# vRealize Suite Overview

vRealize Suite 2019

vmware®

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

https://docs.vmware.com/

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

# Contents

Introducing VMware vRealize Suite 4

1 Introduction to vRealize Suite 5
- vRealize Suite Capabilities 5
- vRealize Suite Editions and Products 6
- vRealize Suite Licensing 9

2 vRealize Suite Architecture Overview 11
- Software Defined Data Center 11
- Conceptual Design of a vRealize Suite Environment 13
- vRealize Suite Products in the Management Cluster 15
- SDDC Core Infrastructure 16
  - Virtualization and Management of vRealize Suite Infrastructure 17
  - Manage vRealize Suite Core Infrastructure 21
  - Monitoring vRealize Suite Core Infrastructure 22
  - Delivering an Infrastructure Service 23
  - Delivering Platform as a Service 24
- vRealize Suite Security Considerations 25
  - Authentication and Authorization in vRealize Suite 26
  - TLS and Data Protection 29
  - Securing the Physical Layer 30
  - Securing the Virtual Layers 34
  - Using VMware NSX to Secure Workloads 36

3 Checklist for Installing vRealize Suite 42

4 Upgrading from Older Versions of vRealize Suite or vCloud Suite 44

# Introducing VMware vRealize Suite

The *VMware vRealize Suite Overview* provides an architecture overview and information about installing, configuring, and using vRealize Suite.

To help you get started, high-level discussions of installation, configuration, and use direct you to the dedicated sets of individual products for detailed concepts and procedures.

## Intended Audience

This information is intended for anyone who wants to deploy and use the vRealize Suite of products to monitor and manage a software-defined data center (SDDC). This information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

# Introduction to vRealize Suite

1

vRealize Suite provides a comprehensive cloud management platform for application delivery, monitoring, and management across VMware vSphere® and other hypervisors, including physical infrastructure, and private and public clouds. vRealize Suite is available in standard, advanced, and enterprise editions.

This chapter includes the following topics:


- vRealize Suite Capabilities
- vRealize Suite Editions and Products
- vRealize Suite Licensing


## vRealize Suite Capabilities

Intelligent operations, automated IT, Infrastructure as a Service (IaaS), and DevOps-ready IT are the most common uses of a cloud management solution. Intelligent operations help deliver streamlined and automated data center operations. Automated IT, IaaS, and DevOps-ready IT enable application and infrastructure service delivery.

### Intelligent Operations Management

Intelligent operations proactively addresses health, performance, and capacity management of IT services across heterogeneous and hybrid cloud environments to improve IT service performance and availability.

### Automated IT to IaaS

Automated IT and IaaS automates the delivery and ongoing management of IT infrastructure to reduce response time to requests for IT resources and to improve the ongoing management of provisioned resources.

## DevOps-Ready IT

DevOps-ready IT helps you build a cloud solution for development teams that can deliver a complete application stack with these capabilities:

- Support developer choice in the form of API and GUI access to resources.
- Provision resources across a hybrid cloud.
- Extend the solution scope by addressing continuous delivery to further speed up application delivery.

# vRealize Suite Editions and Products

vRealize Suite is available in standard, advanced, and enterprise editions. A vRealize Suite edition contains individual products with different product editions and different capabilities.

The standard, advanced, and enterprise editions of vRealize Suite each provide a different set of features, outlined in the following table.

**Note** vRealize Business for Cloud was available as Standard and Advanced editions in vRealize Suite 2018. In vRealize Suite 2019, the hybrid cloud costing capabilities that include on-premises SDDC deployments and VMware Cloud on AWS, are now included in vRealize Operations, as Advanced and Enterprise editions. VMware announced the End of Availability (EOA) of VMware VMware Business for Cloud, effective January 29th, 2021. Hence, VMware Business for Cloud is no longer available for vRealize Suite 2019. For more information, refer to KB 81827.

Table 1-1. vRealize Suite Edition Capabilities

| vRealize Suite Product | vRealize Suite Capability | Standard Edition | Advanced Edition | Enterprise Edition |
|---|---|---|---|---|
| vRealize Operations Manager (includes vRealize Log Insight) | Log analysis | Yes | Yes | Yes |
| | Operations platform | Yes | Yes | Yes |
| | Visualization | Yes | Yes | Yes |
| | Policy management | Yes | Yes | Yes |
| | Performance monitoring and analytics | Yes | Yes | Yes |
| | Capacity management | Yes | Yes | Yes |
| | Workload balancing | Yes | Yes | Yes |
| | Change, configuration, and compliance management | Yes | Yes | Yes |
| | Application dependency mapping | Yes | Yes | Yes |
| | Application monitoring | No | No | Yes |

Table 1-1. vRealize Suite Edition Capabilities (continued)

| vRealize Suite Product | vRealize Suite Capability | Standard Edition | Advanced Edition | Enterprise Edition |
|---|---|---|---|---|
| vRealize Business for Cloud | Automatic virtual infrastructure metering, costing, and pricing | Yes | Yes | Yes |
| | Automatic service catalog pricing, integrated with vRealize Automation | Yes | Yes | Yes |
| | Virtual infrastructure consumption analysis | Yes | Yes | Yes |
| | Exportable data set that allows automatic reporting | Yes | Yes | Yes |
| | Public cloud and virtualization infrastructure cost comparison | Yes | Yes | Yes |
| | Public cloud costing, consumption analysis, and pricing | No | Yes | Yes |
| | Role-based showback in virtual infrastructure and public cloud | No | Yes | Yes |
| | Data center optimization, integrated with vRealize Operations Manager | No | Yes | Yes |
| | Quantifying virtual infrastructure reclamation opportunities, integrated with vRealize Operations Manager | No | Yes | Yes |
| | Custom reporting, visual charts, and API for automatic data extraction | No | Yes | Yes |
| vRealize Automation | Infrastructure as a Service | No | Yes | Yes |
| | Unified Service Catalog | No | Yes | Yes |
| | Self-service Provisioning | No | Yes | Yes |
| | Governance and Compliance Policies | No | Yes | Yes |
| | Resource lifecycle management (Day 2 Operations) | No | Yes | Yes |
| | Extensibility | No | Yes | Yes |
| | Xaas | No | Yes | Yes |
| | Hybrid Cloud (VMware Cloud on AWS) | No | Yes | Yes |
| | Mulit-Cloud capabilities, including cloud agnostics blueprints | No | No | Yes |
| | Code stream for DevOps | No | No | Yes |

Table 1-1. vRealize Suite Edition Capabilities (continued)

| vRealize Suite Product | vRealize Suite Capability | Standard Edition | Advanced Edition | Enterprise Edition |
|---|---|---|---|---|
| | Application provisioning and management | No | No | Yes |
| | Kubernetes Support | No | No | Yes |

## vRealize Suite Products

VMware vRealize Suite includes certain products or a subset of these products, depending on the vRealize Suite edition you purchase.

Table 1-2. Products Included with vRealize Suite

| Product Name | Description |
|---|---|
| vRealize Suite Lifecycle Manager | Automates Day 0 to Day 2 operations of the entire vRealize Suite, enabling a simplified operational experience. vRealize Suite Lifecycle Manager automates lifecycle management with a single pane of glass, freeing customer resources to focus on business-critical initiatives, while improving time to value, reliability, and consistency. |
| vRealize Operations Manager | Collects performance data from each object at every level of your virtual environment, from individual virtual machines and disk drives to entire clusters and data centers. It stores and analyzes the data, and uses that analysis to provide real-time information about problems, or potential problems, anywhere in your virtual environment. |
| vRealize Log Insight | Provides scalable log aggregation and indexing for vRealize Suite, including all editions of vSphere, with real-time search and analytics capabilities. Log Insight collects, imports, and analyzes logs to provide real-time answers to problems related to systems, services, and applications across physical, virtual, and cloud environments. |
| vRealize Automation | Helps deploy and provision business-relevant cloud services across private and public clouds, physical infrastructure, hypervisors, and public cloud providers. vRealize Automation Enterprise includes vRealize Automation Application Services. |
| vRealize Orchestrator | Simplifies the automation of complex IT tasks and integrates with vRealize Suite products to adapt and extend service delivery and operational management, effectively working with existing infrastructure, tools, and processes. |
| vRealize Business for Cloud | Provides information about financial aspects of your cloud infrastructure and lets you optimize and improve these operations. |

## vRealize Suite Editions and Their Product Editions

Certain product editions are available in the standard, advanced, and enterprise edition of vRealize Suite.

Table 1-3. vRealize Suite Software Product Editions in Suite Editions

| vRealize Product Edition | vRealize Suite Standard Edition | vRealize Suite Advanced Edition | vRealize Suite Enterprise Edition |
|---|---|---|---|
| VMware vRealize Automation Advanced Edition | No | Yes | No |
| VMware vRealize Automation Enterprise Edition | No | No | Yes |
| VMware vRealize Automation SaltStack Config | No | Yes | Yes |
| VMware vRealize Automation SaltStack SecOps | No | No | No |
| VMware vRealize Operations Management Suite (Advanced) | Yes | Yes | Yes |
| VMware vRealize Operations Management Suite Application Monitoring | No | No | Yes |
| VMware vRealize Business for Cloud Standard Edition | Yes | No | No |
| VMware vRealize Business for Cloud Advanced Edition | No | Yes | Yes |
| VMware vRealize Orchestrator | No | Yes | Yes |
| VMware vRealize Log Insight | Yes | Yes | Yes |

# vRealize Suite Licensing

You can license the products in vRealize Suite individually or as part of vRealize Suite 2017.

You obtain and use a license type to license vRealize Suite products.

Table 1-4. License Types Compatible with vRealize Suite Products

| License Type | License Capabilities |
|---|---|
| Individual product license | Some products are available as standalone products that you can license on a per-virtual machine basis by using the product license. Individual product licenses are intended for public cloud workloads or workloads on physical hardware. |
| vRealize Suite Portable License Unit (PLU) | With a Portable License Unit (PLU), you can provision and manage workloads across vSphere and hybrid environments, including public and private cloud providers. A PLU is a single SKU that meters workloads in vSphere and hybrid environments, and supports CPU and virtual machine metrics. Each PLU licenses one CPU for an unlimited number of virtual machines or 15 operating system instances. |

See VMware vRealize Suite and vCloud Suite Licensing, Pricing, and Packaging for details about PLUs.

