Introducing VMware Validated Designs for Software-Defined Data Center

22 AUG 2017

VMware Validated Design 4.1

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Introducing VMware Validated Design for Software-Defined Data Center

The *Introducing VMware Validated Design for Software-Defined Data Center* guide provides directions on using the content of VMware Validated Design™ for Software-Defined Data Center. The guide also contains a high-level overview of the Software-Defined Data Center (SDDC) design supported in this VMware Validated Design version.

Introducing VMware Validated Design for Software-Defined Data Center focuses on providing guidance about using the VMware Validated Design and includes the following information:

- Design objectives
- Document structure and purpose
- Supported VMware product versions
- SDDC design overview

Intended Audience

Introducing VMware Validated Design for Software-Defined Data Center is intended for cloud architects, infrastructure administrators, cloud administrators and cloud operators who want to get familiar with VMware Validated Design to deploy and manage an SDDC that meets the requirements for capacity, scalability, business continuity and disaster recovery.

Required Software

Introducing VMware Validated Design for Software-Defined Data Center is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions

Features of VMware Validated Designs 1

Use VMware Validated Designs to build a Software-Defined Data Center that is based on management components by VMware, and has a scalable and best-practice configuration.

VMware Validated Designs have the following advantages:

One path to SDDC

After you satisfy the deployment requirements, follow one consistent path to deploy an SDDC.

VMware Validated Designs offer an extensively tested solution path with specific information about product versions, networking architecture, capabilities, and limitations.

SDDC design for use in production

This VMware Validated Design supports an SDDC that has the following features:

- High-availability of management components
- Backup and restore of management components
- Monitoring and alerting
- Disaster recovery of management components
- Protection of management application by using NSX Distributed Firewall

Validated design and deployment

The prescriptive documentation of a VMware Validated Design is continuously validated by VMware.

Validation provides the following advantages to your organization:

- Validated product interoperability
- Validated SDDC features, such as:
  - Churn rate of tenant workloads
  - High availability of management components
  - Operational continuity
  - Design with dual-region support in mind
- Reduced risk of deployment and operational problems
- Reduced test effort

Fast SDDC standup	You can implement a data center without engaging in design work and product research. After you download all SDDC products, follow the detailed design and step-by-step instructions.
Support for latest product releases	Every version of a VMware Validated Design accommodates new product releases. If you have deployed an SDDC according to an earlier version of a VMware Validated Design, you can directly follow the validated design to upgrade your environment.
Foundation of SDDC deployment use cases	This VMware Validated Design provides the foundation for use cases that satisfy the requirements of individual organizations or industry segments, such as VMware Validated Design for Micro-Segmentation and VMware Validated Design for IT Automating IT.

Types of VMware Validated Designs 2

A VMware Validated Design release contains two types of SDDC implementation guidance. A VMware Validated Design for Software-Defined Data Center comes in several flavors and covers all main services in an SDDC. A VMware Validated Design use case is related to the solution to a specific IT case.

Table 2-1. Types of VMware Validated Designs

Feature	VMware Validated Design for Software-Defined Data Center	VMware Validated Design Use Case
Definition	Implements an SDDC that contains the complete set of services for provisioning and monitoring workloads.	Represents a sub- or super-set of VMware Validated Design for Software-Defined Data Center. A use case provides an SDDC solution to achieve specific IT outcomes, such as application security, IT automation, and so on. See *Introducing VMware Validated Design Use Cases*.
Set of management components	Components to build all layers for general provisioning and monitoring services in an SDDC.	Only components that are required to implement the solution.
Documentation	■ *Architecture and Design* ■ *Planning and Preparation* ■ *Deployment* ■ *Operational guidance*	A use case contains one of the following documentation sets: ■ *Architecture and Design* and *Planning and Preparation* ■ *Scenarios*
Set of design objectives	Full set	Full set
Support of workflows	No	Yes Each VMware Validated Design use case supports a set of validated workflows. The workflows are related to the common operations that you perform in the covered case.
Flavors	Yes You can deploy a flavor of a VMware Validated Design for Software-Defined Data Center with the same set of management components, and different deployment model and resource requirements. See Chapter 3, "SDDC Implementations According to VMware Validated Design for Software-Defined Data Center," on page 11.	No A VMware Validated Design use case focus on the solution to a concrete market case.

SDDC Implementations According to VMware Validated Design for Software-Defined Data Center

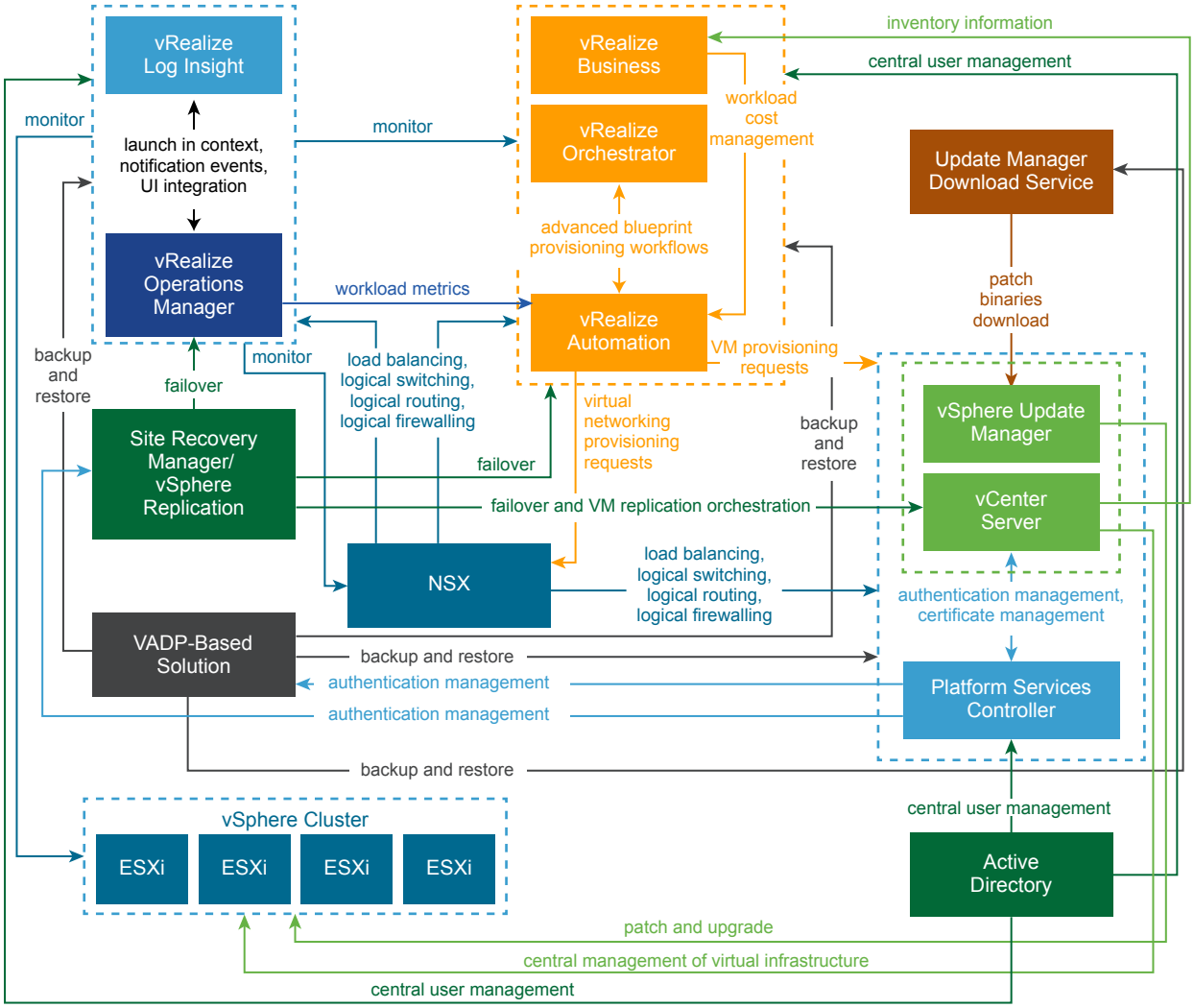
3

You can select an SDDC implementation according to requirements of your organization and the resource capabilities of your environment.

High-Level Logical Design of the SDDC

The SDDC according to VMware Validated Design for Software-Defined Data Center contains the main services that are required to cover workload provisioning, operations management and business continuity.

Figure 3-1. Logical Design of the SDDC



SDDC Implementations

The VMware Validated Design for Software-Defined Data Center family provides the following SDDC implementations:

Table 3-1. SDDC Implementations by VMware Validated Design for Software-Defined Data Center

SDDC Flavor	Product Name	Description
Standard SDDC	VMware Validated Design for Software-Defined Data Center	Implements a production-ready SDDC that is dual-region, each region deployed on 2 pods.
Consolidated SDDC	VMware Validated Design for Management and Workload Consolidation	Consolidates the resources that are used in the Standard SDDC to provide a single-region environment with a smaller hardware footprint and less strict availability. For example, you can use this design in a smaller environment with less virtual machines, or as a proof of concept or production pilot.
Remote Office and Branch Office (ROBO) SDDC	VMware Validated Design for Remote Office and Branch Office	Extends the Standard SDDC with support for remote offices that are located at a distance from the main office. The main office runs an instance of the Standard SDDC. ROBO SDDC provides decentralized management, such as on-site vCenter Server and NSX Manager, but connects to an existing Standard SDDC over a WAN link. Monitoring and cloud management functions are centralized.

Design Objectives of VMware Validated Designs for Software-Defined Data Center

4

According to the SDDC implementation type, a VMware Validated Design has a number of objectives to deliver prescriptive content about an SDDC that is fast to deploy and is suitable for use in production.

Table 4-1. Objectives of VMware Validated Design for Software-Defined Data Center

VMware Validated Design Objective	Description
Main objective	SDDC capable of automated provisioning of workloads
Scope of deployment	Greenfield and brownfield deployment of the SDDC management components
Cloud type	Private cloud
Number of regions and disaster recovery support	Dual-region SDDC that supports disaster recovery The documentation provides guidance for a deployment that supports two regions for failover in the following way: ■ The design documentation provides guidance for an SDDC whose management components are designed to operate in the event of planned migration or disaster recovery. This part also includes design of the components that support the failover. ■ The deployment documentation provides guidance for an SDDC that supports two regions for both management and tenant workloads. ■ The operational guidance contains detailed instructions about performing disaster recovery and planned migration.
Maximum number of virtual machines	■ 10,000 running virtual machines ■ Churn rate of 150 virtual machines per hour Churn rate is related to provisioning, power cycle operations, and decommissioning of one tenant virtual machine by using a blueprint in the cloud management platform. A churn rate of 100 means that 100 tenant workloads are provisioned, pass the power cycle operations, and are deleted.

Number of hardware pods in a region	2-pod setup, with minimum 4 ESXi hosts in a pod
	The 2-pod validated design requires the following pods for SDDC deployment:
	■ Management pod. Runs the virtual machines of the management products.
	■ Shared edge and compute pod
	  ■ Runs the tenant workloads.
	  ■ Runs the required NSX services to enable north-south routing between the SDDC and the external network, and east-west routing inside the SDDC.

Data center virtualization	■ Compute virtualization ■ Software-defined storage in the management pod ■ Network virtualization

Table 4-1. Objectives of VMware Validated Design for Software-Defined Data Center (Continued)

VMware Validated Design Objective	Description
Scope of guidance	■ Storage, compute and networking for the management pod. ■ Number of hosts, amount of storage and configuration. ■ Deployment and initial setup of management components at the levels of infrastructure, cloud management platform, and operations. ■ Basic tenant operations such as creating a tenant, assigning tenant capacity, configuring user access, and adding virtual machines to a service catalog from single-machine blueprints. ■ Operations on the management components of the SDDC such as monitoring and alerting, backup and restore, post-maintenance validation, disaster recovery and upgrade.
Overall availability	99% availability Planned downtime is expected for upgrades, patching, and on-going maintenance.
Authentication, authorization, and access control	■ Use of Microsoft Active Directory as a central user repository. ■ Use of service accounts with minimum required authentication and Access Control List configuration. ■ Use of basic tenant accounts.
Certificate signing	Certificates are signed by an external certificate authority (CA) that consists of a root and intermediate authority layers.
Hardening	Tenant workload traffic can be separated from the management traffic. The design uses a distributed firewall to protect all management applications. To secure the SDDC, only other management solutions and approved administration IP addresses can directly communicate with individual components.

Table 4-2. Objectives of VMware Validated Design for Management and Workload Consolidation

VMware Validated Design Objective	Description
Main objective	SDDC capable of automated provisioning of workloads
Scope of deployment	Greenfield deployment of the SDDC management components
Cloud type	Private cloud
Number of regions and disaster recovery support	Single-region SDDC that you can scale out to dual-region.
Maximum number of virtual machines	■ 1,500 running virtual machines ■ Churn rate of 50 virtual machines per hour
Number of hardware pods in a region	1-pod setup, with minimum 4 ESXi hosts in the pod The 1-pod validated design includes a consolidated virtual infrastructure layer for management, edge and compute components.
Data center virtualization	■ Compute virtualization ■ Software-defined storage in the management pod ■ Network virtualization
Scope of guidance	■ Storage, compute and networking for the management pod. ■ Number of hosts, amount of storage and configuration. ■ Deployment and initial setup of management components at the levels of infrastructure, cloud management platform, and operations. ■ Basic tenant operations such as creating a tenant, assigning tenant capacity, configuring user access, and adding virtual machines to a service catalog from single-machine blueprints.
Overall availability	95% availability Planned downtime is expected for upgrades, patching, and on-going maintenance.

Table 4-2. Objectives of VMware Validated Design for Management and Workload Consolidation (Continued)

VMware Validated Design Objective	Description
Authentication, authorization, and access control	■ Use of Microsoft Active Directory as a central user repository. ■ Use of service accounts with minimum required authentication and Access Control List configuration. ■ Use of basic tenant accounts.
Certificate signing	Certificates are signed by an external certificate authority (CA) that consists of a root and intermediate authority layers.
Hardening	Tenant workload traffic can be separated from the management traffic. The design uses a distributed firewall to protect all management applications. To secure the SDDC, only other management solutions and approved administration IP addresses can directly communicate with individual components.

Table 4-3. Objectives of VMware Validated Design for Remote Office and Branch Office

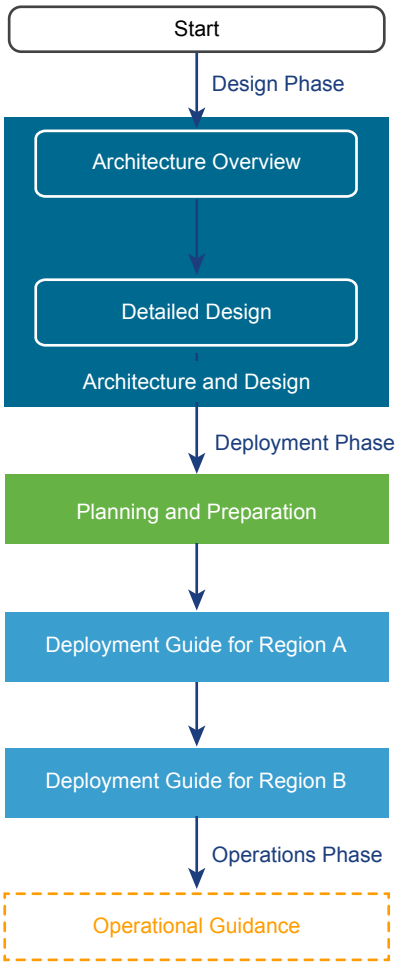
VMware Validated Design Objective	Description
Main objective	SDDC capable of automated provisioning of workloads
Scope of deployment	Greenfield deployment of the SDDC management components
Cloud type	Private cloud
Maximum number of remote regions	10
Maximum number of virtual machines	■ 100 virtual machines per remote region ■ 1,000 running virtual machines across all remote regions ■ Churn rate of 100 virtual machines per hour
Number of hardware pods in a remote region	1-pod, with minimum 4 hosts in the pod The 1-pod region includes a consolidated virtual infrastructure layer for management, edge and compute components.
WAN capacity	10 Mbps, latency up to 100 ms
Data center virtualization	■ Compute virtualization ■ Software-defined storage in the management pod ■ Network virtualization
Scope of guidance	■ Storage, compute and networking for the consolidated pod. ■ Number of hosts, amount of storage and configuration. ■ Deployment and initial setup of management components at the levels of infrastructure, cloud management platform, and operations. ■ Basic tenant operations such as creating a tenant, assigning tenant capacity, configuring user access, and adding virtual machines to a service catalog from single-machine blueprints.
Overall availability	95% availability Planned downtime is expected for upgrades, patching, and on-going maintenance.
Authentication, authorization, and access control	■ Use of Microsoft Active Directory as a central user repository. ■ Use of service accounts with minimum required authentication and Access Control List configuration.
Certificate signing	Certificates are signed by an external certificate authority (CA) that consists of a root and intermediate authority layers.
Hardening	The design uses a distributed firewall to protect all management applications. To secure the SDDC, only other management solutions and approved administration IP addresses can directly communicate with individual components.

