White Paper

Cisco Virtualized Multiservice Data Center Framework: Deliver IT as a Service

What You Will Learn

This document provides an overview of the Cisco® Virtualized Multiservice Data Center (VMDC) reference architecture for the Cisco Unified Data Center. The Cisco Unified Data Center changes the economics of the data center by unifying resources into a single, fabric-based platform.

The Cisco Unified Data Center platform is designed from the foundation to deliver networking, computing, storage, security, and management as a fabric-based infrastructure to help IT evolve to IT-as-a-service (ITaaS). Consisting of three elements - Cisco Unified Fabric, Unified Computing, and Unified Management - the Cisco Unified Data Center is designed to dramatically simplify IT infrastructure, enable better agility, and enable greater operating efficiency. But these three elements do far more than increase the efficiency of the hardware, software, and networking resources that comprise the data center infrastructure. The integration of these best-in-class components has a broader impact on the enterprise and its operations, increasing pervasive IT simplicity, business agility, and financial efficiency, streamlining overarching organizational costs, improving productivity, and freeing resources to focus on innovation.

The ideal audience for this document is the technical decision maker in an enterprise.

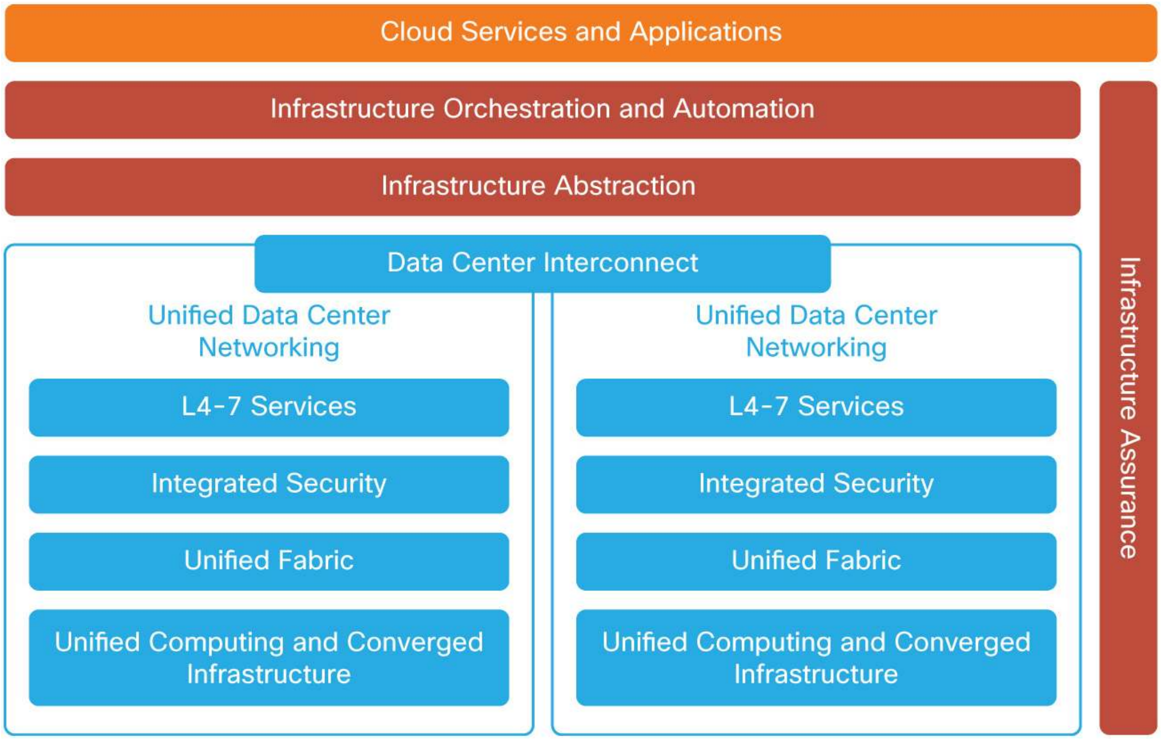
Introduction

The Cisco VMDC is a tested and validated reference architecture for the Cisco Unified Data Center. It provides a set of guidelines and best practices for the creation and deployment of a scalable, secure, and resilient infrastructure in the data center. The Cisco VMDC architecture demonstrates how to bring together the latest Cisco routing and switching technologies, network services, data center and cloud security, automation, and integrated solutions with those of Cisco's ecosystem of partners to develop a trusted approach to data center transformation. Specific benefits include:

- Demonstrated solutions to critical technology-related problems in evolving IT infrastructure: Provides support for cloud computing, applications, desktop virtualization, consolidation and virtualization, and business continuance
- Reduced time to deployment: Provides best-practice recommendations based on a fully tested and validated architecture, helping enable technology adoption and rapid deployment
- Reduced risk: Enables enterprises and service providers to deploy new architectures and technologies with confidence
- Increased flexibility: Enables rapid, on-demand, workload deployment in a multitenant environment using a comprehensive automation framework with portal-based resource provisioning and management capabilities
- Improved operating efficiency: Integrates automation with a multitenant pool of computing, networking, and storage resources to improve asset use, reduce operation overhead, and mitigate operation configuration errors

The Cisco VMDC architecture, consisting of the Cisco Unified Data Center and Cisco Data Center Interconnect (DCI) together with other architectural components such as infrastructure abstraction, orchestration and automation, assurance, and integrated services and applications, as shown in Figure 1, provide comprehensive guidelines for deployment of cloud infrastructure and services at multiple levels.

Figure 1. Cisco VMDC Components


Cloud Services and Applications
Infrastructure Orchestration and Automation
Infrastructure Abstraction
Data Center Interconnect
Unified Data Center Networking
L4-7 Services
Integrated Security
Unified Fabric
Unified Computing and Converged Infrastructure
Unified Data Center Networking
L4-7 Services
Integrated Security
Unified Fabric
Unified Computing and Converged Infrastructure
Infrastructure Assurance

This document is a high-level description of the main infrastructure components for the Cisco VMDC architecture. Specific details of the Cisco VMDC architecture are covered in complementary release-specific documents such as data sheets, design guides, implementation guides, and technical white papers. Details of other Cisco cloud offerings such as cloud management and automation and cloud-enabled applications are covered in their respective solution documentation contexts.

