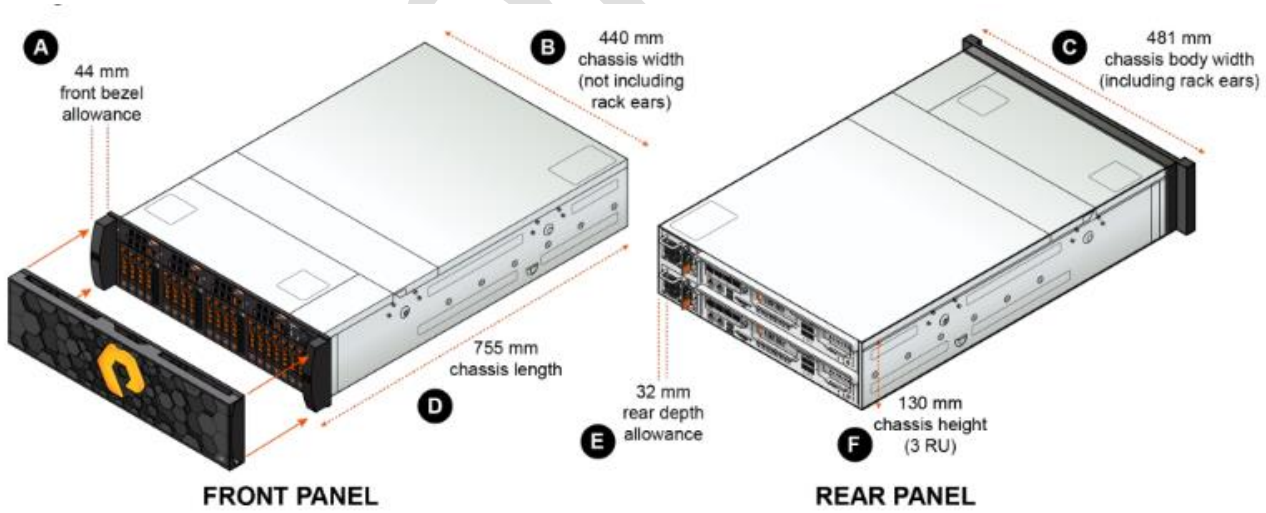


Figure 16 - HPE Pure Storage Device

The following arrays will be deployed in Wootton Basset

Array Name	Manufacture	Model Type	Location	Use
WB-PURE-01-SDDC-PRD	PURE	X70	Wooton Basset	IT SDDC On Premise
WB-PURE-01-SDDC-NPRD	PURE	X70	Wooton Basset	IT SDDC On Premise

Storage Breakdown

As part of the Next Gen2.0 programme, the storage vendor selected is Pure Storage with their X70R3 storage array. These arrays are provided with a minimum of 100TB of effective storage. Pure provides a commitment for the Effective Capacity, equating to 300TiBe for the production and Non Production arrays sized. The assumption from Pure is that there will be 4:1 Data Reduction Ratio (noted in the RAID log) which will provide the desired effective capacity. The numbers as provided by Pure are:

Production Pure Storage Configuration – Wooton Basset (Production)					
Model	**Raw Capacity TB**	**Useable Capacity TB**	**Useable Capacity TiB**	**Effective Capacity TBe**	**Effective Capacity TiBe**
X70	127	86.96	79.09	347.84	316.36

Table 24 - Pure Storage Capacity (Production)

Production Pure Storage Configuration – Wooton Basset (Production)					
Model	**Raw Capacity TB**	**Useable Capacity TB**	**Useable Capacity TiB**	**Effective Capacity TBe**	**Effective Capacity TiBe**
X70	127	86.96	79.09	347.84	316.36

Table 25 - Pure Storage Capacity (Non Production)

Pure Storage Connectivity

The diagram below represents the connectivity for the Pure Storage to both Network and SAN fabric's.

The array configurations include the following:

- 2 storage controllers/nodes
- 12 x 16Gb FC HBA, 6 per controller (so 6 to SAN fabric A and 6 to SAN fabric B) for the X70.
- 4 x 10Gb fibre network connections for replication.
- All software is fully licenced.

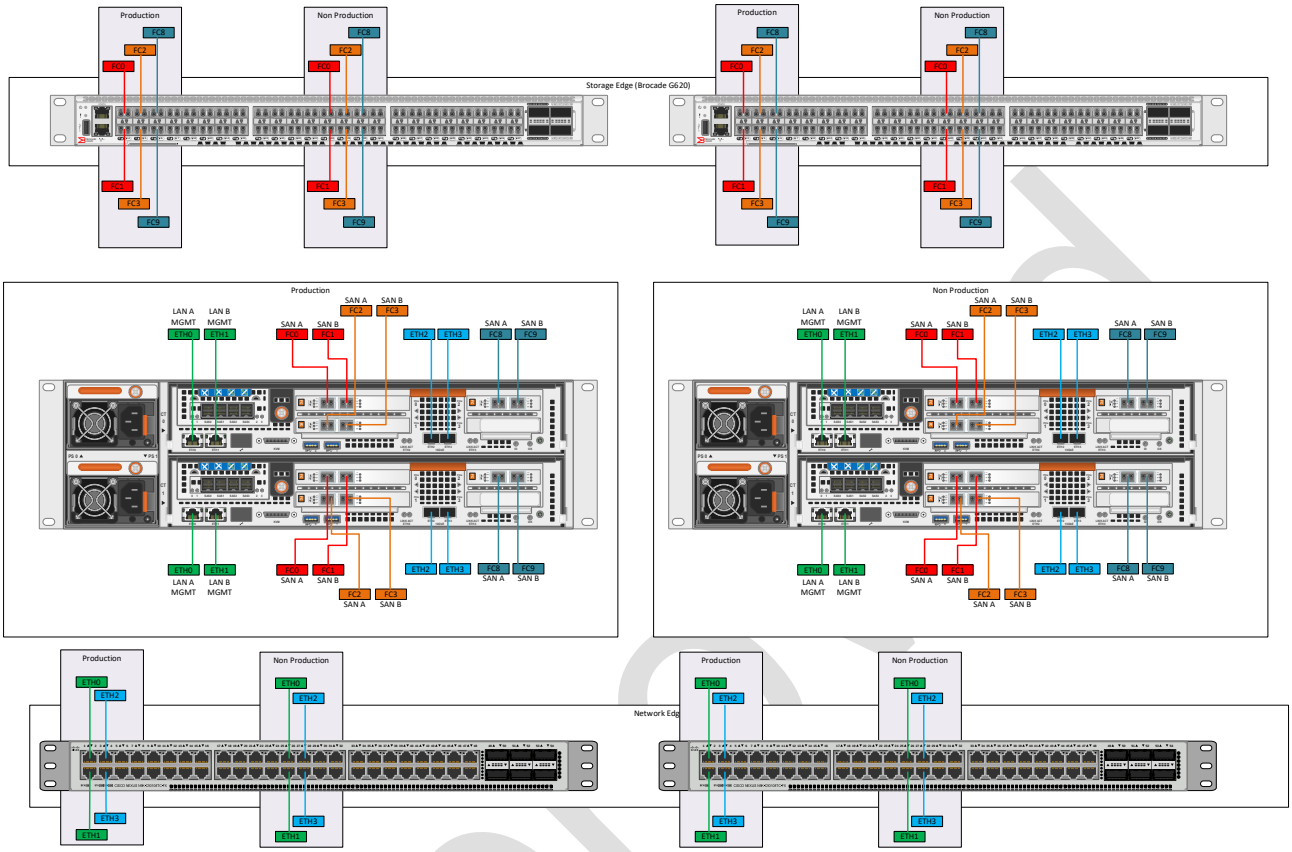


Figure 17 - Pure Storage Connectivity

NOTE: Port allocation is for visual only and the datacenter team may change these ports.

Pure Storage Application Connectivity.

The Pure Storage devices will need to connect to the following:

- DNS
- Active Directory
- Connectivity between Pure Storage and Pure 1
- Connectivity between Pure Storage and Netcool
- Connectivity between Pure Storage and SMTP

LUN Sizing

The following LUNS will need to be presented to the following ESXi Servers in the Workload Domain

Edge Environment

Edge Pure Storage Configuration – Wooton Basset (Edge)			
LUN Name	**Useable Capacity TB**	**Array Name**	**Hosts Allocated to**
WB-WKD-CLU01-EDGE-DS01	1TB	WB-PURE-01-SDDC-PRD	WB1PEDGTR0UK401 WB1PEDGTR0UK402

Table 26 - Pure Storage LUN Allocation (Edge)

Production Environment

Production Pure Storage Configuration – Wooton Basset (Production)			
LUN Name	**Useable Capacity TB**	**Array Name**	**Hosts Allocated to**
WB-WKD-CLU01-PRD-DS01	6TB	WB-PURE-01-SDDC-PRD	WB1PESXICPUK601 WB1PESXICPUK602 WB1PESXICPUK603 WB1PESXICPUK604 WB1PESXICPUK605 WB1PESXICPUK606
WB-WKD-CLU01-PRD-DS02	6TB	WB-PURE-01-SDDC-PRD	WB1PESXICPUK601 WB1PESXICPUK602 WB1PESXICPUK603 WB1PESXICPUK604 WB1PESXICPUK605 WB1PESXICPUK606
WB-WKD-CLU01-PRD-DS03	6TB	WB-PURE-01-SDDC-PRD	WB1PESXICPUK601 WB1PESXICPUK602 WB1PESXICPUK603 WB1PESXICPUK604 WB1PESXICPUK605 WB1PESXICPUK606
WB-WKD-CLU01-PRD-DS04	6TB	WB-PURE-01-SDDC-PRD	WB1PESXICPUK601 WB1PESXICPUK602 WB1PESXICPUK603 WB1PESXICPUK604 WB1PESXICPUK605 WB1PESXICPUK606

WB-WKD-CLU01-PRD-DS05	6TB	WB-PURE-01-SDDC-PRD	WB1PESXICPUK601 WB1PESXICPUK602 WB1PESXICPUK603 WB1PESXICPUK604 WB1PESXICPUK605 WB1PESXICPUK606
WB-WKD-CLU01-PRD-DS06	6TB	WB-PURE-01-SDDC-PRD	WB1PESXICPUK601 WB1PESXICPUK602 WB1PESXICPUK603 WB1PESXICPUK604 WB1PESXICPUK605 WB1PESXICPUK606

Table 27 - Pure Storage LUN Allocation (Production)

Non Production Environment

Production Pure Storage Configuration – Wooton Basset (Production)			
LUN Name	**Useable Capacity TB**	**Array Name**	**Hosts Allocated to**
WB-WKD-CLU01-NPRD-DS01	6TB	WB-PURE-01-SDDC-NPRD	WB1NESXICPUK601 WB1NESXICPUK602 WB1NESXICPUK603 WB1NESXICPUK604 WB1NESXICPUK605 WB1NESXICPUK606
WB-WKD-CLU01-NPRD-DS02	6TB	WB-PURE-01-SDDC-NPRD	WB1NESXICPUK601 WB1NESXICPUK602 WB1NESXICPUK603 WB1NESXICPUK604 WB1NESXICPUK605 WB1NESXICPUK606
WB-WKD-CLU01-NPRD-DS03	6TB	WB-PURE-01-SDDC-NPRD	WB1NESXICPUK601 WB1NESXICPUK602 WB1NESXICPUK603 WB1NESXICPUK604 WB1NESXICPUK605 WB1NESXICPUK606
WB-WKD-CLU01-NPRD-DS04	6TB	WB-PURE-01-SDDC-NPRD	WB1NESXICPUK601 WB1NESXICPUK602 WB1NESXICPUK603 WB1NESXICPUK604 WB1NESXICPUK605 WB1NESXICPUK606

WB-WKD-CLU01-NPRD-DS05	6TB	WB-PURE-01-SDDC-NPRD	WB1NESXICPUK601 WB1NESXICPUK602 WB1NESXICPUK603 WB1NESXICPUK604 WB1NESXICPUK605 WB1NESXICPUK606
WB-WKD-CLU01-NPRD-DS06	6TB	WB-PURE-01-SDDC-NPRD	WB1NESXICPUK601 WB1NESXICPUK602 WB1NESXICPUK603 WB1NESXICPUK604 WB1NESXICPUK605 WB1NESXICPUK606

Table 28 - Pure Storage LUN Allocation (Non Production)

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET vSAN Storage design will use the following design decisions to meet our Business and Technical requirements as well as VMware Best Practices.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-002	I/O Controllers that are running vSAN disk group(s) should not be used for another purpose.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-003	Configure vSAN in all-flash mode in the first cluster of the management domain.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5	Use a 600 GB or greater flash-based drive for the cache tier in each disk group	VCF	

WOOTON BASSET-004			
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-005	Have at least 5TB of flash-based drives for the capacity tier in each disk group.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-006	Provide the first cluster in the management with a minimum of 37 TB of raw capacity for vSAN.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-007	On all vSAN datastores, ensure that at least 30% of free space is always available	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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	Not applicable as we are using a single availability zone
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-010	Configure vSAN with a minimum of two disk groups per ESXi host.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-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	Not applicable as we are using a single availability zone
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-012	Deploy a medium-size witness appliance.	VCF	Not applicable as we are using a single availability zone
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-013	When using a single availability zone, use the default VMware vSAN storage policy	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5	When using two availability zones, add the following setting to the default vSAN storage policy: Secondary Failures to Tolerate = 1	VCF	Not applicable as we are using a single

WOOTON BASSET-014			availability zone
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-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	Not applicable as we are using a single availability zone
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-016	Leave the default virtual machine swap file as a sparse object on VMware vSAN.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-017	Use the existing vSphere Distributed Switch instances in the first cluster in the management domain.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-018	Configure jumbo frames on the VLAN dedicated to vSAN traffic.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-019	Connect the first VMkernel adapter of the vSAN witness appliance to the management network in the witness site.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-020	Configure the vSAN witness appliance to use the first VMkernel adapter, that is the management Interface, for vSAN witness traffic.	VCF	Not applicable as we are using a single availability zone
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-021	Place witness traffic on the management VMkernel adapter of all the ESXi hosts in the management domain.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-022	Allocate a statically assigned IP address and host name to the management adapter of the vSAN witness appliance.	VCF	
SDDC-MGMT-SDS-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-024	Configure time synchronization by using an internal NTP time for the vSAN witness appliance.	VCF	

Table 29 - SDDC Software Defined Storage Decisions

4.13 SDDC Manager

VMware SDDC Manager will be deployed into the management cluster to manage the cluster and allow for additional workload domains to be added. The SDDC manager can also be used for other functions listed below.

- Commissioning or decommissioning ESXi hosts
- Deployment of workload domains
- Extension of clusters in the management and workload domains with ESXi hosts
- Adding clusters to the management domain and workload domains
- Support for network pools for host configuration in a workload domain
- Product licenses storage
- Deployment of vRealize Suite components.
- Life cycle management of the virtual infrastructure components in all workload domains, and of vRealize Suite Lifecycle Manager components.
- Certificate management
- Password management and rotation
- NSX-T Edge cluster deployment in the management domain and workload domains
- Backup configuration

SDDC Manger Overview and Connectivity

The diagram below shows the main components that connect to the SDDC Manager.

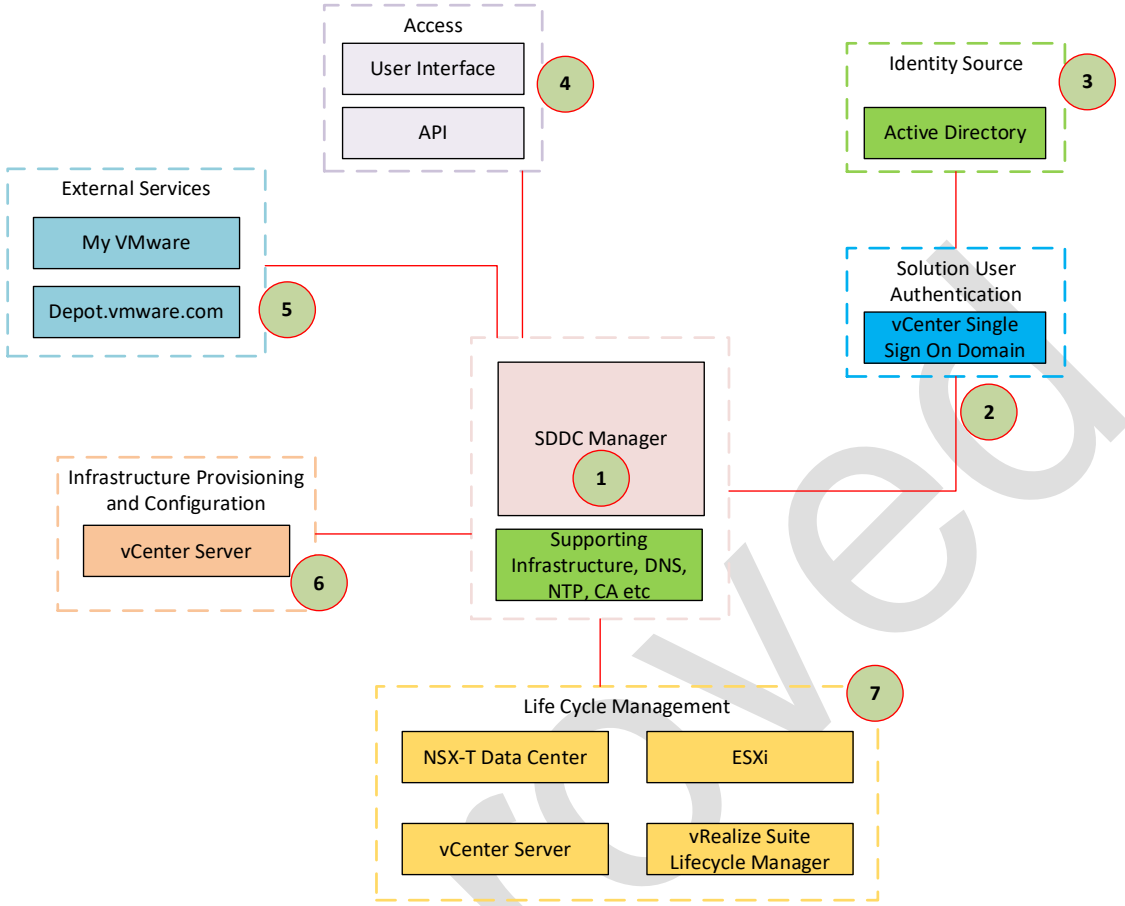


Figure 18 - SDDC Manager and Connectivity

SDDC Manager Points of Interest

The table below details the points of interest for the SDDC solution.

Number	Component	Description
1	SDDC Manager	The single interface into the solution
2	Single sign on provided by PSC	Allows seamless authentication to the solution.
3	Identity Source	For this solution this will be provided by the systems.private Active Directory.
4	Access	Access to the platform is via web portal or API

5	External Services	These are required to download VMware patches / fixes as well as the latest software bundles.
6	Infrastructure Provisioning and Configuration	This is provided via the vCenter server in the solution
7	Life Cycle Management	This provides all the interfaces into the solution.

Table 30 - SDDC Manager Points of Interest

4.14 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.
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

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 design.
The product will be deployed into the Management Domain and will be connected to the Management vCenter.