Documentation Structure and Audience

5

The structure of the VMware Validated Design documentation reflects the best practices in designing and deploying a data center that is capable of automated workload provisioning. The documentation components of the validated design are organized according to the audience and deployment stage. You use the documents in a specific order.

Figure 5-1. VMware Validated Design Documentation Flow



Architecture Overview

The first part of a VMware Validated Design is *Architecture Overview* and it introduces the terms and components in the design.

Table 5-1. Architecture Overview Information

Section Attribute	Description
Guide	*Architecture and Design*
Purpose	■ Introduce the fundamentals and components in the SDDC design. ■ Provide information about the layered structure of the SDDC. ■ Describe the building modules and basic behavior of each management component.
Audience	Cloud architects and cloud administrators
SDDC Flavor	■ Standard SDDC ■ Consolidated SDDC ■ ROBO SDDC

Detailed Design

After you learn about the basic modules in the SDDC design, you proceed with detailed design of the management components and the required infrastructure.

Table 5-2. Detailed Design Information

Section Attribute	Description
Guide	*Architecture and Design*
Purpose	■ Provide complete details about the configuration of each layer and of the components that are a part of the layer. ■ Describe available design alternatives. ■ Provide design decisions to reflect the main design issues and the rationale behind a chosen solution path.
Audience	Cloud architects and cloud administrators
SDDC Flavor	■ Standard SDDC ■ Consolidated SDDC ■ ROBO SDDC

Planning and Preparation

After you understand the details of the design, you plan your environment according to the requirements of the design so that you can deploy the designed SDDC directly without additional testing and troubleshooting efforts.

Table 5-3. Planning and Preparation Information

Section Attribute	Description
Guide	*Planning and Preparation*
Purpose	Collect all requirements that your environment must meet so that you can follow a VMware Validated Design to create an SDDC. The *Planning and Preparation* section provides prerequisites about the following areas: ■ Required software including VMware products, scripts, and third-party software ■ Networking configuration including VLANs, example IP addresses, and DNS names ■ Active Directory user configuration ■ Specifications of the virtual machines that you must provide in advance
Audience	Cloud architects, infrastructure administrators, cloud administrators, and cloud operators
SDDC Flavor	■ Standard SDDC ■ Consolidated SDDC ■ ROBO SDDC

Deployment Guide for Region A

After you make sure that your environment has the required structure and configuration, follow the *Deployment Guide for Region A* to start the SDDC implementation in the first region.

Table 5-4. Deployment Guide Information

Section Attribute	Description
Guide	*Deployment for Region A* for Standard SDDC *Deployment* for ROBO SDDC and Consolidated SDDC
Purpose	■ Provide step-by-step instructions for each management component of the SDDC according to the selected design path in *Detailed Design*. ■ Cover the single-region setup of the SDDC. ■ Provide details about setting up the virtual infrastructure for both management and tenant workloads. ■ Provide procedures for integration of the products to form one functional system.
Audience	Cloud architects, infrastructure administrators, cloud administrators, and cloud operators
SDDC Flavor	■ Standard SDDC ■ Consolidated SDDC ■ ROBO SDDC

Deployment Guide for Region B

After you make sure that your environment has the required structure and configuration, follow the *Deployment Guide for Region B* to start the SDDC implementation in the second region.

Table 5-5. Deployment Guide Information

Section Attribute	Description
Guide	*Deployment for Region B*
Purpose	■ Provide step-by-step instructions for each management component of the SDDC according to the selected design path in *Detailed Design*. ■ Cover the dual-region setup of the SDDC. ■ Provide details about setting up the virtual infrastructure for both management and tenant workloads. ■ Provide procedures for integration of the products to form one functional system.
Audience	Cloud architects, infrastructure administrators, cloud administrators, and cloud operators
SDDC Flavor	■ Standard SDDC

Operational Guidance

After you deploy the SDDC, follow the *Operational Guidance* documentation to operate the environment and the management workloads.

Table 5-6. Operational Guidance Information

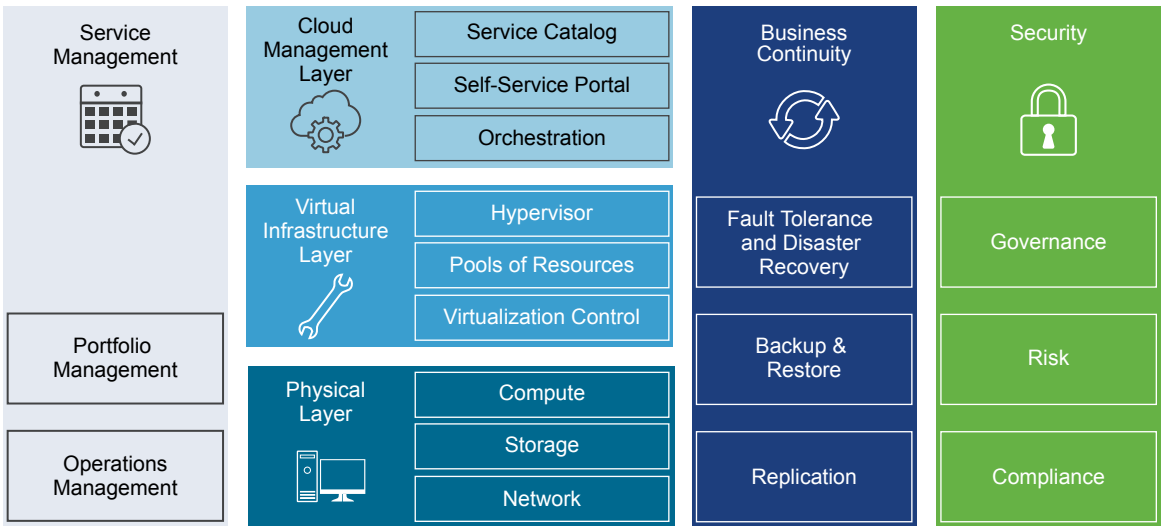
Section Attribute	Description
Guide	*Operational Guidance* that is delivered as a set of add-on packages that could be asynchronously delivered.
Purpose	For each management component, provide the following information: ■ Step-by-step instructions about backing and restoring the components of each management product. ■ Step-by-step instructions about setting up dashboards and activating alerts for monitoring the SDDC, and lists of notifications that are most symptomatic. ■ Step-by-step instructions about verifying the operation of the SDDC after software maintenance such as restore, upgrade, or failover . ■ Step-by-step instructions about setting up and performing for disaster recovery or planned migration. ■ Step-by-step instructions about upgrading from earlier versions of a VMware Validated Design. ■ Step-by-step instructions about replacing certificates on the management components ■ High-level guidance about migration to a validated SDDC
Audience	Cloud architects, infrastructure administrators, cloud administrators, and cloud operators
SDDC Flavor	■ Standard SDDC ■ ROBO SDDC (Certificate Replacement)

Overview of Standard SDDC 6

The SDDC architecture in this VMware Validated Design consists of layers. The layered structure enables you to create the SDDC in modules and to handle each set of components separately.

For information about the design and deployment of each layer, see *VMware Validated Design Architecture and Design*, *VMware Validated Design Deployment for Region A* and *VMware Validated Design Deployment for Region B*.

Figure 6-1. Components of a Software-Defined Data Center

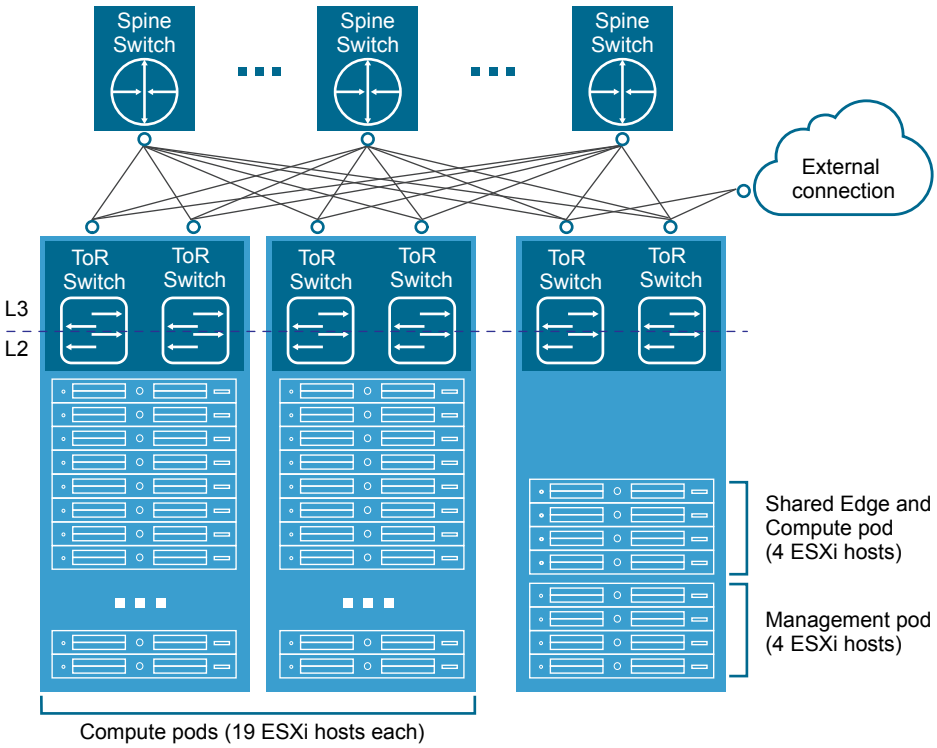


Physical Infrastructure Layer in Standard SDDC

The physical layer in Standard SDDC contains the compute, storage, and network resources in your data center.

The compute, storage and network resources are organized in pods. The physical layer also includes the physical network infrastructure, and storage setup.

Figure 6-2. Physical Configuration of the SDDC



Pods

At the physical layer, a pod is a logical grouping of hardware that supports a certain function and is easy to replicate. Pods can have different configurations of server, storage, and network equipment. In large environments, each pod spans one rack, but in smaller environments you can aggregate multiple pods into a single rack.

This VMware Validated Design uses the following types of pods:

Management Pod

Runs the virtual machines of the components that manage the data center, such as vCenter Server, NSX Manager, and NSX Controller.

This VMware Validated Design uses one management pods that occupies half a rack.

Shared Edge and Compute Pod

The shared edge and compute pod runs the required NSX services to enable north-south routing between the data center and the external network, and east-west routing inside the data center. This shared pod also hosts the tenant virtual machines (sometimes referred to as workloads or payloads). As the environment grows, additional compute-only pods can be added to support a mix of different types of workloads for different types of Service Level Agreements.

Compute Pod

Compute pods host the tenant virtual machines (sometimes referred to as workloads or payloads). You can mix different types of compute pods and provide separate compute pools for different types of SLAs.

Network

This VMware Validated Design uses a Layer 3 leaf-and-spine network architecture.

- A leaf switch is typically located inside a rack and provides network access to the servers inside that rack. Leaf switches are also called Top of Rack (ToR) switches.
- A spine switch is in the spine layer and provides connectivity between racks. Links between spine switches are typically not required. If a link failure between a spine switch and a leaf switch occurs, the routing protocol ensures that no traffic is sent to the spine switch that has lost connectivity.

Regions and Availability Zones

Availability zone

Represent the fault domain of the SDDC. Multiple availability zones can provide continuous availability of an SDDC. This VMware Validated Design supports one availability zone per region.

Region

Each region is a separate SDDC instance. You use multiple regions for disaster recovery across individual SDDC instances.

In this VMware Validated Design, regions have similar physical and virtual infrastructure design but different naming.

Table 6-1. Regions in VMware Validated Design

Region	Disaster Recovery Role	Region-Specific Domain Name
Region A	Protected	sfo01.rainpole.local
Region B	Recovery	lax01.rainpole.local

Storage

This VMware Validated Design provides guidance for the storage of the management components. The design uses two storage technologies:

Primary Storage

vSAN storage is the default storage type for the SDDC management components. All design, deployment and operational guidance are performed on vSAN.

The storage devices on vSAN ready servers provide the storage infrastructure. Because this VMware Validated Design uses vSAN in hybrid mode, each rack server must have minimum one SSD and two HDD devices that form a disk group with capacity.

Secondary Storage

NFS storage is the secondary storage for the SDDC management components. It provides space for workload backup, archiving log data and application templates.

Virtual Infrastructure Layer in Standard SDDC

The virtual infrastructure layer of the Standard SDDC contains the components that provide compute, networking, and storage resources to the management and tenant workloads.

vCenter Server Design

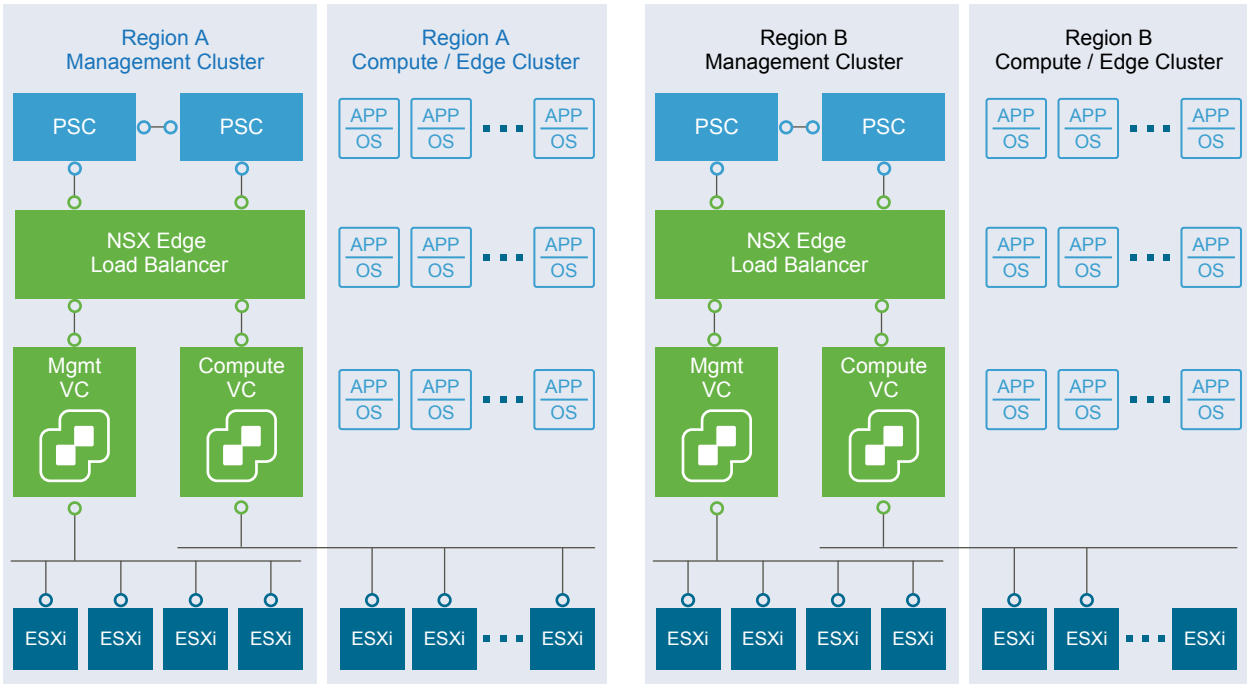
Table 6-2. vCenter Server Design Details

Design Area	Description
vCenter Server instances	You deploy two vCenter Server instances in the following way: ■ One vCenter Server instance supporting the SDDC management components. ■ One vCenter Server instance supporting the edge components and tenant workloads. Using this model provides the following benefits: ■ Isolation of management and compute vCenter Server operations ■ Simplified capacity planning ■ Separated upgrade ■ Separated roles
Clusters	You distribute hosts and workloads in the following clusters: ■ Management cluster that contains all management hosts and handles resources for the management workloads. ■ Shared edge and compute cluster that contains tenant workloads, NSX Controllers, and associated NSX Edge gateway devices used for the tenant workloads.
Resource pools for tenant workloads and dedicated NSX components	On the shared edge and compute cluster, you use resource pools to distribute compute and storage resources to the tenant workloads and the NSX components carrying their traffic.