Cisco VMDC Overview

The Cisco VMDC architecture is based on the cloud design concepts described in this section.

Flexible Modular Design

The architecture is designed to support different deployment models at different scales to facilitate gradual growth and expansion as needed by enterprises ranging from small businesses to large service providers. This support is provided through definition of modular standardized building blocks that can be replicated as needed. A deployment can start very small and grow as the business demands with no need for major overhaul or redesign. In this way, Cisco VMDC helps administrators scale their build-outs in predictable, logical units, easing their planning and capacity management and ultimately lowering their operating costs.

High Availability

The architecture is designed to optimize service uptime by enabling availability and fault tolerance at all layers of the data center through the use of a combination of physical redundancy best practices as well as virtualized failover features at the networking, computing, and storage layers.

At the networking layer, physical redundancy includes hardware redundancy within a node and the use of redundant nodes and redundant links, with optimized failover convergence throughout the entire network. Other network-based features that enable high availability include the virtual PortChannel (vPC) technology for Layer 2 multipathing, Hot-Standby Router Protocol (HSRP), Multiple Spanning Tree Protocol (MSTP), Border Gateway Protocol (BGP) with nonstop forwarding (NSF), and bidirectional forwarding detection.

At the computing layer, in addition to the physical redundancy of Cisco Unified Computing System™ (Cisco UCS®) servers, the following features are provided: Cisco UCS end-host mode, Cisco Nexus® 1000V Series Switches and MAC address pinning, redundant virtual switching modules (VSMs) in active-standby mode, high availability in clusters, and automated disaster recovery plans.

At the storage layer, Cisco VMDC architecture uses best-practice methodologies for SAN high availability, prescribing full hardware redundancy at each device in the I/O path from the host to the SAN, beginning at the server, with dual port adapters for each host. Redundant paths from the hosts lead to dual, redundant Cisco MDS 9000 Family SAN switches (with dual supervisors) and then to redundant SAN arrays with tiered RAID protection. RAID 1 and 5 were deployed in the validations tests as two commonly used levels; however, the selection of a RAID protection level will depend on a balance of the cost and the critical nature of the data that is stored. In addition to a comprehensive high-availability design, end-to-end availability of the Cisco VMDC architecture is validated in real-world scaling labs to help ensure quality of deployment.

Security and Multitenancy

By embedding security at each layer of the data center, Cisco VMDC provides a comprehensive and powerful set of tools for operators to use to secure their deployments, enabling highly secure multitenant deployments, one of the primary features of cloud computing. Several features of the networking devices and of the computing infrastructure combine to provide the robust security desired to give organizations the confidence to use cloud computing infrastructure to deploy applications to address their business needs.

Multitenancy refers to the capability of the data center to host multiple separate zones, each of which can serve a separate group of users with a specific service profile. Tenants can be organizations, departments, customers, enterprises, regions, etc. Using a comprehensive set of security features that separate and secure tenant traffic and interactions, Cisco VMDC enables both simple, loose separation as is needed in private clouds, and very strict and secure separation as is needed in public cloud deployments.

In the enterprise context, tenants can be departments of an organization that is operating a private cloud. Each department may have different computational needs, applications, or storage scale, while at the same time all the departments need to be managed and maintained under a single unified operational domain. The secure separation requirements in this type of private cloud may be simple traffic separation in addition to user access control.

In the service provider context, tenants can be different enterprises that lease or use the service provider's cloud infrastructure in a shared public cloud environment. As in the private cloud case, each of these enterprises may have very specific computation, application, and storage needs; however, in addition, the security, use, and service-level agreement (SLA) conformance of each tenancy needs to be strictly enforced, as do independent operation models, to meet both the leasing enterprise's requirements and the hosting service provider's business requirements.

The Cisco VMDC architecture enables either model of tenancy and secure separation using a mix of physical and logical segmentation, monitoring, detection, and policy application.

Service Differentiation

Cisco VMDC architecture enables a cloud operator to either define custom service classes or use predefined service classes to differentiate service offerings over the cloud. Components of a service may include computing allocations in the form of CPU and virtual machine limits, storage and data protection allocations, network-based services such as VLAN segment allocations, quality-of-service (QoS) capabilities, security, disaster recovery and business continuity, and other application-level features. The Cisco VMDC architecture includes four predefined service tiers: Bronze, Silver, Gold, and Palladium. These tiers are not meant to define the only levels of service that can be offered, but are simply representative service levels that were used in the validation tests.

One of the main objectives of the Cisco VMDC architecture is to enable faster and smoother application deployment. To achieve this, the architecture is validated with specific application-level requirements such as QoS, and in turn cloud-enabled application solutions such as Cisco Hosted Collaboration Solution Software and hosted Cisco Virtual Desktop Infrastructure Services are validated on a Cisco VMDC infrastructure.

Comprehensive Service Management

Cisco VMDC architecture is closely integrated with the service orchestration and service assurance subsystems that provide configuration and provisioning automation for both the operator offering services through the cloud and the users using these services. Service orchestration is a multidomain configuration abstraction layer on top of the data center infrastructure. It enables a portal-based configuration model in which the subscriber can select from a defined number of service options and host applications as virtual machines. On the basis of these selections, configuration actions are performed on the devices to achieve the service represented in the portal. This self-service, portal-based model offers customization per customer and reduces the number of manual tasks required of the IT department. Service orchestration also automates configuration across many devices based on the services advertised through the portal.

Transition to IT as a Service

The transition to ITaaS, in which IT essentially provides services to internal "customers," involves the same technology and design principles as can be applied to any organization that wants to monetize its service offerings. Service providers can use the same technology to deliver cloud or hosting services. Enterprises can take excess data center capacity and sell these services in a community cloud model.