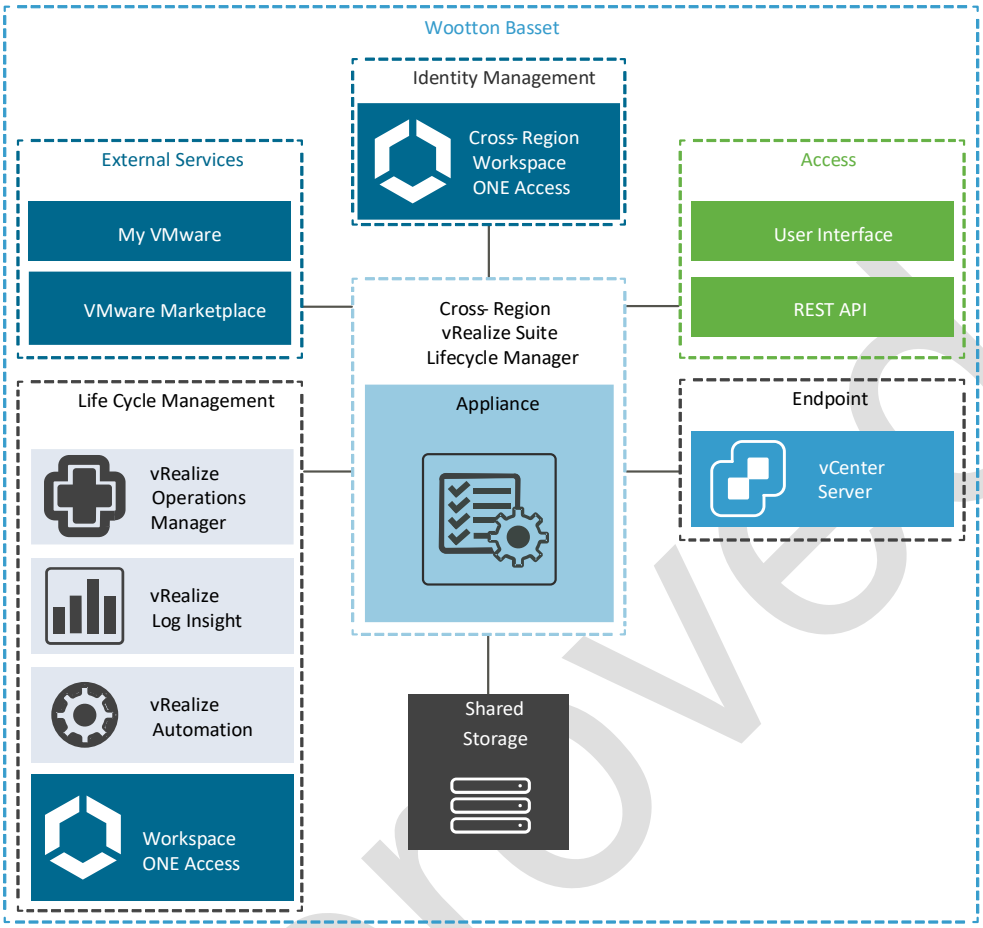


Figure 19 - Architecture of vRealize Suite Lifecycle Manager

Authentication Model

You can authenticate into vRealize Suite Lifecycle Manager by either local admin accounts or Workspace One Access. In the this deployment we will setup local admin accounts for emergency use but the main authentication method will be via Workspace One Access.

VMware Market Place Integration

Connectivity back to VMware market place will be required so we can pull own and deploy management packs for vRLI, vROP's and vRA.

Cloud Operations Design

The Cloud Operations design includes software components that make up the operations management layer. This operations management layer will provide deployment, sizing, networking, diagnostics, security and integration into other management solutions within VMO2.

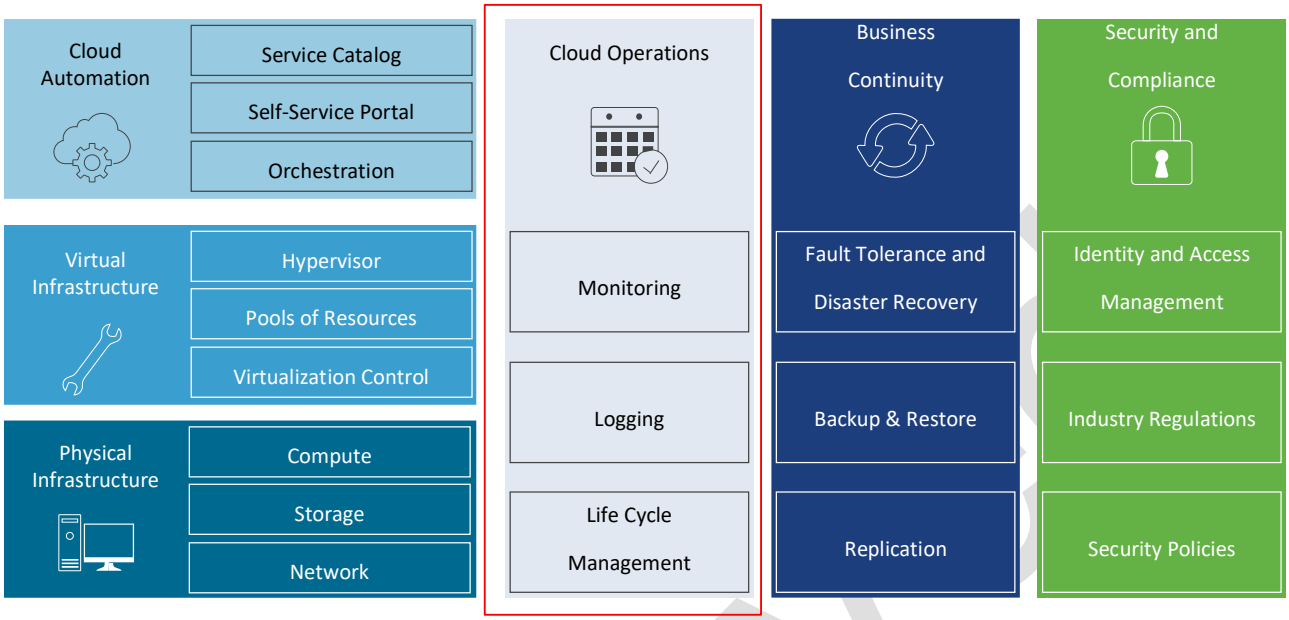


Figure 20 - Cloud Management in the SDDC

- Features of vRealize Suite Lifecycle Manager support initial installation and configuration of 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.

Design Decision

The following design decisions have been made for the vRealize Suite Lifecycle Manager solution for the VMO2 SDDCV2.5 WOOTON BASSET solution.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-LCM-VCF-VMO2 SDDCV2.5 WOOTON BASSET-001	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- VMO2 SDDCV2.5 WOOTON BASSET-002	Protect vRealize Suite Lifecycle Manager by using vSphere High Availability.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-003	Deploy vRealize Suite Lifecycle Manager by using SDDC Manager.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-005	If required Place the cross-region vRealize Suite Lifecycle Manager appliance in a dedicated virtual machine folder.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-006	Increase the initial storage of the vRealize Suite Lifecycle Manager appliance by 100 GB.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-007	Use SDDC Manager to perform the life cycle management of vRealize Suite Lifecycle Manager.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-008	If Required 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- VMO2 SDDCV2.5 WOOTON BASSET-009	Communicate with vRealize Log Insight using the default Ingestion API (cfapi) port 9000 with ssl=no.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5	Place the vRealize Suite Lifecycle Manager appliance on the cross-region virtual network segment.	VCF	

WOOTON BASSET-010			
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-012	Configure forward and reverse DNS records for the vRealize Suite Lifecycle Manager appliance.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-013	Configure NTP on the vRealize Suite Lifecycle Manager appliance.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-014	Upload and discover the vRealize Suite product binaries for install, patch, and upgrade binaries.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-015	If Required 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- VMO2 SDDCV2.5 WOOTON BASSET-016	Create a global environment in vRealize Suite Lifecycle Manager to support the deployment of Workspace ONE Access.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-017	If Required 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- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2	Enable integration between vRealize Suite Lifecycle Manager in Region A and your	VCF	

SDDCV2.5 WOOTON BASSET-019	corporate identity source by using the cross-region Workspace ONE Access instance.		
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-021	Assign the enterprise group for vRealize Suite Lifecycle Manager administrators, the LCM Cloud Admin role.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5	Configure a service account, in vCenter Server for application-to-application communication from vRealize Suite Lifecycle Manager to vSphere.	VCF	

WOOTON BASSET-027			
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-030	Rotate the root password on or before 365 days post-deployment.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-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- VMO2 SDDCV2.5 WOOTON BASSET-032	Use a SHA-2 or higher algorithm when signing certificates	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-033	Replace the default store passwords in the locker repository for use by life cycle operations.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-034	Import Certificate Authority-signed certificates to the locker repository for product life cycle operations.	VCF	
SDDC-MGMT-LCM-VCF- VMO2 SDDCV2.5 WOOTON BASSET-035	Import vRealize Suite product licenses to the locker repository for product life cycle operations.	VCF	

Table 31 - SDDC vRealize Suite Lifecycle Manager Design Decisions

4.15 Software Defined Networking Design for the Management and Workload Domains

We use NSX-T Data Center for connecting the management and workloads 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 and workload domains. 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 and workload domains, all these components run in the first cluster in the management domain.

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.

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.

Design Decision

Within the VMO2 SDDCV2.5 WOOTON BASSET design we will use multiple T0's and T1's, these will be used to separate the Production and Non Production traffic.

Logical Design for NSX-T Data Center for the Management and Workload Domains

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.

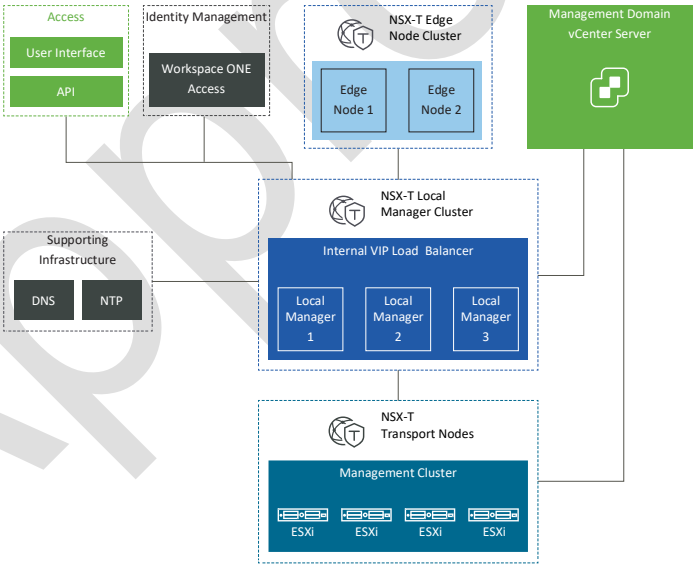


Figure 21 - NSX-T Logical Design for the Management Domain

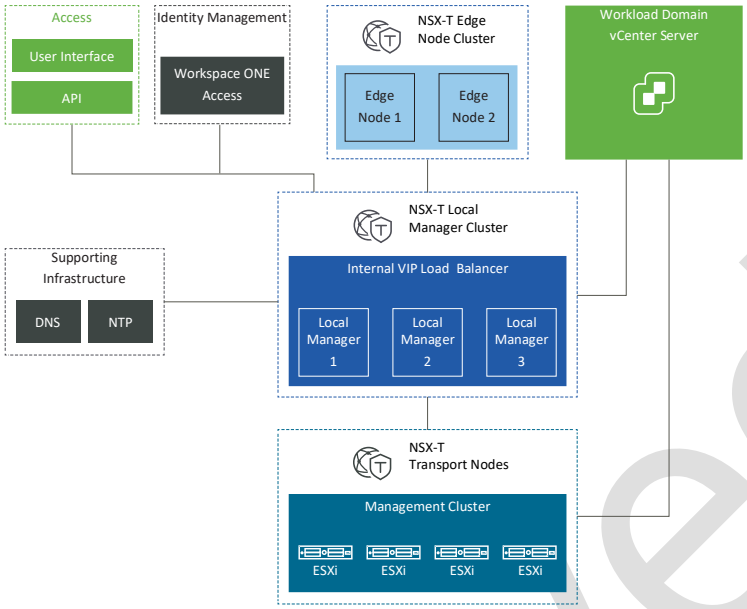


Figure 22 - NSX-T Logical Design for the Workload Domain

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 and Workload Domains

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

> ***Design Decision***
>
> Within the VMO2 SDDCV2.5 WOOTON BASSET design we will use the Leaf Spine topology.

In the environment 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.
This design uses BGP as the dynamic routing protocol, as such, BGP must be present to all environments within the solution.

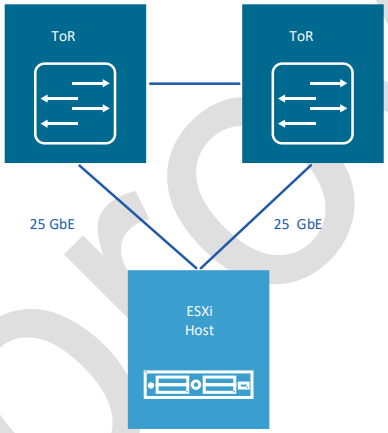


Figure 23 - Host to ToR Connectivity

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

Within the solution we will deploy highly available NSX-T manager instances. We will also deploy large size appliances so as to cope with future expansion over the next few years.

Appliance Size	vCPU	Memory (GB)	Storage (GB)	Scale
Large	12	48	300	More than 64 ESXi hosts

Table 32 - NSX-T Resource Specification

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

We will deploy NSX-T Edge nodes as physical appliances.

Form Factor		Appliance Size	CPU or vCPU	Memory (GB)	Storage (GB)
NSX-T Edge virtual appliance		Large Use in large environments that require load balancers	16 vCPU	768	480

Table 33 - Resource Specifications of NSX-T Edge Nodes

High Availability Design for the NSX-T Edge Nodes for the Management and Workload Domains

The NSX-T Edge clusters run on the management cluster in the management domain. vSphere HA and vSphere DRS protect the NSX-T Edge appliances.

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.

Edge Cluster

With this solution we will be using a dedicated Edge Cluster.

Network Design for the NSX-T Edge Nodes for the Management and Workload Domains

We will implement an NSX-T Edge configuration with a single N-VDS. We will 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.

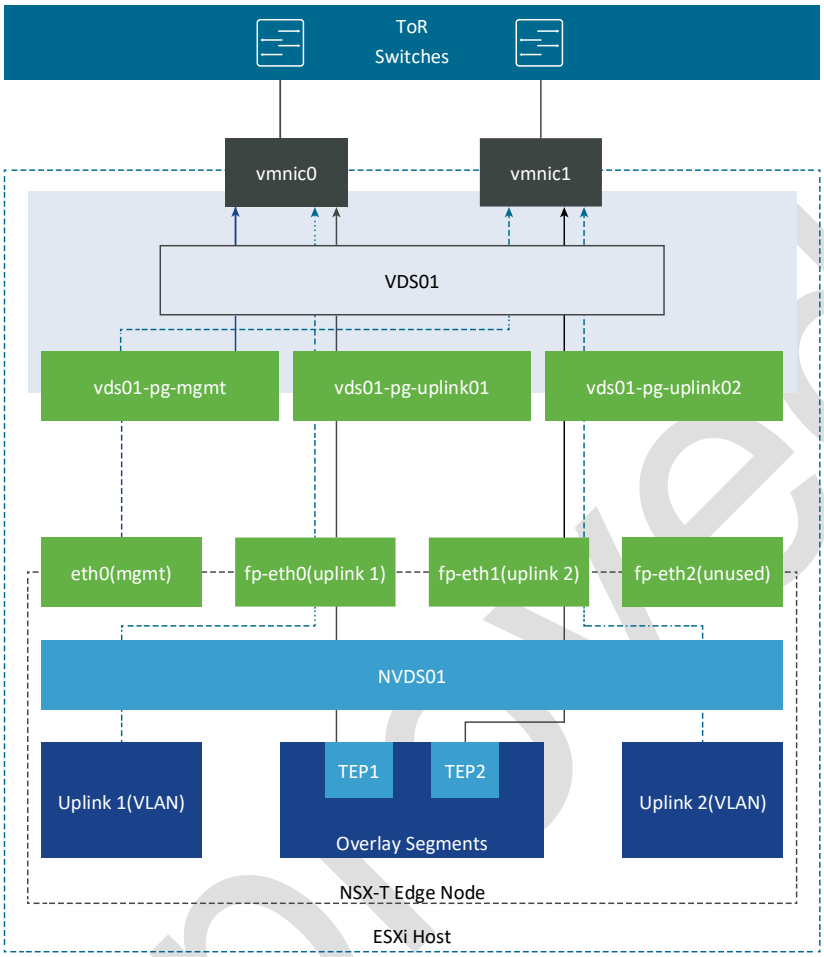


Figure 24 - NSX-T Edge Network Configuration

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

We will use the life cycle management of the NSX-T Data Center components. 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, we will perform life cycle management by using the Upgrade Coordinator which is a service in NSX-T Manager. When we implement the solution by using VMware Cloud Foundation, we will use SDDC Manager for life cycle management to provide automatic patching, upgrade, and product compatibility verification, are included as part of the life cycle management process.

NSX-T Services Design for the Management and Workload Domains

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, we will 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.

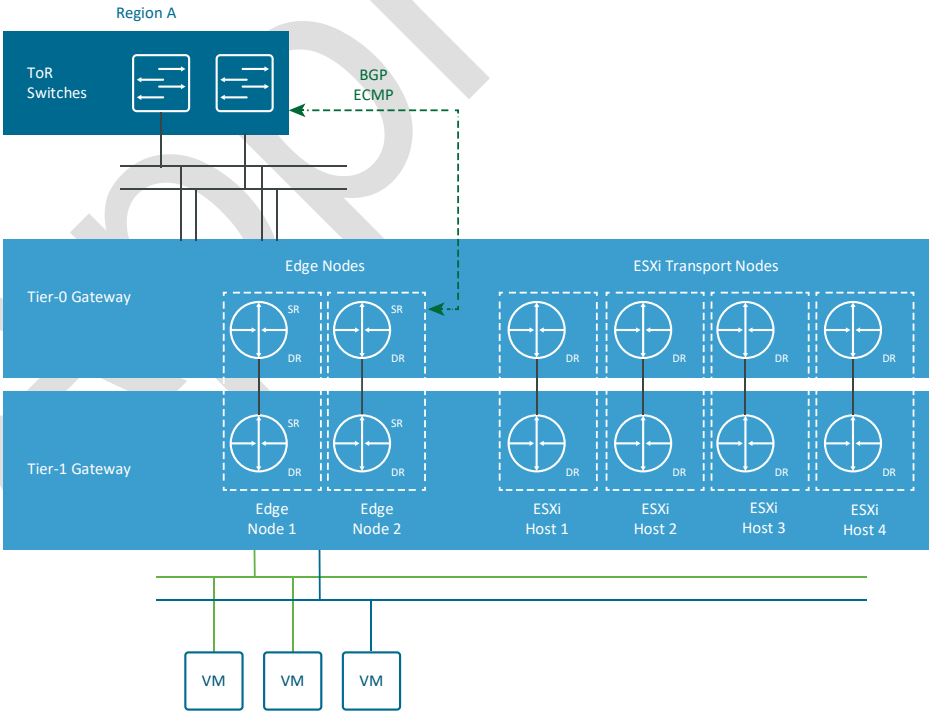


Figure 25 - NSX-T Dynamic Routing

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.

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

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.

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, we 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 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.

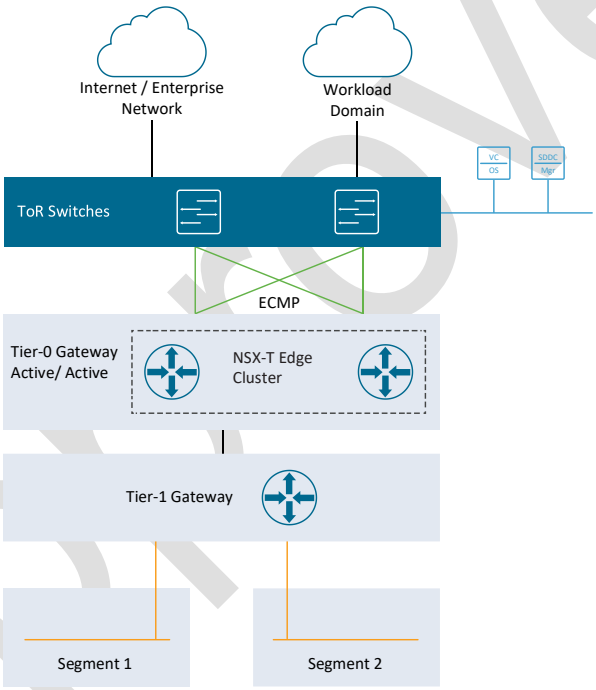


Figure 26 - Virtual Network Segments in SDDC

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

Authentication access, controls, and certificate management for the NSX-T Data Center instance in the management and workload domains will meet VMO2 standards.