# vRealize Suite Architecture Overview

2

The architecture describes how vRealize Suite products interact with each other and with systems in the data center to deliver a Software Defined Data Center (SDDC).

This chapter includes the following topics:


- Software Defined Data Center
- Conceptual Design of a vRealize Suite Environment
- vRealize Suite Products in the Management Cluster
- SDDC Core Infrastructure
- vRealize Suite Security Considerations

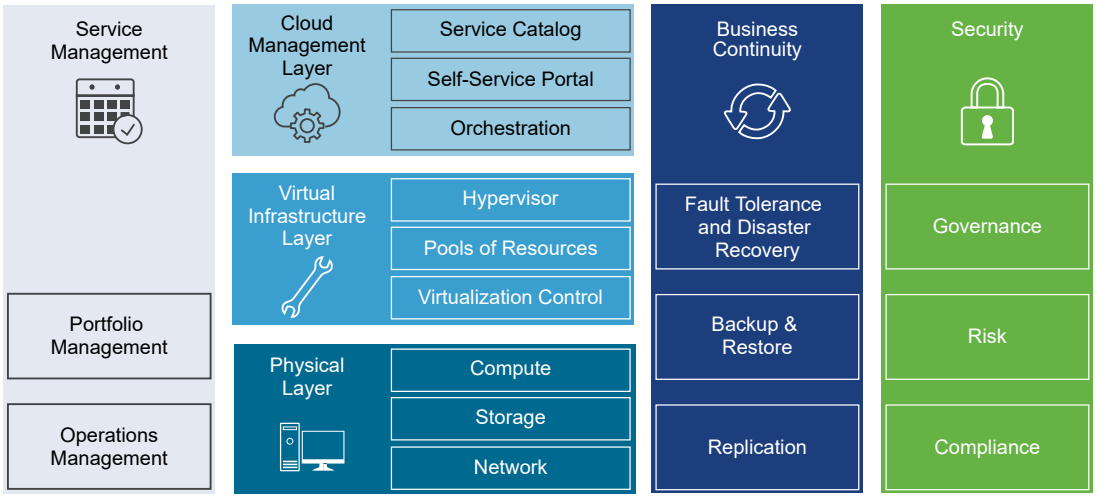

## Software Defined Data Center

The software-defined data center (SDDC) provides different types of capabilities, with more complex features building on the underlying infrastructure. To enable all vRealize Suite features, you must perform a series of installation and configuration operations.

Delivering the full operational capabilities of vRealize Suite to your organization or clients is a structured process. In a large organization, it might involve cycles of assessment, design, deployment, knowledge transfer, and solution validation. Depending on your organization, you should plan for an extended process that involves different roles.

Not every environment needs the full scope of vRealize Suite capabilities at a given time. Begin by deploying the core data center infrastructure, which enables you to add capabilities as your organization requires them. Each of the SDDC layers might require that you plan and perform a separate deployment process.

Figure 2-1. Layers of the SDDC




### Physical Layer

The lowest layer of the solution includes Compute, Network, and Storage components. The compute component contains the x86-based servers that run the management, edge, and tenant compute workloads . The storage components provide the physical foundation for the SDDC and the IT Automation Cloud.

### Virtual Infrastructure Layer

The virtual infrastructure layer includes the virtualization platform with the hypervisor, resource pooling, and virtualization control. VMware products in this layer are vSphere, VMware NSX, ESXi, and vCenter Server. These products establish a robust virtualized environment into which all other solutions integrate. Abstracting resources from the physical layer provides the foundation for the integration of VMware orchestration and monitoring solutions. Additional processes and technologies build on the infrastructure to enable Infrastructure as a Service (IaaS) and platform as a service (PaaS).

### Cloud Management Layer

The Cloud Management layer includes the service catalog, that houses the facilities to be deployed, orchestration, that provides the workflows to deploy catalog items, and the self-service portal that allows end users to use the SDDC. vRealize Automation provides the portal and the catalog, and embedded vRealize Orchestrator capabilities help manage workflows to automate complex IT processes.

### Service Management

Use service management to track and analyze the operation of multiple data sources in the multiregion SDDC. Deploy vRealize Operations Manager and vRealize Log Insight across multiple nodes for continued availability and increased log ingestion rates.

### Business Continuity

Use business continuity to create backup jobs in vSphere Data Protection for vRealize Operations Manager, vRealize Log Insight, VMware NSX, and vRealize Automation. If a hardware failure occurs, you can restore the components of these products from the saved backups.

**Security**

VMware delivers the Compliance Reference Architecture Framework and Compliance Capable, Audit Ready platform. Customers use the platform to meet demanding compliance requirements for virtualized workloads and to manage business risk. VMware products and compatible partner products are carefully mapped to meet requirements from authoritative sources such as PCI DSS, HIPAA, FedRAMP, and CJIS. The core Compliance Reference Architecture Framework documents are:

- Product Applicability Guides provide descriptions of VMware product suites on a product-by-product basis discussing regulation along with a mapping of the regulatory controls to product features.
- Architecture Design Guides provide considerations for building a secure, compliant, VMware vRealize environment that adheres to specific regulations.
- Validated Reference Architecture documents provide regulation evidence from an audit study that you can apply to your environment.

To access the documents, please navigate to VMware Market Place and select Compliance Solutions.

You can enhance your vRealize Suite environment by integrating additional VMware products and services. These products have capabilities such as disaster recovery to cloud, software-defined storage, and software-defined networking.

# Conceptual Design of a vRealize Suite Environment

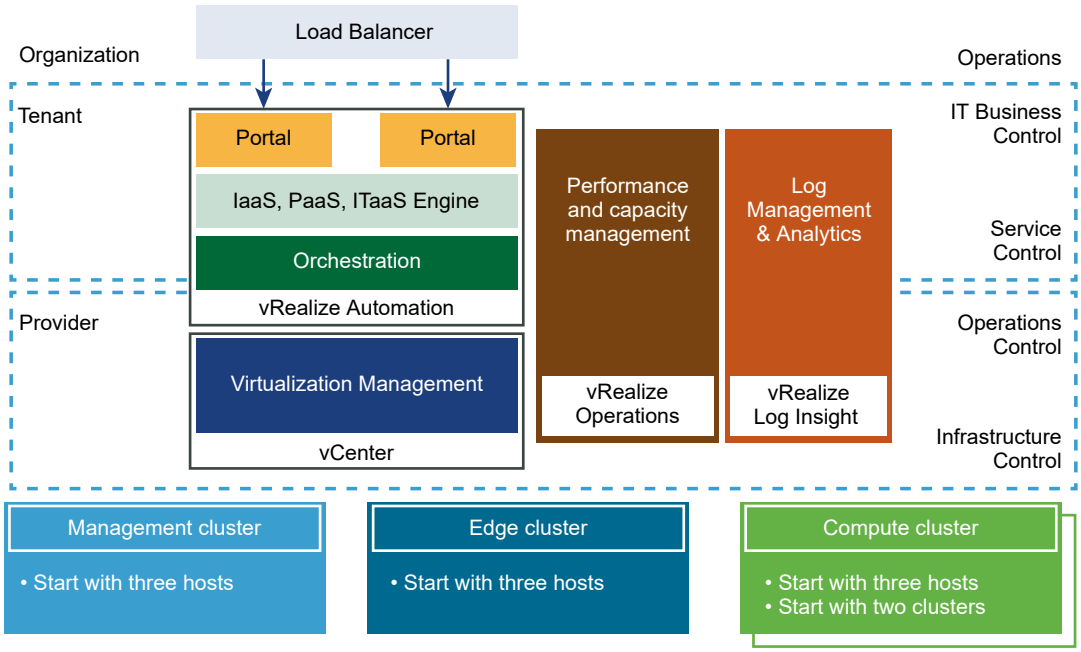
To start deploying vRealize Suite, you need only a small number of physical hosts. The best and most secure basis for scaling your environment is to distribute your hosts into management, edge, and payload clusters to establish the foundation of a deployment that can later scale to tens of thousands of VMs.

The clusters run the entire vRealize Suite infrastructure, including customer workloads.

Deploying and using vRealize Suite involves technological and operational transformation. As new technologies are deployed in the data center, your organization must also implement appropriate processes and assign the necessary roles. For example, you might need processes to handle new information that is collected. Each management product needs one or more administrators, some of whom might have varying levels of access.

The diagram shows technological capabilities and organizational constructs.

Figure 2-2. Conceptual Design of a vRealize Suite Environment




The clusters, each with a minimum of three hosts, are the basis for your vRealize Suite implementation.

### Management cluster

The hosts in the management cluster run the management components required to support the SDDC. A single management cluster is required for each physical location. You can manually install ESXi hosts that run the management cluster and configure them to use local hard drives to boot.

A management cluster provides resource isolation. Production applications, test applications, and other types of applications cannot use the cluster resources reserved for management, monitoring, and infrastructure services. Resource isolation helps management and infrastructure services to operate at optimum performance level. A separate cluster can satisfy an organization's policy to have physical isolation between management and customer payload hardware.

### Edge cluster

The edge cluster supports network devices that provide interconnectivity between environments. It provides protected capacity by which internal data center networks connect through gateways to external networks. Networking edge services and network traffic management take place in the cluster. All external-facing network connectivity terminates in this cluster.

A dedicated vCenter Server instance that is paired with VMwareNSXmanages the ESXi hosts in the edge cluster. The same vCenter Server instance manages the payload clusters that require access to external networks.

The edge cluster can be small and can consist of ESXi hosts that have less capacity than those in the management and payload clusters.