Table 6-2. vCenter Server Design Details (Continued)

Design Area	Description
Deployment model	This VMware Validated Design uses two external Platform Services Controller instances and two vCenter Server instances. For redundancy, the design joins the two Platform Services Controller instances to the same vCenter Single Sign-On domain, and points the vCenter Server instances to a load balancer that distributes the requests between the two Platform Services Controller instances.
Management host provisioning	You use host profiles to apply the networking and authentication configuration on the ESXi hosts in the management pod and in the shared edge and compute pod.

Figure 6-3. Layout of vCenter Server Clusters



Dynamic Routing and Application Virtual Networks

This VMware Validated Design supports dynamic routing for both management and tenant workloads, and also introduces a model of isolated application networks for the management components.

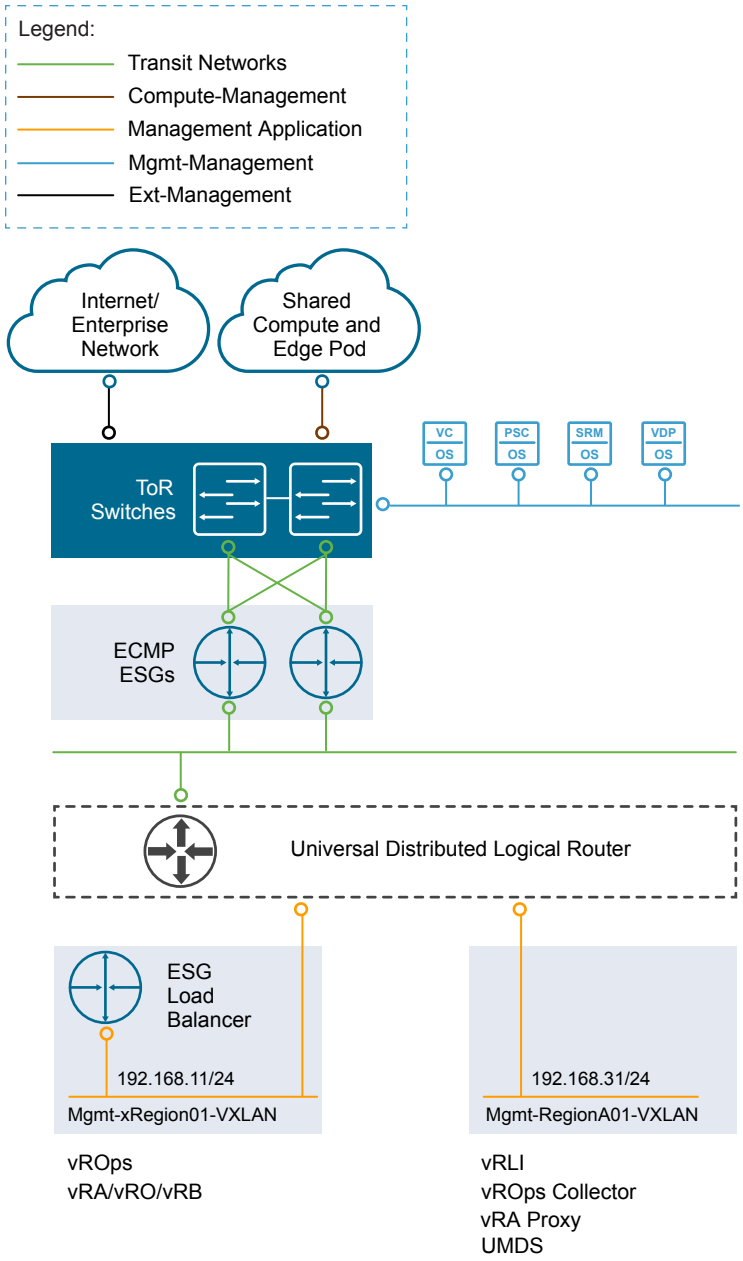
Dynamic routing support includes the following nodes:

- Pair of NSX Edge service gateways (ESGs) with ECMP enabled for north/south routing across all regions.
- Universal distributed logical router (UDLR) for east/west routing across all regions.
- Distributed logical router (DLR) for the shared edge and compute cluster and compute clusters to provide east/west routing for workloads that require on-demand network objects from vRealize Automation.

Application virtual networks provide support for limited access to the nodes of the applications through published access points. Three application virtual networks exist:

- Cross-region application virtual network that connects the components that are designed to fail over to a recovery region.
- Region-specific application virtual network in Region A for components that are not designed to fail over.
- Region-specific application virtual network in Region B for components that are not design to fail over.

Figure 6-4. Virtual Application Network Components and Design



Distributed Firewall

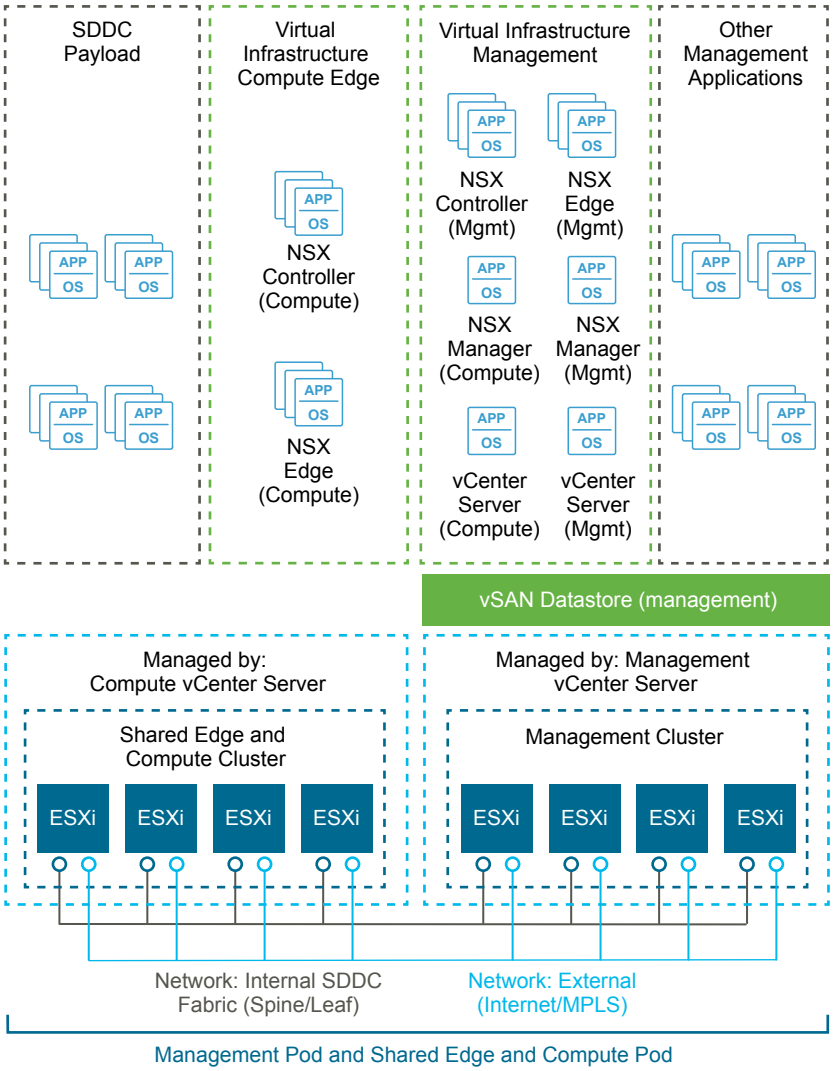
This VMware Validated Design uses the distributed firewall functionality that is available in NSX to protect all management applications attached to application virtual networks.

Software-Defined Storage Design for Management Products

In each region, workloads on the management cluster store their data on a vSAN datastore. The vSAN datastore spans all 4 ESXi hosts of the management cluster. Each host adds one disk group to the datastore.

Applications store their data according to the default storage policy for vSAN.

Figure 6-5. vSAN Conceptual Design



vSphere Data Protection, vRealize Log Insight and vRealize Automation Content Library use NFS exports as secondary storage. You create two datastores: one in the management cluster for vSphere Data Protection and one in the shared edge and compute cluster for vRealize Automation.

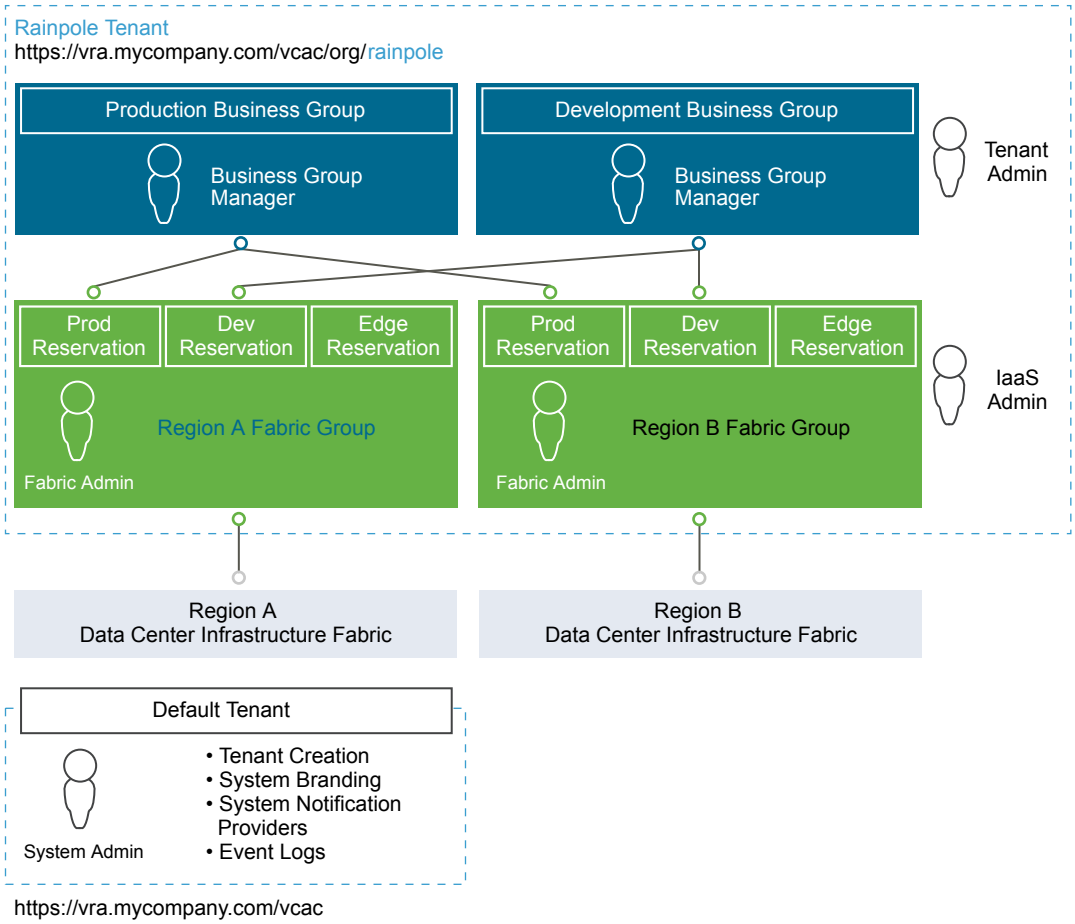
Cloud Management Layer in Standard SDDC

The cloud management layer enables you to deliver tenants with automated workload provisioning by using a self-service portal.

Table 6-3. Cloud Management Design Details

Design Attribute	Description
Software components	■ vRealize Automation ■ Embedded vRealize Orchestrator ■ vRealize Business
Deployment model of vRealize Automation	Distributed deployment with support for vSphere endpoints by using vSphere Proxy Agent virtual machines. You install the vRealize Automation components on multiple machines.
High availability and load balancing	Supported for all nodes except the Microsoft SQL database server and vRealize Business.
Endpoints	■ vCenter Server for the compute and edge clusters ■ NSX Manager for the compute and edge clusters
Blueprint configuration	Single-machine blueprints
Tenants	A single tenant company called Rainpole
Fabric groups	One fabric group in a region with all resources in the compute and edge cluster assigned
Business groups	According to the internal structure and workload configuration of your organization. Allocate business groups for separate business units, for example, for development and production.

Figure 6-6. Example vRealize Automation Tenant Design



Operations Management Layer in Standard SDDC

The operations layer of the SDDC provides capabilities for performance and capacity monitoring, and for backup and restore of the cloud management components.

vRealize Operations Manager

You use vRealize Operations Manager to monitor the management components of the SDDC including vSphere, NSX for vSphere and vRealize Automation.

vRealize Operations Manager is also sized to accommodate the number of tenant workloads per the design objectives.