Identity Management

Users will authenticate to NSX-T Managers via Active Directory by using Workspace One Access.

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 30 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 a Secure Sockets Layer (SSL) connection.All out of the box self signed certificates will be replaced with certificates that are signed by a third- party or enterprise Certificate Authority (CA).

Required NSX-T Components

The following NSX-T Components will be required for the solution.

Wootton Basset Management Domain

Component	vCPU	Memory	Disk Space
NSX Manager / Controller 1	6	24	200GB
NSX Manager / Controller 2	6	24	200GB
NSX Manager / Controller 3	6	24	200GB
NSX Manager Load Balancer			
Edge Node 1			
Edge Node 2			
NSX Edge Load Balancer			

Table 34 - Required NSX-T Components – Wooton Basset Management Domain

Wootton Basset Workload Domain

Component	vCPU	Memory	Disk Space
NSX Manager / Controller 1	6	24	200GB
NSX Manager / Controller 2	6	24	200GB
NSX Manager / Controller 3	6	24	200GB

NSX Manager Load Balancer			
Edge Node 1			
Edge Node 2			
NSX Edge Load Balancer			

Table 35 - Required NSX-T Components – Wootton Basset Workload Domain

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET SDN design will use the following design decisions to meet our Business and Technical requirements as well as VMware Best Practices.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-001	Use two ToR switches for each rack.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-003	Do not use EtherChannel (LAG, LACP, or vPC) configuration for ESXi host uplinks	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-004	Use a physical network that is configured for BGP routing adjacency	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-005	Assign static IP addresses to all management components in the SDDC infrastructure except for NSX-T tunnel endpoints (TEPs).	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-006	Set the lease duration for the TEP DHCP scope to at least 7 days.	VCF	

SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-007	Use VLANs to separate physical network functions.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-010	Configure VRRP, HSRP, or another Layer 3 gateway availability method for these networks: Management, Edge Overlay	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-013	Create a virtual IP (VIP) address for the NSX-T Manager cluster for the management domain.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-014	Apply VM-VM anti-affinity rules in vSphere Distributed Resource Scheduler (vSphere DRS) to the NSX-T Manager appliances.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-015	In vSphere HA, set the restart priority policy for each NSX-T Manager appliance to high.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5	Create a virtual machine group for the NSX-T Manager appliances.	VCF	

WOOTON BASSET-016			
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-017	Place the appliances of the NSX- T Manager cluster on the management VLAN network.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-018	Allocate a statically assigned IP address and host name to the nodes of the NSX-T Manager cluster.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-020	Configure NTP on each NSX-T Manager appliance.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-021	Use large-size NSX-T Edge virtual appliances.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-022	Deploy the NSX-T Edge virtual appliances. Do not configure a dedicated vSphere cluster for edge nodes.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-023	Deploy two NSX-T Edge appliances in an edge cluster in the first cluster in the management domain.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-024	Apply VM-VM anti-affinity rules for vSphere DRS to the virtual machines of the NSX-T Edge cluster.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-025	In vSphere HA, set the restart priority policy for each NSX-T Edge appliance to high.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-026	Configure all edge nodes as transport nodes.	VCF	

SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-029	Connect the management interface eth0 of each NSX-T Edge node to the management VLAN.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-031	Use a single N-VDS in the NSX-T Edge nodes.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-033	Use a dedicated VLAN for edge overlay that is different from the host overlay VLAN	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-035	Deploy an active-active Tier-0 gateway.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5	To enable ECMP between the Tier-0 gateway and the Layer 3 devices (ToR switches or upstream devices), create two	VCF	

WOOTON BASSET-036	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.		
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-037	Assign a named teaming policy to the VLAN segments to the Layer 3 device pair.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-038	Create a VLAN transport zone for Edge uplink traffic.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-039	Use BGP as the dynamic routing protocol	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-041	Do not enable Graceful Restart between BGP neighbors.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-042	Enable helper mode for Graceful Restart mode between BGP neighbors	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-043	Enable Inter-SR iBGP routing.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-044	Deploy a Tier-1 gateway and connect it to the Tier-0 gateway.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-045	Deploy a Tier-1 gateway to the NSX-T Edge cluster	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-046	Deploy a Tier-1 gateway in non-preemptive failover mode.	VCF	

SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-054	Configure Availability Zone 2 neighbors to use the route maps as In and Out filters respectively.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-055	Deploy a standalone Tier-1 gateway to support advanced stateful services such as load balancing for other management components.	VCF	

SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-056	Connect the standalone Tier-1 gateway to the cross- region virtual network.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-057	Configure the standalone Tier-1 gateway with static routes to the gateways of the networks it is connected to.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-058	Enable all ESXi hosts in the management domain as NSX-T transport nodes.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-059	Configure each ESXi host as a transport node without using transport node profiles	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-061	To provide virtualized network capabilities to management workloads, use overlay networks with NSX-T Edge nodes and distributed routing.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-062	Create a single overlay transport zone for all overlay traffic across the management domain and NSX-T Edge nodes.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-063	Create a single VLAN transport zone for uplink VLAN traffic that is applied only to NSX-T Edge nodes.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-064	Create an uplink profile with the load balance source teaming policy with two active uplinks for ESXi hosts.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-065	Use hierarchical two-tier replication on all segments.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-068	Limit the use of local accounts.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-069	Enable NSX-T Manager integration with your corporate identity source by using the region-specific Workspace ONE Access instance.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-070	Use Active Directory groups to grant privileges to roles in NSX-T Data Center.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-074	Restrict end-user access to both NSX-T Manager user interface and its RESTful API endpoint.	VCF	
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5	Configure the passwords for access to the NSX-T Manager user interface and RESTful API or the root, admin, and audit	VCF	

WOOTON BASSET-077	users, and account lockout behavior for CLI according to the industry standard for security and compliance of your organization.		
SDDC-MGMT-SDN-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-079	Use a SHA-2 algorithm or stronger when signing certificates.	VCF	

Table 36 - NSX-T Data Center Design Decisions

5 INFRASTRUCTURE - VMWARE CLOUD ARCHITECTURE

5.1 VMware vRealize Log Insight

vRealize Log Insight is deployed as part of the core VMware Cloud Foundation platform in the Management Domain. This instance of vRealize Log Insight that we are deploying consists of three medium sized nodes with an integrated load balancer. vRealize Log Insight should be protected from unauthorized access by integrating it with Active Directory.

All components, management VM,s and ESXi hosts are automatically configured to send their logs to vRealize Log Insight. The vRealize Suite components are not automatically configured and these will need to be done manually post installation. vRealize Operations Manager comes with the vRealize Log Insight agent pre installed, although each agent needs to be configured to send their logs to the appropriate destination.

vRealize Log Insight Overview

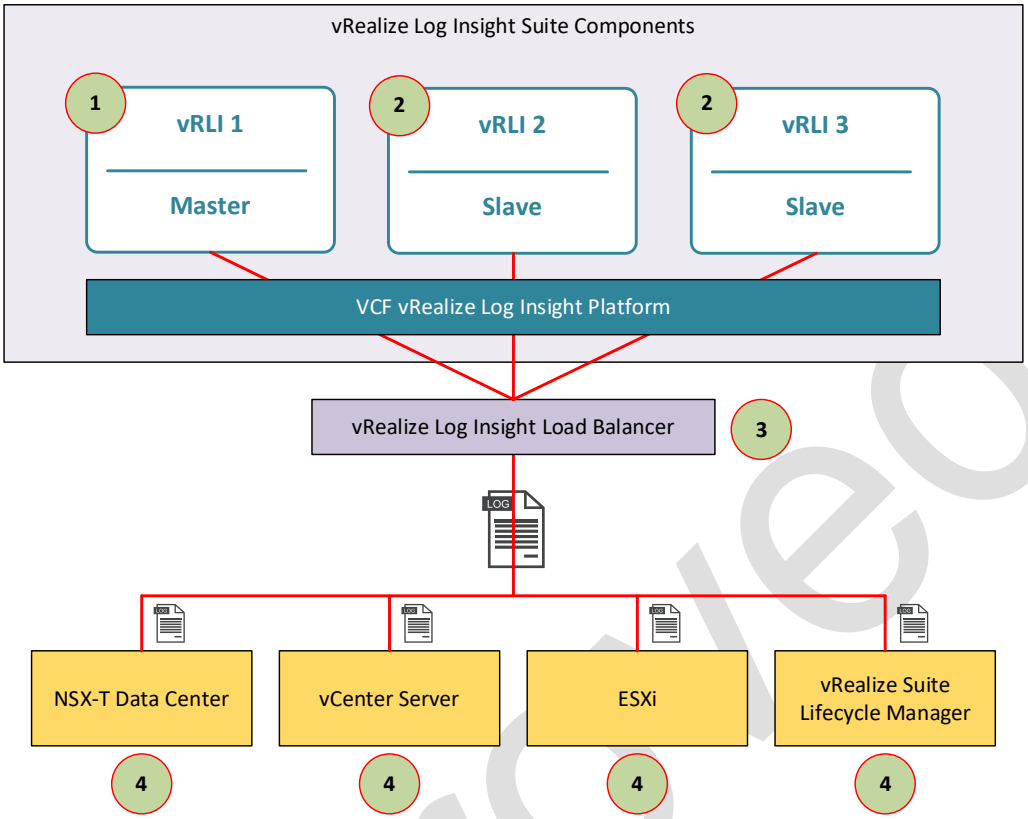


Figure 27 - vRealize Log Insight Overview

vRealize Log Insight Points of Interest

the table below shows highlights the main components in the solution.

Number	Component	Description
1	vRLI Master	All alerts are sent to the load balancer. The master server provides control over the vRLI Cluster and it servers.
2	vRLI Slave	The Slave vRLI server handle logs and can be promoted into a master via the vRLI interface

3	vRLI Load Balancer	This can either be an NSX load balancer of AVI Advanced load Balancer
4	SDDC Components	The SDDC components will forward their logs into the vRLI Solution.

Table 37 - vRealize Log Insight Points of Interest

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

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).

Design Decision

The vRealize Log Insight solution in VMO2 SDDCV2.5 WOOTON BASSET will use a Master and Worker solution via a High Availability Cluster.

Design Decision

The VMO2 SDDCV2.5 WOOTON BASSET VRLI design will use the following design decisions.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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	VCF	

	first cluster in the management domain.		
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-002	Deploy vRealize Log Insight by using vRealize Suite Lifecycle Manager.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-003	Protect all vRealize Log Insight nodes by using vSphere High Availability.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-004	Apply vSphere Distributed Resource Scheduler (DRS) anti-affinity rules to the vRealize Log Insight cluster nodes.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-006	Place the region-specific vRealize Log Insight nodes in a dedicated virtual machine folder in Region A,	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-007	Deploy each node in the vRealize Log Insight cluster as a medium-size appliance.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-008	Use vRealize Suite Lifecycle Manager to perform the lifecycle management of vRealize Log Insight.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-009	Configure a retention period of 7 days for the medium-size vRealize Log Insight appliance.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-011	Enable alert notifications.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-012	Forward alerts to vRealize Operations Manager.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-013	Support launch in context with vRealize Operation Manager.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-014	Enable embedded vRealize Log Insight user interface in vRealize Operations Manager.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-015	Place the vRealize Log Insight nodes on the region-specific virtual network segment	VCF	

SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-016	Allocate statically assigned IP addresses and host names to the vRealize Log Insight nodes in the management domain.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-017	Configure forward and reverse DNS records for all vRealize Log Insight nodes and the ILB VIP address.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-018	Enable the vRealize Log Insight Integrated Load Balancer (ILB) for balancing incoming.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-019	Configure NTP on each vRealize Log Insight appliance	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-020	Install the following content packs: VMware – Linux, VMware - Linux Systemd, NSX-T Data Center	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-021	Configure the following agent groups that are related to content packs: SDDC - Linux OS, SDDC - Photon OS	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-025	Configure all vCenter Server instances as direct syslog sources to send log data directly to vRealize Log Insight.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-026	Configure the vRealize Log Insight agent on the SDDC Manager appliance.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-027	Configure the vRealize Log Insight agent on the vRealize Suite Lifecycle Manager appliance.	VCF	

SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-028	Configure the Fluentd vRealize Log Insight plugin on the vRealize Automation appliance instances.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-029	Configure the vRealize Log Insight agent for the vRealize Operations Manager appliances including: Analytics nodes, Remote Collector instances	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-031	Communicate with the syslog clients, such as ESXi, vCenter Server, NSX-T Data Center, using the TCP protocol.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-032	Do not configure vRealize Log Insight to update automatically all deployed agents.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-035	Assign the enterprise group for vRealize Log Insight administrators the Super Admin role.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-037	Assign the enterprise group for vRealize Log Insight users the User role.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-039	Assign the enterprise group for vRealize Log Insight viewers the View Only Admin role.	VCF	

SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-041	Enable vRealize Operations Manager integration in vRealize Log Insight using the vRealize Operations Manager service account	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-045	Rotate the root password on or before 365 days post deployment.	VCF	
SDDC-MGMT-VRLI-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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 38 - VMO2 SDDC Design Decisions for vRealize Log Insight

5.2 VMware vRealize Operations Manager.

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.

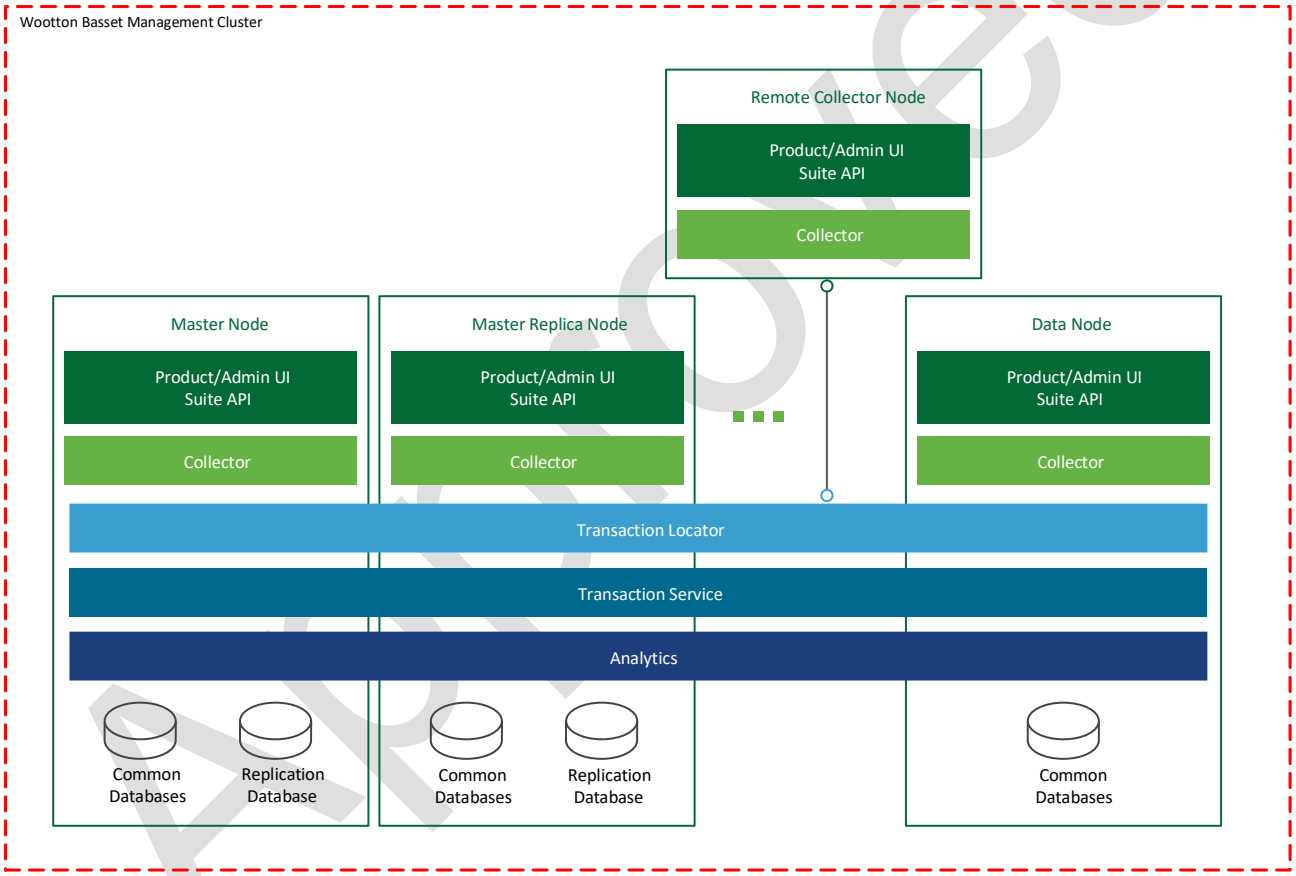


Figure 28 - vRealize Operations Manager Architecture

Node Types

There are various types of nodes within the vRealize Operations Manager architecture but in this design, we will be using a mixture of Master, Data and Collector nodes in an Analytics Cluster.

Master Node

The master Node manages all other nodes within the cluster.

Master Replica Node

This node allows us to use high availability within the Analytic Cluster.

Remote Collector Nodes

These will be used on some of the workload cluster and forward collected data onto the Master Nodes.

Data Nodes

Data nodes have adapters installed to perform data collection and analysis. Data nodes also host vRealize Operations Manager management packs.

Cluster Type

There are two cluster types with vRealize Operations Manager, in this design we will be using and Analytic Cluster.

Analytic Cluster

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

vRealize Operations Manager Logical Design

The initial deployment will utilize a vROPs Master, Data and Replica servers in the analytics cluster, when a new workload domain is introduced then a vROPs remote collector server can be introduced if required.

vRealize Operation Manager will be integrated into Active Directory for centralized audits and authentication.