**Payload cluster**

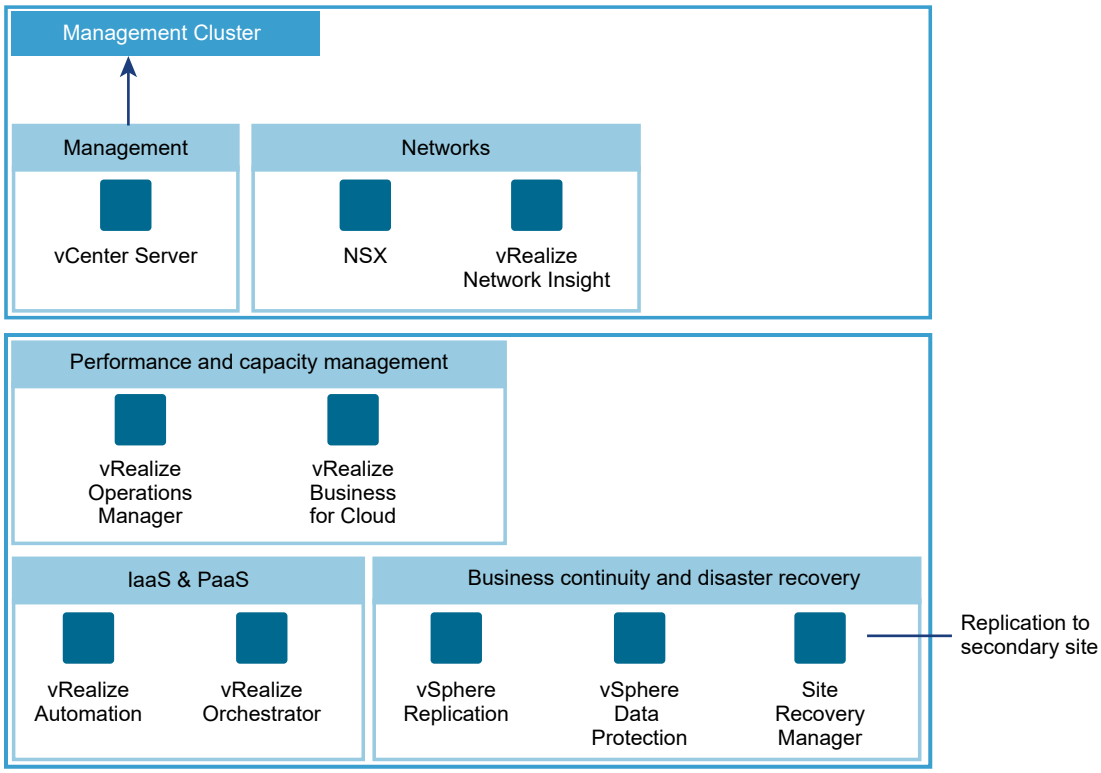
The payload cluster supports the delivery of all other, non-edge client workloads. The cluster remains empty until a consumer of the environment begins to populate it with virtual machines. You can scale up by adding more payload clusters.

As the data center grows in size you can create new edge and payload clusters, scale up by adding resources, or scale out by adding hosts.

# vRealize Suite Products in the Management Cluster

The number of vRealize Suite products in the management cluster increases as you add capabilities. A management cluster must contain a minimum set of products. You can expand the product set when you require additional capabilities.

Figure 2-3. VMware Products in the Management Cluster




## Minimum Set of Management Cluster Products

The management cluster always includes a vCenter Server instance.

vRealize Suite does not include VMware networking solutions by default. NSX for vSphere can fulfill the networking functions of the vRealize Suite management cluster. NSX provides Layer 2 to Layer 7 network virtualization, with security policies that follow workloads across the data center for faster network provisioning and management. You can purchase NSX for vSphere at a reduced, add-on price.

**Note** vCloud Networking and Security was included with the previous version of vRealize Suite, and performed management cluster networking functions. vCloud Networking and Security is no longer a part of vRealize Suite.

## Extended Set of Products

As the complexity of the environment increases, you install and configure additional products. For example, vRealize Operations Manager and related products provide advanced monitoring features. vRealize Automation is the key element of your IaaS solution because it enables rapid modelling and provisioning of servers and desktops across virtual and physical, private and public, or hybrid cloud infrastructures. A vCenter Site Recovery Manager instance can provide replication to a secondary site for disaster recovery.

# SDDC Core Infrastructure

The SDDC core infrastructure consists of vSphere and vRealize Suite products such as vRealize Operations Manager and vRealize Log Insight for monitoring, vRealize Automation and vRealize Orchestrator for managing workflows, and vRealize Business for Cloud for costing.

The core infrastructure includes the physical layer, virtual infrastructure layer, and cloud management layer. The core virtualization is part of the virtual infrastructure layer and the service catalog and orchestration services are part of the cloud management layer. The virtual infrastructure layer enables consolidation and pooling of underlying physical resources. The cloud management layer provides the orchestration capabilities and reduces the costs associated with operating an on-premises data center. The service management layer provides monitoring capabilities to pro-actively identify and solve emerging issues with predictive analysis and smart alerts, ensuring optimal performance and availability of applications and infrastructure.

The vRealize Suite products of the SDDC infrastructure help to effectively manage performance, availability, and capacity of resources across a virtual and hybrid cloud environment. The core infrastructure helps to manage across hybrid and heterogeneous cloud environments, on premise or off premise, based on vSphere or other third-party technologies.

When the SDDC infrastructure is in place, you can extend it to provide Infrastructure as a service (IaaS) and platform as a service (PaaS) to consumers of IT resources inside or outside the organization. IaaS and PaaS complete the SDDC platform, and provide further opportunities for extending capabilities. With IaaS and PaaS, you increase the agility of IT and developer operations.

Figure 2-4. Stages of Building the SDDC Infrastructure


# Virtualization and Management of vRealize Suite Infrastructure

The different VMware products that are included in vRealize Suite provide the virtualization and management capabilities required for the vRealize Suite foundation. To establish a robust foundation for your data center, install and configure vCenter Server, ESXi, and supporting components.

## Hybrid Cloud Deployment

With vRealize Suite, enterprises can extend their private cloud workloads to the public cloud, capitalizing the on-demand, self-service and elastic provisioning of end points while taking advantage of the same management environment, reliability, and performance of the vRealize Suite powered private cloud.

Using vRealize Automation and vRealize Orchestrator in the Cloud Management Layer in an SDDC allows enterprises to provision VMs and end points that extend beyond vSphere environments to environments that are not based on vSphere. The non-vSphere environments that are not based on vSphere can be in private datacenters or service providers of public clouds. The Service Management Layer of SDDC allows the monitor vSphere end points and end points that are not based on vSphere. vRealize Operations Manager and vRealize Log Insight are the key products of the Service Management Layer that help enterprises to provide analytics on the VMs.

## ESXi and vCenter Server Design Considerations

Design decisions for virtualization of the SDDC must address the deployment and support specifics of ESXi and vCenter Server.

Consider the following design decisions when you plan the deployment of ESXi hosts.

### ESXi

- Use a tool such as VMware Capacity Planner to analyze the performance and use of existing servers.
- Use supported server platforms that are listed in the VMware Compatibility Guide.
- Verify that your hardware meets the minimum required system requirements for running ESXi.
- To eliminate variability and achieve a manageable and supportable infrastructure, standardize the physical configuration of the ESXi hosts.

- You can deploy ESXi hosts either manually, or by using an automated installation method such as vSphere Auto Deploy. One valid approach is to deploy the management cluster manually, and implement vSphere Auto Deploy as your environment grows.

vCenter Server

- You can deploy vCenter Server as a Linux-based virtual appliance or on a 64-bit Windows physical or virtual machine.

  **Note** vCenter Server on Windows scales up to support up to 10,000 powered-on virtual machines. The vCenter Server Appliance is an alternative choice that is preconfigured and enables faster deployment and reduced operating system licensing costs. When using an external Oracle database, the vCenter Server Appliance can support a maximum of 10,000 virtual machines.

- Provide sufficient virtual system resources for vCenter Server.
- Deploy the vSphere Web Client and the vSphere Client for user interfaces to the environment. Deploy the vSphere Command Line Interface (vCLI) or vSphere PowerCLI for command-line and scripting management. vCLI and vSphere SDK for Perl are included in the vSphere Management Assistant.

## Network Design Considerations

As virtualization and cloud computing become more popular in the data center, a shift in the traditional three-tier networking model is taking place. The traditional core-aggregate-access model is being replaced by the leaf and spine design.

The network must be designed to meet the diverse needs of different entities in an organization. These entities include applications, services, storage, administrators, and users.

- Use controlled access where required and isolation where necessary to provide an acceptable level of security.
- Use a leaf and spine design to simplify the network architecture.
- Configure common port group names across hosts to support virtual machine migration and failover.
- Separate the network for key services from one another to achieve greater security and better performance.

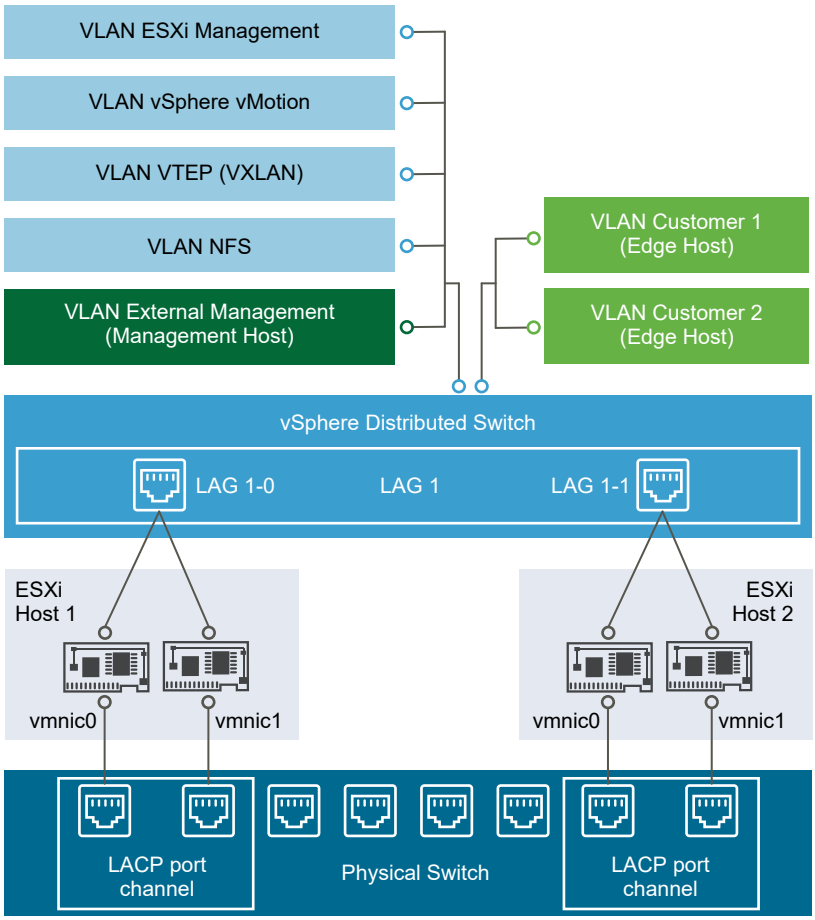
Network isolation is often recommended as a best practice in the data center. In a vRealize Suite environment, you might have several key VLANs, spanning two or more physical clusters.