Figure 6-7. vRealize Operations Manager Logical Design

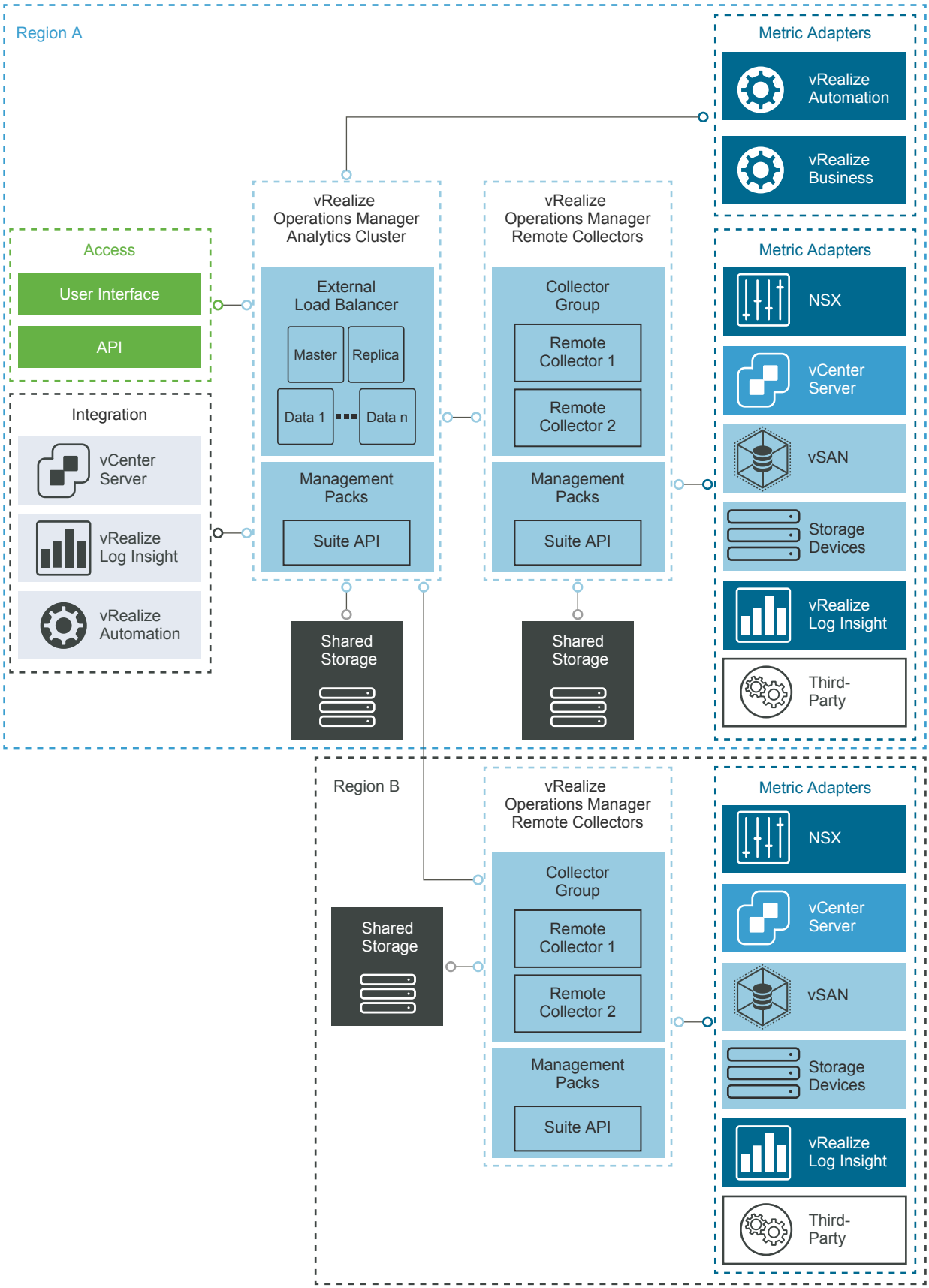


Table 6-4. vRealize Operations Manager Design Details

Design Attribute	Description
Deployment model	■ Analytics cluster of three nodes: master, master replica and data node ■ Remote collector group that consists of two remote collectors that communicate with the region-specific components in the region
Monitored components	■ vCenter Server and Platform Services Controller ■ ESXi hosts in the management cluster and the shared edge and compute cluster ■ All components of NSX for vSphere for the management cluster and the shared edge and compute cluster ■ vRealize Automation and vRealize Orchestrator ■ vRealize Log Insight including Launch in Context ■ vRealize Business including integration in the vRealize Operations Manager operations interface ■ vSAN ■ vRealize Operations Manager (self-health monitoring)

vRealize Log Insight

You use vRealize Log Insight to access the logs of the SDDC management components from a central place and view this information in visual dashboards.

Figure 6-8. vRealize Log Insight Logical Design

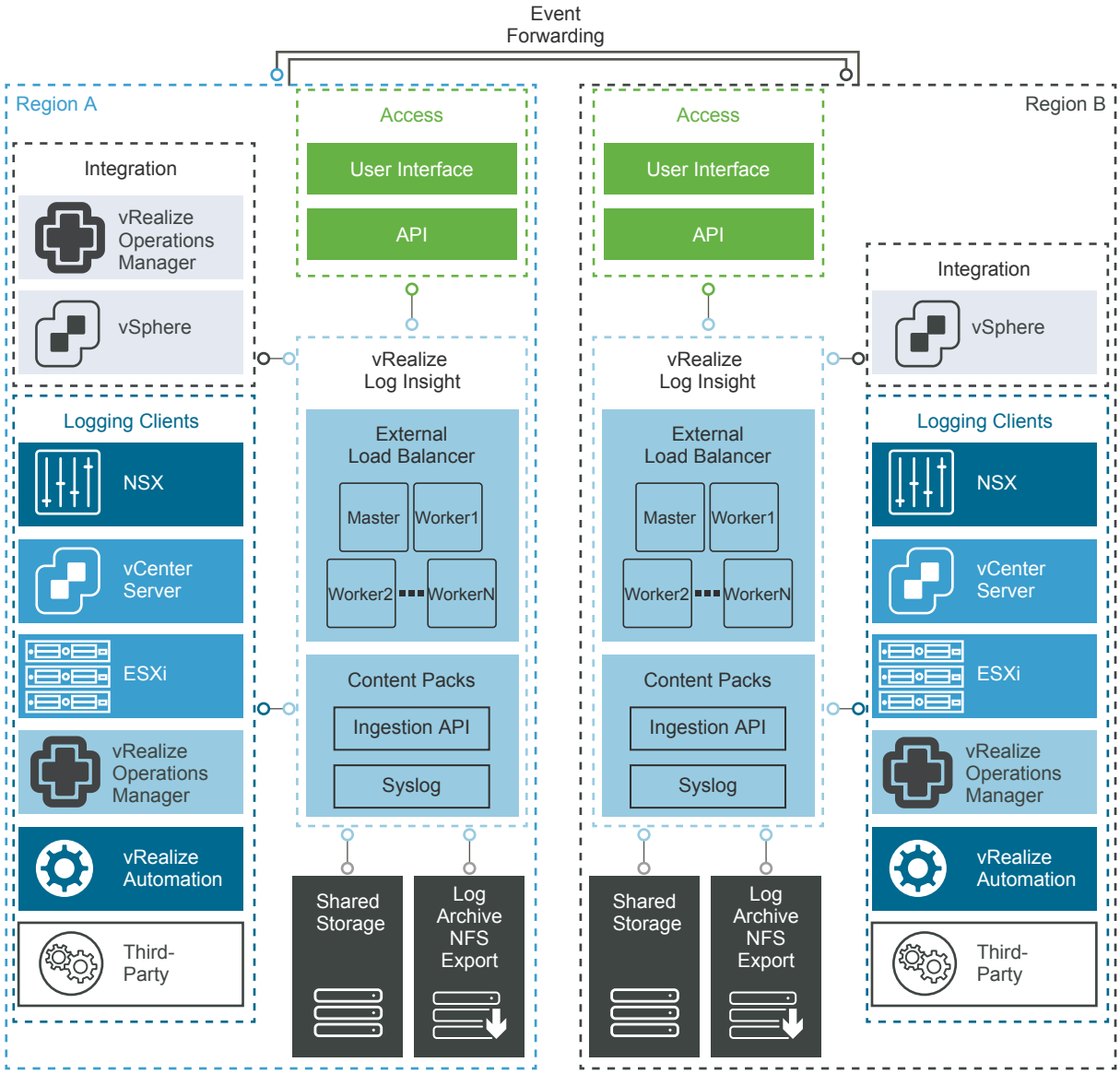


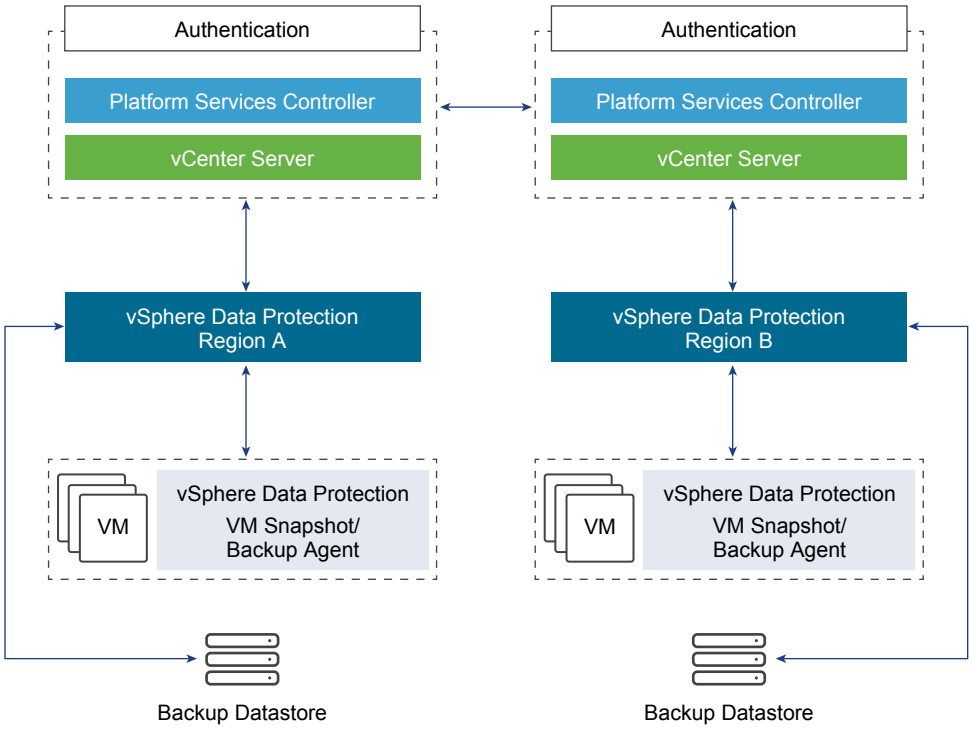
Table 6-5. vRealize Log Insight Design Details

Design Attribute	Description
Deployment model	Cluster of master node and two worker nodes.
Monitored components	■ vCenter Server and Platform Services Controller ■ Management, shared edge and compute ESXi hosts ■ All components of NSX for vSphere for the management cluster and the shared edge and compute clusters ■ vRealize Automation and vRealize Orchestrator ■ vRealize Business ■ Analytics cluster nodes of vRealize Operations Manager ■ Management virtual appliances
Archiving	Archiving location on an NFS export

vSphere Data Protection

You deploy vSphere Data Protection to back up the virtual machines of the SDDC management components. vSphere Data Protection stores its data and the backup copies of virtual machines on the NFS datastore in the management cluster.

Figure 6-9. vSphere Data Protection Design

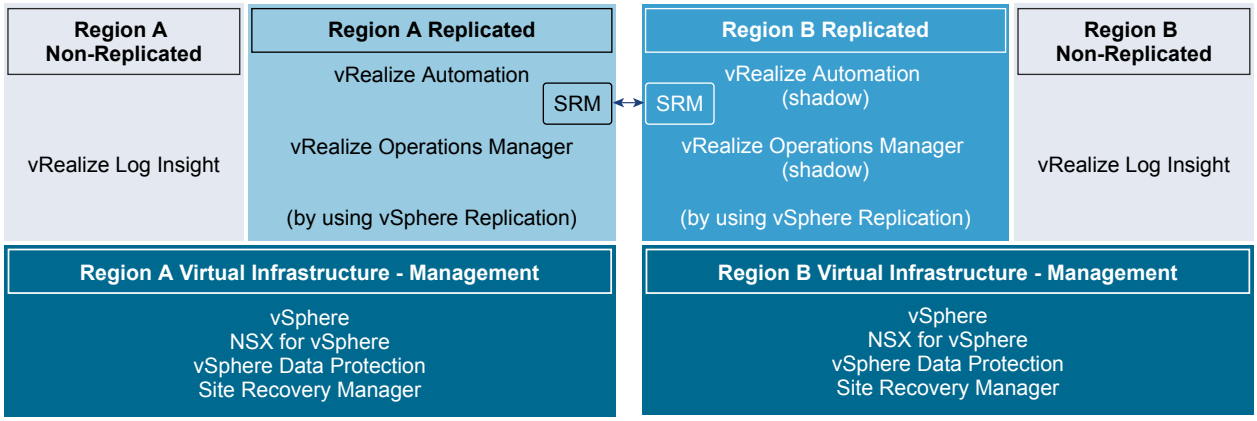


Disaster Recovery Design

This VMware Validated Design implements a disaster recovery configuration that uses Site Recovery Manager and vSphere Replication to replicate the management applications and to mirror them on the second recovery region.

- The following management applications are a subject of disaster recovery protection:
  - vRealize Automation together with vRealize Orchestrator and vRealize Business
  - Analytics cluster of vRealize Operations Manager
- The virtual infrastructure components that are not in the scope of the disaster recovery protection, such as vRealize Log Insight, are available as separate instances in each region.

Figure 6-10. Disaster Recovery Architecture

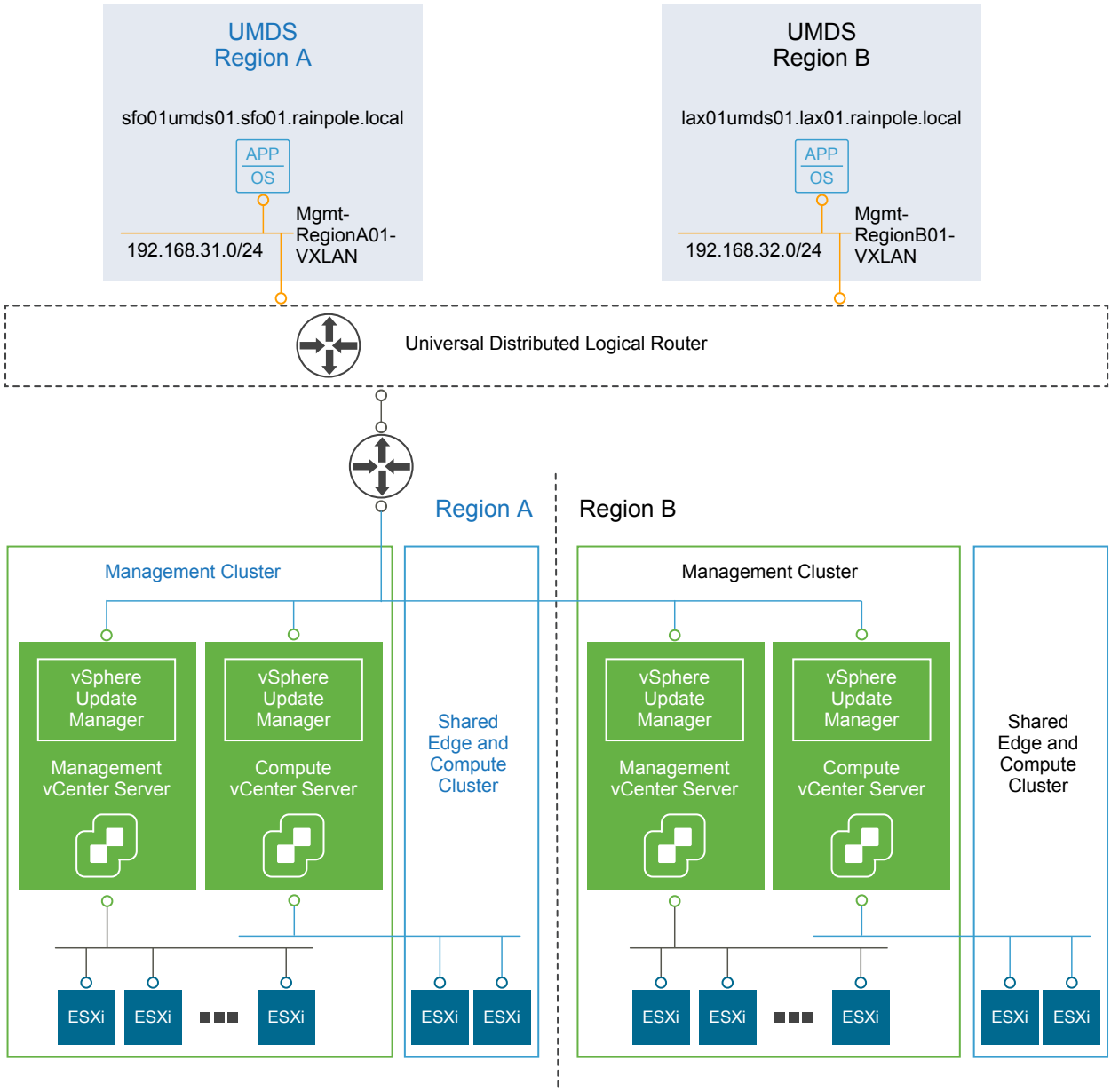


vSphere Update Manager

This VMware Validated Design version uses vSphere Update Manager for upgrade of the ESXi hosts from previous VMware Validated Design versions.

vSphere Update Manager server and client components are a part of vCenter Server Appliance in vSphere 6.5 or later. This design also deploys an instance of vSphere Update Manager Download Service (UMDS) in each region. Using a region-specific UMDS instance restricts the direct access to the external network from multiple vSphere Update Manager and vCenter Server instances, and reduces storage requirements across vSphere Update Manager.