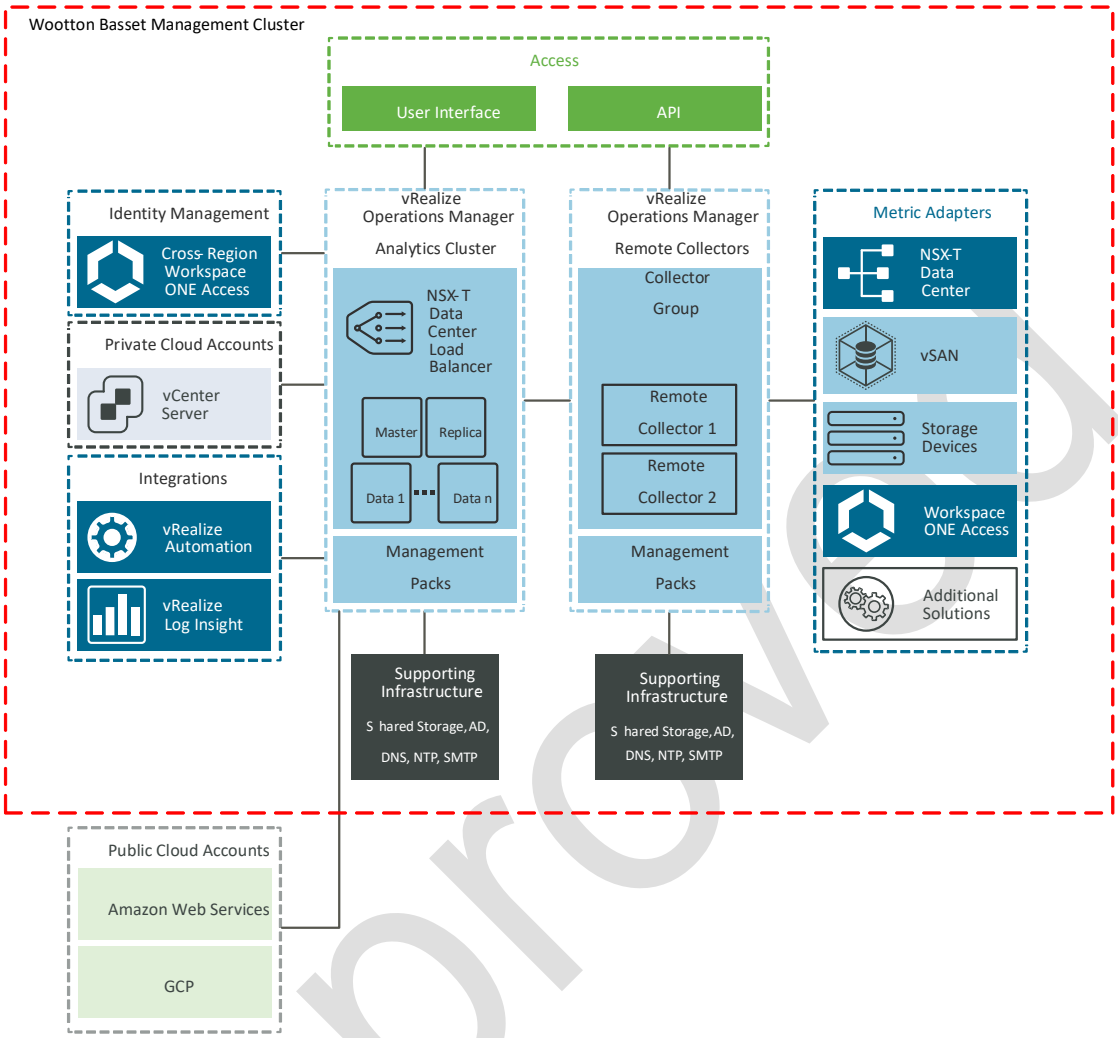


Figure 29 - Logical Design for vRealize Operations Manager

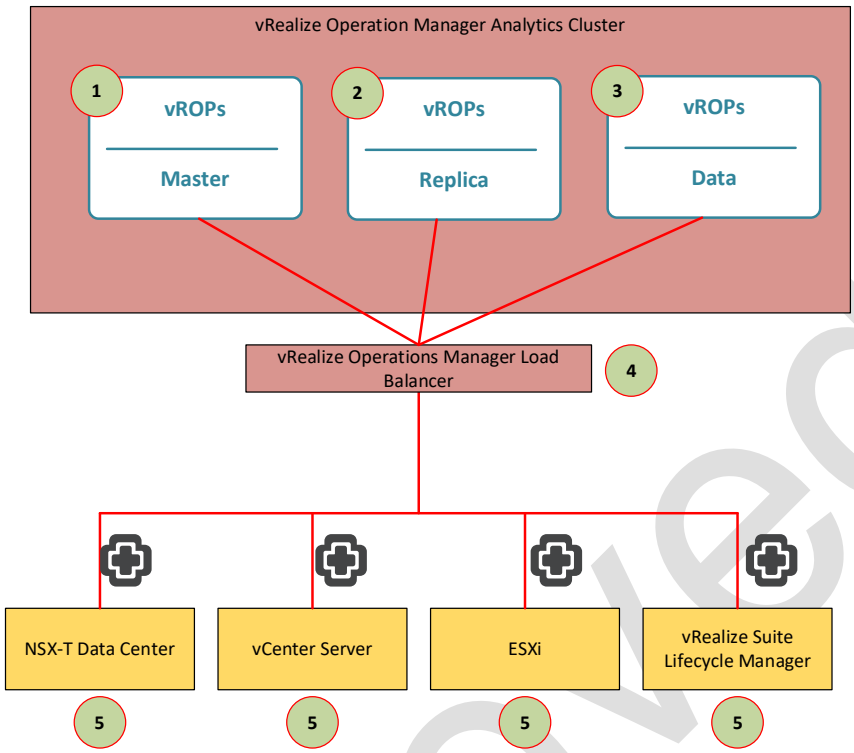


Figure 30 - VMO2 vROPs Logical Design

vRealize Operations Manager Points of Interest

the table below shows highlights the main components in the solution.

Number	Component	Description
1	vROPs Master Node	All alerts are sent to the load balancer. The master server provides control over the analytics cluster
2	vROPs Replica Node	The Replica server does the same as the master and can take ownership of the cluster if required.
3	vROPs Data Node	The Data Node collects data and provides reports.
4	vROPs Load Balancer	This will be via and NSX load balancer
5	VMO2 SDDC Components	The SDDC components will be connected to the Operations Master to gather information from them.

Table 39 - vROPs Points of Interest

vRealize Operations Manager Sizing

vRealize Operations manager can be rolled out in different sizing configurations, however for the deployment we will use the Medium configuration, this will allow the environment to grow without the need to increase the sizing of the Analytics Cluster.

vRealize Operations Manager Management Packs

In order to get the most of vRealize Operations Manager you can download and add in various Management Packs from the VMware marketplace. Once these have been added the analytics and information contained in the solution will give deep insights as to how the systems is running etc.

Design Decision

The following design decisions have been made for the vRealize Operations Manager solution for the VMO2 SDDCV2.5 WOOTON BASSET solution.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-002	Deploy two remote collector nodes on the first cluster in the management domain in the region.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-003	Use vRealize Suite Lifecycle Manager to deploy vRealize Operations Manager.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-004	Protect all vRealize Operations Manager nodes by using vSphere High Availability.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-005	Apply vSphere Distributed Resource Scheduler (DRS) anti-affinity rules to the vRealize	VCF	

	Operations Manager analytics cluster.		
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-006	Apply vSphere Distributed Resource Scheduler (DRS) anti-affinity rules to the vRealize Operations Manager remote collector group.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-008	Place the cross-region vRealize Operations Manager nodes in a dedicated virtual machine folder in Region A	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-010	Deploy each node in the analytics cluster as a medium-size appliance.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-011	If the number of SDDC objects exceeds 12,500, add more medium-size nodes to the analytics cluster.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-012	Increase the initial storage of each vRealize Operations Manager analytics cluster node by 1 TB.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-013	Deploy each remote collector node as a standard-size appliance.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-014	Use vRealize Suite Lifecycle Manager to perform the life cycle management of vRealize Operations Manager.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-015	Configure vRealize Operations Manager to send logs to the vRealize Log Insight cluster in Region A.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-016	Communicate with the vRealize Log Insight using the default Ingestion API (cfapi) port 9000 and ssl=no.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-017	Configure vRealize Operations Manager to use an outbound SMTP mail server to route notifications for system events.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-018	Configure the correct currency in the vRealize Operations Manager global options.	VCF	

SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-019	Place the vRealize Operations Manager analytics nodes on the cross-region virtual network segment	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-020	Place the vRealize Operations Manager remote collector nodes on the region-specific virtual network segment	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-023	Configure forward and reverse DNS records for all vRealize Operations Manager nodes and the VIP address.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-027	Add an NSX-T Data Center load balancer fast TCP application profile for vRealize Operations Manager.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-028	Add an NSX-T Data Center load balancer source IP persistence profile for vRealize Operations Manager.	VCF	

SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-032	Do not use a load balancer for the vRealize Operations Manager remote collector nodes.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-033	Configure NTP on each vRealize Operations Manager appliance.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-034	Configure the timezone of vRealize Operations Manager to use UTC.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-035	Configure a vCenter Server cloud account for each vCenter Server instance in the SDDC.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-036	Configure each vCenter Server cloud account to use the remote collector group for its region.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-037	Enable the vSAN integration in the vCenter Server cloud accounts.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-038	Configure the vRealize Automation integration in vRealize Operations Manager.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-039	Configure the vRealize Automation integration to use the default collector group.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-040	Configure the vRealize Log Insight integration in vRealize Operations Manager.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-041	Configure the vRealize Log Insight integration to use the remote collector group.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-042	Install the Storage Devices management pack for vRealize Operations Manager.	VCF	

SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-043	Install the Workspace ONE Access management pack for vRealize Operations Manager.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-045	Configure the cross-region Workspace ONE Access integration to use the default collector group.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-046	Enable vRealize Operations Manager integration with your corporate identity source by using Workspace ONE Access.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-048	Assign the enterprise group for vRealize Operations Manager administrators, the Administrator role.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-050	Assign the enterprise group for vRealize Operations Manager content administrators the ContentAdmin role.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-052	Assign the enterprise group for vRealize Operations Manager read-only users, the ReadOnly role.	VCF	

SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-055	Configure each vCenter Server cloud account to use the vCenter Server service account	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-058	Configure the vSAN integration in the vCenter Server cloud account to use the vSAN service account	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-059	Create a service in the directory services and ensure it is synchronized in Workspace ONE Access.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-061	Create a service in the directory services and ensure it is synchronized in Workspace ONE Access.	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-063	Configure the endpoint of the NSX-T management pack for vRealize Operations Manager	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-067	Rotate the root password on or before 365 days post deployment	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-068	Rotate the admin password on or before 60 days post deployment	VCF	
SDDC-MGMT-VROP-VCF-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-070	Use a SHA-2 or higher algorithm when signing certificates.	VCF	

Table 40 - VMO2 SDDC Design Decisions for vRealize Operations Manager

vRealize Network Insight Overview

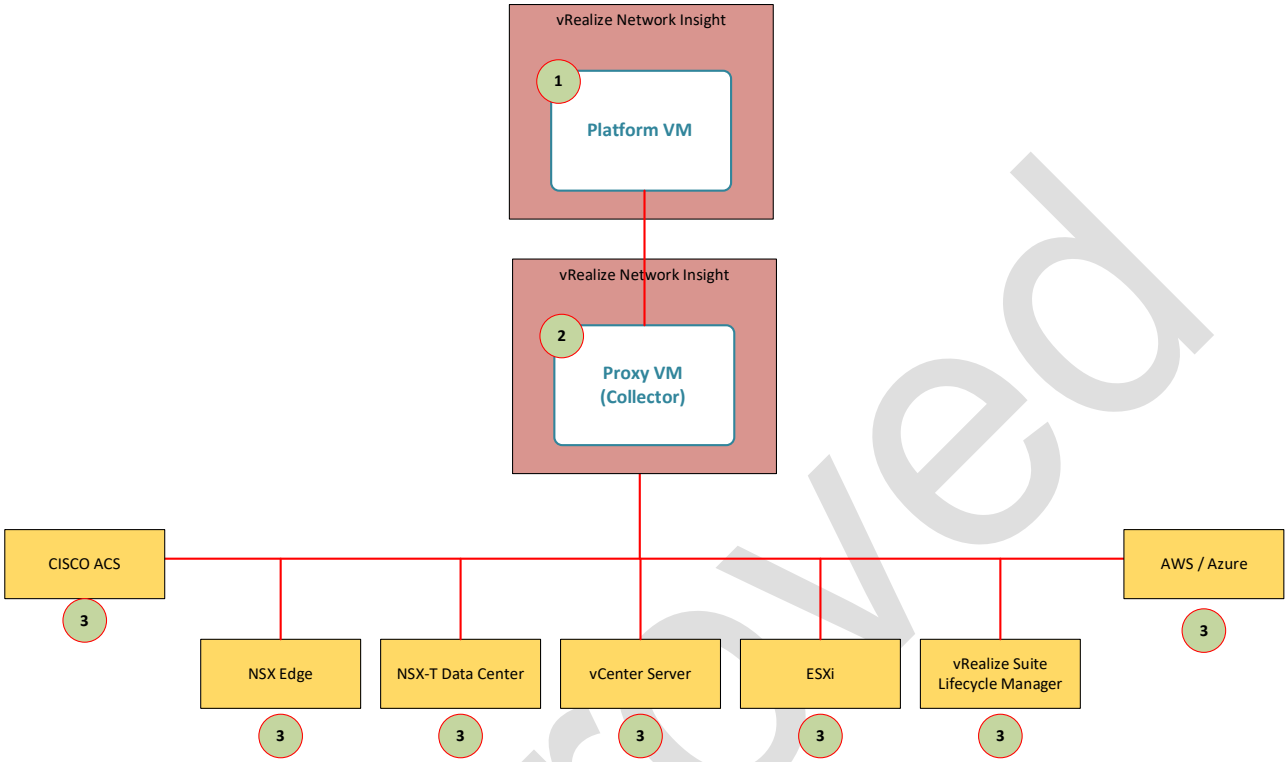


Figure 31 - vRealize Network Insight Overview

vRealize Network Insight Points of Interest

Number	Component	Description
1	vRNI Platform VM	Used to receive all the data, user access is via this portal
2	vRNI Collector VM	Used to collect data from endpoints on the network, additional servers can be provided to scale out into additional workload clusters
3	Collection points	End points that provide data into the solution.

Table 41 - vRNI Points of Interest

5.3 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.

In the context of our SDDC, Workspace ONE Access is the broker between our existing authentication provider Active Directory and the SDDC solution, 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 solution. In this design, the identity and access management function is provided by VMware Workspace ONE Access.

Logical Design for Workspace One Access

The solution will integrate with our systems.private Active Directory. The Workspace One cluster will comprise of three Workspace One servers that will be load balanced to provide one Access URL point. This design allows for the capacity required but also has built in resilience in the situation of a node becoming unstable or unusable.

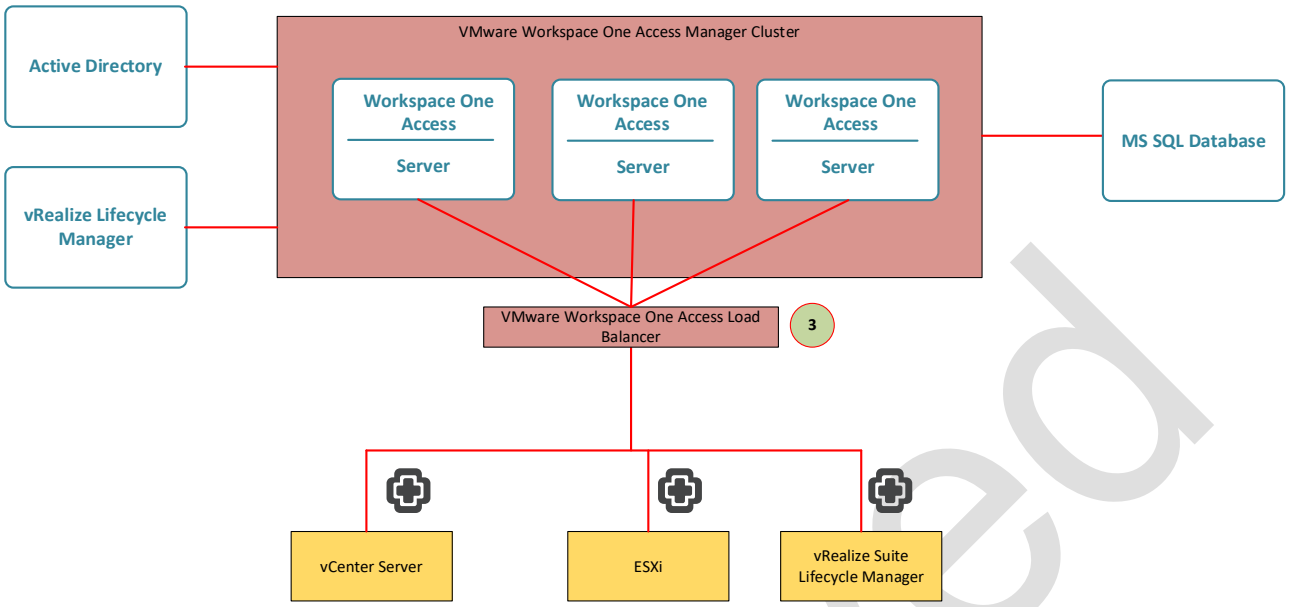


Figure 32 - Workspace One Access Logical Design

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)

Design Decision

The following design decisions have been made for the Workspace One Access solution for the VMO2 SDDCV2.5 WOOTON BASSET solution.

Design Decision ID	Design Decision Description	Applicable to Architecture Model	Technical / Business Requirement.

SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-001	Deploy a standalone Workspace ONE Access instance on the first cluster in the management domain in the region.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-003	Protect each Workspace ONE Access node by using vSphere High Availability.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-004	When using two availability zones, add the Workspace ONE Access appliance to the primary availability zone VM group	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-005	Place each region-specific Workspace ONE Access node in a dedicated VM folder for its region	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-006	Configure a directory service connection, rainpole.io, for the Workspace ONE Access instance in each region.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-007	Use Active Directory with Integrated Windows Authentication as the Directory Service connection option.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-008	Use an account with the Account Operators role in Active Directory, VMO2 SDDCV2.5 WOOTON BASSET.rainpole\svc-domain-join, to perform domain join operations for the Workspace ONE Access connectors.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-009	Use an account with the Domain Users role in Active Directory, to perform domain bind operations.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-010	Configure the directory to synchronize only groups required for the integrated SDDC solutions.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-012	Enable Workspace ONE Access to synchronize nested group members by default.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-013	Add a filter to the directory settings to exclude users from the directory replication	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-014	Configure the mapped attributes included when a user is added to the Workspace ONE Access directory.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-015	Configure the directory synchronization frequency to a reoccurring schedule, for example, 15 minutes.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-019	Configure forward and reverse DNS records for each Workspace ONE Access appliance IP address for each regional instance.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-020	Configure NTP for each Workspace ONE Access appliance.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-022	Assign roles to groups, synchronized from your corporate identity source for Workspace ONE Access.	VCF	

SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-024	Assign the enterprise group for super administrators, the Super Admins Workspace ONE Access role.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-026	Assign the enterprise group for directory administrator users,the Directory Admins Workspace ONE Access role.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-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-VMO2 SDDCV2.5 WOOTON BASSET-028	Assign the enterprise group for read-only users, the ReadOnly Admin Workspace ONE Access role.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-029	Rotate the appliance root user password on a schedule post deployment.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-030	Rotate the appliance sshuser user password on a schedule post deployment.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-031	Rotate the admin application user password on a schedule post deployment.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-032	Configure a password policy for the Workspace ONE Access local directory admin user.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-033	Replace the default self- signed certificates with a Certificate Authority-signed certificate during the deployment.	VCF	

SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-034	Import the certificate for the Root Certificate Authority to each Workspace ONE Access instance.	VCF	
SDDC-MGMT-IAM-VMO2 SDDCV2.5 WOOTON BASSET-035	Use a SHA-2 or higher algorithm when signing certificates.	VCF	

Table 42 – VMO2 SDDC Design Decisions for Workspace ONE Access

5.4 VMware Hybrid Cloud Extension (HCX) - Optional

VMware Hybrid Cloud Extension is initially deployed as a virtual appliance (HCX Manager), along with a vCenter plug-in that enables the HCX feature. After the HCX Manager virtual appliance is deployed, it is responsible for deploying the other appliances required for HCX. Mirror appliances are deployed at both the source and target (cloud provider) locations. These deployments provide the capabilities outlined below.