In the following illustration, all hosts are part of the ESXi Management, vSphere vMotion, VXLAN, and NFS VLANs. The Management host is also connected to the external VLAN, and each edge host is connecting to its customer-specific VLAN.

In this case, connections use Link Aggregation Control Protocol (LACP) provided by a vSphere Distributed Switch to aggregate the bandwidth of physical NICs on ESXi hosts that are connected to LACP port channels. You can create multiple link aggregation groups (LAGs) on a distributed switch. A LAG includes two or more ports and connects physical NICs to the ports. LAG ports are teamed in the LAG for redundancy, and the network traffic is load balanced between the ports by using an LACP algorithm.

See LACP Support on a vSphere Distributed Switch.

**Figure 2-5. Different Types of ESXi Hosts Connect to Different VLANs**




## Shared Storage Design Considerations

A proper storage design provides the basis for a virtual data center that performs well.

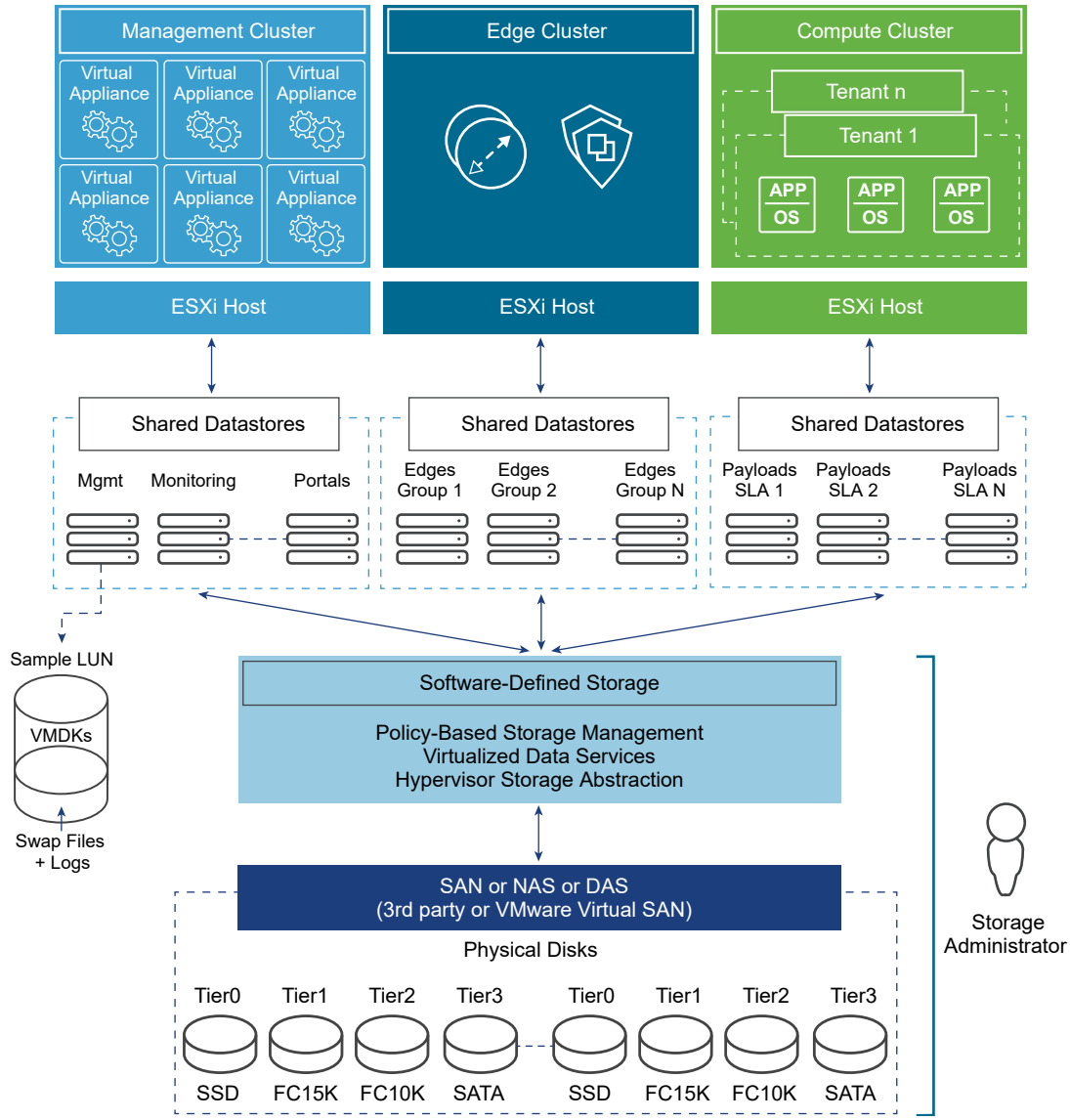
- The storage design must be optimized to meet the diverse needs of applications, services, administrators, and users.
- Tiers of storage have different performance, capacity, and availability characteristics.
- Designing different storage tiers is cost efficient, because not every application requires expensive, high-performance, highly available storage.

- Fibre Channel, NFS, and iSCSI are mature and viable options to support virtual machine needs.

The following illustration shows how different types of hosts take advantage of different storage arrays. Hosts in the management cluster need storage for management, monitoring, and portals. Hosts in the edge cluster need storage that the customer can access. A host in the payload cluster has access to customer-specific storage. Different payload cluster hosts have access to different storage.

The storage administrator can manage all storage, however, the storage administrator does not have access to customer data.

Figure 2-6. Storage Supporting the Different Hosts



## Manage vRealize Suite Core Infrastructure

Managing an SDDC involves many, often repetitive, operations. In vRealize Suite, you can use vRealize Orchestrator to manage complex processes through workflows.

With the cloud management layer, you can build macro-like workflows that automate manual processes. Orchestration makes it possible to deliver repeatable operations.

Within the cloud management layer, workflows can be triggered automatically or manually.

- vRealize Automation can trigger vRealize Orchestrator workflows.
- You can also publish workflows in your service catalog and trigger them manually.

Establishing the orchestration engine early in the process benefits all levels of customer maturity and provides a foundation that the rest of the solution builds on. Deploy at least one vCenter Server instance for each vCenter Server system in your environment depending on your scale requirements.

The orchestration layer contains the following main elements.

- vRealize Orchestrator
- vRealize Orchestrator plug-ins

**Figure 2-7. Design of the vRealize Suite Orchestration Layer**

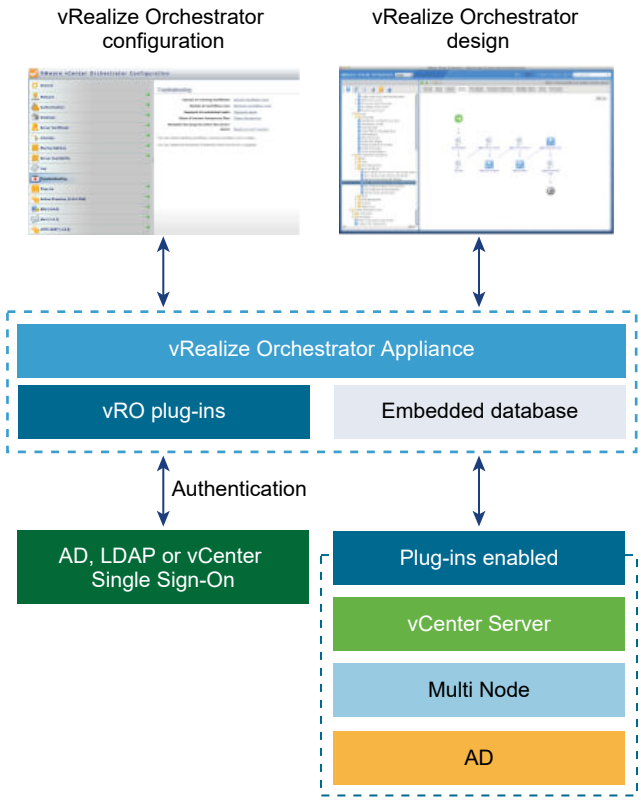


Table 2-1. Components of the vRealize Suite Orchestration Layer

| Component | Description |
|---|---|
| vRealize Orchestrator Appliance | You can deploy vRealize Orchestrator as a virtual appliance. The vRealize Orchestrator Appliance, running in stand-alone mode, not HA, is the recommended approach for smaller deployments. |
| Authentication | Provided by Active Directory or vCenter Single Sign-On. |
| vRealize Orchestrator configuration interface | Use the Web-based configuration interface to configure the appliance database, TLS certificate, license, and so on. |
| vRealize Orchestrator designer interface | Use the Web-based designer interface to create and customize workflows. |
| vCenter Server plug-in | Use the vRealize Orchestrator plug-in to manage multiple vCenter Server instances. The plug-in provides a library of standard workflows that automate vCenter Server operations. |
| Multi Node plug-in | Use the vRealize Orchestrator multinode plug-in to remotely manage vRealize Orchestrator and workflow execution. |

## Monitoring vRealize Suite Core Infrastructure

Monitoring capability is a required element of an SDDC. The monitoring element provides capabilities for performance and capacity management of related infrastructure components, including satisfying requirements, specifications, management, and their relationships.

vRealize Suite monitoring products include several VMware products.

Table 2-2. Monitoring Products in vRealize Suite

| Monitoring Product | Description |
|---|---|
| vRealize Operations Manager | Provides information about the performance, capacity, and health of your infrastructure. Distributed as a virtual appliance that you can deploy on ESXi hosts. Configure the virtual appliance and register it with a vCenter Server system. See the vRealize Operations Manager Documentation. |
| vRealize Log Insight | Collects and analyzes log data to provide real-time answers to problems related to systems, services, and applications, and to derive important insights. See the vRealize Log Insight Documentation. |

You can deploy all monitoring products or only some of the products without damaging the integrity of the solution.

## Delivering an Infrastructure Service

The ability to deliver Infrastructure as a service (IaaS) represents the technological and organizational transformation from traditional data center operations to cloud. You can model and provision VMs and services across private, public, or hybrid cloud infrastructure.