The Cisco Unified Data Center changes the economics of the data center by unifying computing, storage, networking, virtualization, and management resources into a single, fabric-based platform designed to increase operating efficiency, simplify IT operations, and provide business agility. Unlike other solutions, which add layers of complexity management software to achieve integration, the Cisco Unified Data Center is specifically designed for virtualization and automation and enables on-demand provisioning from shared pools of infrastructure across physical and virtual environments in a simpler and more cost-effective design. This approach allows IT to move from being a cost center to providing IT services that create a competitive advantage.

Cisco VMDC Architecture

This section describes the primary components of the Cisco VMDC architecture:

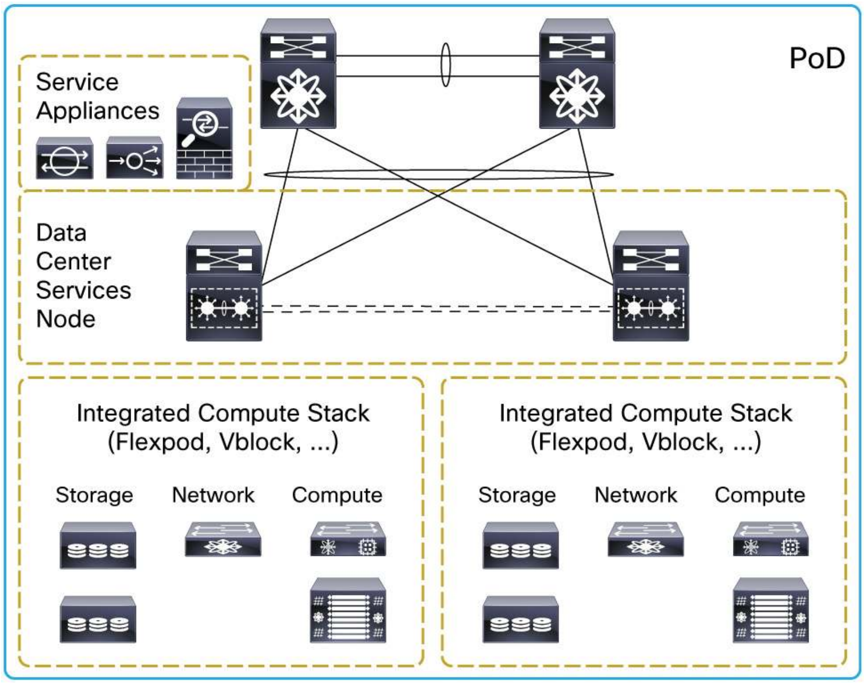
- Modular building blocks
- Resilient network fabric
- Multilayer end-to-end security
- Intelligent network-based services
- Efficient data center interconnection for business continuity
- Comprehensive cloud service management
- Integrated applications and services

Modular Building Blocks: Integrated Systems, Points of Delivery (PoDs), and Data Centers

The Cisco VMDC architecture builds on existing integrated system components such as FlexPod (using the Cisco UCS platform and NetApp storage) and Vblock™ Infrastructure Packages (using the Cisco UCS platform and EMC storage, integrated through the Virtual Computing Environment (VCE) coalition). In both cases, VMware software is used for virtualization; however, other hypervisors such as Microsoft Hyper-V, Red Hat KVM, and Citrix XenServer can also be used in designing basic integrated system building blocks. The Cisco VMDC architecture supports all variations.

Another modular building block of the Cisco VMDC architecture is the point of delivery (PoD), as shown in Figure 2, which contains standardized computing, storage, and networking components, as predefined integrated FlexPod or Vblock systems, and customized computing and storage systems, as needed by the deployment. The PoD concept and architecture is not limited to Cisco UCS and can be modified and extended to include other computing and storage stacks.

Figure 2. Point of Delivery

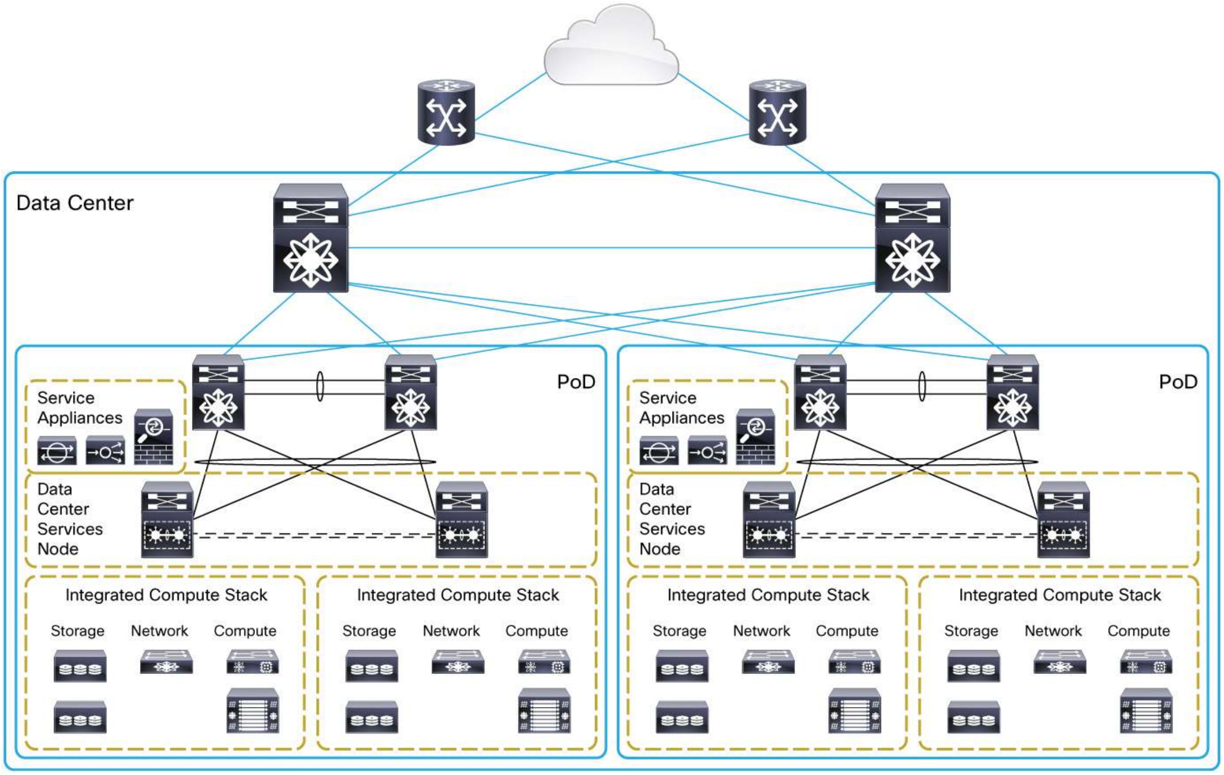

PoD
Service Appliances
Data Center Services Node
Integrated Compute Stack (Flexpod, Vblock, ...)
Storage
Network
Compute
Integrated Compute Stack (Flexpod, Vblock, ...)
Storage
Network
Compute