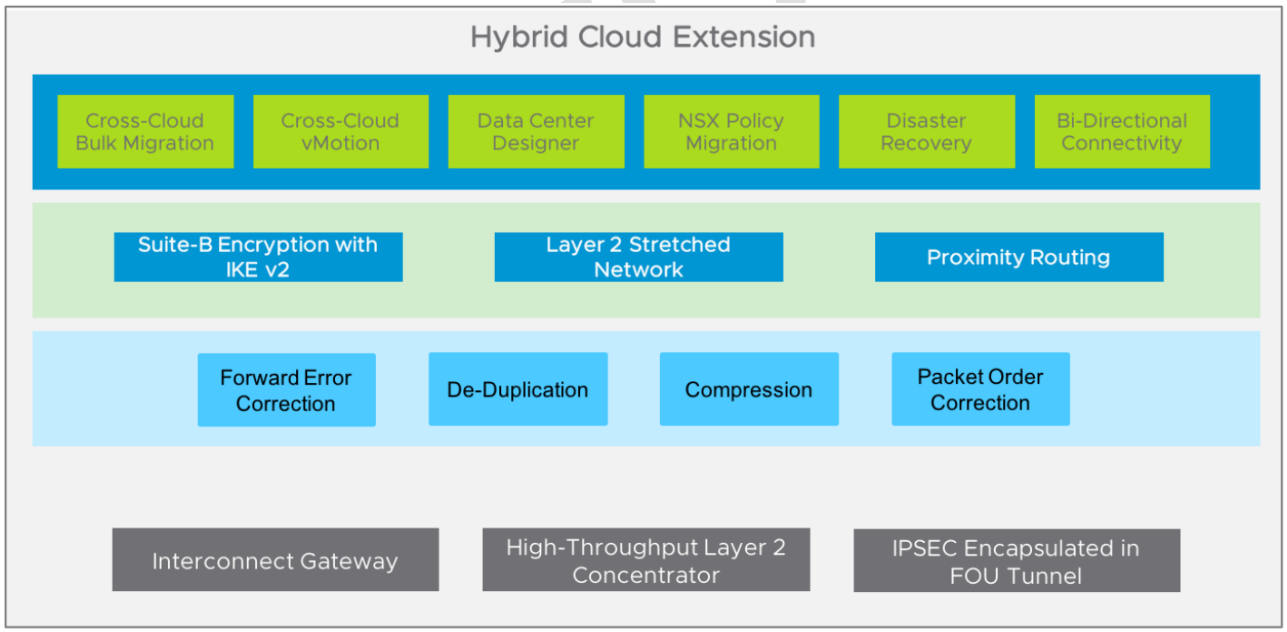


Figure 33 - HCX Solution Overview

HCX Infrastructure Components

HCX Manager

The HCX Manager is an open virtual appliance (OVA) downloaded from the VMware HCX service after logging in to VMware Cloud Services. It provides a management plug-in for vCenter that bootstraps the HCX services and manages virtual appliance deployment and connectivity. There can only be one HCX Manager per vCenter. After HCX Manager has been deployed and activated with connect.hxc.vmware.com, the administrator will select the data center location and complete the vCenter Single Sign-On (SSO) configuration.
The HCX virtual appliances are:

- HCX Manager
- HCX Interconnect service (CGW)
- Network Extension service (L2C), required for L2 extension
- WAN Optimization service

HCX Interconnect Appliance

The HCX interconnect service, also referred to as the WAN Edge, provides resilient access over the Internet and interconnects multiple private lines to the target site. This service provides strong Suite B encryption and traffic optimization between the source and target sites. It also simplifies secure pairing of site and management of HCX components.
The Interconnect appliance provides connectivity between the source and target data centers by using site pairing, and bootstraps the bi-directional hybrid connection, providing resilient connectivity over multiple circuits
The WAN Edge provides WAN Optimization (compression and de-duplication), intelligent routing and IPSEC with Suite B encryption (using certificates, and not pre-shared keys). Features such as vMotion and vSphere Replication are securely proxied behind this abstraction layer with a fully encrypted connection. Although vSphere 6.0 provides cross-vCenter vMotion, the two vCenter servers must be linked (for initiating vMotion from the GUI) and reside on the same SSO domain. Other considerations such as Fault Domain and routing requirements might not be suited to tenant and cloud provider environment. Using HCX these constraints do not need to be considered.

WAN Optimization Appliance

This is the second service to install by the bootstrap process. The WAN optimization service provides compression and deduplication across the WAN. WAN optimization improves performance characteristics of the private lines or internet paths by leveraging techniques like data de-duplication and line conditioning. This optimization makes performance closer to a LAN environment. VMware HCX requires a minimum throughput

of 100Mbps and excels on the Internet connections where workloads can be securely and optimally migrated.

Network Extension Appliance

The network extension service provides high-throughput connectivity with integrated proximity routing that unlocks seamless mobility and simple disaster recovery plans across sites. This service enables the mobility of VMs seamlessly and keeps the same IP and MAC address across sites without the need for NSX at the source site. Proximity routing can eliminate the traffic trombone effect, and vMotion-aware proximity routing ensures that vMotion tasks are not aborted due to spikes in network latency. HCX is bi-directional. When a network is extended from the source site to the target site, it will deploy the HCX layer 2 concentrator on the source, and a mirror image of the concentrator will be deployed on the destination to prepare for network to be stretched

HCX Migration Options

HCX provides multiple ways to Migrate / Move Virtual Machines.

VMware HCX Bulk Migration

This migration method uses the VMware vSphere Replication protocols to move the virtual machines to a destination site.

- The Bulk migration option is designed for moving virtual machines in parallel.
- This Migration type can be set to complete on a pre defined schedule.
- The virtual machine runs at the source site until the failover begins. The service / application is interrupted with the bulk migration. It is equivalent to a reboot.

VMware HCX vMotion

This migration method uses the VMware vMotion protocol to move the virtual a single virtual machine to a remote site.

- The vMotion migration option is designed for moving a single virtual machine at a time.
- Virtual machine state is migrated. There is no service interruption during the VMWare HCX vMotion migration.

VMware HCX Cold Migration

This migration method uses the VMware NFC protocol. It is automatically selected when the source virtual machine is powered off.

VMware HCX Replication Assisted vMotion

VMware HCX Replication Assisted vMotion (RAV) combines advantages from VMware HCX Bulk Migration (Parallel operations, resiliency and scheduling) with VMware HCX vMotion (zero downtime virtual machine state migration).

VMware HCX OS Assisted vMotion

This migration method provides for the Bilk Migration of a guest (non vSphere – KVM and Hyper-V) virtual machines using the OS Assisted Migration to VMware vSphere on premise or cloud based data center. This migration method has some downtime (2 reboots of target VM).

HCX Versions

HCX Enterprise

HCX Enterprise has the following components included within it.

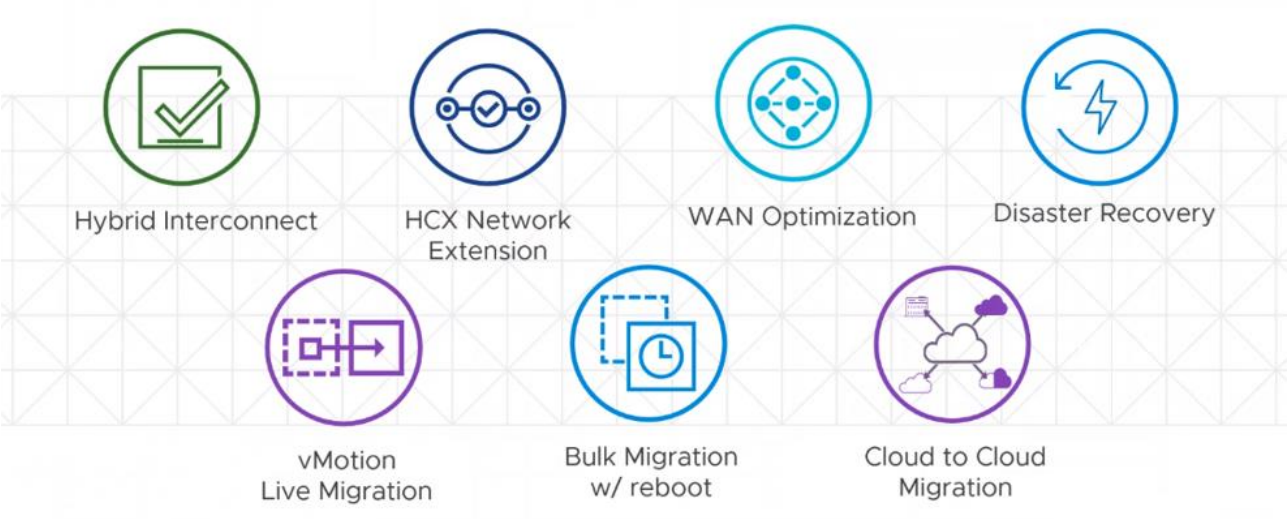


Figure 34 - HCX Enterprise Components

HCX Enterprise Plus

HCX Enterprise Plus has the following components included within it.

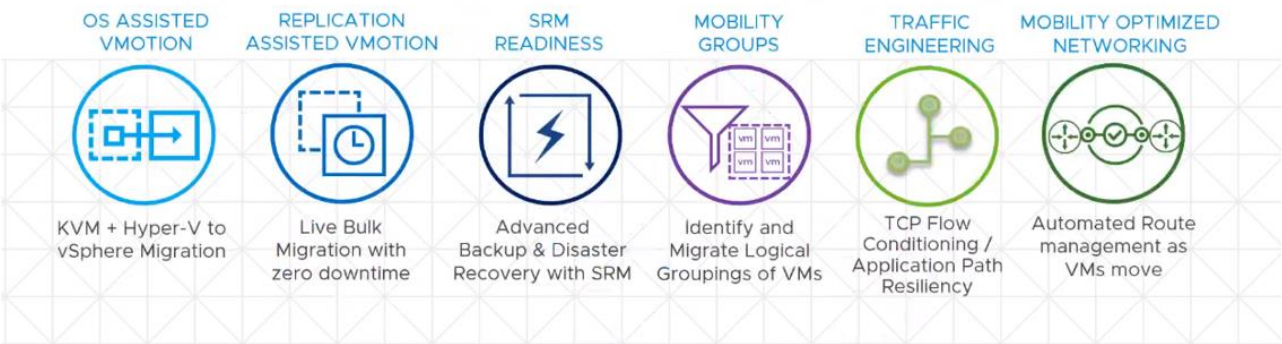


Figure 35 - HCX Enterprise Plus Components

5.5 vRealize Network Insight

VMware vRealize Network Insight

vRealize Network Insight helps you build an optimized, highly available and secure network infrastructure across hybrid and multi-cloud environments. It provides network visibility and analytics to accelerate micro-segmentation security, minimize risk during application migration, optimize network performance and confidently manage and scale NSX deployments.

vRealize Network Insight Overview

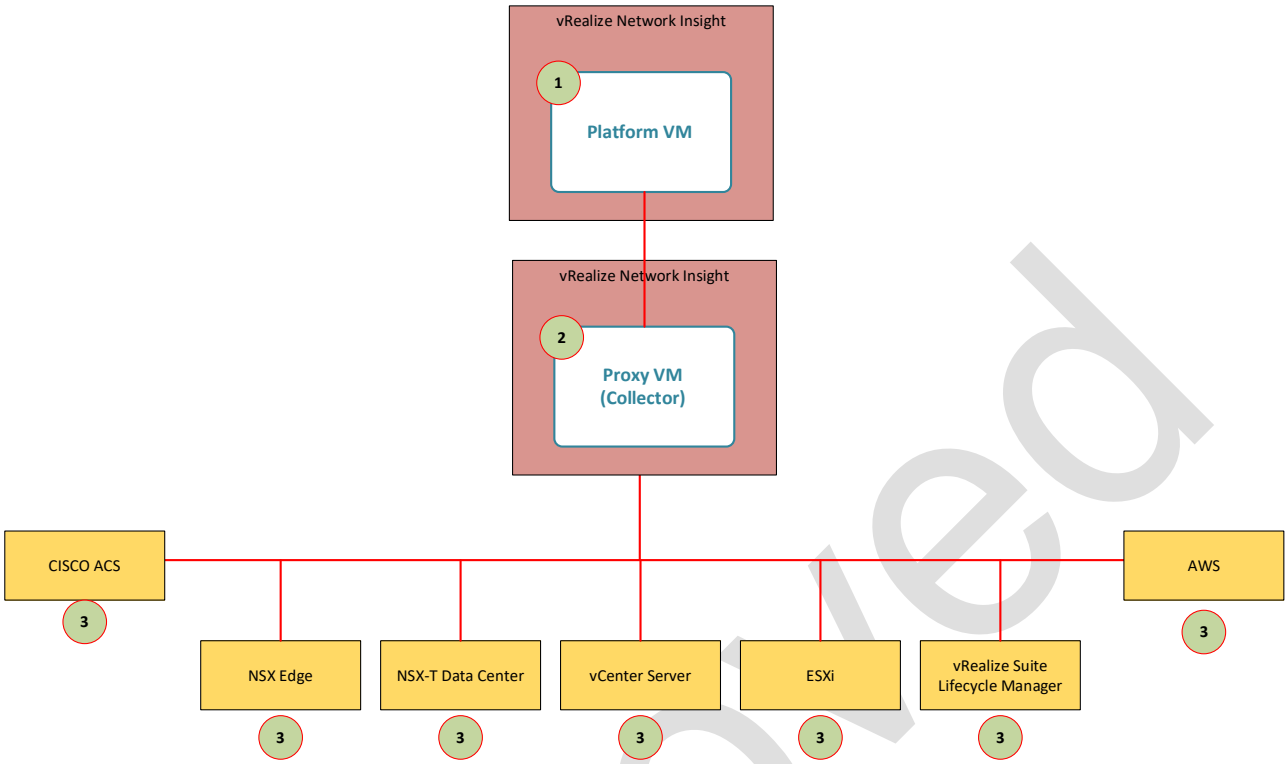


Figure 36 - vRealize Network Insight Overview

vRealize Network Insight Points of Interest

Number	Component	Description
1	vRNI Platform VM	Used to receive all the data, user access is via this portal
2	vRNI Collector VM	Used to collect data from endpoints on the network, additional servers can be provided to scale out into additional workload clusters
3	Collection points	End points that provide data into the solution.

Table 43 - vRNI Points of Interest

5.6 NSX Advanced Load Balancer (AVI)

The NSX Advanced Load Balancer (NSX ALB) Controller Manager cluster provides the centralised management plane for the NSX ALB architecture.

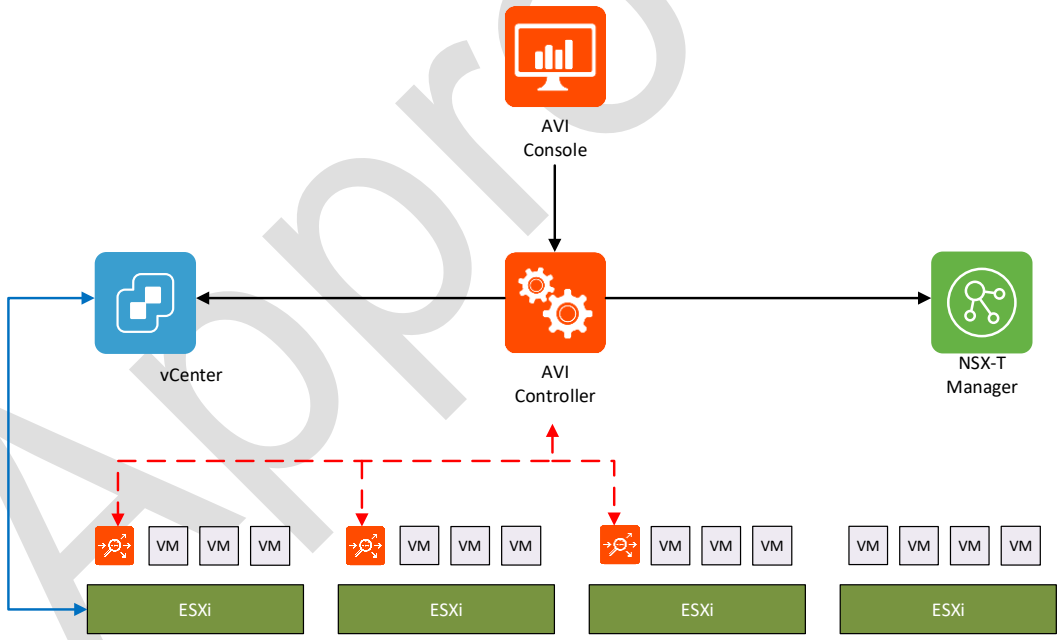


Figure 37 - NSX ALB Infrastructure Design

This design implements software-defined networking by using VMware NSX-T for Data Center and NSX Advanced Load Balancer (NSX ALB), delivering for networking what has already been delivered for compute and storage.

For stability and reliability of management and control planes, the NSX ALB Controller cluster is deployed as a cluster of three highly available virtual appliances that are responsible for the UI/API and the programmatic deployment of Load Balancer services across the entire NSX ALB architecture. The benefit of clustering is that it provides high availability of all management services such as the UI and API access to the cluster. Combining the NSX ALB Controller, policy and central control plane reduces the number of appliances deployed and allows for greater flexibility.

Controller Deployment

The solution comprises of the NSX ALB Controller which uses APIs to interface with the NSX-T manager and vCenter to discover the infrastructure. It also manages the lifecycle and network configuration of Service Engines (SE). The NSX ALB Controller provides the control plane and management console for users to configure the load balancing for their applications and the Service Engine provide a distributed and elastic load balancing fabric. The NSX ALB Controller uploads the SE OVA image to the content library on vCenter and uses vCenter APIs to deploy the SE VMs. It does not interface directly with the ESXi hosts. A Content library must be created by vCenter admin, before cloud configuration

For optimal operation, it is critical to understand the availability requirements of NSX ALB Controller cluster. The cluster must have three (3) nodes running for normal operation; however, the cluster can operate with reduced capacity in the event of a single node failure. To be fully operational, the cluster requires that a majority of NSX ALB Controller Nodes (i.e., two out of three) be available. It is recommended to spread the deployment of the NSX ALB Controller Nodes across separate hypervisors to ensure that the failure of a single host does not cause the loss of a majority of the cluster.

Cluster VIP

Cluster virtual IP address is an IP address floating among the cluster nodes: one of the cluster nodes is assigned as the owner of the cluster VIP. If case of failure, a new owner will be assigned by the system. Since the cluster VIP must remain the same, it assumes that other nodes are available in in the same subnet. The VIP feature uses gratuitous ARP to update the mac-address and the ARP table. Thus, it is mandatory to have all nodes in the cluster must be in the same subnet for the VIP to work.

By default, NSX ALB transport nodes access the NSX ALB Controller based on their IP addresses. Alternatively, this can be based on the DNS name of the NSX ALB Controllers. This is highly recommended for ease of backup and restore and is required for disaster recovery or multisite configurations. By enabling FQDN usage (DNS) on NSX ALB Controller, the IP address of the manager instances can change without affecting the NSX

ALB transport nodes. FQDN usage is enabled by publishing the FQDNs of the NSX ALB Controller.

Controller Backup

VMware recommends that you configure automated backups after NSX Advanced Load Balancer (NSX ALB) Controller installation. If the NSX ALB Controller becomes inoperable, or if you want to restore your environment to a previous state, you can restore from a backup. While the NSX ALB Controller is inoperable, the data plane is not affected, but you cannot make configuration changes. Backups are saved to a remote location that must be accessible by the NSX ALB Controller Backups can be manual or scheduled on an hourly, daily, or weekly basis, down to the minute. The backup file can be saved locally or to a remote location that the NSX ALB Controller can access.

Note SCP is currently the only supported protocol. Turning this option on causes the Controller to log onto the indicated server using SSH user credentials, and then secure copy (scp) the backup data to the indicated directory.

NSX Advanced Load Balancer Service Engine Design

NSX Advanced Load Balancer (NSX ALB) Service Engines (SEs) handle all data plane operations within SX ALB by receiving and executing instructions from the Controller. The SEs perform load balancing, and all client and server facing network interactions. It collects real-time application telemetry from application traffic flows. High availability is supported.

NSX ALB currently supports load balancing only in an NSX-T transport zone of type overlay. The SE supports only one arm mode of deployment in NSX-T environments i.e., for a virtual service the Client to VIP traffic and SE to backend server traffic both use the same SE data interface. An SE VM has nine data interfaces so it can connect to multiple logical segments but each one will be in a different VRF and hence will be isolated from all other interfaces.

In a typical load balancing scenario, a client will communicate with a virtual service, which is an IP address and port hosted in NSX ALB by an SE.