In the SDDC, provider groups or organizations can isolate and abstract resources in the form of infrastructure and application services, and make them available to tenant groups or organizations.

The cloud management layer delivers a self-service user portal that lowers administrative overhead through the use of policies to provision infrastructure services. Administrators use policies to control the consumption of services in a detailed and flexible fashion. Approval requirements can be part of each service.

You can build the infrastructure service by using several components.

**Table 2-3. Infrastructure Service Components**

| Infrastructure Service Section | Design Components |
|---|---|
| vRealize Automation virtual appliance | ■ vRealize Automation Portal Web server or App server<br>■ vRealize Automation vPostgreSQL database |
| vRealize Automation IaaS | ■ vRealize Automation IaaS Web server<br>■ vRealize Automation IaaS Manager services |
| Distributed execution manager | vRealize Automation distributed execution managers consist of DEM Orchestrator instances and DEM Worker instances. |
| Integration | vRealize Automation Agent machines |
| Cost management | vRealize Business for Cloud |
| Provisioning infrastructure | ■ vSphere environment<br>■ vRealize Orchestrator environment<br>■ Other supported physical, virtual, or cloud environment |
| Supporting infrastructure | ■ Microsoft SQL database environment<br>■ LDAP or Active Directory environment<br>■ SMTP and email environment |

An infrastructure service is deployed in multiple stages.

**Figure 2-8. Stages of an IaaS Deployment**

For an in-depth discussion of key IaaS concepts, see the vRealize Automation information about Infrastructure as a Service.

**Self-Service Portal**

vRealize Automation provides a secure portal where authorized administrators, developers, or business users can request new IT services.

**Infrastructure Components**

To deploy vRealize Automation, you configure some VMware products such as vSphere and vCloud Air, and you configure vRealize Automation components such as physical machine endpoints, fabric groups, and blueprints.

**Services and Tenants**

The service catalog provides a unified self-service portal for consuming IT services. Users can browse the catalog to request items, track their requests, and manage their provisioned items.

**Cost Management**

Solutions that integrate with vRealize Automation, such as vRealize Business for Cloud, support cost exploration and management.

## Delivering Platform as a Service

Use platform-as-a-service (PaaS) to model and provision applications across private, public, and hybrid cloud infrastructures.

PaaS is a type of cloud computing service that provides a computing platform and a solution stack as a service. Along with software-as-a-service (SaaS) and infrastructure-as-service (IaaS), PaaS is a service model of cloud computing that lets you use tools and libraries that the provider supplies to create an application, or service. You control software deployment and configuration settings. The provider provides the networks, servers, storage, and other services required to host your application.

### Automate Application Provisioning

A key aspect of PaaS is the ability to automate the provisioning of applications. vRealize Automation is a model-based application provisioning solution that simplifies creating and standardizing application deployment topologies on cloud infrastructures. Application architects use the application drag-and-drop features to create application deployment topologies called application blueprints. Application blueprints define the structure of the application, enable the use of standardized application infrastructure components, and include installation dependencies and default configurations for custom and packaged enterprise applications. You can use the prepopulated and extensible catalog of standard logical templates, application infrastructure service, components, and scripts to model an application blueprint. Application blueprints are logical deployment topologies that are portable across IaaS clouds, such as vRealize Automation, and across public clouds such as Amazon EC2 .

Using vRealize Automation, you specify the application and service structure with the assumption that the underlying cloud infrastructure delivers the necessary compute, network, and storage requirements. You can deploy the vRealize Automation blueprints on any private or public cloud that is based on VMware vSphere. This application provisioning model frees developers and application administrators from dealing with infrastructure, OS, and middleware configuration, and allows your company to focus on delivering business value with its applications.

Enterprise users can standardize, deploy, configure, update, and scale complex applications in dynamic cloud environments. These applications can range from simple Web applications to complex custom applications and packaged applications. With its catalog of standard components, or services, vRealize Automation Application Services automates and manages the update life cycle of deployments for multitier enterprise applications in hybrid cloud environments.

### Monitor Application Performance

Monitoring provides capabilities for performance management related to applications.

### Prebuilt Application Components

VMware Cloud Management Marketplace provides blueprints, services, scripts, and plug-ins that you can download and use to develop your own application services. Leading middleware, networking, security, and application vendors provide prebuilt components that use reusable and flexible configurations that you can insert into any multitier application-provisioning plan.

## vRealize Suite Security Considerations

Each vRealize Suite product must meet security requirements. You must consider authentication and authorization for each product, ensure that certificates meet company requirements, and implement network isolation.

Documentation for product families or individual products can help you secure your environment. This document focuses especially on additional steps you can take to secure the suite of products.

**Table 2-4. Security Documentation for vRealize Suite Products**

| Product | Documentation |
|---|---|
| vCenter ServerESXi | See the vSphere Security documentation for information on many topics including certificate management, securing ESXi, securing vCenter Server, and authentication and authorization.<br>See the Security of the VMware Hypervisor white paper for ESXi security information. |
| vSphere | See the vSphere Security Hardening Guides for your vSphere products. |

Table 2-4. Security Documentation for vRealize Suite Products (continued)

| Product | Documentation |
| --- | --- |
| vRealize Automation and related products. | See Preparing for Installation in the vRealize Automation documentation for information about certificates, pass phrases, user security, using security groups, and so on.<br>See the vRealize Automation Secure Configuration Guide for information on optimizing the secure configuration of your vRealize Automation environment. |
| vRealize Suite Lifecycle Manager | See the vRealize Suite Lifecycle Manager Security Hardening Guide for information on optimizing the secure configuration of your vRealize Suite Lifecycle Manager environment. |

# Authentication and Authorization in vRealize Suite

Authentication with vCenter Single Sign-On ensures that only users in supported identity sources can log in to vRealize Suite. Authorization ensures that only a user with corresponding privileges can view information or perform tasks. Authorization applies to both services and human users.

## Authentication with vCenter Single Sign-On

vCenter Single Sign-On supports authentication in your management infrastructure. Only users that can authenticiate to vCenter Single Sign-On can view and manage infrastructure components. You can add identity sources such as Active Directory or OpenLDAP to vCenter Single Sign-On.

### vCenter Single Sign-On Overview

vCenter Single Sign-On is an authentication broker and security token exchange infrastructure for users and solution users, which are sets of VMware services. When a user or a solution user authenticates to vCenter Single Sign-On, that user receives a SAML token. Going forward, the user can use the SAML token to authenticate to vCenter Server services. The user can then view the information and perform the actions that user has privileges for.

By using vCenter Single Sign-On, the vRealize Suite products communicate with each other through a secure token exchange mechanism, instead of requiring each product to authenticate a user separately with a directory service like Microsoft Active Directory. During installation or upgrade, vCenter Single Sign-On constructs an internal security domain, for example, vsphere.local, where the vSphere solutions and products are registered. Instead of using this internal security domain for company-specific authentication information, you can add one or more identity sources such as an Active Directory Domain to vCenter Single Sign-On.

### Configuring vCenter Single Sign-On

You can configure vCenter Single Sign-On from the vSphere Web Client.

Starting with vSphere 6.0, vCenter Single Sign-On is part of the Platform Services Controller. The Platform Services Controller contains shared services that support vCenter Server and vCenter Server components. To manage vCenter Single Sign-On, you connect to the Platform Services Controller associated with your environment. See vSphere Authentication with vCenter Single Sign-On for background and details on configuration.

## Authorization in vRealize Suite

Authorization determines which user or process can access or modify which components in your vRealize Suite deployment. Different products within vRealize Suite handle authorization at different levels of granularity.

Different types of administrators are responsible for giving access to different types of users for different products or product components.

### vCenter Server Authorization

The vCenter Server permissions model allows administrators to assign roles to a user or group for a certain object in the vCenter Server object hierarchy. Roles are sets of privileges. vCenter Server includes predefined roles, but you can also create custom roles.

In many cases, permissions must be defined on both a source object and a destination object. For example, if you move a virtual machine, you need some privileges on that virtual machine, but also privileges on the destination data center.

In addition, Global Permissions allow you to give certain users privileges to all objects in the vCenter object hierarchy. Use Global Permissions with care, especially if you propagate them down the object hierarchy.

See the vSphere Security documentation for details and for instructional videos about vCenter Server permissions.

### vRealize Automation Authentication

vRealize Automation allows you to use predefined roles to determine which user or group can perform which tasks. In contrast to vCenter Server, you cannot define custom roles, but a rich set of predefined roles is available.

Authentication and authorization proceed as follows:

1. The system administrator performs the initial configuration of single sign-on and basic tenant setup, including designating at least one identity store and a tenant administrator for each tenant.
2. Thereafter, a tenant administrator can configure additional identity stores and assign roles to users or groups from the identity stores.

   Tenant administrators can also create custom groups within their own tenant and add users and groups defined in the identity store to custom groups. Custom groups, like identity store groups and users, can be assigned roles

3 Administrators can then assign roles to users and groups, depending on the role that they themselves belong to.

- A set of system-wide roles, such as system administrator, IaaS administrator, and fabric administrator are predefined.
- A separate set of tenant roles such as tenant administrator or application catalog administrator, are also predefined.

See the vRealize Automation documentation.

## Federated Identity Management

Federated identity management enables electronic identities and attributes from one domain to be accepted and used to access resources in other domains. You can enable federated identity management between vRealize Automation, vRealize Operations Manager,and vSphere Web Client using vCenter Single Sign-On and VMware Identity Manager.

Federated identity environments divide users into categories called personas based on how they interact with federated identity systems. Users use the systems to receive services. Administrators configure and manage federation among systems. Developers create and extend services consumed by users. The following table describes the benefits of federated identity management enjoyed by these persona.

Table 2-5. Benefits to Persona

| User Types | Federated Identity Benefit |
|---|---|
| Users | ■ Convenient single sign on to multiple applications<br>■ Fewer passwords to manage<br>■ Improved security |
| Administrators | ■ More control over applications entitlements and access<br>■ Context and policy-based authentication |
| Developers | ■ Simple integration<br>■ Benefits of multitenancy, user and group management, extensible authentication, and delegated authorization with little effort |

You can set up federation between VMware Identity Manager and vCenter Single Sign-On by creating a SAML connection between the two parties. vCenter Single Sign-On acts as the identity Provider and VMware Identity Manager as the service provider. An identity provider provides an electronic identity. A service provider grants access to resources after evaluating and accepting the electronic identity.