PoDs can contain localized network-based services such as firewalls and load balancers. PoDs can be created to house different application or service loads. Each PoD can be mapped to a class of applications, such as IT applications (print and file services, for example) or dedicated application servers (for SAP, for example). For orchestration and automation, a PoD represents a shared resource pool in a common administrative domain and can be autodiscovered by the operation software and configured for the specific defined service profile. Factors that go into PoD sizing and definition include:

- Storage capacity: Balance of computing needs to storage I/O operations per second (IOPS)
- Computing capacity: VMware vSphere cluster sizing and VMware vCenter domain management considerations
- Layer 2 scale considerations: MAC address and Address Resolution Protocol (ARP) capacity and VLAN scaling budgets
- Service insertion requirements: Scale and performance of network-based services such as load balancing and firewalling; a PoD may have its own dedicated set of load balancing and firewall service engines
- Application requirements: Requirements of specific applications; for example, some PoDs can be dedicated to VDI, and others can be dedicated to media applications
- Management requirements: Some PoDs can be dedicated to specific functions such as management

Multiple PoDs can be connected together to make up a data center, as shown in Figure 3. To design the optimal network for PoD connectivity, organizations need to consider the data center scale, network resiliency and tolerance to failure, security through traffic separation and protection, consumer and operator access control, and traffic characteristics and requirements of the applications and services that are hosted in the PoDs. The Cisco VMDC architecture provides all necessary details for these design considerations in a modular fashion, hence enabling creation of data centers that can grow and expand with ease.

Figure 3. Connecting Multiple PoDs



In addition to the basic connectivity within a data center, which may span multiple buildings in a campus or metropolitan network, the Cisco VMDC architecture specifies optimal connectivity between multiple sites that can be separated by farther distances. These specifications are part of the Cisco DCI module of Cisco VMDC. Use of resilient, secure, and efficient DCI methods enables application mobility at scale and the capacity to provide disaster recovery and business continuance.

Resilient Network Fabric: Scalable and Flexible

In the network layer, Cisco VMDC architecture uses best practices in network design, such as hierarchical campus designs, as well as innovative new technologies, such as Cisco FabricPath, to create a flexible, resilient, and scalable network fabric. Cisco VMDC provides multiple design options for the network layer that customers can use based on their specific requirements.

Hierarchical designs have been commonly used in networking to achieve scalability and high availability, and they are used similarly in Cisco VMDC to create a robust network framework for the data center. In a hierarchical design, at the PoD the Cisco VMDC network is organized into core, aggregation, and access layers.

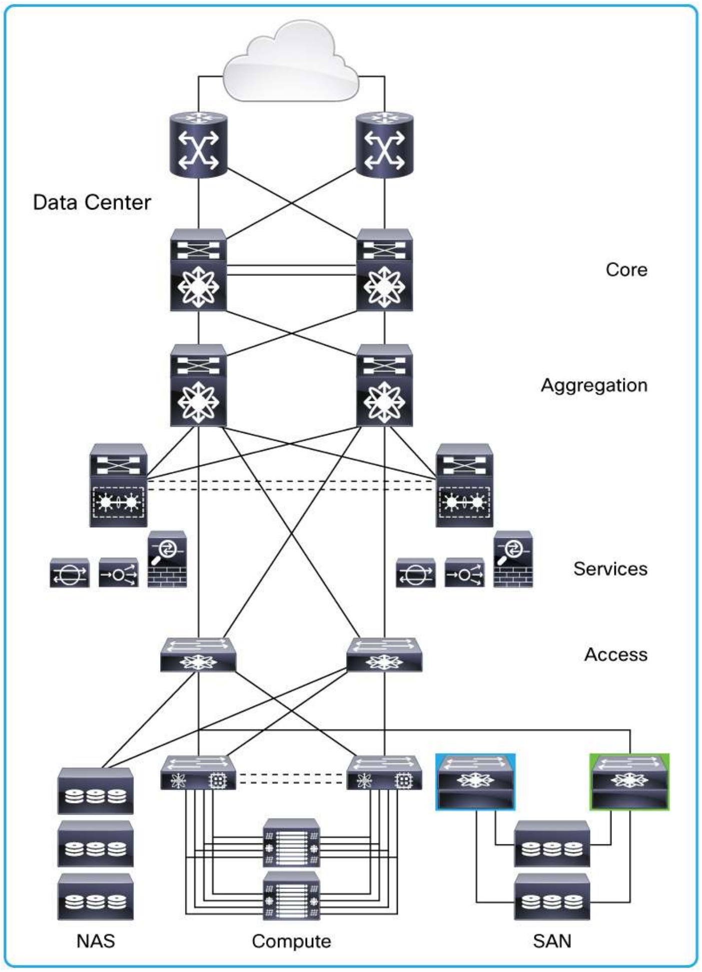
The core layer consists of pairs of high-performance, highly available chassis-based switches providing rapidly converging Layer 3 switching for IP traffic for various functional blocks of the network, such as intracampus, Internet edge, and WAN traffic.