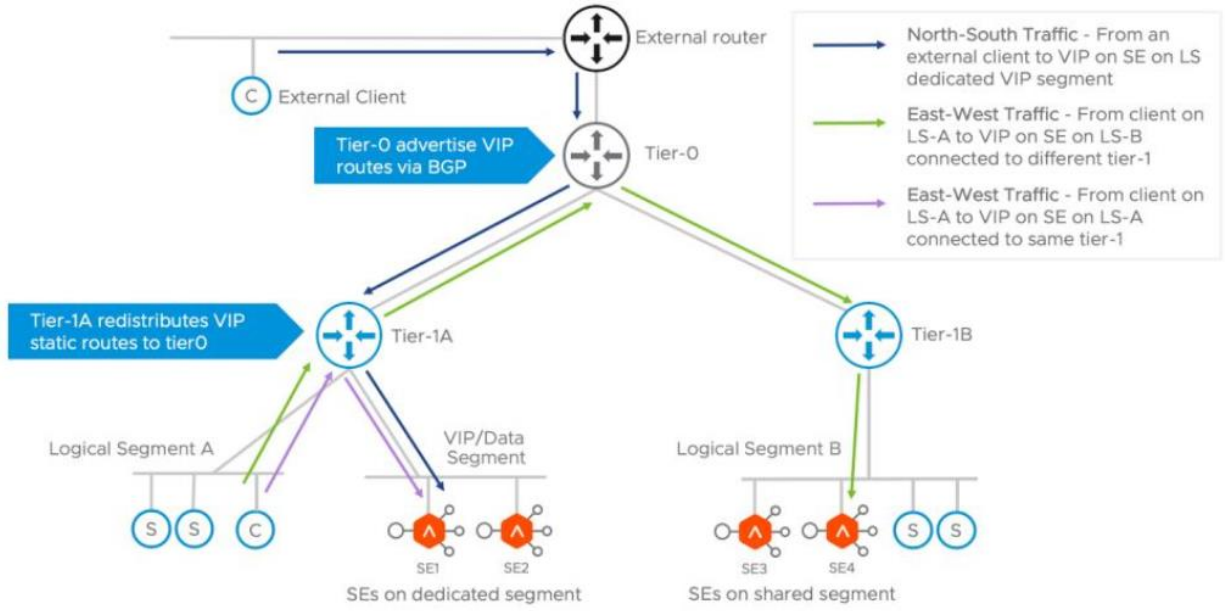


Figure 38 - Topology Diagram of Data flow

NSX Advanced Load Balancer Service Engine Deployment

The Controller cluster will be able to access vCenter and will automatically deploy NSX ALB SEs. The SE deployment and network placement are performed by NSX ALB, NSX-T and vCenter administrators. The Controller cluster will be able to provide the VM properties of the SE VM analytics. However, it continues to provide virtual service analytics

NSX Advanced Load Balancer Service Engine Groups

Service Engines (SE) are created within a group, which contains the definition of how the SEs should be sized, placed, and made highly available.
Each cloud will have at least one SE group. The options within an SE group may vary based on the type of cloud within which they exist and its settings, such as no access versus write access mode. SEs may only exist within one group. Each group acts as an isolation domain. SE resources within an SE group may be moved around to accommodate virtual services, but SE resources are never shared between SE groups. Multiple SE groups may exist within a cloud. A newly created virtual service will be placed on the default SE group, except if specifically specified during creation via the advanced wizard.
Moving an existing virtual service between SE groups, will require the VS to be disabled before moving and re-enabled when the move is completed.

SE groups provide data plane isolation; therefore, moving a VS from one SE group to another is disruptive to existing connections through the virtual service

VRF – Virtual Routing Framework

NSX Advanced Load Balancer (NSX ALB) can implement VRF to segregate IP traffic, this is a method of isolating traffic within a system. This is also referred to as a “route domain” within the load balancer community. VRF contexts simplify virtual service deployment by grouping network objects or discovered portgroups in subsets.
The workflow for creating a virtual service begins with selecting the VRF in which to place the virtual service. The web interface presents only the networks in the selected VRF context as valid targets for placing that virtual service. With VRF the Pool and VS must be created referring the same VRF.

NSX Advanced Load Balancer IPAM

NSX Advanced Load Balancer (NSX ALB) supports IPAM configuration to allow dynamically allocating IP Addresses while creating virtual service and keep track of IP Addresses assigned to any virtual service. IPAM configuration NSX ALB is VRF aware.

SLB - Topology

The NSX Advanced Load Balancer (NSX ALB) Controllers will be deployed in the management cluster. The NSX ALB Controllers are deployed as a three-node cluster for redundancy. A separate VM is required for each of the three NSX ALB Controller nodes. However, the requirements for each VM would remain the same.
For optimal performance, VMware recommends that the Controller VM vCPU and Memory be reserved in vCenter. The NSX ALB Controllers will be deployed on the management cluster and connected to the management network. The NSX ALB Service Engines will be connected to a Logical segment attached to the respective T1 Router in the Edge cluster. The Service Engines need access to the following networks:

- Data Network segment where the Service Engines will have their *data interface*, where virtual service traffic and data traffic for backend servers will flow (data plane/data traffic)

- Service Engine management segment for the management interface to allow communication with the NSX ALB Controller cluster (management plane)

As per the topology, VIP Traffic will come to the Service Engine via T0 Router, a T1 Router, a Service Engine, a T1 Router, an Application server.
External/Internal Logical Segments will be used to place VIP traffic and transit Logical Segment to route the traffic towards T1 Router via T0.
We don't need to connect multiple Logical segments to Service engine to reach multiple T1 Routers, the routing to reach T1 routers will be taken care by T0 Router.
For the virtual services placed on these SEs, the VIP can be part of the subnet of the logical segment connected to the data interface of the SE or any other unused subnet.
Once the virtual service is configured on the SE, the NSX ALB Controller updates the VIP static routes on the tier-1 router associated with the logical segment selected for the virtual service placement. The NSX admin is expected to configure the tier-1 router to redistribute these static routes with tier-0. For north-south reachability of the VIP, admin should configure the tier-0 to advertise the VIP routes to external router via BGP.

Virtual Service

Virtual services are the core of the NSX Advanced Load Balancer (NSX ALB) load-balancing and proxy functionality. A virtual service advertises an IP address and ports to the external world and listens for client traffic. When a virtual service receives traffic, it may be configured to:

Proxy the client's network connection.
Perform security, acceleration, load balancing, gather traffic statistics, and other tasks.
Forward the client's request data to the destination pool for load balancing.

A virtual service can be thought of as an IP address that NSX ALB is listening to, ready to receive requests. In a normal TCP/HTTP configuration, when a client connects to the virtual service address, the Service Engine will process the client connection or request against a list of settings, policies and profiles, then send valid client traffic to a back-end server that is listed as a member of the virtual service's pool. Typically, the connection between the client and server is terminated or proxied at the SE, which opens a new TCP connection between itself and the server. The server will respond back directly to the virtual service IP address, not to the original client address. the Service Engine forwards the response to the client via the TCP connection between itself and the client.

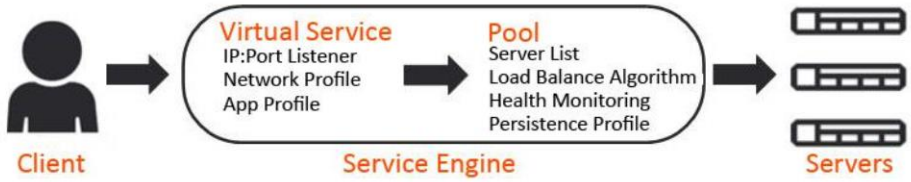


Figure 39 - Service Engine data plane flow

NSX ALB Access Control

The NSX Advanced Load Balancer (NSX ALB) Controller has one built-in user (admin) but can also be integrated with LDAP, TACACS+ or SAML. The admin user account is a unique account used for initial setup of NSX ALB. This account cannot be deleted. Additional users can be created if required and privileges assigned accordingly.

User Roles

Each NSX Advanced Load Balancer (NSX ALB) user account is associated with a role. The role defines the type of access the user has to each area of the NSX ALB system. Roles provide granular Role-Based Access Control (RBAC) within NSX ALB. The role, in combination with the tenant (optional), comprise the authorisation settings for an NSX ALB user.

Access Types

For each NSX ALB system area, the role can be one of the following:

• **Write:** User has full access to create, read, modify, and delete items. For example, the user may be able to create a virtual service, modify its properties, view its health and metrics, and later delete that virtual service.

• **Read:** User may only read the existing configuration of the item. For example, the user may see how a virtual service is configured while being unable to view the current metrics, modify, or delete that virtual service.

• **No Access:** User can neither see nor modify this section of NSX ALB. For example, the user would be prohibited from creating, modifying, deleting, or even viewing (reading) any virtual services at all.

Pre-Defined NSX ALB User Roles

NSX ALB comes with the following pre-defined roles:

• **Application-Admin:** User has write access to the **Application** and **Profiles** sections of NSX ALB, read access to the Infrastructure settings, and no access to the **Account** or **System** sections.

• **Application-Operator:** User has read access to the **Application** and **Profiles** sections of NSX ALB, and no access to the **Infrastructure**, **Account**, and **System** sections.

• **Security-Admin:** User has read/write access only to the **Templates** > **Security** section.

• **System-Admin:** User has write access to all sections of NSX ALB.

• **Tenant-Admin:** User has write access to all sections of NSX ALB except the System section, to which the user has no access.

• **WAF-Admin:** User has write access to **WAF Profiles and Policies**, read access to application VSs, pools and pool groups, read access to clouds, and no access to the rest.

Each user must be associated with at least one role. The role can be either predefined or a custom role. If multitenancy is configured, a user can be assigned to more than one tenant and can have a separate role for each tenant.

6 INFRASTRUCTURE – ESXI JUMP SERVERS

To allow users to administrate the infrastructure we will build two standalone ESXi servers. These will connect to the same underlay, and infrastructure but once built they will run multiple Windows and Linux servers.

Jump Host ESXi Specifications

The below table details the specification for the hosts

Attribute	Specification
Vendor and Model	HPE DL380 G10
Processor Speed	2x 6244R
Total number of Cores	16 (2x8) – (32 with Hyperthreading)
System Memory	384GB
NIC Ports and Speed	2x 25GB
Boot Disks	2x 480GB SSD's
Capacity Disks	2x 3.84TB SSD's

Table 44 - ESXi Host Specification – Jump Hosts

ESXi Connectivity

The following shows the connectivity into the infrastructure.

The two standalone ESXi hosts will be added to the Management vCentre for ease.

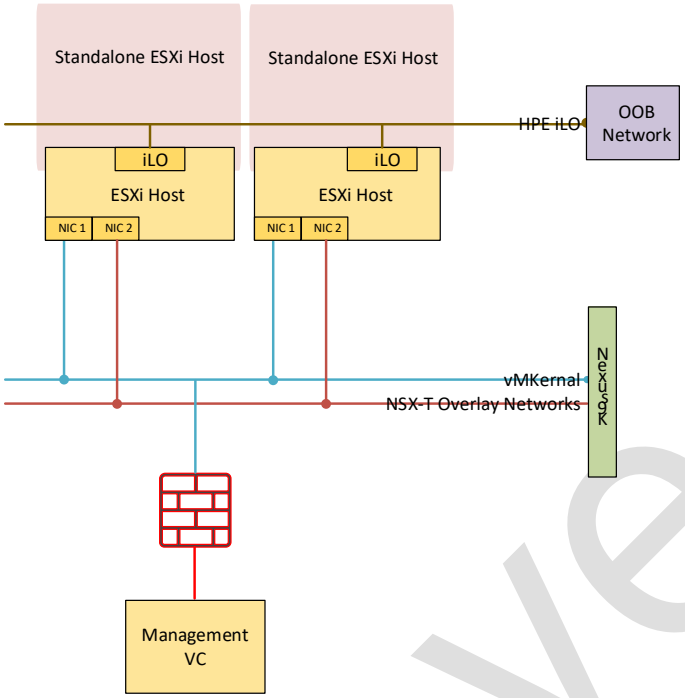


Figure 40 - Standalone ESXi Host Connectivity

Initial Jump Servers Deployed

Once the two standalone jump servers have been deployed, we will deploy the following virtual servers onto them.

Host One

- Windows Server 01
- Windows Server 02
- Linux Server 01
- Linus Server 02

Host Two

- Windows Server 01
- Windows Server 02
- Linux Server 01
- Linus Server 02

6.1 Servers

The following servers will be required in the Environment.

Wootton Basset Management Domain

Production ESXi Infrastructure Server Requirements - Management											
Component	**Host Name**	**Datacenter Name**	**Cluster Name**	**Datastore Name**	**Management IP**	**Management Subnet**	**Management Gateway**	**vMotion IP**	**vMotion Subnet**	**vSAN IP**	**vSAN Subnet**
ESXi Host	WB1PESXIMGUK601	WB1-MGMT-DC	WB1-MGMT-CLU01	WB1-MGMT-CLU01-PRD-DS01 WB1-MGMT-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	xxx	xxx
ESXi Host	WB1PESXIMGUK602	WB1-MGMT-DC	WB1-MGMT-CLU01	WB1-MGMT-CLU01-PRD-DS01 WB1-MGMT-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	xxx	xxx
ESXi Host	WB1PESXIMGUK603	WB1-MGMT-DC	WB1-MGMT-CLU01	WB1-MGMT-CLU01-PRD-DS01 WB1-MGMT-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	xxx	xxx
ESXi Host	WB1PESXIMGUK604	WB1-MGMT-DC	WB1-MGMT-CLU01	WB1-MGMT-CLU01-PRD-DS01 WB1-MGMT-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	xxx	xxx

Table 45 - Production ESXi Infrastructure Server Requirements Management

Wootton Basset Edge Services Cluster

Infrastructure Requirements – Workload Domain – Edge Services											
	Host Name	**Datacenter Name**	**Cluster Name**	**Datastore Name**	**Management IP**	**Management Subnet**	**Management Gateway**	**vMotion IP**	**vMotion Subnet**	**vSAN IP**	**vSAN Subnet**
ESXi Host	WB1PEGETR0UK401	KN3-COMPUTE-DC	WB1-EDGE-CLU01	Local Storage	xxx	xxx	xxx	xxx	xxx	N/A	N/A

ESXi Host	WB1PEGETR0UK402	KN3-COMPUTE-DC	WB1-EDGE-CLU01	Local Storage	xxx	xxx	xxx	xxx	xxx	N/A	N/A

Table 46- Production ESXi Infrastructure Server Requirements Edge Services

Wooton Basset Workload Domain – Production Cluster

Infrastructure Requirements – Workload Domain – Production Cluster											
	Host Name	**Datacenter Name**	**Cluster Name**	**Datastore Name**	**Management IP**	**Management Subnet**	**Management Gateway**	**vMotion IP**	**vMotion Subnet**	**vSAN IP**	**vSAN Subnet**
ESXi Host	WB1PESXICPUK601	WB1-COMPUTE-DC	WB1-PROD-CLU01	WB1-WLK-CLU01-PRD-DS01 WB1-WKD-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A
ESXi Host	WB1PESXICPUK602	WB1-COMPUTE-DC	WB1-PROD-CLU01	WB1-WLK-CLU01-PRD-DS01 WB1-WKD-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A
ESXi Host	WB1PESXICPUK603	WB1-COMPUTE-DC	WB1-PROD-CLU01	WB1-WLK-CLU01-PRD-DS01 WB1-WKD-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A
ESXi Host	WB1PESXICPUK604	WB1-COMPUTE-DC	WB1-PROD-CLU01	WB1-WLK-CLU01-PRD-DS01 WB1-WKD-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A
ESXi Host	WB1PESXICPUK605	WB1-COMPUTE-DC	WB1-PROD-CLU01	WB1-WLK-CLU01-PRD-DS01	xxx	xxx	xxx	xxx	xxx	N/A	N/A

				WB1-WKD-CLU01-PRD-DS02							
ESXi Host	WB1PESXICPUK606	WB1-COMPUTE-DC	WB1-PROD-CLU01	WB1-WLK-CLU01-PRD-DS01 WB1-WKD-CLU01-PRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A

Table 47 - Production ESXi Infrastructure Server Requirements Production Cluster

Wootton Basset Workload Domain – Non Production Cluster

Infrastructure Requirements – Workload Domain – Non Production Cluster											
	Host Name	**Datacenter Name**	**Cluster Name**	**Datastore Name**	**Management IP**	**Management Subnet**	**Management Gateway**	**vMotion IP**	**vMotion Subnet**	**vSAN IP**	**vSAN Subnet**
ESXi Host	WB1NESXICPUK601	WB1-COMPUTE-DC	WB1-NONPROD-CLU01	WB1-WLK-CLU01-NONPRD-DS01 WB1-WKD-CLU01-NONPRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A
ESXi Host	WB1NESXICPUK602	WB1-COMPUTE-DC	WB1-NONPROD-CLU01	WB1-WLK-CLU01-NONPRD-DS01 WB1-WKD-CLU01-NONPRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A
ESXi Host	WB1NESXICPUK603	WB1-COMPUTE-DC	WB1-NONPROD-CLU01	WB1-WLK-CLU01-NONPRD-DS01 WB1-WKD-CLU01-NONPRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A
ESXi Host	WB1NESXICPUK604	WB1-COMPUTE-DC	WB1-NONPROD-CLU01	WB1-WLK-CLU01-NONPRD-DS01	xxx	xxx	xxx	xxx	xxx	N/A	N/A

				WB1-WKD-CLU01-NONPRD-DS02							
ESXi Host	WB1NESXICPUK605	WB1-COMPUTE-DC	WB1-NONPROD-CLU01	WB1-WLK-CLU01-NONPRD-DS01 WB1-WKD-CLU01-NONPRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A
ESXi Host	WB1NESXICPUK606	WB1-COMPUTE-DC	WB1-NONPROD-CLU01	WB1-WLK-CLU01-NONPRD-DS01 WB1-WKD-CLU01-NONPRD-DS02	xxx	xxx	xxx	xxx	xxx	N/A	N/A

Table 48 - Production ESXi Infrastructure Server Requirements Non Production Cluster

Wootton Basset Standalone ESXi Hosts

Infrastructure Requirements – Standalone ESXi Hosts											
	Host Name	**Datacenter Name**	**Cluster Name**	**Datastore Name**	**Management IP**	**Management Subnet**	**Management Gateway**	**vMotion IP**	**vMotion Subnet**	**vSAN IP**	**vSAN Subnet**
ESXi Host	WBYPESXICPUK601	WB1-MGMT-DC	N/A	Local Disks	xxx	xxx	xxx	N/A	N/A	N/A	N/A
ESXi Host	WBYPESXICPUK602	WB1-MGMT-DC	N/A	Local Disks	xxx	xxx	xxx	N/A	N/A	N/A	N/A