Figure 6-11. vSphere Update Manager Design

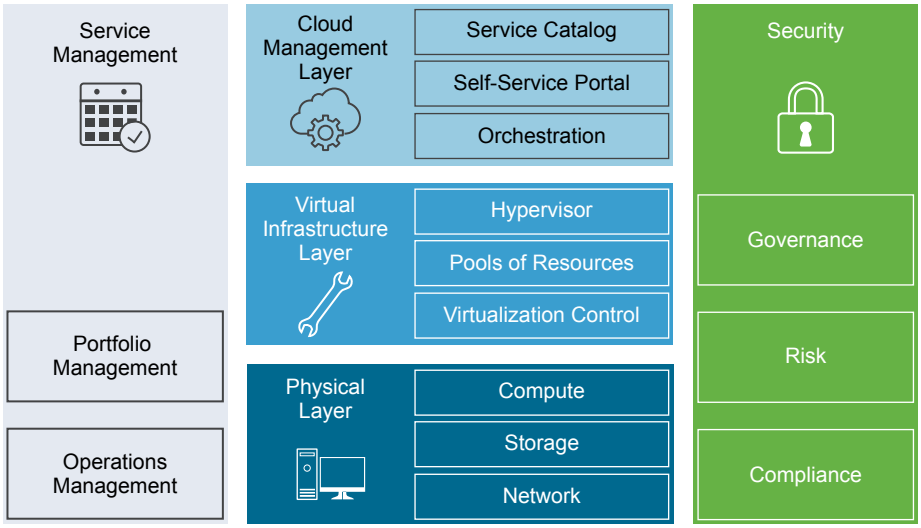


Overview of Consolidated SDDC 7

The SDDC architecture in this VMware Validated Design consists of layers. The layered structure enables you to create the SDDC in modules and to handle each set of components separately.

For information about the design and deployment of each layer, see *VMware Validated Design Architecture and Design* and *VMware Validated Design Deployment*.

Figure 7-1. Components of a Consolidated Software-Defined Data Center



This chapter includes the following topics:

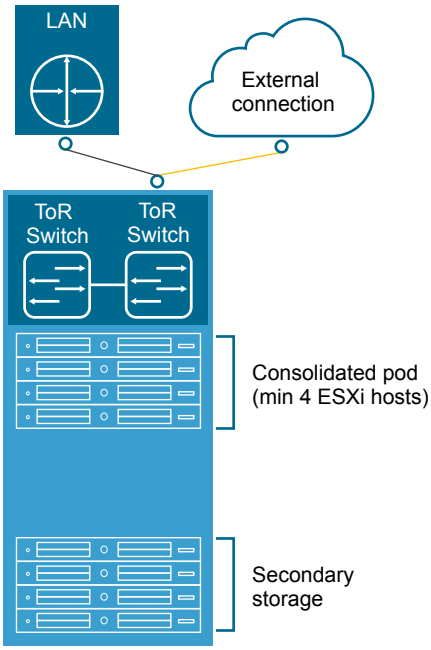
- "Physical Infrastructure Layer in Consolidated SDDC," on page 39
- "Virtual Infrastructure Layer in Consolidated SDDC," on page 41
- "Cloud Management Layer in Consolidated SDDC," on page 44
- "Operations Management Layer in Consolidated SDDC," on page 45

Physical Infrastructure Layer in Consolidated SDDC

The physical layer in Consolidated SDDC contains the compute, storage, and network resources in your data center.

The compute, storage and network resources are organized in pods. The physical layer also includes the physical network infrastructure, and storage setup.

Figure 7-2. Physical Configuration of the Consolidated SDDC



Pods

At the physical layer, a pod is a logical grouping of hardware that supports a certain function and is easy to replicate. Pods can have different configurations of server, storage, and network equipment. In large environments, each pod spans one rack, but in smaller environments you can aggregate multiple pods into a single rack.

This VMware Validated Design uses the following types of pods:

Consolidated Pod

The consolidated pod runs the following services:

- Virtual machines to manage the SDDC such as vCenter Server, NSX Manager, vRealize Automation, vRealize Log Insight, vRealize Operations Manager and vSphere Data Protection.
- Required NSX services to enable north-south routing between the SDDC and the external network, and east-west routing inside the SDDC.
- Virtual machines running business applications that support varying Service Level Agreements (SLAs).

Storage Pod

Storage pods provide secondary storage using NFS, iSCSI or Fibre Channel. Different types of storage pods can provide different levels of SLA, ranging from just a bunch of disks (JBODs) with minimal to no redundancy, to fully redundant enterprise-class storage arrays. For bandwidth-intense IP-based storage, the bandwidth of these pods can scale dynamically.

Network

This VMware Validated Design uses a Layer 3 leaf-and-spine network architecture.

- A leaf switch is typically located inside a rack and provides network access to the servers inside that rack. Leaf switches are also called Top of Rack (ToR) switches.

- A spine switch is in the spine layer and provides connectivity between racks. Links between spine switches are typically not required. If a link failure between a spine switch and a leaf switch occurs, the routing protocol ensures that no traffic is sent to the spine switch that has lost connectivity.

Regions and Availability Zones

Region

Each region is a separate SDDC instance with one or more availability zones. You use multiple regions for disaster recovery across individual SDDC instances.

This VMware Validated Design uses a single region.

Table 7-1. Regions in Consolidated SDDC

Region	Region-Specific Domain Name
Region A	sfo01.rainpole.local

Availability zone

Represent the fault domain of the SDDC. Multiple availability zones can provide continuous availability of an SDDC. This VMware Validated Design supports one availability.

Storage

This VMware Validated Design provides guidance about the storage of the management components. The design uses two storage technologies:

Primary Storage

vSAN storage is the default storage type for the SDDC management components. All design, deployment and operational guidance are performed on vSAN.

The storage devices on vSAN ready servers provide the storage infrastructure. Because this VMware Validated Design uses vSAN in hybrid mode, each rack server must have minimum one SSD and two HDD devices that form a disk group with capacity.

Secondary Storage

NFS storage is the secondary storage for the SDDC management components. It provides space for workload backup, archiving log data and application templates.

Virtual Infrastructure Layer in Consolidated SDDC

The virtual infrastructure layer of the Consolidated SDDC contains the components that provide compute, networking, and storage resources to the management and tenant workloads.

vCenter Server Design

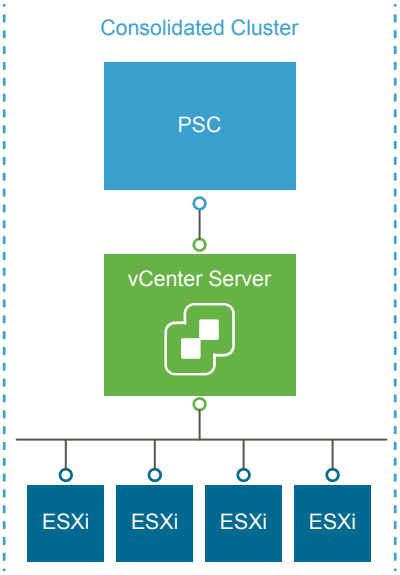
Table 7-2. vCenter Server Design Details in Consolidated SDDC

Design Area	Description
vCenter Server instances	You deploy a single vCenter Server instance that supports both the SDDC management components, and the tenant workloads and connecting edge components.
Clusters	You place hosts and workloads in a consolidated cluster. The cluster contains the management virtual machines, NSX controllers and edges, and tenant workloads.

Table 7-2. vCenter Server Design Details in Consolidated SDDC (Continued)

Design Area	Description
Resource pools for management components, tenant workloads and dedicated NSX components	On the consolidated cluster, you use resource pools to distribute compute and storage resources between the management components, and the tenant workloads and NSX components carrying their traffic. The Consolidated SDDC uses resource pools for the following components: ■ Management virtual machines ■ NSX Edge devices for the management components ■ NSX Edge devices for the tenant workloads ■ Tenant workloads
Deployment model	This VMware Validated Design uses a vCenter Server instance and a connected external Platform Services Controller instance .
Management host provisioning	You use a host profile to apply the networking and authentication configuration on the ESXi hosts in the consolidated pod.

Figure 7-3. Layout of Consolidated Cluster in Consolidated SDDC



Dynamic Routing and Application Virtual Networks

This VMware Validated Design supports dynamic routing for both management and tenant workloads, and also introduces a model of isolated application networks for the management components.

Dynamic routing support includes the following nodes:

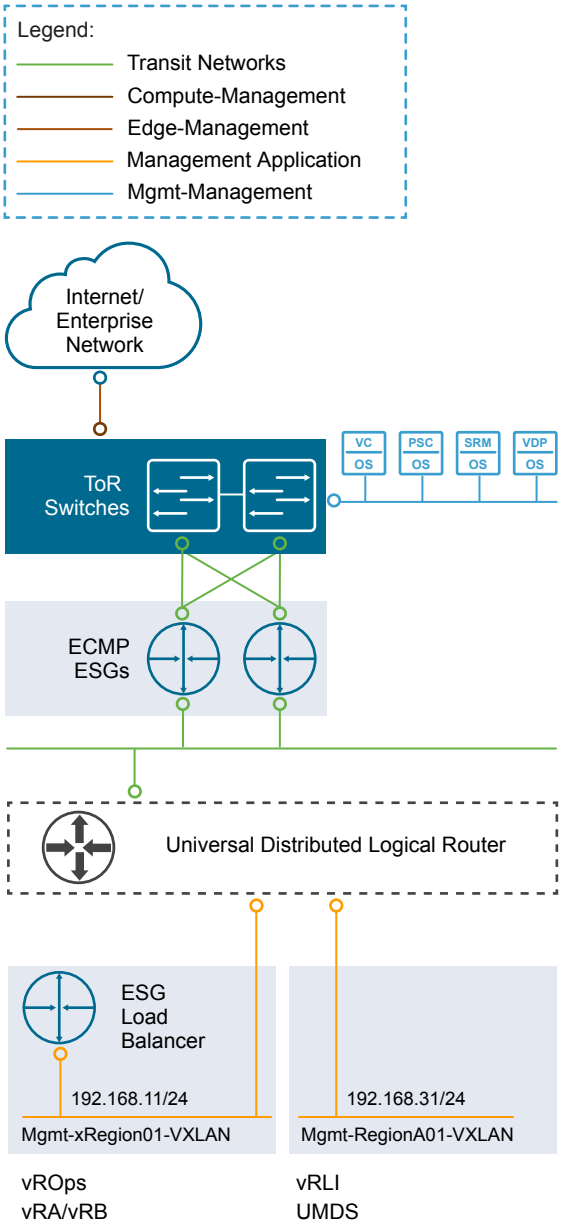
- Pair of NSX Edge service gateways (ESGs) with ECMP enabled for north/south routing across all regions.
- Universal distributed logical router (UDLR) for east/west routing between applications and to a potential second region.

Application virtual networks provide support for limited access to the nodes of the applications through published access points. Three application virtual networks exist:

- Cross-region application virtual network that connects the components that are designed to fail over to a recovery region if the SDDC is scaled out to a dual-region configuration.

- Region-specific application virtual network in Region A for components that are not designed to fail over.

Figure 7-4. Virtual Application Network Components and Design in Consolidated SDDC



Distributed Firewall

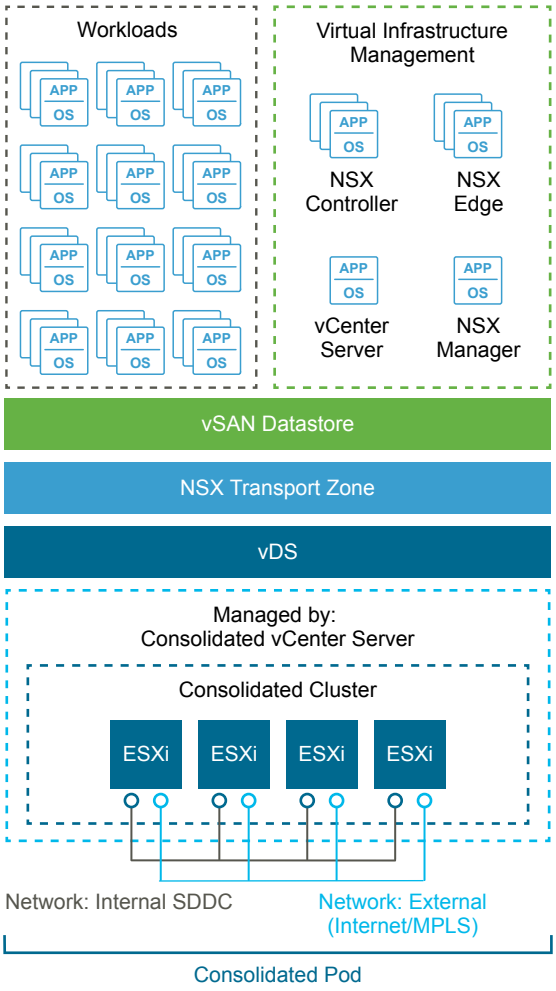
This VMware Validated Design uses the distributed firewall functionality that is available in NSX to protect all management applications attached to application virtual networks.

Software-Defined Storage Design for Management Products

Workloads store their data on a vSAN datastore. The vSAN datastore spans all 4 ESXi hosts of the consolidated cluster. Each host adds one disk group to the datastore.

Applications store their data according to the default storage policy for vSAN.

Figure 7-5. vSAN Conceptual Design in Consolidated SDDC



vSphere Data Protection and vRealize Log Insight use NFS exports as secondary storage. You create one datastore for vSphere Data Protection.

Cloud Management Layer in Consolidated SDDC

The cloud management layer in the Consolidated SDDC enables you to deliver tenants with automated workload provisioning by using a self-service portal.