The aggregation layer provides connectivity for the access-layer switches in the server farm, and aggregates them into a smaller number of interfaces to be connected to the core layer. In most data center environments, the aggregation layer is the transition point between the purely Layer 3 routed core layer, and the Layer 2-switched access layer. IEEE 802.1Q trunks extend the server farm VLANs between the access and aggregation layers. The aggregation layer also provides a common connection point for inserting services into the data flows between clients and servers or between tiers of servers in a multitier application.

The access layer of the network provides connectivity for server farm end nodes residing in the data center. Design of the access layer is tightly coupled to decisions on server density, form factor, and server virtualization, which can result in higher interface-count requirements. Traditional data center access-layer designs are strongly influenced by the need to locate switches in a way that most conveniently provides cabling connectivity for racks full of server resources. The most commonly used traditional approaches for data center server farm connectivity are end-of-row, top-of-rack, and integrated switching. Each design approach has advantages and disadvantages, and many enterprises use multiple access models in the same data center facility as dictated by server hardware and application requirements.

The data center network is less concerned with distributing network access across multiple geographically disparate wiring closets and is more focused on aggregating server resources and providing an insertion point for shared data center services. This model uses redundant switches at each layer of the network topology for device-level failover, creating a highly available transport between end nodes. Data center networks often require additional services beyond basic packet forwarding, such as server load balancing, firewall, and intrusion prevention. These services are introduced as modules populating a slot of one of the switching nodes in the network or as standalone appliance devices. Each service approach also supports the deployment of redundant hardware to preserve the high-availability standards set by the network topology. Figure 4 illustrates the hierarchical network design for larger data centers.

Figure 4. Hierarchical Network Design



Multilayer End-to-End Security

Successful deployment of cloud architectures depends heavily on complete end-to-end security of both the data center infrastructure and the virtualized environments that host the cloud consumer's application and service loads. The Cisco VMDC architecture addresses the security challenges by providing a complete framework for end-to-end security at multiple layers of the network.

A proper security approach requires deployment of a number of complementary security services at appropriate points in the data center network. These data center security requirements include:

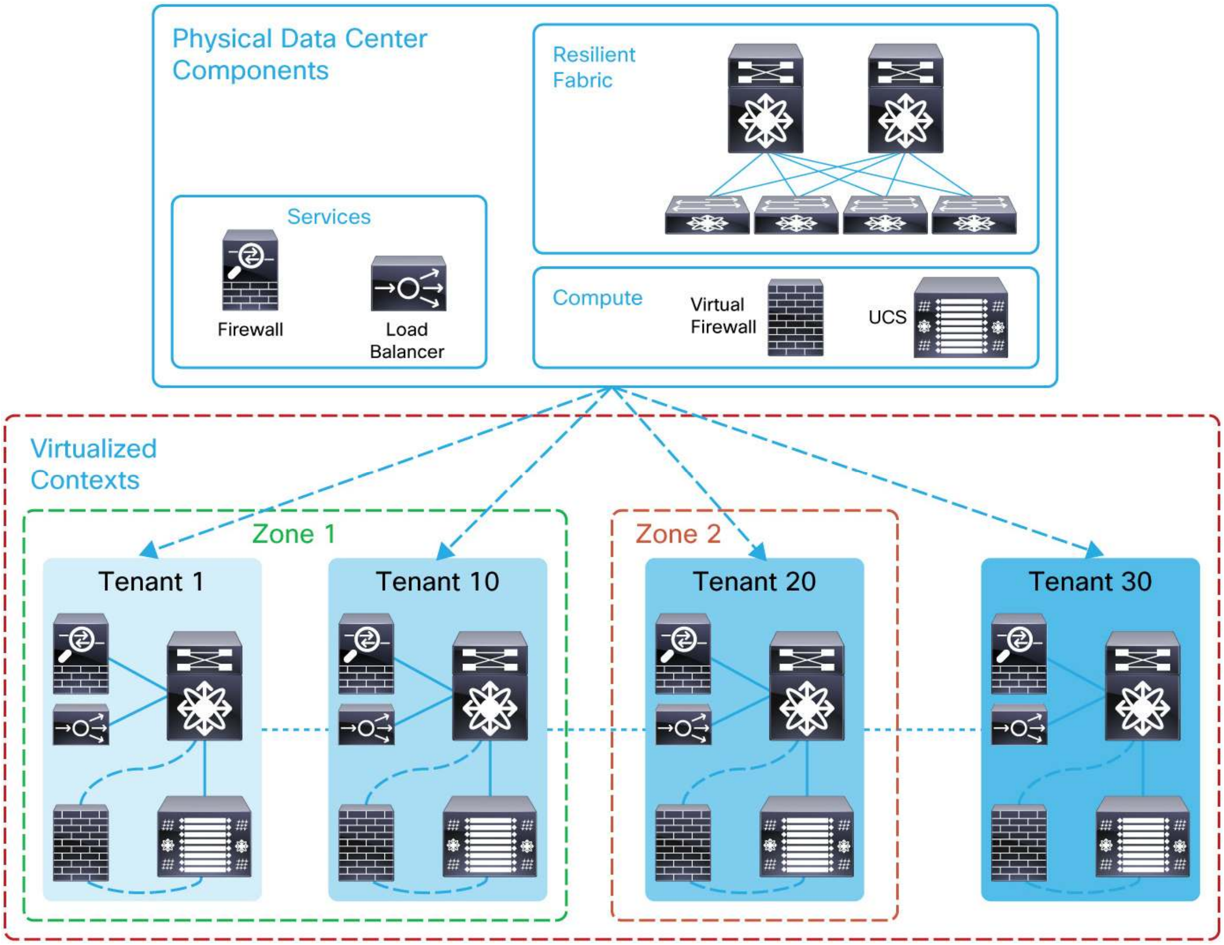
- Defending the data center from unauthorized users and outside attacks
- Preventing intrusion and data containing malware
- Defending the tenant edge with a proven firewall to secure the virtual and cloud infrastructures
- Assigning virtual machines to segmented trust zones within the virtual network and enforcing access policies at the virtual server level
- Providing centralized multitenant policy management
- Supporting virtual machine mobility

- Securing access to the virtualized data center and applications
- Providing a security solution that scales with the rest of the cloud-ready infrastructure
- Separating security, network, and server administrator duties

The Cisco VMDC architecture uses Cisco's physical and virtual security portfolio, which includes the Cisco ASA 5585-X Adaptive Security Appliance, Cisco ASA 1000V Cloud Firewall, Cisco Virtual Secure Gateway (VSG), Cisco Nexus 1000V Series Switches, and Cisco Virtual Network Management Center (VNMC) for consistent physical and tenant edge and intratenant security and policy management. Cisco vPath through the Cisco Nexus 1000V Series Switch improves secure agility and efficiency, and dynamic context-aware multitenant management security is available using Cisco VNMC.