For users to be authenticated by vCenter Single Sign-On, the same account must exist in VMware Identity Manager and vCenter Single Sign-On. Minimally, the userPrinicpalName of the user must match on both ends. Other attributes can differ because they are not used to identify the SAML subject.

For local users in vCenter Single Sign-On such as admin@vsphere.local, corresponding accounts must be created in VMware Identity Manager where at least the userPrinicpalName of the user matches. The corresponding accounts must be created manually or by a script using the VMware Identity Manager local user creation APIs.

Setting up SAML between SSO2 and vIDM involves the following tasks.

1 Import the SAML token from vCenter Single Sign-On to VMware Identity Manager before updating the VMware Identity Manager default authentication.

2 In VMware Identity Manager, configure vCenter Single Sign-On as a third-party identity provider on VMware Identity Manager and update VMware Identity Manager default authentication.

3 On vCenter Single Sign-On, configure VMware Identity Manager as a service provider by importing the VMware Identity Manager `sp.xml` file.

See the following product documentation:

- For information about Configuring SSO2 as an identity provider for vRealize Automation, see Using VMware vCenter SSO 5.5 U2 with VMware vCloud Automation Center 6.1.
- For vRealize Automation VMware Identity Manager documentation, see Update Your Single Sign-On Password for VMware Identity Manager.
- For information about how to configure federation between Directories Management and SSO2, see Configure SAML Federation Between Directories Management and SSO2.
- For vRealize Operations Manager SSO documentation, see Configure a Single Sign-On Source in vRealize Operations Manager.

## TLS and Data Protection

The different vRealize Suite products use TLS to encrypt session information between products. By default, the VMware Certificate Authority (VMCA), which is part of the Platform Services Controller, supplies certificates to some of the products and services. Other components are provisioned with self-signed certificates.

If you want to replace the default certificates with your own enterprise certificates or CA-signed certificates, the process differs for different components.

Certificate checking is enabled by default and TLS certificates are used to encrypt network traffic. Starting with vSphere 6.0, the VMCA assigns certificates to ESXi hosts and vCenter Server systems as part of the installation process. You can replace these certificates to use VMCA as an intermediate CA, or you can use custom certificates in your environment. vSphere version 5.5 and earlier uses self-signed certificates and you can use or replace these certificates as needed.

You can replace vSphere 6.0 certificates by using the vSphere Certificate Manager utility or certificate management CLIs. You can replace vSphere 5.5 and earlier certificates by using the Certificate Automation Tool.

### Products that Use VMCA

Several VMware products receive certificates from the VMCA during installation. For those products, you have several options.

- Leave the certificates in place for internal deployments, or consider replacing external-facing certificates but leaving internal-facing VMCA-signed certificates in place.
- Make VMCA an intermediate certificate. Going forward, uses the full chain to sign.
- Replace the VMCA-signed certificates with custom certificates.

See vSphere Security Considerations.

### Products that Use Self-Signed Certificates

You can use products that use self-signed certificates as is. Browsers prompt users to accept or reject a self-signed certificate on first use. Users can click a link to open and view the certificate details before accepting or rejecting it. Browsers store accepted certificates locally and silently accept them for subsequent uses. You can avoid the acceptance step by replacing self-signed certificates with enterprise certificates or CA-signed certificates where needed. Product documentation explains how to replace self-signed certificates.

**Table 2-6. Replacing Self-Signed Certificates**

| Product | Documentation |
|---|---|
| vSphere Replication | See Change the SSL Certificate of the vSphere Replication Appliance. |
| vRealize Automation | See Updating vRealize Automation Certificates. |
| vRealize Log Insight | See Install a Custom SSL Certificate. |
| vRealize Orchestrator | See Changing SSL Certificates. |
| vRealize Operations Manager | See Add a Custom Certificate to vRealize Operations Manager. |
| vRealize Business for Cloud Standard | See Change or Replace the SSL Certificate of vRealize Business for Cloud. |

## Securing the Physical Layer

Securing the physical layer includes securing or hardening the hypervisor, setting you the physical network for maximum security, and securing your storage solution.

### Securing Standard Switch Ports

As with physical network adapters, a virtual network adapter can send frames that appear to be from a different machine or impersonate another machine. Also, like physical network adapters, a virtual network adapter can be configured so that it receives frames targeted for other machines.

When a standard switch is created, port groups are added to impose a policy configuration for the virtual machines and storage systems attached to the switch. Virtual ports are created through the vSphere Web Client or the vSphere Client.

As part of adding a port or standard port group to a standard switch, the vSphere Client configures a security profile for the port. The host can then prevent that any of its virtual machine impersonate other machines on the network. The guest operating system responsible for the impersonation does not detect that the impersonation was prevented.

The security profile determines how strongly the host enforces the protection against impersonation and interception attacks on virtual machines. To correctly use the settings in the security profile, you must understand the basics of how virtual network adapters control transmissions and how attacks are staged at this level.

Each virtual network adapter has a MAC address that is assigned to it when the adapter is created. This address is called the initial MAC address. Although the initial MAC address can be reconfigured from outside the guest operating system, it cannot be changed by the guest operating system. In addition, each adapter has an effective MAC address that filters out incoming network traffic with a destination MAC address different from the effective MAC address. The guest operating system is responsible for setting the effective MAC address, and typically matches the effective MAC address to the initial MAC address.

When sending packets, an operating system typically places its own network adapter's effective MAC address in the source MAC address field of the Ethernet frame. It also places the MAC address for the receiving network adapter in the destination MAC address field. The receiving adapter accepts packets only when the destination MAC address in the packet matches its own effective MAC address.

Upon creation, a network adapter's effective MAC address and initial MAC address are the same. The virtual machine's operating system can alter the effective MAC address to another value at any time. If an operating system changes the effective MAC address, its network adapter receives network traffic destined for the new MAC address. The operating system can send frames with an impersonated source MAC address at any time. This means an operating system can stage malicious attacks on the devices in a network by impersonating a network adapter that the receiving network authorizes.

Standard switch security profiles can be used on hosts to protect against this type of attack by setting three options. If any default settings for a port are changed, the security profile must be modified by editing standard switch settings in the vSphere Client.

## Securing iSCSI Storage

The storage configured for a host might include one or more storage area networks (SANs) that use iSCSI. When iSCSI is configured on a host, administrators can take several measures to minimize security risks.

iSCSI is a means of accessing SCSI devices and exchanging data records by using TCP/IP over a network port rather than through a direct connection to a SCSI device. In iSCSI transactions, blocks of raw SCSI data are encapsulated in iSCSI records and transmitted to the requesting device or user.

One means of securing iSCSI devices from unwanted intrusion is to require that the host, or initiator, be authenticated by the iSCSI device, or target, whenever the host attempts to access data on the target LUN. Authentication proves that the initiator has the right to access a target,

ESXi and iSCSI support Challenge Handshake Authentication Protocol (CHAP), which verifies the legitimacy of initiators that access targets on the network. Use the vSphere Client or the vSphere Web Client to determine whether authentication is being performed and to configure the authentication method. For information about configuring CHAP for iSCSI see the vSphere documentation

## Securing ESXi Management Interfaces

Security of the ESXi management interface is critical to protect against unauthorized intrusion and misuse. If a host is compromised in certain ways, the virtual machines it interacts with might also be compromised. To minimize the risk of an attack through the management interface, ESXi is protected with a built-in firewall.

To protect the host against unauthorized intrusion and misuse, VMware imposes constraints on several parameters, settings, and activities. Constraints can be relaxed to meet configuration needs, but if you do so, you must take measures to protect the network as a whole and the devices connected to the host.

Consider the following recommendations when evaluating host security and administration.

- To improve security, restrict user access to the management interface and enforce access security policies such as setting up password restrictions.
- Provide only trusted users with ESXi Shell login access. The ESXi Shell has privileged access to certain parts of the host.
- When possible, run only the essential processes, services, and agents such as virus checkers, and virtual machine backups.
- When possible, use the vSphere Web Client or a third-party network management tool to administer ESXi hosts instead of working though the command-line interface as the root user. When you use the vSphere Web Client, you always connect to the ESXi host through a vCenter Server system.

The host runs several third-party packages to support management interfaces or tasks that an operator must perform. VMware does not support upgrading these packages from anything other than a VMware source. If a download or patch is used from another source, management interface security or functions might be compromised. Regularly check third-party vendor sites and the VMware knowledge base for security alerts.

In addition to implementing the firewall, you can mitigate risks to ESXi hosts using other methods.

- Make sure that all firewall ports that are not specifically required for management access to the host are closed. Ports must be specifically opened if additional services are required.
- Replace the default certificates, and do not enable weak ciphers. By default, weak ciphers are disabled and all communications from clients are secured by TLS. The exact algorithms used for securing the channel depend on the TLS handshake. Default certificates created on ESXi use SHA-1 with RSA encryption as the signature algorithm.
- Install security patches. VMware monitors all security alerts that might affect ESXi security, and if needed, issues a security patch.
- Non secure services such as FTP and Telnet are not installed, and the ports for these services are closed. Because more secure services such as SSH and SFTP are easily available, always avoid using these insecure services in favor of their safer alternatives. If you must use non secure services, implement sufficient protection for the ESXi hosts and open the corresponding ports.

You can put ESXi hosts in lockdown mode. When lockdown mode is enabled, the host can be managed only from vCenter Server. No users other than vpxuser have authentication permissions, and direct connections to the host are rejected.

## Securing vCenter Server Systems

Securing vCenter Server includes ensuring security of the machine where vCenter Server is running, following best practices for assigning privileges and roles, and verifying the integrity of the clients that connect to vCenter Server.

Control vCenter Server administrator privileges strictly to increase security for the system.

- Remove full administrative rights to vCenter Server from the local Windows administrator account, and grant them only to a special-purpose local vCenter Server administrator account. Grant full vSphere administrative rights only to those administrators who are required to have it. Do not grant this privilege to any group whose membership is not strictly controlled.
- Do not allow users to log in to the vCenter Server system directly. Allow access only to those users who have legitimate tasks to perform and confirm that their actions are audited.
- Install vCenter Server using a service account instead of a Windows account. A service account or a Windows account can be used to run vCenter Server. Using a service account allows Windows authentication to SQL Server, which provides more security. The service account must be an administrator on the local machine.
- Check for privilege reassignment when restarting vCenter Server. If the user or user group that is assigned the Administrator role on the root folder of the server cannot be verified as a valid user or group, the administrator privileges are removed and assigned to the local Windows Administrators group.