Table 49 - Standalone ESXi Hosts

Wootton Basset Infrastructure Servers

Infrastructure Requirements – Infrastructure Servers											
	Host Name	**Datacenter Name**	**Cluster Name**	**Datastore Name**	**Management IP**	**Management Subnet**	**Management Gateway**	**vMotion IP**	**vMotion Subnet**	**vSAN IP**	**vSAN Subnet**

vCenter											
Management vCenter Server	WBVPMGTVCSUK601	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
Workload vCenter Server	WBVPWLDVCSUK601	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
SDDC Manager											
SDDC Manager	WBVPSDDCMGUK401	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T											
NSX-T Manager 01 – Management Domain	WBVPNSXMGRUK601	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T Manager 01 – Management Domain	WBVPNSXMGRUK602	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T Manager 01 – Management Domain	WBVPNSXMGRUK603	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T Manager VIP – Management Domain	WBVPNSXMGTUK601	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T Manager 01 – Workload Domain	WBVPNSXMGRUK605	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T Manager 01 – Workload Domain	WBVPNSXMGRUK606	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T Manager 01 – Workload Domain	WBVPNSXMGRUK607	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T Manager VIP – Workload Domain	WBVPNSXWLDUK601	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
Life Cycle Manager											
Lifecycle Manager	WBVPVRSLCMUK401	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vRealize Log Insight											
vRealize Log Insight Master	WBVPVRLMGRUK401	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A

vRealize Log Insight Node 1	WBVPVRLMGRUK402	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vRealize Log Insight Node 2	WBVPVRLMGRUK403	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vRealize Log Insight VIP	WBVPVRLVIPUK401	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vRealize Operations Manager											
vRealize Operations Master	WBVPVROPMGUK401	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vRealize Operations Replica	WBVPVROPMGUK402	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vRealize Operations Load Balancer	WBVPVROPSUK601	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vRealize Operations Collector	WBVPVROPCLUK401	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
Windows and Linux Jump Servers											
Windows Jump Server – Management	WBVPMGTJMPUK401	N/A	N/A		xxx	xxx	xxx	N/A	N/A	N/A	N/A
Linux Jump Server - Management	WBVPMGTJMPUK402	N/A	N/A		xxx	xxx	xxx	N/A	N/A	N/A	N/A
Windows Jump Server – Workload	WBVSWINJUMUK401	N/A	N/A		xxx	xxx	xxx	N/A	N/A	N/A	N/A
Linux Jump Server - Workload	WBVSLNXJMPUK401	N/A	N/A		xxx	xxx	xxx	N/A	N/A	N/A	N/A
WorkSpace ONE Identity Manager											
vIDM Server 1	WBVPVIDMGR601	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vIDM Server 2	WBVPVIDMGR602	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vIDM Server 3	WBVPVIDMGR603	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vIDM Server VIP	WBVPVIDVIPUK601	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
vRealize Network Insight											
vRNI Platform Server	WBVPVRNPVMUK401	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A

vRNI Controller Server	WBVPVRNCOLUK401	WB1-MGMT-DC	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A
NSX-T Advanced Load Balancer (AVI)											
AVI Controller 1	WBVPALBCNTUK401	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
AVI Controller 2	WBVPALBCNTUK402	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
AVI Controller 3	WBVPALBCNTUK403	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
AVI Controller VIP	WBVPALBVIPUK401	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
AVI Internal Service Engine 1	WBVPALB_WBVPSEINTUK40x-SE-XXX	WB1-PROD-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
AVI Internal Service Engine 2	WBVPALB_WBVPSEINTUK40x-SE-XXX	WB1-PROD-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
AVI External Service Engine 1	WBVPALB_WBVPSEEXUK40x-SE-XXX	WB1-PROD-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
AVI External Service Engine 2	WBVPALB_WBVPSEEXUK40x-SE-XXX	WB1-PROD-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
HCX											
HCX Management Server	WBVPHCXMGRUK401	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
HCX WAN Optimiser Server	WBVPHCXWANUK401	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A

HCX Interconnect Server	WBVPHCXINTUK401	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
HCX Network Interconnect Server	WBVPHCXNISUK401	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
Management NSX-T Edges											
NSX-T Edge Server 01 (Management)	WBVPMGTEDGEUK401	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
NSX-T Edge Server 02 (Management)	WBVPMGTEDGEUK401	WB1-MGMT-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
Workload NSX-T Edges											
NSX-T Edge Server 01 Internal (Workload)	WBVPWLDEDGEUK401	WB1-PROD-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
NSX-T Edge Server 02 Internal (Workload)	WBVPWLDEDGEUK402	WB1-PROD-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
NSX-T Edge Server 01 External (Workload)	WBVPWLDEDGEUK201	WB1-PROD-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A
NSX-T Edge Server 02 External (Workload)	WBVPWLDEDGEUK202	WB1-PROD-CLU01		xxx	xxx	xxx	N/A	N/A	N/A	N/A	N/A

Table 50 - Wootton Basset Infrastructure Servers

6.2 Backups

In order to allow for a solution restore it is recommended all of the following solution elements are backed up as full image based backups, as well as file based backups where possible.

- SDDC Manager (image based / file based)
- vCenter Server (image based / file based)
- Platform Services Controllers (image based / file based)
- vRealize Log Insight (image based)
- vRealize Operations (image based)
- vRealize LifeCycle (image based)
- SDDC Manager (image based / file based)
- NSX Managers (image based / file based)

The backup of the NSX Manager virtual machines also backs up the configuration of the following:

- DLR Controller VM
- NSX Edge VM's
- Distributed Firewall Rules
- Logical Switches.

Important Note

Where possible it is wise to backup all the components at the same time to avoid any configuration drift.

6.3 Management

Management of the platform will be via some new Windows RDP and Linux Jump servers. These will be deployed onto the stand alone ESXi Servers as virtual servers.

Application access (VC, vSAN, NSX-T etc) will be via Active Directory groups and managed by the cloud team.

6.4 Monitoring

The VCF solution will be monitored by it's own vRealize Operations Manager, vRealize Log Insight and vRealize Network Insight. Once deployed the alerts and dashboards will be created.

There will be a requirement to integrate these alerts into the Netcool solution and costings for this will need to be obtained.

Important Note

Integration into Netcool will required additional Netcool licenses that are not detailed in the document.

6.5 Certificates

The solution will require some internal certificates for elements within the solution.

6.6 Traffic Flow

The following diagram shows the main traffic flow between the core VCF components.

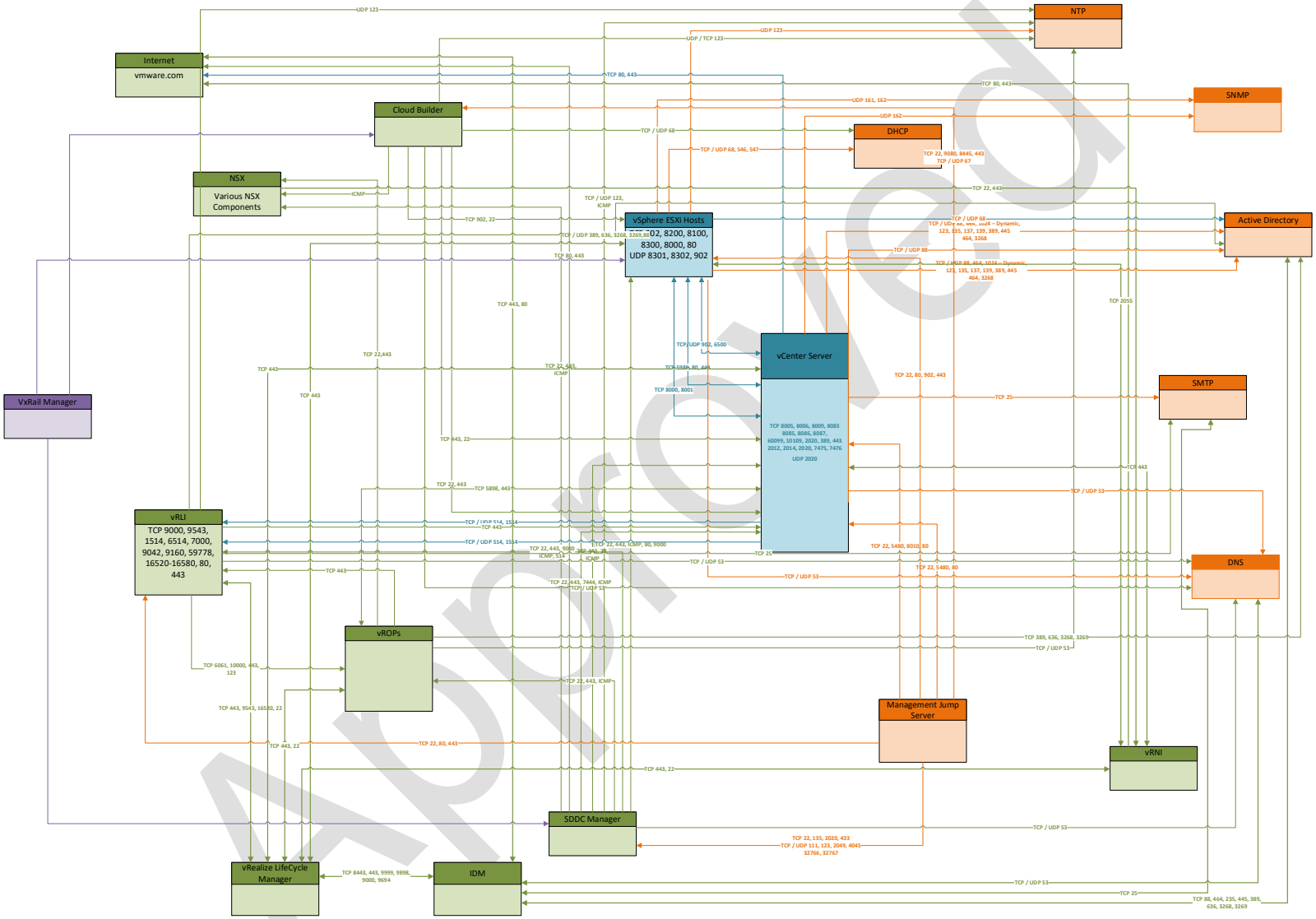


Figure 41 - VCF Traffic Flow

7 NETWORKING

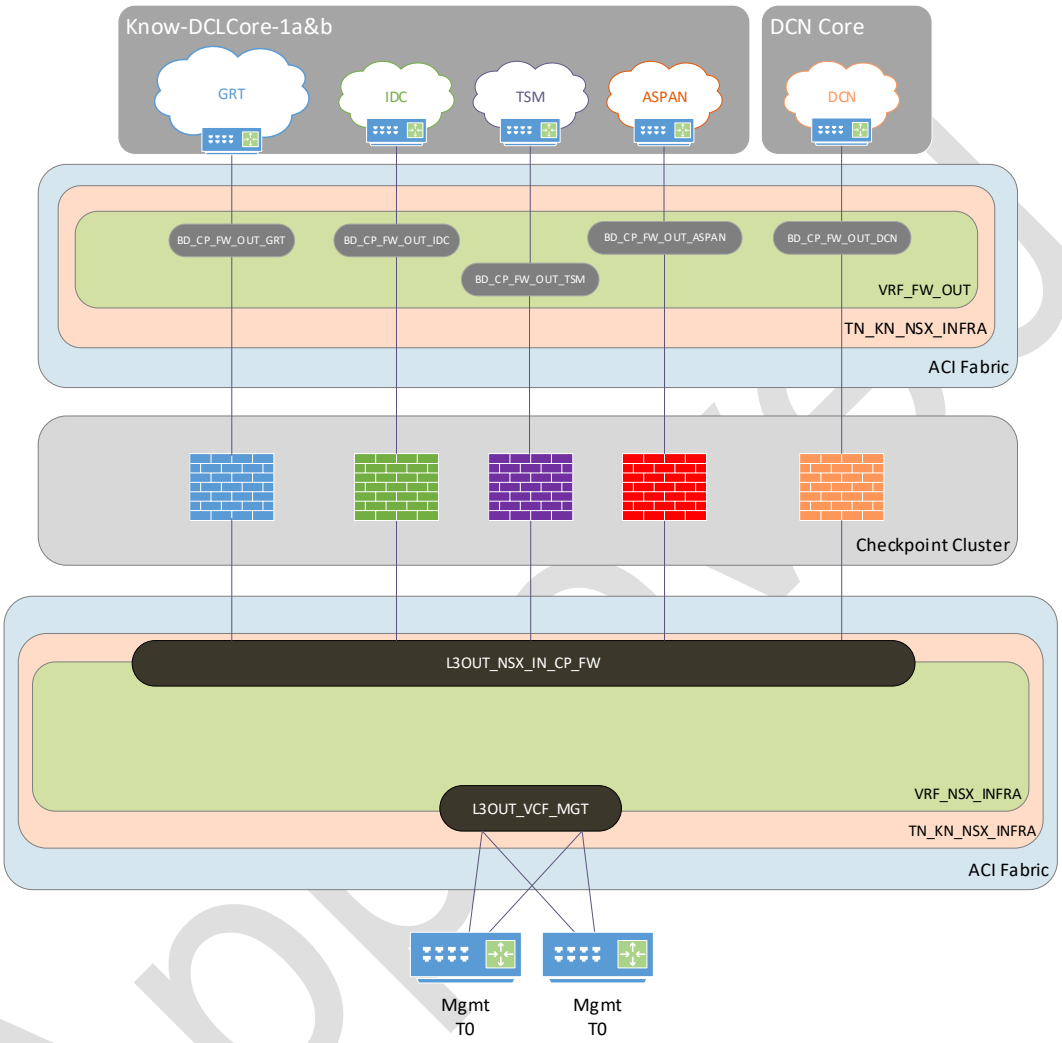


Figure 42 - VCF WAN Connectivity

7.1 Infrastructure IP Requirements

The following IP Addresses will be required for the solution.

ESXi Hosts – Wootton Basset

vMKernal Addresses – Management – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vMkernal (ESX Management)	WB1PESXIMGUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PESXIMGUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PESXIMGUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PESXIMGUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 51 - vMKernal IP Details – Management – Wootton Basset

vMKernal Addresses – Edge – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vMkernal (ESX Management)	WB1PEGETR0UK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PEGETR0UK402	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 52 - vMKernal IP Details – Edge – Wootton Basset

vMKernal Addresses – Production – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vMkernal (ESX Management)	WB1PESXICPUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PESXICPUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PESXICPUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PESXICPUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PESXICPUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1PESXICPUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 53 - vMKernal IP Details – Production – Wootton Basset

vMKernal Addresses – Non Production – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vMkernal (ESX Management)	WB1NESXICPUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1NESXICPUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1NESXICPUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1NESXICPUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1NESXICPUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMkernal (ESX Management)	WB1NESXICPUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 54 - vMKernal IP Details – Non Production – Wootton Basset

vMotion Addresses – Management – Wooton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vMotion	WB1PESXIMGUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PESXIMGUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PESXIMGUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PESXIMGUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 55 - vMotion IP Details – Management – Wootton Basset

vMotion Addresses – Edge – Wooton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vMotion	WB1PEGETR0UK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PEGETR0UK402	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 56 - vMotion IP Details – Edge – Wooton Basset

vMotion Addresses – Production – Wooton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vMotion	WB1PESXICPUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PESXICPUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PESXICPUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PESXICPUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PESXICPUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1PESXICPUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 57 - vMotion IP Details – Production – Wooton Basset

vMotion Addresses – Non Production – Wooton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vMotion	WB1NESXICPUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1NESXICPUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1NESXICPUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1NESXICPUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1NESXICPUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vMotion	WB1NESXICPUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 58 - vMotion IP Details – Non Production – Wooton Basset

vSAN Addresses – Production – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vSAN	WB1PESXICPUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1PESXICPUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1PESXICPUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1PESXICPUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1PESXICPUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1PESXICPUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 59 - vSAN IP Details – Production – Wooton Basset

vSAN Addresses – Non Production – Wooton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
vSAN	WB1NESXICPUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1NESXICPUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1NESXICPUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1NESXICPUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1NESXICPUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vSAN	WB1NESXICPUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 60 - vSAN IP Details – Non Production – Wootton Basset

iLO Addresses – Management – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
iLO Address	WB1PESXIMGUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PESXIMGUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PESXIMGUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PESXIMGUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 61 – iLO IP Details – Management -Wootton Basset

iLO Addresses – Edge – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
iLO Address	WB1PEGETR0UK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PEGETR0UK402	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 62 - iLO IP Details – Edge – Wootton Basset

iLO Addresses – Production – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
iLO Address	WB1PESXICPUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PESXICPUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PESXICPUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PESXICPUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PESXICPUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1PESXICPUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 63 - iLO IP Details – Production – Wootton Basset

iLO Addresses – Non Production – Wootton Basset

Component	Server Name	IP Address	MASK	Gateway	vLAN
iLO Address	WB1NESXICPUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1NESXICPUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1NESXICPUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1NESXICPUK604	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1NESXICPUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
iLO Address	WB1NESXICPUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 64 - iLO IP Details – Non Production – Wootton Basset

Infrastructure Servers (SDDC) – Wooton Basset

SDDC Manager

Component	Server Name	IP Address	MASK	Gateway	vLAN
SDDC Manager	WBVPSDDCMGUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 65 - SDDC Manager IP Details

vCenter Infrastructure

Component	Server Name	IP Address	MASK	Gateway	vLAN
Management vCenter Server	WBVPMGTVCSUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Workload vCenter Server	WBVPWLDVCSUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 66 - vCenter Infrastructure IP Details

NSX Infrastructure

Component	Server Name	IP Address	MASK	Gateway	vLAN
NSX-T Manager 01 – Management Domain	WBVPNSXMGRUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
NSX-T Manager 01 – Management Domain	WBVPNSXMGRUK602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
NSX-T Manager 01 – Management Domain	WBVPNSXMGRUK603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
NSX-T Manager VIP – Management Domain	WBVPNSXMGTUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
NSX-T Manager 01 – Workload Domain	WBVPNSXMGRUK605	x.x.x.x	x.x.x.x	x.x.x.x	xxx
NSX-T Manager 01 – Workload Domain	WBVPNSXMGRUK606	x.x.x.x	x.x.x.x	x.x.x.x	xxx
NSX-T Manager 01 – Workload Domain	WBVPNSXMGRUK607	x.x.x.x	x.x.x.x	x.x.x.x	xxx
NSX-T Manager VIP – Workload Domain	WBVPNSXWLDUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 67 - NSX Infrastructure IP Details

vRealize Log Insight Infrastructure

Component	Server Name	IP Address	MASK	Gateway	vLAN
vRealize Log Insight Master	WBVPVRLMGRUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vRealize Log Insight Node 1	WBVPVRLMGRUK402	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vRealize Log Insight Node 2	WBVPVRLMGRUK403	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vRealize Log Insight VIP	WBVPVRLVIPUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 68 - vRealize Life Cycle Manager IP Details

vRealize Operations Manager Infrastructure

Component	Server Name	IP Address	MASK	Gateway	vLAN
vRealize Operations Master	WBVPVROPMGUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vRealize Operations Replica	WBVPVROPMGUK402	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vRealize Operations Load Balancer	WBVPVROPSUK601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vRealize Operations Collector	WBVPVROPCLUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 69 - vRealize Operations Manager IP Details

General Infrastructure Servers

Component	Server Name	IP Address	MASK	Gateway	vLAN
Windows Jump Server – Management	WBVPMGTJMPUK401				
Linux Jump Server - Management	WBVPMGTJMPUK402				
Windows Jump Server – Workload	WBVSWINJUMUK401				
Linux Jump Server - Workload	WBVSLNXJMPUK401				

Table 70 - General Infrastructure IP Details

vIDM Infrastructure

Component	Server Name	IP Address	MASK	Gateway	vLAN
vIDM Server 1	WBVPVIDMGR601	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vIDM Server 2	WBVPVIDMGR602	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vIDM Server 3	WBVPVIDMGR603	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vIDM Server VIP	WBVPVIDVIPUK601				

Table 71 - vIDM Infrastructure IP Details

vRNI Infrastructure

Component	Server Name	IP Address	MASK	Gateway	vLAN
vRNI Platform Server	WBVPVRNPVMUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
vRNI Controller Server	WBVPVRNCOLUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 72 - vRNI Infrastructure IP Details

HCX Infrastructure (Optional)

Component	Server Name	IP Address	MASK	Gateway	vLAN
HCX Management Server	WBVPHCXMGRUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
HCX WAN Optimiser Server	WBVPHCXWANUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
HCX Interconnect Server	WBVPHCXINTUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
HCX Network Interconnect Server	WBVPHCXNISUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 73 - HCX Infrastructure IP Details

AVI Infrastructure

Component	Server Name	IP Address	MASK	Gateway	vLAN
AVI Controller 1	WBVPALBCNTUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
AVI Controller 2	WBVPALBCNTUK402	x.x.x.x	x.x.x.x	x.x.x.x	xxx
AVI Controller 3	WBVPALBCNTUK403	x.x.x.x	x.x.x.x	x.x.x.x	xxx
AVI Controller VIP	WBVPALBVIPUK401	x.x.x.x	x.x.x.x	x.x.x.x	xxx
AVI Internal Service Engine 1	WBVPALB_WBVPSEINTUK40x-SE-XXX	x.x.x.x	x.x.x.x	x.x.x.x	xxx
AVI Internal Service Engine 2	WBVPALB_WBVPSEINTUK40x-SE-XXX	x.x.x.x	x.x.x.x	x.x.x.x	xxx

AVI External Service Engine 1	WBVPALB_WBVPSEEXUK40x-SE-XXX	x.x.x.x	x.x.x.x	x.x.x.x	xxx
AVI External Service Engine 2	WBVPALB_WBVPSEEXUK40x-SE-XXX	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 74 - AVI Infrastructure IP Details

Pure Storage – Wooton Basset

Production Pure Array

Component	Device Name	IP Address	MASK	Gateway	vLAN
Pure Array 1 – MGMT Port 1	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Pure Array 1 – MGMT Port 2	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Pure Array 1 – MGMT Port 3	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Pure Array 1 – MGMT Port 4	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 75 - Pure Array Production Details

Non Production Pure Array

Component	Device Name	IP Address	MASK	Gateway	vLAN
Pure Array 2 – MGMT Port 1	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Pure Array 2 – MGMT Port 2	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Pure Array 2 – MGMT Port 3	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Pure Array 2 – MGMT Port 4	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 76 - Pure Array None Production Details

Infrastructure Servers (Jump) – Wooton Basset

Production Jump Servers

Component	Server Name	IP Address	MASK	Gateway	vLAN
Windows Server 01	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Windows Server 02	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Linux Server 01	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Linux Server 02	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 77 - Production Jump Servers IP Details

Non Production Jump Servers

Component	Server Name	IP Address	MASK	Gateway	vLAN
Windows Server 01	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Windows Server 02	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Linux Server 01	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx
Linux Server 02	TBC	x.x.x.x	x.x.x.x	x.x.x.x	xxx

Table 78 – Non Production Jump Servers IP Details

7.2 Connectivity Matrix

The following connectivity will be required by the solution to allow successful deployment and operational usage.