For multitenancy, a dedicated infrastructure traditionally is deployed for each tenant that is hosted. However, this approach does not scale well because of cost, complexity to manage, and inefficient use of resources. In Cisco VMDC, multiple tenants in a common infrastructure can efficiently use shared resources to achieve lower costs. Each tenant may require path isolation for security and privacy from others sharing the common infrastructure. Logical separation or virtualization, which is a fundamental concept for multitenancy is achieved in the Cisco VMDC architecture at the networking, computing, and storage levels (Figure 5).

Figure 5. Multitenancy Design



Intelligent Network-Based Services

The Cisco VMDC reference architecture provides an open and flexible model for integrating intelligent network services such as server load balancing (SLB) and firewall security. These services can be integrated using either appliances or service modules. Each tenant using the Cisco VMDC infrastructure is entitled to some computing, networking, and storage resources according to the SLA. One tenant may have higher SLA requirements than another based on a business model or organizational hierarchy. The Cisco VMDC architecture helps ensure that tenants receive their subscribed SLAs while their data, communication, and application environments are securely separated, protected, and isolated from other tenants.

Efficient Data Center Interconnection for Business Continuity

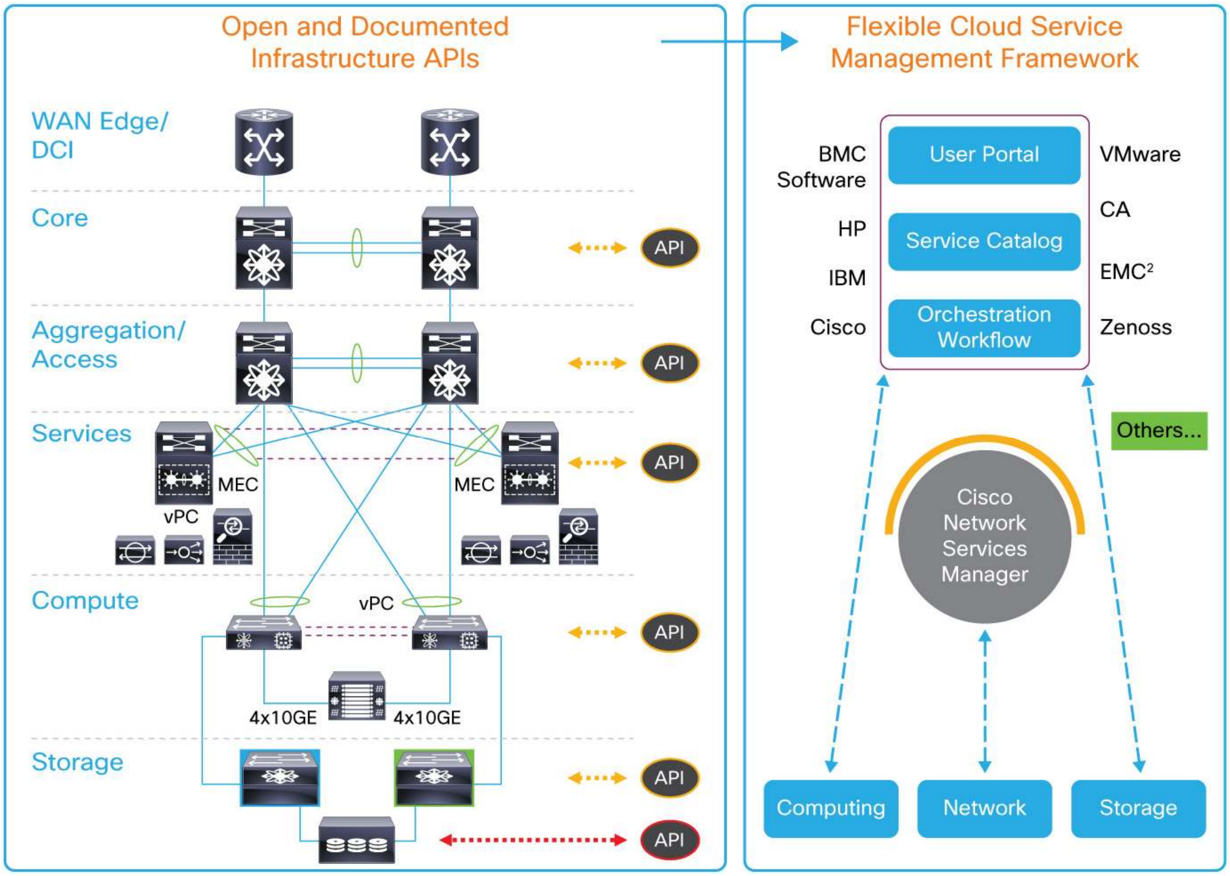
Cisco DCI solutions enable cloud deployments to meet business continuity and corporate compliance objectives through transparent connectivity between geographically distributed data centers that can function as backups in the event of massive failure in a disaster scenario. These solutions transparently extend LAN and SAN connectivity and provide accelerated, highly secure data replication, server clustering, and workload mobility between geographically dispersed data centers. The Cisco VMDC architecture supports multiple DCI options including the following:

- Point-to-point and point-to-multipoint interconnection using virtual switching system (VSS), vPC, and optical technologies
- Point-to-point interconnection using Ethernet over Multiprotocol Label Switching (EoMPLS) natively (over an MPLS core) and over a Layer 3 IP core
- Point-to-multipoint interconnections using virtual private LAN services (VPLS) or advanced VPLS (A-VPLS) natively (over an MPLS core) or over a Layer 3 IP core

Comprehensive Cloud Service Management

The vision and promise of cloud computing can be achieved only through robust and complete service management enabling automated provisioning of cloud consumer instances and resource use monitoring to enforce SLAs. Security and high availability of these management operations have to be ensured to give providers, operators, and consumers confidence in the use of the cloud. Furthermore, the service management components have to be able to build on a highly flexible and varied set of infrastructure components. To facilitate cloud service management, Cisco provides open and documented APIs for all infrastructure components, which Cisco and partner service management software developers can use to provide necessary cloud service management functions (Figure 6).