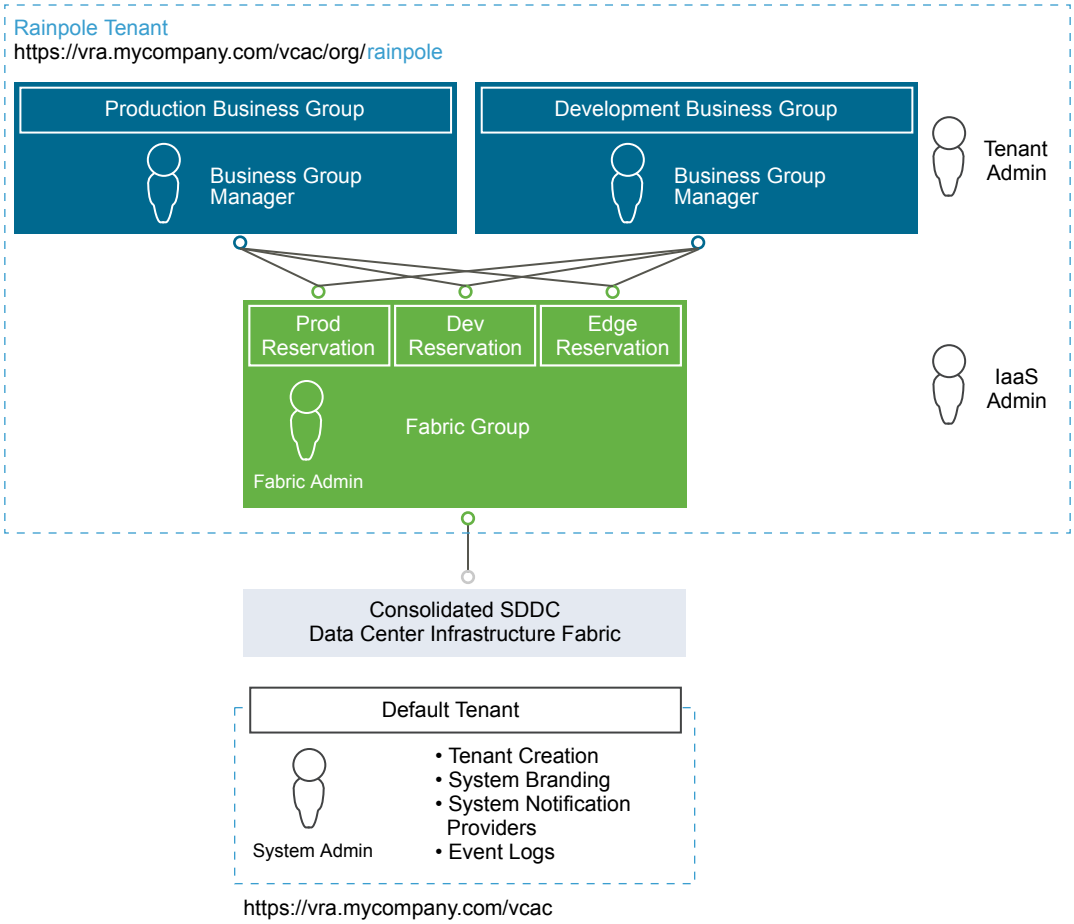
Table 7-3. Cloud Management Design Details in Consolidated SDDC

Design Attribute	Description
Software components	■ vRealize Automation ■ Embedded vRealize Orchestrator ■ vRealize Business
Deployment model of vRealize Automation	Distributed deployment with support for vSphere endpoints by using vSphere Proxy Agent virtual machines. You install the vRealize Automation components on multiple machines.
High availability and load balancing	Disabled
Endpoints	■ vCenter Server for the consolidated cluster ■ NSX Manager for the consolidated cluster

Table 7-3. Cloud Management Design Details in Consolidated SDDC (Continued)

Design Attribute	Description
Blueprint configuration	Single-machine blueprints
Tenants	A single tenant company called Rainpole
Fabric groups	One fabric group with all resources in the consolidated cluster assigned
Business groups	According to the internal structure and workload configuration of your organization. Allocate business groups for separate business units, for example, for development and production.

Figure 7-6. Example vRealize Automation Tenant Design



Operations Management Layer in Consolidated SDDC

The operations layer of the Consolidated SDDC provides capabilities for performance and capacity monitoring, and for backup and restore of the cloud management components.

vRealize Operations Manager

You use vRealize Operations Manager to monitor the management components of the SDDC including vSphere, NSX for vSphere and vRealize Automation.

vRealize Operations Manager is also sized to accommodate the number of tenant workloads per the design objectives.

Figure 7-7. vRealize Operations Manager Logical Design in Consolidated SDDC

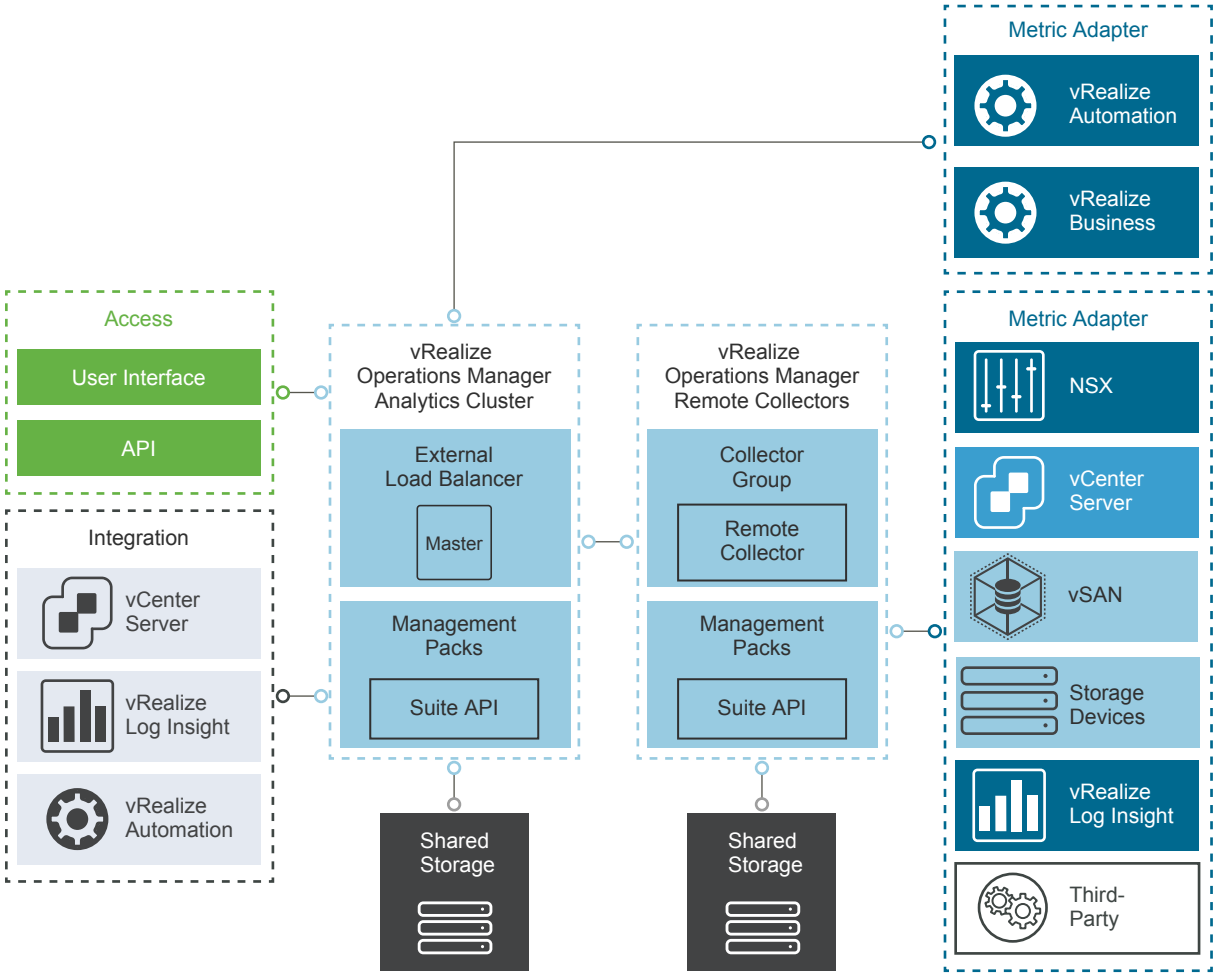


Table 7-4. vRealize Operations Manager Design Details in Consolidated SDDC

Design Attribute	Description
Deployment model	■ Analytics cluster of 1 node: master ■ Remote collector group that consists of one remote collector that communicates with the management components in the single region
Monitored components	■ vCenter Server and Platform Services Controller ■ ESXi hosts in the consolidated cluster ■ All components of NSX for vSphere for the consolidated cluster ■ vRealize Automation and vRealize Orchestrator ■ vRealize Log Insight including Launch in Context ■ vRealize Business including integration in the vRealize Operations Manager operations interface ■ vSAN ■ vRealize Operations Manager (self-health monitoring)

vRealize Log Insight

You use vRealize Log Insight to access the logs of the SDDC management components from a central place and view this information in visual dashboards.

Figure 7-8. vRealize Log Insight Logical Design in Consolidated SDDC

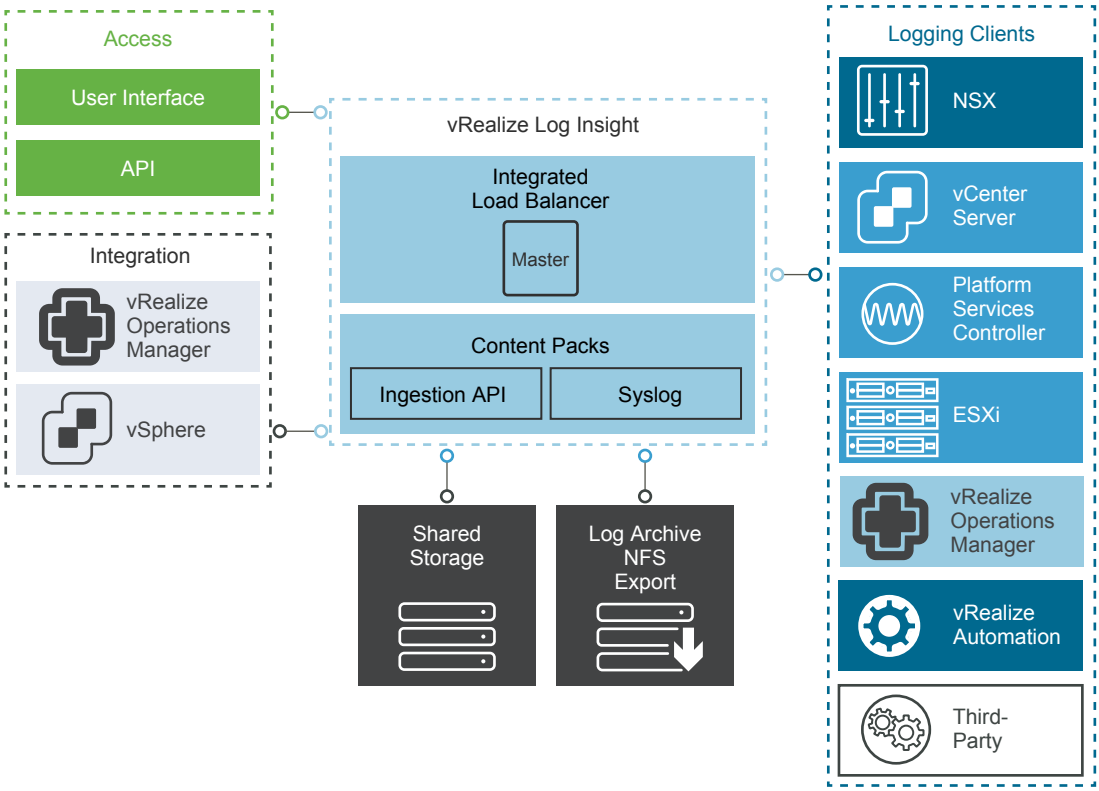


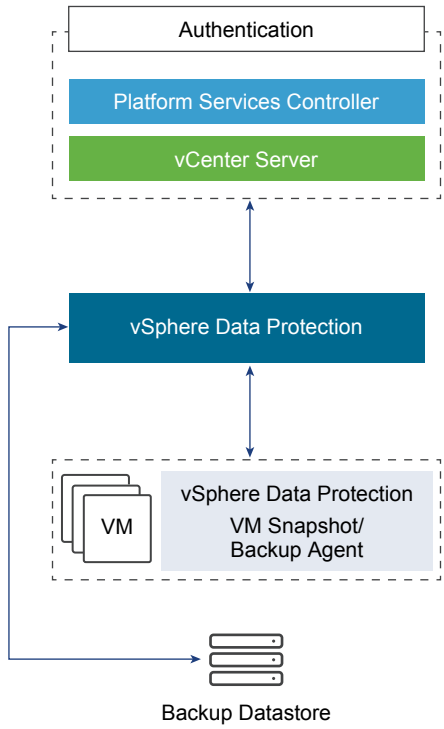
Table 7-5. vRealize Log Insight Design Details in Consolidated SDDC

Design Attribute	Description
Deployment model	Cluster of a master node.
Monitored components	■ vCenter Server and Platform Services Controller ■ ESXi hosts in the consolidated cluster ■ All components of NSX for vSphere for the consolidated cluster ■ vRealize Automation and vRealize Orchestrator ■ vRealize Business ■ Analytics cluster nodes of vRealize Operations Manager ■ Management virtual appliances
Archiving	Archiving location on an NFS export

vSphere Data Protection

You deploy vSphere Data Protection to back up the virtual machines of the SDDC management components. vSphere Data Protection stores its data and the backup copies of virtual machines on the NFS datastore in the consolidated cluster.

Figure 7-9. vSphere Data Protection Design

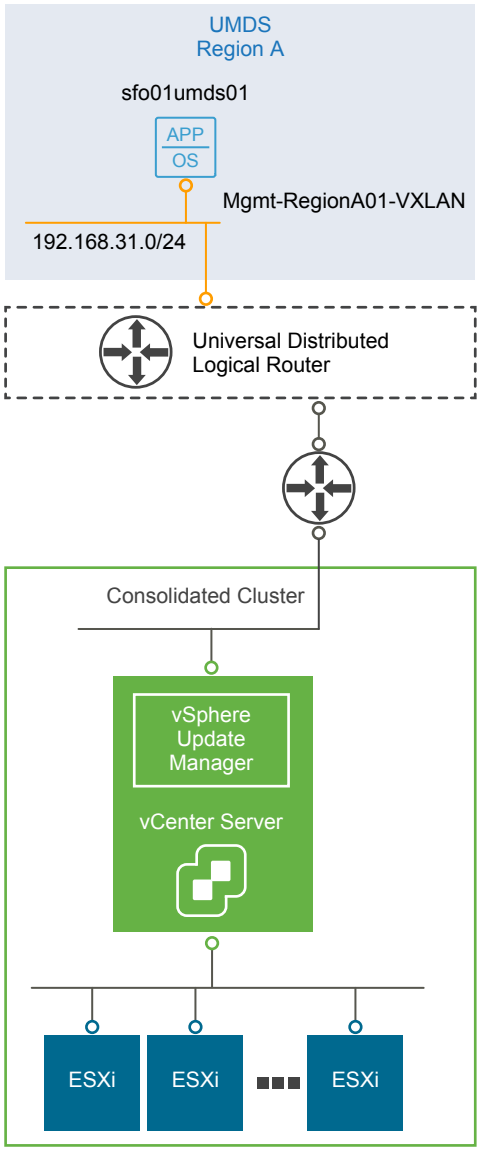


vSphere Update Manager

This VMware Validated Design version uses vSphere Update Manager for upgrade of the ESXi hosts from previous VMware Validated Design versions.

vSphere Update Manager server and client components are a part of vCenter Server Appliance in vSphere 6.5 or later. This design also deploys an instance of vSphere Update Manager Download Service (UMDS). Using a region-specific UMDS instance restricts the direct access to the external network from multiple vSphere Update Manager and vCenter Server instances, and reduces storage requirements across vSphere Update Manager.