Grant minimal privileges to the vCenter Server database user. The database user requires only certain privileges specific to database access. In addition, some privileges are required only for installation and upgrade. These can be removed after the product is installed or upgraded.

## Securing the Virtual Layers

In addition to securing the physical layers, which include the hardware, the switches, and so on, you must secure the virtual layers. Secure the virtual machines, including the operating system and the virtual networking layer.

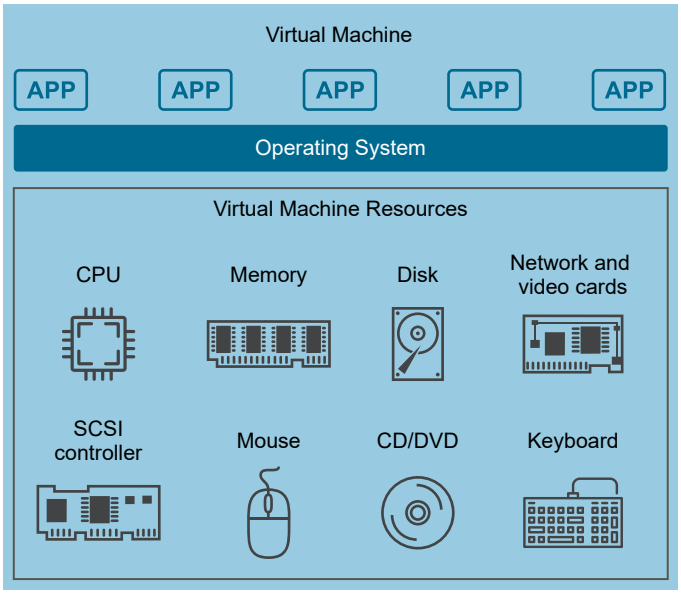
### Security and Virtual Machines

Virtual machines are the logical containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware, and provides both their ability to access hardware and their uninterrupted performance.

Even a user with system administrator privileges on a virtual machine's guest operating system cannot breach this layer of isolation to access another virtual machine without privileges explicitly granted by the ESXi system administrator. As a result of virtual machine isolation, if a guest operating system running in a virtual machine fails, other virtual machines on the same host continue to run. Users can still access other virtual machines, and the performance of other virtual machines is not affected.

Each virtual machine is isolated from other virtual machines running on the same hardware. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine can only detect the virtual devices that you make available to it.

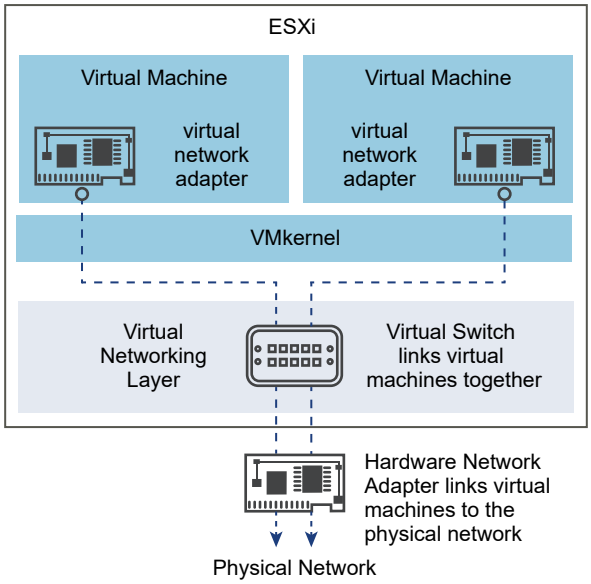
Figure 2-9. Virtual Machine Isolation



The VMkernel mediates all physical resources. All physical hardware access takes place through the VMkernel and virtual machines cannot circumvent this level of isolation.

Just as a physical machine communicates with other machines in a network through a network card, a virtual machine communicates with other virtual machines running on the same host through a virtual switch. Further, a virtual machine communicates with the physical network, including virtual machines on other ESXi hosts, through a physical network adapter.

Figure 2-10. Virtual Networking Through Virtual Switches




Virtual networking is also affected by virtual machine isolation.

- If a virtual machine does not share a virtual switch with any other virtual machine, it is completely isolated from virtual machines within the host.
- If no physical network adapter is configured for a virtual machine, the virtual machine is completely isolated. This includes isolation from any physical or virtual networks.
- Virtual machines are as secure as physical machines if you protect them from the network with firewalls, antivirus software, and so on.

You can further protect virtual machines by setting up resource reservations and limits on the host. For example, you can use resource allocation to configure a virtual machine so that it always receives at least 10 percent of the host's CPU resources, but never more than 20 percent.

Resource reservations and limits protect virtual machines from performance degradation that might result if another virtual machine consumed excessive shared hardware resources. For example, if one of the virtual machines on a host is incapacitated by a denial-of-service (DoS) attack, a resource limit on that machine prevents the attack from taking up so much of the

hardware resources that the other virtual machines are also affected. Similarly, a resource reservation on each of the virtual machines ensures that in the event of high resource demands by the virtual machine targeted by the DoS attack, all the other virtual machines have enough resources to operate.

By default, ESXi imposes a form of resource reservation by applying a distribution algorithm that divides the available host resources equally among the virtual machines while keeping a certain percentage of resources for use by other system components. This default behavior provides a degree of natural protection from DoS and distributed denial-of-service (DDoS) attacks. Specific resource reservations and limits are set on an individual basis to customize the default behavior so that the distribution is not equal across the virtual machine configuration.

### Security and Virtual Networks

If an ESXi host is accessed through vCenter Server, it is typical to protect vCenter Server using a firewall. This firewall provides basic protection for the network.

You usually provide a firewall at what is considered to be an entry point for the system. A firewall might lie between the clients and vCenter Server. Alternatively, vCenter Server and the clients might be behind the firewall for your deployment.

Networks configured with vCenter Server can receive communications through the vSphere Client or third-party network management clients. vCenter Server listens for data from its managed hosts and clients on designated ports. vCenter Server also assumes that its managed hosts listen for data from vCenter Server on designated ports. Firewalls between ESXi, vCenter Server, and other vSphere components must have open ports to support data transfer.

Firewalls might also be included at a variety of other access points in the network, depending on how the network is planned to be used and the level of security various devices require. Select the locations for firewalls based on the security risks that have been identified for network configuration.

## Using VMware NSX to Secure Workloads

VMware NSX provides software-defined networking, virtual networking security services of logical firewalling, logical switching, and logical routing. Virtual network designers programmatically assemble these services in any arbitrary combination to produce unique isolated virtual networks. This technology provides more detailed security than traditional hardware appliances. In virtual environments, you can apply these services at the vNIC level. Traditional services are configured on the physical network.

Selected VMware NSX capabilities are described in detail in the VMware NSX for vSphere (NSX) Network Virtualization Design Guide. You can find procedures for implementing these capabilities in the VMware NSX for vSphere documentation.

NSX is the VMware network virtualization security platform that you can use to construct a secure virtual network environment for your software-defined data center. Use NSX to construct a secure virtualized network by deploying and managing software-defined firewalls, routers, gateways, and their policies. Where VMs are independent of the underlying physical platform

and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware. IT can treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand. Using NSX, you can protect the north south edge traffic and the east-west traffic across network and compute stacks that must maintain data integrity. For example, workloads from different tenants can run securely on individual isolated virtual networks even though they share the same underlying physical network.

## NSX Features

NSX provides a full set of logical network elements, boundary protocols, and security services to organize and manage your virtual networks. Installing an NSX plug-in on the vCenter Server gives you centralized control to create and manage NSX components and services throughout your data center.

See the NSX Administration Guide for descriptions of features and capabilities.

### VMware NSX Edge

Provides centralized north-south routing between the logical networks deployed in NSX domains and the external physical network infrastructure. NSX Edge supports dynamic routing protocols such as Open Shortest Path First (OSPF), internal Border Gateway Protocol (iBGP), and external Border Gateway Protocol (eBGP), and can use static routing. The routing capability supports active-standby stateful services and equal-cost multipath routing (ECMP). NSX Edge also provides standard edge services such as network address translation (NAT), load balancing, virtual private network (VPN), and firewall services.

### Logical Switching

NSX logical switches provide L2 logical networks enforcing isolation between workloads on different logical networks. Virtual distributed switches can span multiple ESXi hosts in a cluster over an L3 fabric by using VXLAN technology, adding the advantage of centralized management. You can control the scope of isolation by creating transport zones by using vCenter Server and assigning logical switches to the transport zones as needed.

### Distributed Routing

Distributed routing is provided by a logical element called Distributed Logical Router (DLR). The DLR is a router with directly connected interfaces to all hosts where VM connectivity is required. Logical switches are connected to logical routers to provide L3 connectivity. The supervisory function, the control plane to control forwarding, is imported from a control VM.

### Logical Firewalling

The NSX platform supports the following critical functions for securing multi-tier workloads.

- Native support for logical firewalling capability, which provides stateful protection of multi-tier workloads.

- Support for multivendor security services and service insertion, for example, antivirus scanning, for application workload protection.

The NSX platform includes a centralized firewall service offered by the NSX Edge services gateway (ESG), and a distributed firewall (DFW) enabled in the kernel as a VIB package on all the ESXi hosts that are part of a given NSX domain. The DFW provides firewalling with near-line rate performance, virtualization, identity awareness, activity monitoring, logging, and other network security features native to network virtualization. You configure these firewalls to filter traffic at the vNIC level of each VM. This flexibility is essential for creating isolated virtual networks, even for individual VMs if that level of detail is needed.

Use vCenter Server to manage firewall rules. The rules table is organized as sections with each section constituting a specific security policy that can be applied to specific workloads.

### Security Groups

NSX provides grouping mechanism criteria that can include any of the following items.

- vCenter Server objects such as virtual machines, distributed switches, and clusters
- Virtual machine properties such as vNICs, virtual machine names, and virtual machine operating systems
- NSX objects including logical switches, security tags, and logical routers

Grouping mechanisms can be either static or dynamic, and a security group can be any combination of objects, including any combination of vCenter objects, NSX Objects, VM Properties, or Identity Manager objects such as AD Groups. A security group in NSX is based on all static and dynamic criteria along with static exclusion criteria defined by a user. Dynamic groups grow and shrink as members enter and leave the group. For example, a dynamic group might contain all VMs that begin with the name web_. Security groups have several useful characteristics.