Figure 6. Enabling Comprehensive Management and Orchestration Suites Through Open APIs



Infrastructure Abstraction

Cisco Network Services Manager (NSM) is designed to help enable customers to organize their network resources into a flexible multitenant infrastructure that integrates the network with their existing IT operational tools and processes. The Cisco NSM network abstraction layer allows customers to automatically provision a set of network features into an end-to-end topology, or network container, much more easily and quickly than previously possible with template- and script-based systems, dramatically reducing network operating costs and the potential for misconfiguration while optimizing capacity utilization and accelerating service delivery.

Network infrastructure can now be virtualized and fully automated to support multitenant data center deployments through the use of network hypervisor technology. Cisco NSM extends the capabilities of traditional network hypervisors by helping enable customers to create dynamic, automated network containers, providing security, partitioning, and access control: the building blocks needed to provide ITaaS for any class of customer.

Cisco NSM offers a flexible, policy-based approach to the management and control of network services. This approach is achieved by abstracting the components needed to build an isolated virtual network infrastructure for each tenant. Through an administrative interface, Cisco NSM helps enable administrators to dynamically define and control sets of features from across multiple physical and virtual platforms in combination with behavior policies that support:

- Creation of different levels of service capability, or service tiers, for tenant use
- Definition of the capabilities and resources available in each tier
- Structuring of a system of containment tailored to tenant application and deployment model needs

Infrastructure Orchestration and Automation

Cloud service orchestration is a multidomain configuration abstraction layer that sits on top of the cloud data center infrastructure. This abstraction layer enables a portal-based configuration model in which the customer subscribing (application-hosting community) to the infrastructure can choose from a set of configurable, access-controlled services. On the basis of these choices, configuration actions are run across multiple domains and for the devices within these domains that together make up the service as represented in the customer-facing portal.

Orchestration (integration across the domain tools) is fundamental because there is no single tool in the data center that can configure the bundled services presented within the service catalog end to end. Orchestration coordinates the configuration requirements on top of the domain tools and helps ensure that all the services defined in the service catalog or portal are appropriately sequenced and correctly run within each specific domain. Moreover, orchestration aggregates all the individual service components in the service catalog as a total services pool and determines whether sufficient resources exist across all the components to provide the service.

The basic components used for managing this environment are:

- User and administration portal interface along with an equivalent API
- Workload and automation engine built alongside a data model system based on a high-performance database engine (managing policies, cloud resources, and the automation data model)
- Set of domain managers providing domain-level resource and automation management

These components connect to the Cisco VMDC architecture, based on the Cisco UCS platform, the Cisco Nexus Family of data center switches and routing systems, the Cisco ASA and Cisco Application Control Engine (ACE) network services deployed as a data services node (DSN), and the Cisco Aggregation Services Router (ASR) and Carrier Routing System (CRS) core routing platforms deployed as specified in the Cisco VMDC 2.0 infrastructure design and implementation guide. In addition to the automation platform and physical infrastructure, the solution uses the VMware vSphere 5.0 computing virtualization infrastructure, which provides greater computing scalability than the physical Cisco UCS infrastructure on its own.

These infrastructure components and systems are then automated based on either an administrative or tenant request delivered through the portal interface (or an equivalent request delivered through the northbound portal API), providing end-to-end service deployment often consisting of the deployment of a single or a set of computing components and changes to or deployment of specific network services components.

Infrastructure Assurance

One of the main barriers to deployment of virtual private cloud services is lack of trust in the quality of virtualized services that can be offered over the cloud. Providers want the capability to offer end-to-end contractual SLAs with confidence, which in turn will increase cloud consumers' trust in cloud services. To address this challenge, cloud deployments must be secured with end-to-end monitoring and service-level assurance capabilities. These functions should enable cloud providers to monitor their cloud deployments to achieve optimal fault troubleshooting and recovery and resource allocation and measurement, and enable consumers to monitor their resource use. Only with a complete assurance solution can end-to-end SLAs be defined, offered, and fulfilled.

Cisco provides a full service assurance solution based on Cisco and partner tools and built on of the Cisco VMDC architecture. The solution offers the following functions:

- Monitoring of devices in the data center and network (Cisco UCS, Cisco Nexus 7000 Series Switches, Cisco MDS 9000 Family, etc.)
- Monitoring of subcomponents of devices and their relationships (Cisco UCS chassis, blades, fabric interconnects, etc.)
- Monitoring of logical entities such as tenants
- Tenant-based service-impact analysis (SIA) model for computing (mapping of the tenant virtual machine to the service affecting dedicated and shared VMware vCenter and Cisco UCS Manager managed resources, etc.)