Figure 7-10. vSphere Update Manager Design in Consolidated SDDC



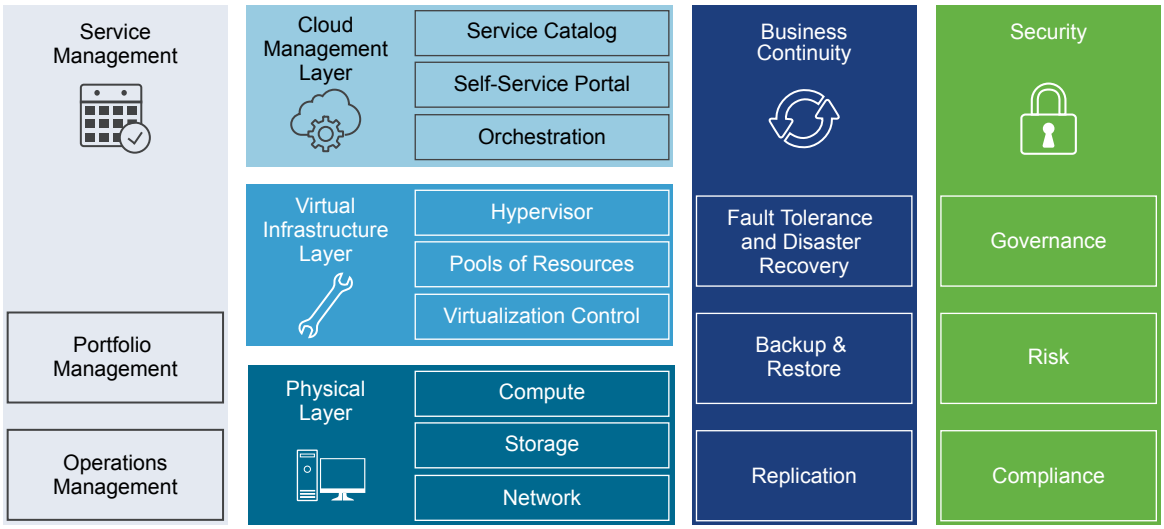
Overview of ROBO SDDC

8

The SDDC architecture in this VMware Validated Design consists of layers. The layered structure enables you to create the SDDC in modules and to handle each set of components separately.

For information about the design and deployment of each layer, see *VMware Validated Design Architecture and Design* and *VMware Validated Design Deployment*.

Figure 8-1. Components of a ROBO SDDC



This chapter includes the following topics:

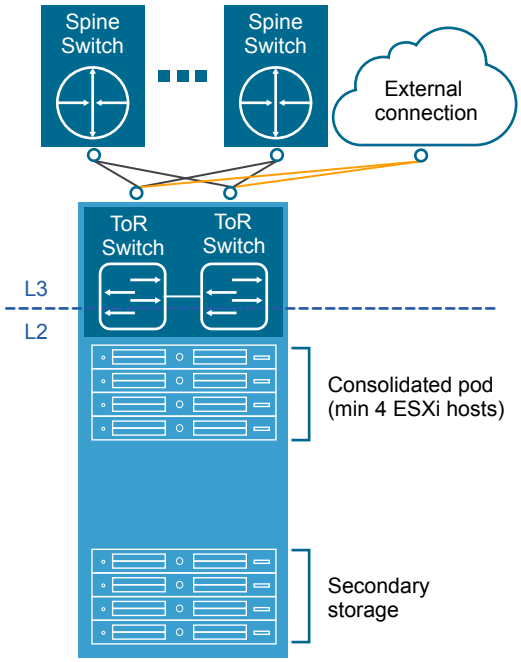
- "Physical Infrastructure Layer in ROBO SDDC," on page 51
- "Virtual Infrastructure Layer in ROBO SDDC," on page 54
- "Cloud Management Layer in ROBO SDDC," on page 58
- "Operations Management Layer in ROBO SDDC," on page 59

Physical Infrastructure Layer in ROBO SDDC

The physical layer in ROBO SDDC contains the compute, storage, and network resources in your data center.

The compute, storage and network resources are organized in pods. The physical layer also includes the physical network infrastructure, and storage setup.

Figure 8-2. Physical Configuration of the Consolidated SDDC



Pods

At the physical layer, a pod is a logical grouping of hardware that supports a certain function and is easy to replicate. Pods can have different configurations of server, storage, and network equipment. In large environments, each pod spans one rack, but in smaller environments you can aggregate multiple pods into a single rack.

This VMware Validated Design uses the following types of pods:

Consolidated Pod

The consolidated pod runs the following services:

- Virtual machines to manage the SDDC such as vCenter Server, NSX Manager, vRealize Automation, vRealize Log Insight, vRealize Operations Manager and vSphere Data Protection.
- Required NSX services to enable north-south routing between the SDDC and the external network, and east-west routing inside the SDDC.
- Virtual machines running business applications that support varying Service Level Agreements (SLAs).

Storage Pod

Storage pods provide secondary storage using NFS, iSCSI or Fibre Channel. Different types of storage pods can provide different levels of SLA, ranging from just a bunch of disks (JBODs) with minimal to no redundancy, to fully redundant enterprise-class storage arrays. For bandwidth-intense IP-based storage, the bandwidth of these pods can scale dynamically.

Network

This VMware Validated Design uses a Layer 3 leaf-and-spine network architecture.

- A leaf switch is typically located inside a rack and provides network access to the servers inside that rack. Leaf switches are also called Top of Rack (ToR) switches.

- A spine switch is in the spine layer and provides connectivity between racks. Links between spine switches are typically not required. If a link failure between a spine switch and a leaf switch occurs, the routing protocol ensures that no traffic is sent to the spine switch that has lost connectivity.

Regions, Hubs and ROBO Sites

Hub

A hub is the centralized provisioning and monitoring components of the SDDC. A hub can be dedicated to ROBO sites (depending on the number of remote office connections required) or a part of the VMware Validated Design for Software-Defined Data Center. In either case, the hub has the capability for fail over between regions in the event of a disaster.

Region

Each region is a separate SDDC instance and can contain one or more availability zones. This VMware Validated Design uses two example regions in the hub: one in San Francisco (SFO) and the other in Los Angeles (LAX).

Table 8-1. Regions in VMware Validated Design for Remote Office and Branch Office

Region	Disaster Recovery Role	Region-Specific Domain Name
Region A	Protected	sfo01.rainpole.local
Region B	Recovery	lax01.rainpole.local

Availability zone

Represent the fault domain of the SDDC. Multiple availability zones can provide continuous availability of an SDDC. This VMware Validated Design supports one availability zone in each region in the hub.

ROBO Site

A ROBO site is a location that you use to support specific services such as manufacturing, hospitals, or call centers. These locations require minimal workload deployment and have hardware located in space constrained rooms.

Table 8-2. Sites in VMware Validated Design for Remote Office and Branch Office

Site Identifier	Description
NYC01	New York City, NY, USA based Remote Office and Branch Office

Storage

This VMware Validated Design provides guidance about the storage of the management components. The design uses two storage technologies:

Primary Storage

vSAN storage is the default storage type for the SDDC management components. All design, deployment and operational guidance are performed on vSAN.

The storage devices on vSAN ready servers provide the storage infrastructure. Because this VMware Validated Design uses vSAN in hybrid mode, each rack server must have minimum one SSD and two HDD devices that form a disk group with capacity.

Secondary Storage

NFS storage is the secondary storage for the SDDC management components. It provides space for workload backup, archiving log data and application templates.

Virtual Infrastructure Layer in ROBO SDDC

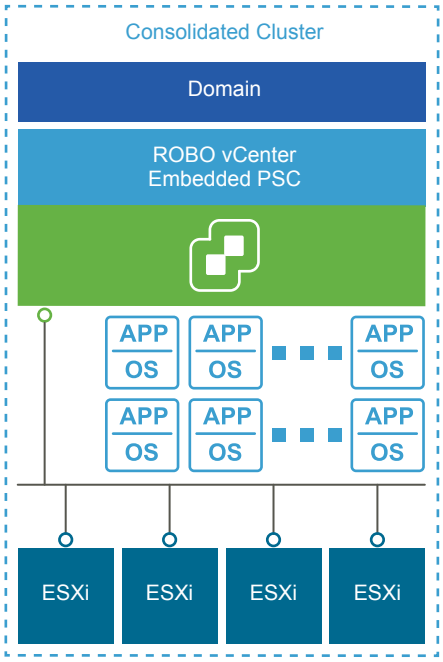
The virtual infrastructure layer of the ROBO SDDC contains the components that provide compute, networking, and storage resources to the management and tenant workloads in the remote office.

vCenter Server Design

Table 8-3. vCenter Server Design Details in ROBO SDDC

Design Area	Description
vCenter Server instances	You deploy a single vCenter Server that supports both the SDDC management components.
Clusters	You place hosts and workloads in a consolidated cluster. The cluster contains the management virtual machines, NSX controllers and edges, and tenant workloads.
Resource pools for tenant workloads and dedicated NSX components	On the consolidated cluster, you use resource pools to distribute compute and storage resources between the management components, and the tenant workloads and NSX components carrying their traffic. The Consolidated SDDC uses resource pools for the following components: ■ Management virtual machines ■ NSX Edge devices for the management components ■ NSX Edge devices for the tenant workloads ■ Tenant workloads
Deployment model	This VMware Validated Design uses a vCenter Server instance with an embedded Platform Services Controller instance.
Management host provisioning	You use a host profile to apply the networking and authentication configuration on the ESXi hosts in the consolidated pod.

Figure 8-3. Layout of vCenter Server Consolidated Cluster in ROBO SDDC



Dynamic Routing and Application Virtual Networks

This VMware Validated Design supports dynamic routing for both management and tenant workloads, and also introduces a model of isolated application networks for the management components.

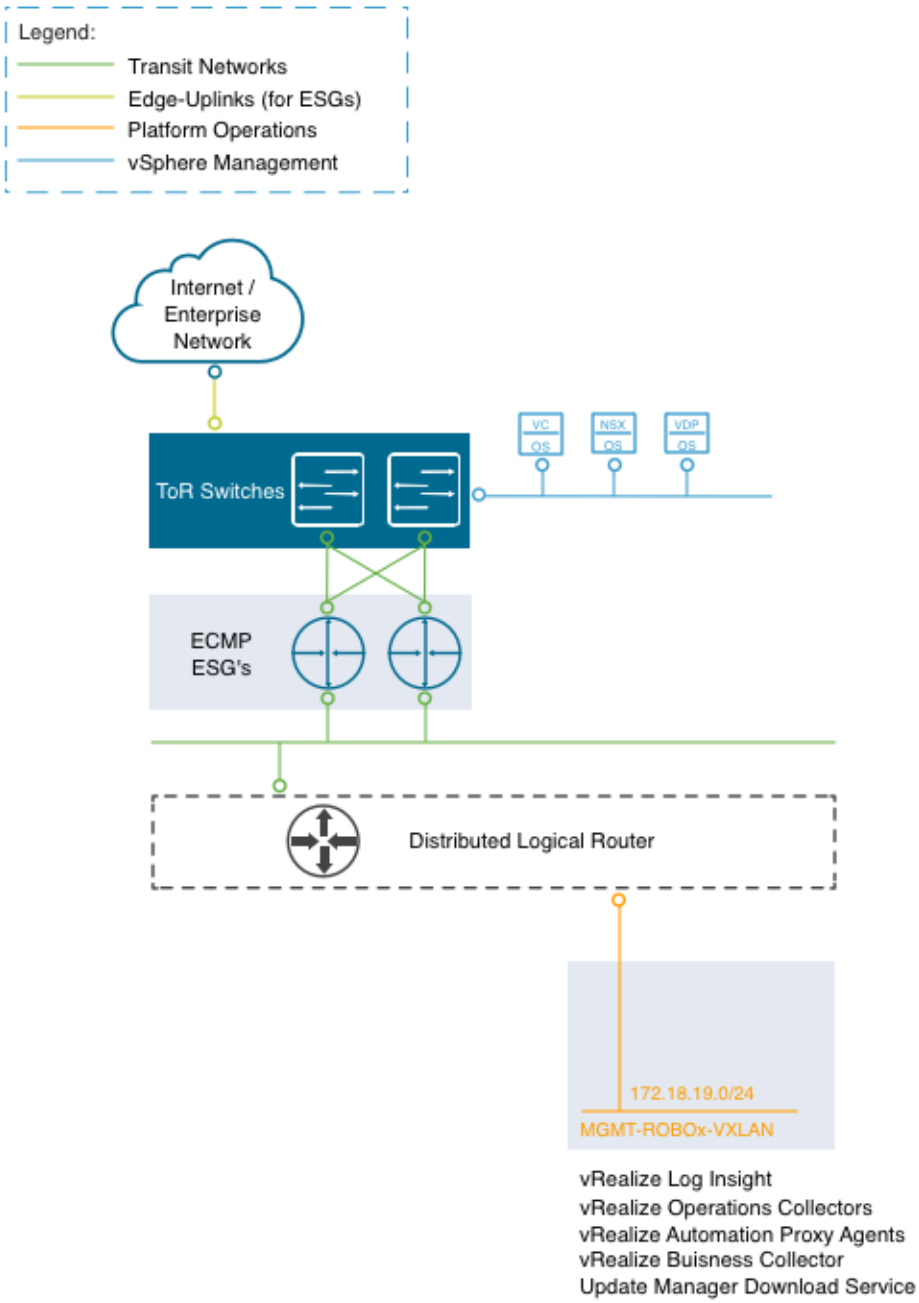
Dynamic routing support includes the following nodes:

- Pair of NSX Edge service gateways (ESGs) with ECMP enabled for north/south routing across all regions.
- Distributed logical router (DLR) for tenant internal network.

Application virtual networks provide support for limited access to the nodes of the applications through published access points. One application virtual networks exists:

- Application virtual network in each site for components that are not designed to fail over.

Figure 8-4. Virtual Application Network Components and Design in ROBO SDDC



Distributed Firewall

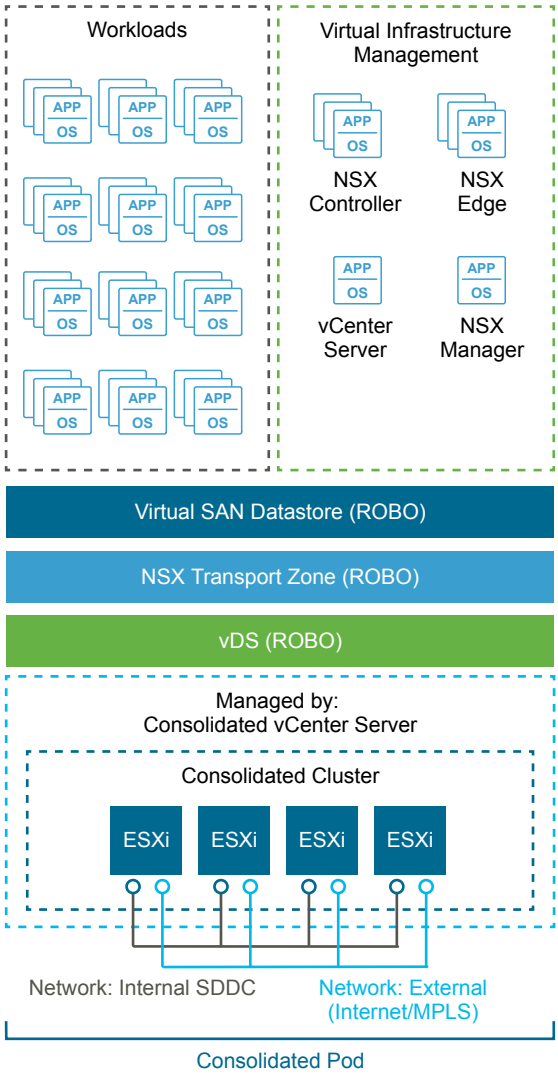
This VMware Validated Design uses the distributed firewall functionality that is available in NSX to protect all management applications attached to application virtual networks.

Software-Defined Storage Design for Management Products

Workloads store their data on a vSAN datastore. The vSAN datastore spans all 4 ESXi hosts of the consolidated cluster. Each host adds one disk group to the datastore.

Applications store their data according to the default storage policy for vSAN.