- You can assign multiple security policies to a security group.
- An object can belong to multiple security groups at the same time.
- Security groups can contain other security groups.

Use NSX Service Composer to create security groups and apply policies. NSX Service Composer provisions and assigns firewall policies and security services to applications in real time. Policies are applied to new virtual machines as they are added to the group.

### Security Tags

You can apply security tags to any virtual machine, adding context about the workload as needed. You can base security groups on security tags. Security tags indicate several common classifications.

- Security state. For example, vulnerability identified.
- Classification by department.
- Data-type classification. For example, PCI Data.

- Type of environment. For example, production or devops.
- VM geography or location.

### Security Policies

Security Policies group rules are security controls that are applied to a security group created in the data center. With NSX you can create sections in a firewall rule table. Sections allow better management and grouping of firewall rules. A single security policy is a section in a firewall rule table. This policy maintains synchronization between rules in a firewall rule table and rules written through the security policy, ensuring consistent implementation. As security policies are written for specific applications or workloads, these rules are organized into specific sections in a firewall rule table. You can apply multiple security policies to a single application. The order of the sections when you apply multiple security policies determines the precedence of rule application.

### Virtual Private Network Services

NSX provides VPN services named L2 VPN and L3 VPN. Create an L2 VPN tunnel between a pair of NSX Edge devices deployed in separate datacenter sites. Create an L3 VPN to provide secure L3 connectivity to the data center network from remote locations.

### Role Based Access Control

NSX has built-in user roles that regulate access to computer or network resources within an enterprise. Users can only have one role.

Table 2-7. NSX Manager User Roles

| Role | Permissions |
|---|---|
| Enterprise Administrator | NSX operations and security. |
| NSX Administrator | NSX operations only. For example, install virtual appliances, configure port groups. |
| Security Administrator | NSX security only. For example, define data security policies, create port groups, create reports for NSX modules. |
| Auditor | Read only. |

### Partner Integration

Services from VMware technology partners are integrated with the NSX platform in the management, control, and data functions to provide a unified user experience and seamless integration with any cloud management platform. See more at: https://www.vmware.com/products/nsx/technology-partners#security.

## NSX Concepts

SDDC administrators configure NSX features to provide network isolation and segmentation in the data center.

### Network Isolation

Isolation is the foundation of most network security, whether for compliance, containment, or isolation of development, test, and production environments. Traditionally, ACLs, firewall rules, and routing policies are used to establish and enforce isolation and multitenancy. With network virtualization, support for those properties is inherently provided. Using VXLAN technology, virtual networks are isolated from other virtual networks and from the underlying physical infrastructure by default, delivering the security principle of least privilege. Virtual networks are created in isolation and remain isolated unless explicitly connected. No physical subnets, VLANs, ACLs, or firewall rules are required to enable isolation.

### Network Segmentation

Network segmentation is related to isolation, but is applied in a multitier virtual network. Traditionally, network segmentation is a function of a physical firewall or router, designed to allow or deny traffic between network segments or tiers. When segmenting traffic between Web, application, and database tiers, traditional configuration processes are time consuming and highly prone to human error, resulting in a large percentage of security breaches. Implementation requires expertise in device configuration syntax, network addressing, and application ports and protocols.

Network virtualization simplifies building and testing configurations of network services to produce proven configurations that can be programatically deployed and duplicated throughout the network to enforce segmentation. Network segmentation, like isolation, is a core capability of NSX network virtualization.

### Microsegmentation

Microsegmentation isolates traffic at the vNIC level by using distributed routers and distributed firewalls. Access controls enforced at the vNIC provide increased efficiency over rules enforced on the physical network. You can use microsegmentation with an NSX distributed firewall and implementation distributed firewall to implement microsegmentation for a three-tier application, for example, web server, application server, and database, where multiple organizations might share the same logical network topology.

### Zero-Trust Model

To achieve the strictest security settings, apply a zero-trust model when configuring security policies. A zero-trust model denies access to resources and workloads unless specifically permitted by a policy. Be certain to allow essential infrastructure traffic. By default, NSX Manager, NSX Controllers, and NSX Edge service gateways are excluded from distributed firewall functions. vCenter Server systems are not excluded and should be explicitly allowed to prevent lockout before applying such a policy.

## Protecting the Management Cluster and Tenant Workloads

If you are an SDDC administrator, you can use NSX capabilities to isolate and protect the vRealize Suite management cluster and tenant workloads in the data center.

The management cluster includes thevCenter Server for the domain, the NSX Manager, and vRealize Suite products and other management products and components. Use Transport Layer Security (TLS) and authentication to protect these systems from unauthorized access. Use NSX capabilities to strengthen isolation and segmentation of the management cluster virtual network systems from the edge cluster and workload systems and clusters. Allow appropriate access to required management system ports as described in the installation and configuration documents for the deployed management systems.

Tenant workloads in the data center might be implemented as three tier-applications consisting of Web, application, and database servers. Use TLS and authentication to protect these systems from unauthorized access. Use provided security services such as database connection strings to secure connections and SSH to secure host access. Apply NSX capabilities at the vNic level where possible to isolate and micro-segment tenant workloads from one another.

For more information about uses of NSX capabilities, see VMware NSX for vSphere (NSX) Network Virtualization Design Guide. For procedures to configure NSX capabilities, see the VMware NSX for vSphere documentation.

# Checklist for Installing vRealize Suite

3

You download, install, and configure vRealize Suite products separately in a specific order. Individual products in vRealize Suite are delivered as either installation packages for Windows or Linux-based machines, or as virtual appliances that you can deploy on virtual machines that are running on ESXi hosts. Suite products you install depends on your vRealize Suite edition.

To ensure interoperability, verify that your vRealize Suite products are the correct versions. For more information about VMware certified compatibility, see VMware Compatibility Guides.

You can also use vRealize Suite Lifecycle Manager to install vRealize Suite together in a single, simplified installation process. See vRealize Suite Lifecycle Manager.

Figure 3-1. Deployment Flow for vRealize Suite

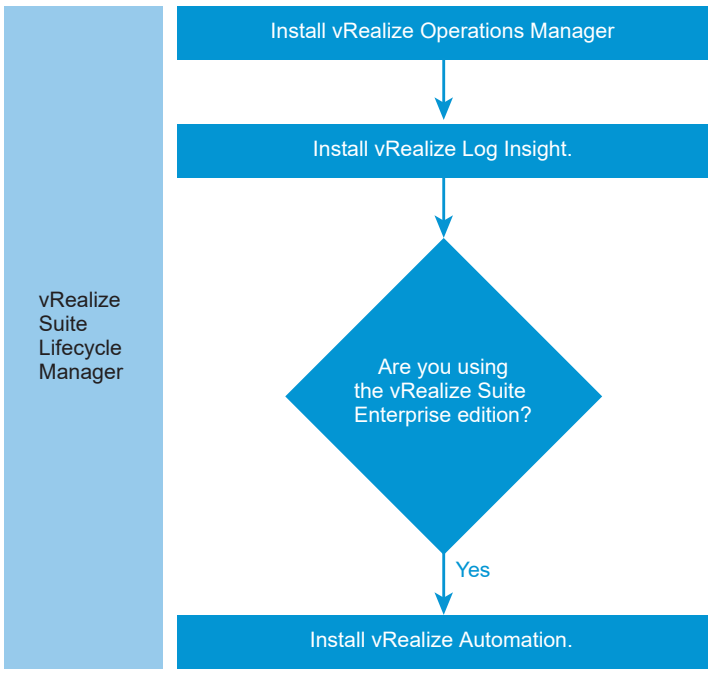


Table 3-1. Checklist for Installing vRealize Suite

| vRealize Suite Products | More information |
| --- | --- |
| ❑ Install vRealize Operations Manager | See the installation documentation of vRealize Operations Manager, click here. |
| ❑ Install vRealize Log Insight as a virtual appliance. | See the installation documentation for your version of vRealize Log Insight, click here. |
| ❑ If you purchased vRealize Suite Advanced or Enterprise edition, install vRealize Automation. You install a vRealize Automation appliance, which provides administration and self-service capabilities, and an Infrastructure as a Service (IaaS) Windows Server, which supports cross-product infrastructure capabilities. | 1 Plan your installation. See the reference architecture documentation for your version of vRealize Automation.<br>■ vRealize Automation 7.6 Reference Architecture<br>■ vRealize Automation 7.4 Reference Architecture<br>■ vRealize Automation 7.3 Reference Architecture<br>■ vRealize Automation 7.2 Reference Architecture<br>■ vRealize Automation 7.1 Reference Architecture<br>■ vRealize Automation 7.0.1 Reference Architecture<br>2 Install vRealize Automation. See the installation documentation for your version of vRealize Automation.<br>■ Installing vRealize Automation with Easy Installer<br>■ Installing vRealize Automation 7.4<br>■ Installing vRealize Automation 7.3<br>■ Installing or Upgrading vRealize Automation 7.2 |
| ❑ Install vRealize Business for Cloud as a virtual appliance. | See the installation documentation for your version of vRealize Business for Cloud.<br>■ vRealize Business for Cloud 7.6<br>■ vRealize Business for Cloud 7.5<br>■ vRealize Business for Cloud 7.4 Installation and Administration |

# Upgrading from Older Versions of vRealize Suite or vCloud Suite

4

You can upgrade vRealize Suite from vCloud Suite or an older version of vRealize Suite by upgrading the individual products to current versions. Follow the recommended update order to ensure that vRealize Suite upgrades finish without problems.

Before upgrading, review the VMware Product Interoperability Matrix for each product you plan to upgrade to ensure that you have supported, compatible product versions. See the VMware Product Interoperability Matrixes Web site.

Table 4-1. Upgrading vRealize Suite Products

| Product | More Information |
| --- | --- |
| VMware vRealize Operations Manager | You can migrate data from vCenter Operations Manager to a fresh installation of VMware vRealize Operations Manager. See Migrate a vCenter Operations Manager Deployment into this Version . |
| vRealize Log Insight | Upgrading vRealize Log Insight |
| vRealize Automation | Upgrading vRealize Automation |
| vRealize Business for Cloud | Upgrading to vRealize Business for Cloud |