To fully automate operating tasks, assurance products need to have visibility into all the components that work together to deliver the service. Segmented visibility will always exist and present challenges in the cloud environment due to business and ownership boundaries. To solve visibility challenges, the Cisco assurance software provides consolidated monitoring and data collection in the following ways:

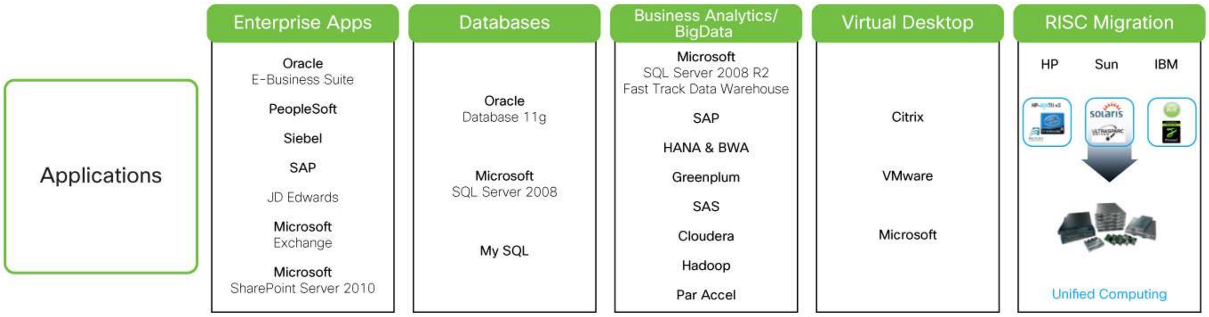
- Monitors all domains (applications, computing, storage, and network) and provides a single pane to monitor components from various domains
- Collects comprehensive fault and performance data and correlates it to accomplish higher functions such as root-cause analysis (RCA) and SIA
- Monitors all available protocols and interfaces to collect valuable data; examples of data sources and protocols include SNMP, syslog, web services API, NetFlow, and customer-opened tickets

Consolidated monitoring provides the visibility necessary to enable the assurance system to provide more value still achieving segmentation of operations through role-based access control (RBAC) and flexible and configurable filtering capabilities.

Integrated Applications and Services

Ultimately, a complete and robust cloud ready infrastructure is one that can offer multiple applications and services to large groups of consumers on the same infrastructure. The applications that have been validated on the Cisco UCS platform and which can run in the Cisco VMDC architecture are shown in Figure 7.

Figure 7. Applications Validated for Cisco UCS and Cisco VMDC



Enterprise Apps	Databases	Business Analytics/ BigData	Virtual Desktop	RISC Migration
Oracle E-Business Suite	Oracle Database 11g	Microsoft SQL Server 2008 R2 Fast Track Data Warehouse	Citrix	HP
PeopleSoft	Microsoft SQL Server 2008	SAP	VMware	Sun
Siebel	My SQL	HANA & BWA	Microsoft	IBM
SAP		Greenplum		
JD Edwards		SAS		
Microsoft Exchange		Cloudera		
Microsoft SharePoint Server 2010		Hadoop		
		Par Accel		

In addition, Cisco VMDC architecture is used as the basis for validation of other, more complex applications and services, including unified communications, hosted collaboration systems, Virtualized Desktop media data centers, video surveillance, and telepresence.

The Cloud Infrastructure Validation Lab

Cisco VMDC and related solutions are tested and validated for end-to-end capabilities, real-world scalability, and optimized performance at the Cisco Cloud Validation Facilities at Research Triangle Park, in Raleigh, North Carolina. The facility is organized on the basis of Cisco VMDC architecture with BMC Cloud Lifecycle Management (CLM) orchestration and automation tools, and provides “development-test-as-a-service” environment to various Cisco and partner groups that need a cloud environment for development and validation of their solutions.

Cisco VMDC architecture conforms to the Cisco Validated Design guidelines for end-to-end system validation and documentation. The Cisco Validated Design status indicates that the solution has undergone rigorous design analysis and validation testing to help ensure end-to-end completeness of functions as well as overall quality. The scope of validation testing for Cisco VMDC and associated solutions includes:

- Verification of functions across the entire data center for SAN and NAS designs: End-to-end feature and integration validation including QoS for all data center network layers, from the access layer to the WAN edge, on all platforms; and VMware ESX and virtual machine provisioning, bootup, and maintenance and SAN storage and network-attached storage (NAS) design verification
- Disaster recovery scenario validation: Verification of the capability to transparently move data center workloads for business continuance (active-backup scenario)
- Automation validation: Validation of service orchestration, and portal, service catalog validation with element manager integration for computing and networking
- Data center services function validation: Validation of service-tier offerings with data center services node (firewall, load balancing, etc.)
- Failover scenario validation: Validation of redundancy designs with baseline steady-state traffic (routing, vPC and multichassis EtherChannel (MEC), Equal-Cost Multipath (ECMP), VSS, HSRP, active-active service modules, clustering, etc.)
- Security validation: End-to-end security validation for various components
- Scalability verification: Validation of multidimensional scalability (VLAN, MAC addresses, HSRP, routes, contexts, virtual machines, etc.) within the scope of the architecture

Cisco VMDC Releases

- **Release 1.0, 1.1:** Introduces architecture foundation for deploying virtualized and multi-tenanted data centers for cloud-based services. It supports high availability, elasticity, and resiliency of virtualized compute, network, and storage services.
- **Release 2.0:** Expands release 1.1 by adding infrastructure orchestration capability using BMC software's Cloud Lifecycle Management, enhances network segmentation and host security, uses integrated compute stacks as building blocks for the PoD, and validates compact and large PoD scale points.
- **Release 2.1:** Generalizes and simplifies release 2.0 architecture for a multi-tenant virtualized data center used for private cloud. Improvements include multicast support, simplified network design, jumbo frame support, improved convergence, performance, scalability for private cloud, quality of service (QoS) best practices, and increased design flexibility with multi-tenant design options.
- **Release 2.2:** Builds on top of releases 2.0 and 2.1 for a common release supporting public, private, and hybrid cloud deployments. Enhancements include "defense in depth" security, multi-media QoS support, and Layer 2 (VPLS) based data center interconnect (DCI).
- **Release 2.3:** Defines a smaller, lower price approach to deploying the Unified Data Center module of the 2.x architecture track. Design to address smaller Enterprise and Tier 2/3 Service Provider customers.
- **Release 3.0/3.0.1:** Introduces a Cisco VMDC design based on Cisco FabricPath for private cloud deployments, providing simple tenant containers suitable for enterprise deployment models, firewalls, and load-balancing services as well as high availability and security. 3.0.01 release includes 3.0 and incremental updates.

For More Information

For more information about Cisco VMDC and access to the relevant documents, please visit http://www.cisco.com/go/vmdc.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-714729-02 04/13