Firewall Rules – Wootton Basset

ID	Source Component	Source Location	Source Interface / IP	Destination Component	Destination Location	Destination Interface / IP	Direction	Protocol/Port
01	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	SDDC vMKernal Network vLAN	Wootton Basset DC1	TBC	◄►	TBC
02	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload ESXi Servers	SDDC vMotion Network vLAN	Wootton Basset DC1	TBC	◄►	TBC
03	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, ESXi Servers	SDDC vSAN Network vLAN	Wootton Basset DC1	TBC	◄►	TBC
04	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Workload, ESXi Servers	SDDC SAN Network vLAN	Wootton Basset DC1	TBC	◄►	TBC
05	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	SDDC OOB Network vLAN	Wootton Basset DC1	TBC	◄►	TBC
06	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26		◄►

			Standalone ESXi Servers					
07	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	NTP Server Time.systems.private	Knowsley Wootton Bassett	10.74.100.60 10.94.100.60		⮜
08	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40		➢
09								

Table 79 - Connectivity Matrix – Firewall Rules – Wootton Basset

NSX Firewall Rules – Wooton Basset

ID	Source Component	Source Location	Source Interface / IP	Destination Component	Destination Location	Destination Interface / IP	Access (NSX)	Direction	Protocol/Port
01	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜➢	TCP \ UDP AD Ports, 464, 1024 – Dynamic, 123, 135, 137, 139, 389, 445

02	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	NTP Server Time.systems.private	Knowsley Wootton Bassett	10.74.100.60 10.94.100.60	✅	⮜⮞	TCP \ UDP 123
03	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✅	⮜⮞	TCP 25
04	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	SNMP	TBC	TBC	✅	⮜⮞	UDP 161, 162
05	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53
06	SDDCv2.5 ESXi Servers (Wootton Basset)	Wootton Basset DC1	Management, Edge, Workload and Standalone ESXi Servers	Internet	TBC	TBC	✅	⮜⮞	TCP 80, 443
vRNI Rules									

07	vRNI Servers	Wootton Basset SDDCv2.5	TBC	Internet	Management, Edge, Workload and Standalone ESXi Servers	TBC	✅	⮜⮞	TCP 80, 443
08	vRNI Servers	Wootton Basset SDDCv2.5	TBC	Management, Edge, Workload and Standalone ESXi Servers	Wootton Basset DC1	Wootton Basset DC1	✅	⮜⮞	TCP 80, 443
vRLI Rules									
09	VRLI Servers	Wootton Basset SDDCv2.5	TBC	NTP Server Time.systems.private	Knowsley Wootton Bassett	10.74.100.60 10.94.100.60	✅	⮜⮞	TCP \ UDP 123
10	VRLI Servers	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜⮞	TCP \ UDP AD Ports, 464, 1024 – Dynamic, 123, 135, 137, 139, 389, 445
11	VRLI Servers	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53

12	VRLI Servers	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✅	⮜⮞	TCP 25
vROPS Rules									
13	vROP's Servers	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜⮞	TCP 2368, 2369, 389, 636
14	vROP's Servers	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53
SDDC Manager Rules									
15	SDDC Manager	Wootton Basset SDDCv2.5	TBC	NTP Server Time.systems.private	Knowsley Wootton Bassett	10.74.100.60 10.94.100.60	✅	⮜⮞	TCP \ UDP 123
16	SDDC Manager	Wootton Basset SDDCv2.5	TBC	Internet	TBC	TBC	✅	⮜⮞	TCP 80, 443
vIDM / Workspace ONE Rules									

17	vIDM	Wootton Basset SDDCv2.5	TBC	Internet	TBC	TBC	✅	⮜⮞	TCP 80, 443
18	vIDM	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✅	⮜⮞	TCP 25
19	vIDM	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445
20	vIDM	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53
vCenter Rules									
21	vCenter (Management)	Wootton Basset SDDCv2.5	TBC	Internet	TBC	TBC	✅	⮜⮞	TCP 80, 443
22	vCenter (Management)	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✅	⮜⮞	TCP 25

23	vCenter (Management)	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445
24	vCenter (Management)	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53
25	vCenter (Workload)	Wootton Basset SDDCv2.5	TBC	Internet	TBC	TBC	✅	⮜⮞	TCP 80, 443
26	vCenter (Workload)	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✅	⮜⮞	TCP 25
27	vCenter (Workload)	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445
28	vCenter (Workload)	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53

NSX-T Management Rules									
29	NSX-T Management Nodes (Management)	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✔	⮜⮞	TCP 25
30	NSX-T Management Nodes (Management)	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✔	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445
31	NSX-T Management Nodes (Management)	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✔	⮜⮞	TCP \ UDP 53
32	NSX-T Management Nodes (Workload)	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✔	⮜⮞	TCP 25
33	NSX-T Management Nodes (Workload)	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✔	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445

34	NSX-T Management Nodes (Workload)	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53
NSX-T AVI Rules									
35	NSX-T AVI Controllers	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✅	⮜⮞	TCP 25
36	NSX-T AVI Controllers	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445
37	NSX-T AVI Controllers	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53
38	NSX-T AVI Service Engine	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✅	⮜⮞	TCP 25

39	NSX-T AVI Service Engine	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445
40	NSX-T AVI Service Engine	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53
Jump Server Rules									
41	Production Jump Servers	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✅	⮜⮞	TCP 25
42	Production Jump Servers	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✅	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445
43	Production Jump Servers	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✅	⮜⮞	TCP \ UDP 53

44	Non Production Jump Servers	Wootton Basset SDDCv2.5	TBC	SMTP Server vESA-SMTP.systems.private	Knowsley Wootton Bassett	10.100.0.39 10.100.0.40 10.102.0.39 10.102.0.40	✓	⮜⮞	TCP 25
45	Non Production Jump Servers	Wootton Basset SDDCv2.5	TBC	ldap.uk.systems.private	Knowsley Wootton Bassett	10.74.100.26 10.94.100.26	✓	⮜⮞	TCP 389, 636, 3268, 3269, 88, 464, 135, 445
46	Non Production Jump Servers	Wootton Basset SDDCv2.5	TBC	DNS know-dbx-00-lb02-gslb woot-dcx-00-lb02-gslb	Knowsley Wootton Bassett	10.94.100.24 10.74.100.24	✓	⮜⮞	TCP \ UDP 53

Table 80 - Connectivity Matrix – NSX Firewall Rules – Wootton Basset

NSX Micro Segmentation Firewall Rules – Wooton Basset

ID	Source Component	Source Location	Source Interface / IP	Destination Component	Destination Location	Destination Interface / IP	Access (NSX)	Direction	Protocol/Port
vRealize Log Insight									
01	VRLI Servers	Wootton Basset SDDCv2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Management)	Wootton Basset SDDCv2.5	TBC	✓	⮜⮞	TCP 80, 443, TCP \ UDP 514, 1514

02	VRLI Servers	Wootton Basset SDDCv2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Workload)	Wootton Basset SDDCv2.5	TBC	✓	⇔	TCP 80, 443, TCP \ UDP 514, 1514
03	VRLI Servers	Wootton Basset SDDCv2.5	TBC	vROP's Servers	Wootton Basset SDDCv2.5	TBC	✓	⇔	TCP 6061, 10000, 443,123
04	VRLI Servers	Wootton Basset SDDCv2.5	TBC	SDDC Manager	Wootton Basset SDDCv2.5	TBC	✓	⇔	TCP 22, 443, 9000 ICMP, 514
05	VRLI Servers	Wootton Basset SDDCv2.5	TBC	VRLI Servers	Wootton Basset SDDCv2.5	TBC	✓	⇔	TCP 9000, 9543, 1514, 6514, 7000, 9042, 9160, 59778, 16520-16580, 80, 443
06	VRLI Servers	Wootton Basset SDDCv2.5	TBC	NSX-T Managers (Management)	Wootton Basset SDDCv2.5	TBC	✓	⇔	TBC
07	VRLI Servers	Wootton Basset SDDCv2.5	TBC	NSX-T Managers (Workload)	Wootton Basset SDDCv2.5	TBC	✓	⇔	TBC
08	VRLI Servers	Wootton Basset SDDCv2.5	TBC	NSX-T AVI Controllers	Wootton Basset SDDCv2.5	TBC	✓	⇔	TBC
09	VRLI Servers	Wootton Basset SDDCv2.5	TBC	NSX-T AVI Service Engines	Wootton Basset SDDCv2.5	TBC	✓	⇔	TBC

10	VRLI Servers	Wootton Basset SDDCv2.5	TBC	WorkSpaceOne Servers	Wootton Basset SDDCv2.5	TBC	✓	◄►	TBC
11	VRLI Servers	Wootton Basset SDDCv2.5	TBC	ESXi Servers (Management)	Wootton Basset SDDCv2.5	TBC	✓	◄►	TBC
12	VRLI Servers	Wootton Basset SDDCv2.5	TBC	ESXi Servers (Edge)	Wootton Basset SDDCv2.5	TBC	✓	◄►	TBC
13	VRLI Servers	Wootton Basset SDDCv2.5	TBC	ESXi Servers (Workload)	Wootton Basset SDDCv2.5	TBC	✓	◄►	TBC
14	VRLI Servers	Wootton Basset SDDCv2.5	TBC	All other WOOTTON BASSET SDDCV2.5 Addresses	Wootton Basset SDDCv2.5	TBC	✗	◄►	TCP
vRealize Network Insight									
01	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Management)	Wootton Basset SDDCv2.5	TBC	✓	◄►	TCP 2055
02	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Edge)	Wootton Basset SDDCv2.5	TBC	✓	◄►	TCP 2055
03	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Workload)	Wootton Basset SDDCv2.5	TBC	✓	◄►	TCP 2055

04	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Management)	Wootton Basset SDDCv2.5	TBC	✓	⮜⮞	TCP 2055
05	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Workload)	Wootton Basset SDDCv2.5	TBC	✓	⮜⮞	TCP 2055
06	VRNI Servers	WOOTTON BASSET SDDCV2.5	Wootton Basset SDDCv2.5	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP
07	VRNI Servers	WOOTTON BASSET SDDCV2.5	Wootton Basset SDDCv2.5	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP
08	VRNI Servers	WOOTTON BASSET SDDCV2.5	Wootton Basset SDDCv2.5	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP
09	VRNI Servers	WOOTTON BASSET SDDCV2.5	Wootton Basset SDDCv2.5	TBC	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP
10	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	NSX-T AVI Controllers	Wootton Basset SDDCv2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP
11	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	NSX-T AVI Service Engines	Wootton Basset SDDCv2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP

12	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	All other WOOTTON BASSET SDDCV2.5 Addresses	WOOTTON BASSET SDDCV2.5	TBC	✗	⮜⮞	TCP
Virtual Center Server									
01	Wootton Basset SDDCv2.5 vCenter Server (Management)	WOOTTON BASSET SDDCV2.5	TBC	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 443
02	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 443
03	Wootton Basset SDDCv2.5 vCenter Server (Management)	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP/UDP 902, 6500, TCP 5989, 443, 80, 8001, 8002
04	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP/UDP 902, 6500, TCP 5989, 443, 80, 8001, 8002
05	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP/UDP 902, 6500, TCP 5989, 443, 80, 8001, 8002

06	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 443, 22, ICMP
07	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 443, 22, ICMP
08	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 5898, 443
09	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 5898, 443
10	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	VRLI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP / UDP 514, 1514, TCP 443
11	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	VRLI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP / UDP 514, 1514, TCP 443
12	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	NSX-T AVI Controllers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC

13	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	NSX-T AVI Service Engines	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
14	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
15	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
16	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
17	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	WorkSpaceOne Servers	Wootton Basset SDDCv2.5	TBC	✓	◄►	TBC
18	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	WorkSpaceOne Servers	Wootton Basset SDDCv2.5	TBC	✓	◄►	TBC
19	WOOTTON BASSET SDDCV2.5 vCenter Server	WOOTTON BASSET SDDCV2.5	TBC	All other WOOTTON BASSET	WOOTTON BASSET SDDCV2.5	TBC	✗	◄►	TCP

				SDDCV2.5 Addresses					
ESXi Hosts									
01	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	✅	◀▶	TCP/UDP 902, 6500, TCP 5989, 443, 80, 8001, 8002
02	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	✅	◀▶	TCP/UDP 902, 6500, TCP 5989, 443, 80, 8001, 8002
03	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✅	◀▶	TCP/UDP 902, 6500, TCP 5989, 443, 80, 8001, 8002
04	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	✅	◀▶	TCP 22, 443, ICMP, 80, 9000
05	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	✅	◀▶	TCP 22, 443, ICMP, 80, 9000
06	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	✅	◀▶	TCP 22, 443, ICMP, 80, 9000
07	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	✅	◀▶	TCP 2055

08	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 2055
09	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 2055
10	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	vROPS Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
11	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	vROPS Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
12	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	vROPS Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
13	SDDCv2.5 ESXi Servers (Knowsley)	Knowsley DB3	Management / Workload / VMB Workload ESXi Servers	All other WOOTTON BASSET SDDCV2.5 Addresses	WOOTTON BASSET SDDCV2.5	TBC	✗	◄►	TCP
vRealize Operations Manager									
01	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	VRLI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 6061, 10000, 443,123
02	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 443, TCP / UDP 514, 1514

				vCenter Server (Management					
03	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 443, TCP / UDP 514, 1514
04	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, 9000, ICMP, 514
05	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
06	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
07	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TBC
08	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	All other WOOTTON BASSET SDDCV2.5 Addresses	WOOTTON BASSET SDDCV2.5	TBC	✗	◄►	TCP
SDDC Manager									
01	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, ICMP

02	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	NSX Components	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, ICMP
03	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 443, 22, ICMP
04	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 443, 22, ICMP
05	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	Internet	TBC	TBC	✓	◄►	TCP 80, 443
06	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	VRLI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, 9000 ICMP, 514
07	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, ICMP, 80, 9000
08	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, ICMP, 80, 9000
09	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, ICMP, 80, 9000

10	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	All other WOOTTON BASSET SDDCV2.5 Addresses	WOOTTON BASSET SDDCV2.5	TBC	✗	⮜⮞	TCP
NSX Components									
01	NSX-T AVI Controllers	WOOTTON BASSET SDDCV2.5	TBC	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443
02	NSX-T AVI Service Engines	WOOTTON BASSET SDDCV2.5	TBC	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443
03	NSX-T AVI Controllers	WOOTTON BASSET SDDCV2.5	TBC	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443
04	NSX-T AVI Service Engines	WOOTTON BASSET SDDCV2.5	TBC	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443
05	NSX-T AVI Controllers	WOOTTON BASSET SDDCV2.5	TBC	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP
06	NSX-T AVI Service Engines	WOOTTON BASSET SDDCV2.5	TBC	SDDC Manager	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP
07	NSX-T AVI Controllers	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5	WOOTTON BASSET SDDCV2.5	TBC	✓	⮜⮞	TCP 22, 443, ICMP

				vCenter Server (Management					
08	NSX-T AVI Service Engines	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, ICMP
09	NSX-T AVI Controllers	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, ICMP
10	NSX-T AVI Service Engines	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, ICMP
11	NSX-T AVI Controllers	WOOTTON BASSET SDDCV2.5	TBC	All other WOOTTON BASSET SDDCV2.5 Addresses	WOOTTON BASSET SDDCV2.5	TBC	✗	◄►	TCP
12	NSX-T AVI Service Engines	WOOTTON BASSET SDDCV2.5	TBC	All other WOOTTON BASSET SDDCV2.5 Addresses	WOOTTON BASSET SDDCV2.5	TBC	✗	◄►	TCP
VMware Life Cycle Manager									

01	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	vROP's Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443
02	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	VRLI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443, 9543, 16520
03	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	VRNI Servers	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 22, 443
04	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	vIDM	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 8443, 443, 9999, 9898, 9000, 9694
05	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Management	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 443
06	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	Wootton Basset SDDCv2.5 vCenter Server (Workload)	WOOTTON BASSET SDDCV2.5	TBC	✓	◄►	TCP 443
07	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Management)	WOOTTON BASSET SDDCV2.5	Management / Workload / VMB Workload ESXi Servers	✓	◄►	TCP 443
08	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Edge)	WOOTTON BASSET SDDCV2.5	Management / Workload / VMB	✓	◄►	TCP 443

						Workload ESXi Servers			
09	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	ESXi Servers (Workload)	WOOTTON BASSET SDDCV2.5	Management / Workload / VMB Workload ESXi Servers	✓	◄►	TCP 443
10	VMware Life Cycle Manager	WOOTTON BASSET SDDCV2.5	TBC	All other WOOTTON BASSET SDDCV2.5 Addresses	WOOTTON BASSET SDDCV2.5	TBC	✗	◄►	TCP

Table 81 - Connectivity Matrix – NSX Micro Micro Segmentation Firewall Rules – Wootton Basset

APPENDIX

NSA Levels

Each tier of the network and systems will be identified as existing within a particular security (trust) level. Each level imposes restrictions and boundaries on the traffic crossing it, and permits only trusted communications to be established, both protecting the information in that level and regulates the access to information in higher security levels.

Level 0 Network Security

Anything that is considered untrusted. e.g.

- Vendors (Network outside Liberty Global) including SaaS
- Liberty Global Wireless
- Internet

Level 1 Network Security

Traffic originated from Liberty Global managed devices in non-managed Liberty Global physical environment

Level 2 Network Security

Any publicly accessible Liberty Global managed and controlled service. e.g.

- Liberty Global office PC/Laptops
- AEM hosted portal website

Level 3 Network Security

Level 3 has a Secure gateway function to bridge access from untrusted networks into protected/trusted networks to allow further into the Liberty global networks. e.g.

- IBM Webseal or F5 WAF
- Connectra client VPN access (with UIM user verification)
- AKANA Ext GW or Similar proxy

Level 4 Network Security

L4 systems handle and process data. e.g.

- AEM Publisher
- Middleware
- AKANA Int GW

Level 5 Network Security

This level is for the protection of Liberty Global critical infrastructure. e.g.

- AEM Author
- Switches, Routers

Level 6 Network Security

This level is the highest security level in Liberty Global for the protection of sensitive information.

- Customer payment systems/accounts
- Firewall management

Penetration Testing

For all new solutions, Global Security require a Pen test to be performed.
The latest guidance should always be sought from Global Security, but some background information on the solution used can be found here:
https://globe.upc.biz/confluence/display/DD/Penetration+Testing+-+SecureLink