Figure 8-5. vSAN Conceptual Design in ROBO SDDC



vSphere Data Protection and vRealize Log Insight use NFS exports as secondary storage. You create one datastore for vSphere Data Protection.

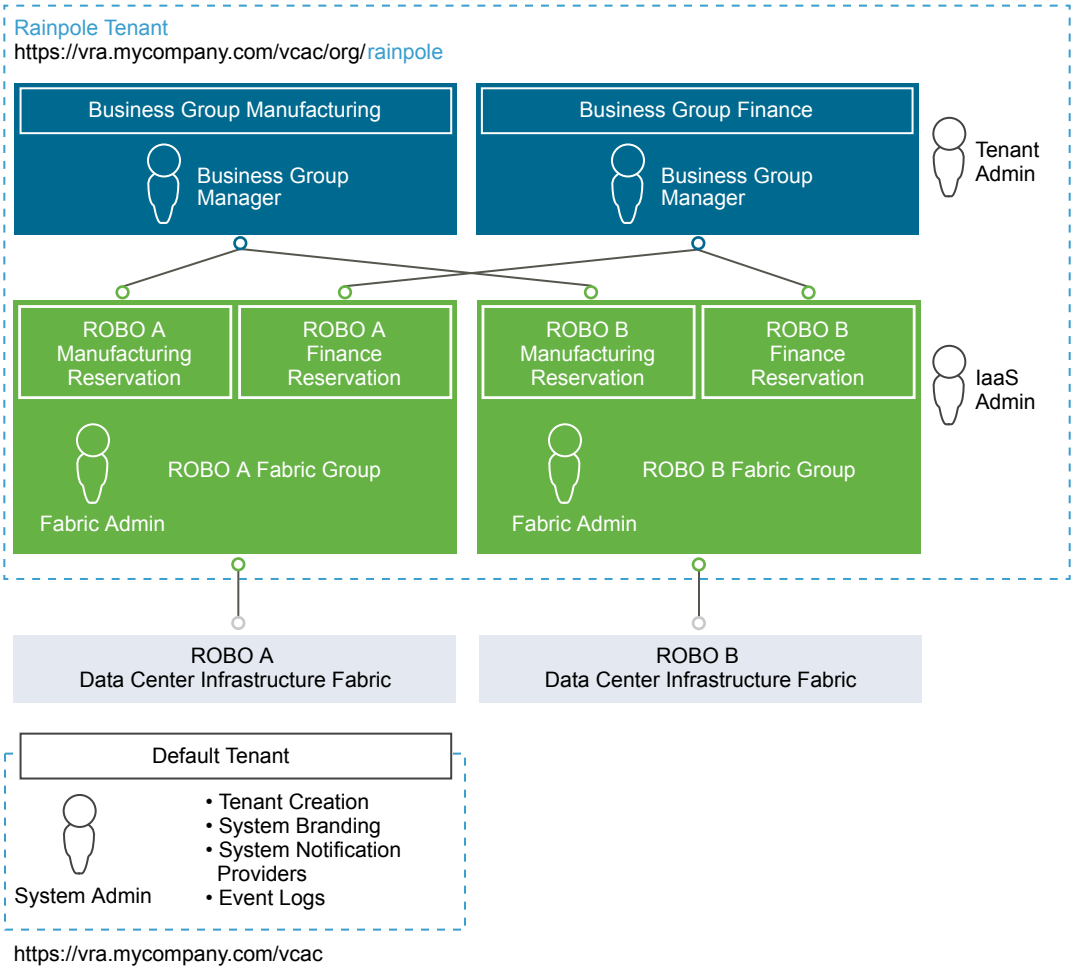
Cloud Management Layer in ROBO SDDC

The cloud management layer in the ROBO SDDC enables you to deliver tenants with automated workload provisioning by using a self-service portal.

Table 8-4. Cloud Management Design Details in ROBO SDDC

Design Attribute	Description
Software components in the hub	■ vRealize Automation ■ vRealize Orchestrator ■ vRealize Business
Deployment model of vRealize Automation and vRealize Business in the ROBO site	Distributed deployment with support for vSphere endpoints by using vSphere Proxy Agent virtual machines in the ROBO sites. You install the vRealize Automation components on multiple machines. The site contains a vRealize Business data collector. The data collector sends cost data back to the vRealize Business server in the hub.
High availability and load balancing	The vSphere Proxy Agents in each site are highly-available.
Endpoints	■ vCenter Server for the consolidated cluster in the site ■ NSX Manager for the consolidated cluster in the site
Blueprint configuration	Single-machine blueprints
Tenants	A single tenant company called Rainpole
Fabric groups	One fabric group with all resources in the consolidated cluster assigned
Business groups	According to the internal structure and workload configuration of your organization. Allocate business groups for separate business units, for example, for development and production.

Figure 8-6. Example vRealize Automation Tenant Design in ROBO SDDC



Operations Management Layer in ROBO SDDC

The operations layer of the ROBO SDDC provides capabilities for performance and capacity monitoring, and for backup and restore of the cloud management components.

vRealize Operations Manager

You use vRealize Operations Manager to monitor the management components of the SDDC including vSphere, NSX for vSphere, and vRealize Automation.

vRealize Operations Manager is also sized to accommodate the number of tenant workloads per the design objectives.

Figure 8-7. vRealize Operations Manager Logical Design in ROBO SDDC

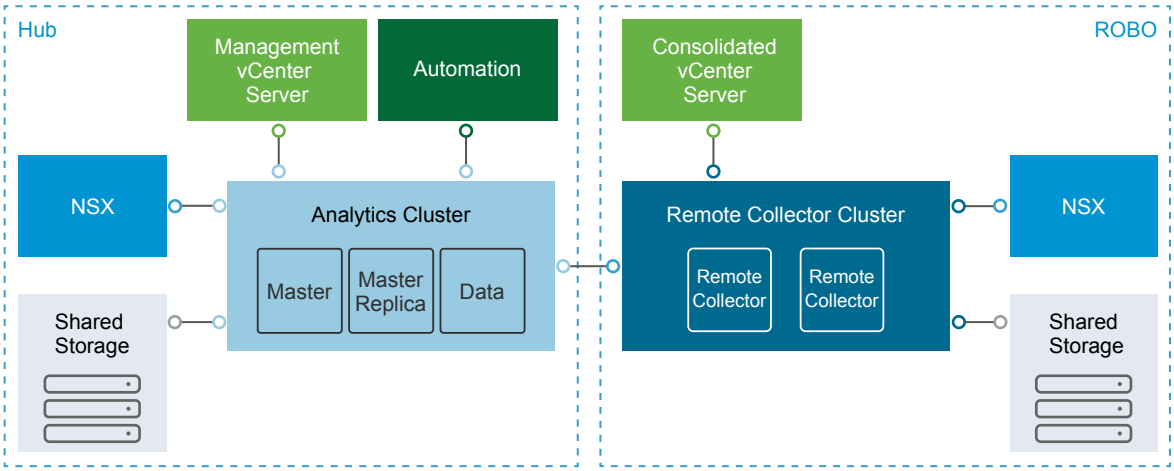


Table 8-5. vRealize Operations Manager Design Details in ROBO SDDC

Design Attribute	Description
Deployment model	■ Analytics cluster of 3 nodes in the hub: master, master replica and data nodes ■ Remote collector group that consists of two remote collectors in each ROBO site
Monitored components from the ROBO site	■ vCenter Server and Platform Services Controller ■ ESXi hosts in the consolidated cluster ■ All components of NSX for vSphere for the consolidated cluster ■ vSphere Proxy Agents in vRealize Automation ■ vRealize Log Insight including Launch in Context

vRealize Log Insight

You use vRealize Log Insight to access the logs of the SDDC management components from a central place and view this information in visual dashboards.

Figure 8-8. vRealize Log Insight Logical Design in ROBO SDDC

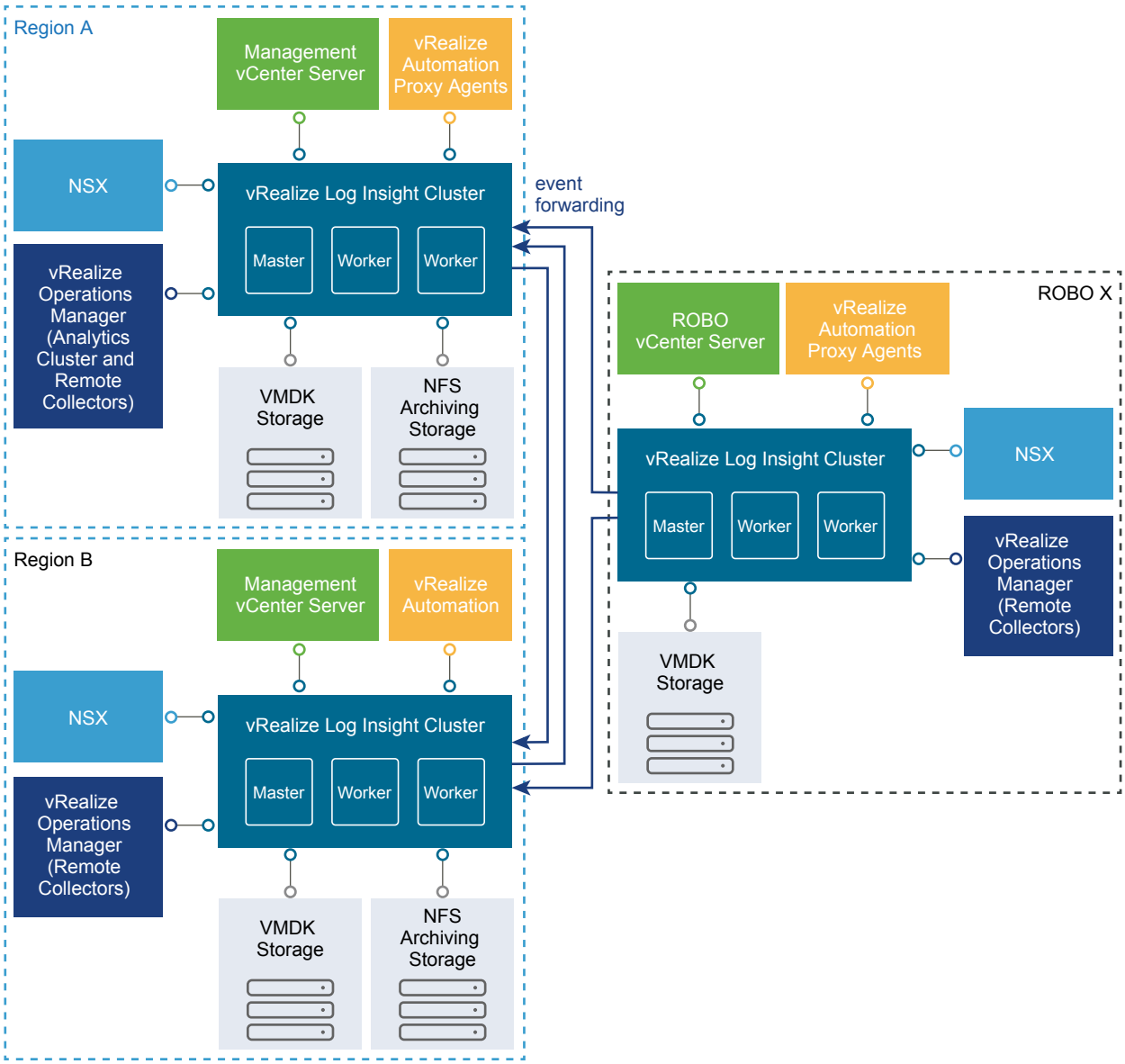


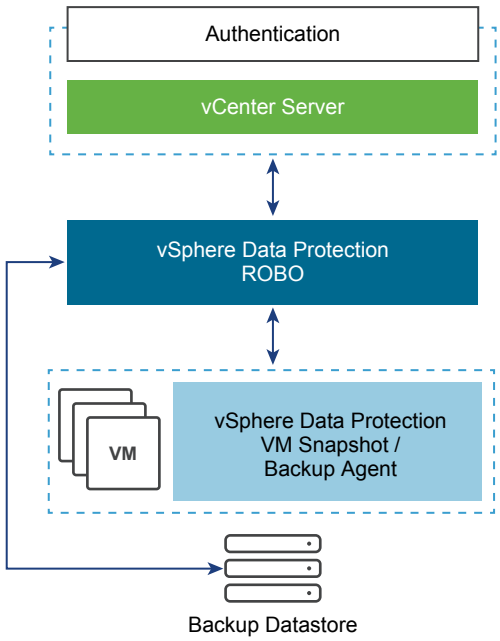
Table 8-6. vRealize Log Insight Design Details in ROBO SDDC

Design Attribute	Description
Deployment model	Cluster of 3 node: one master and two worker nodes.
Monitored components from the ROBO site	■ vCenter Server and Platform Services Controller ■ ESXi hosts in the consolidated cluster ■ All components of NSX for vSphere for the consolidated cluster ■ vSphere Proxy Agents in vRealize Automation ■ Remote collectors in vRealize Operations Manager
Archiving	Archiving location on an NFS export

vSphere Data Protection

You deploy vSphere Data Protection to back up the virtual machines of the SDDC management components. vSphere Data Protection stores its data and the backup copies of virtual machines on the NFS datastore in the consolidated cluster.

Figure 8-9. vSphere Data Protection Design in ROBO SDDC

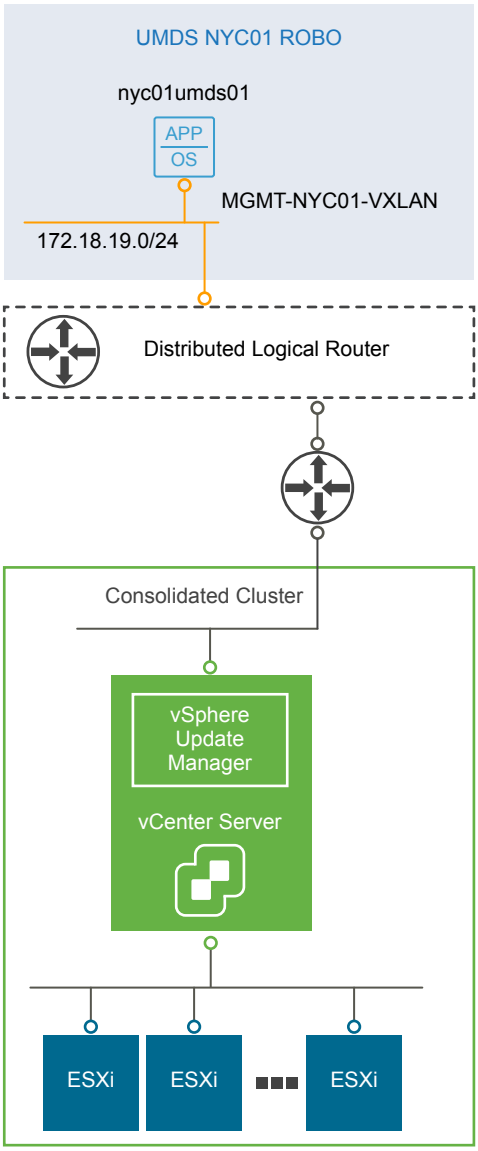


vSphere Update Manager

This VMware Validated Design version uses vSphere Update Manager for upgrade of the ESXi hosts from previous VMware Validated Design versions.

vSphere Update Manager server and client components are a part of vCenter Server Appliance in vSphere 6.5 or later. This design also deploys an instance of vSphere Update Manager Download Service (UMDS). Using a region-specific UMDS instance restricts the direct access to the external network from multiple vSphere Update Manager and vCenter Server instances, and reduces storage requirements across vSphere Update Manager.

Figure 8-10. vSphere Update Manager Design in ROBO SDDC



Index