Cisco Virtualized Multi-Tenant Data Center Solution 2.2

Data Sheet

Overview

The Cisco® Virtualized Multi-Tenant Data Center (VMDC) architecture is a set of specifications and guidelines for creating and deploying a scalable, secure, and resilient infrastructure that addresses the needs of cloud computing. To develop a trusted approach to cloud computing, Cisco VMDC combines the latest routing and switching technologies, advancements in cloud security and automation, and leading edge offerings from cloud ecosystem partners. Cisco VMDC enables service providers (SPs) to build secure public clouds and enterprises to build private clouds with the following benefits:

- Reduced time to deployment—Provides a fully tested and validated architecture that enables 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 multi-tenant environment using a comprehensive automation framework with portal-based resource provisioning and management capabilities.
- Improved operational efficiency—Integrates automation with multi-tenant resource pools (compute, network, and storage) to improve asset use, reduce operational overhead, and mitigate operational configuration errors.

VMDC 2.2 Solution Highlights

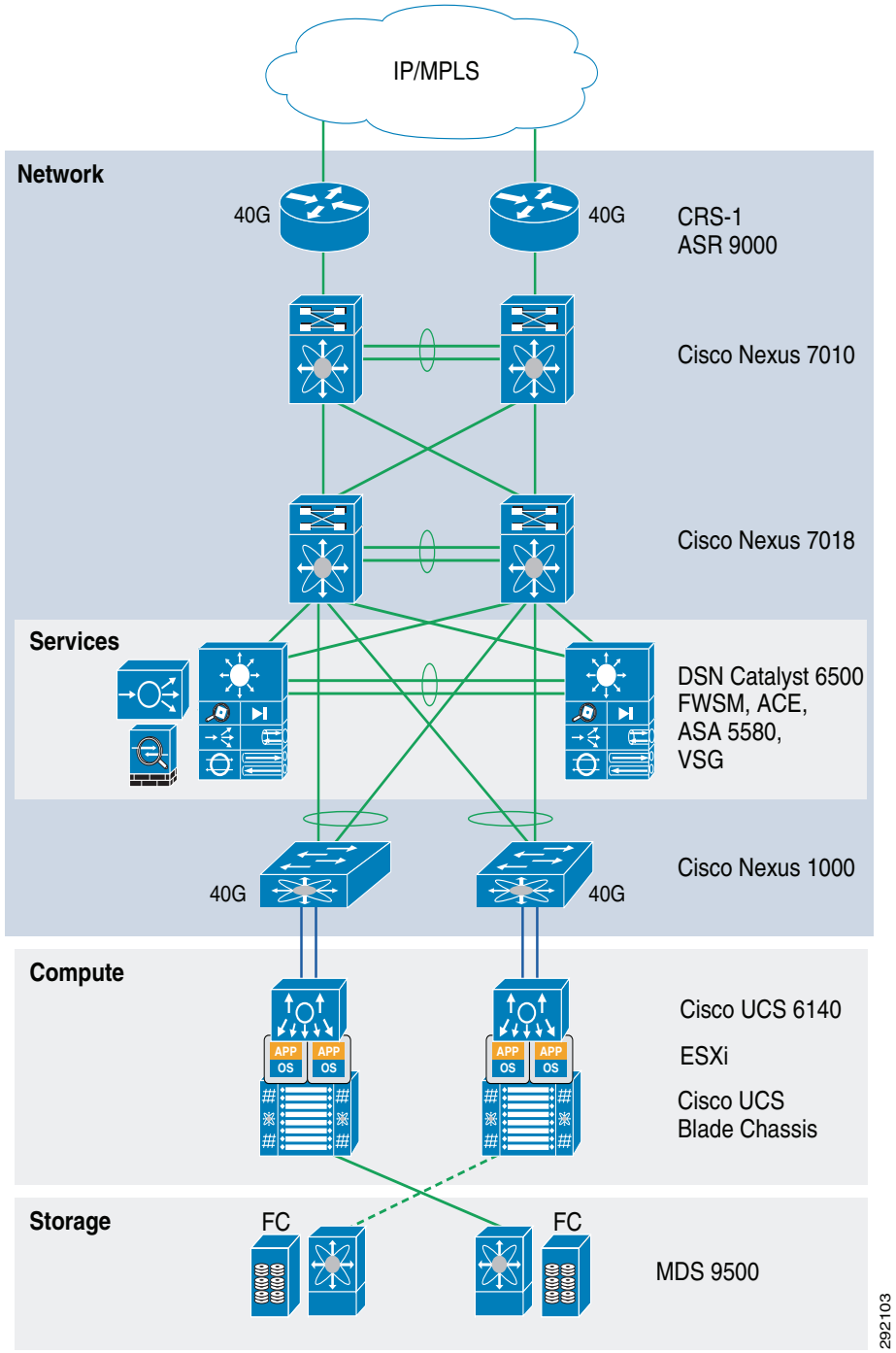
Highlight	Details of Release 2.2
Validated data center design for enterprise or service provider scalability	Builds on top of the baseline that was established in release 2.0, validating standard data center architectures in a multi-tier, Layer 3-centric network architecture with compact to large scale specifications, using standard integrated compute stacks such as Cisco FlexPod™ and VCE Vblock™ Infrastructure Packages.
Enhanced security services for improved secure multi-tenancy	Extends the security model that was established in release 2.0, which among other benefits enabled secure multi-tenancy by adding "defense in depth" strategy using Cisco Virtual Security Gateway (VSG) and Cisco Adaptive Security Appliances (ASA).
Differentiated services	Supports the same set of differentiated services defined in release 2.0 and 2.1, Gold, Silver, Bronze, and Palladium.
Multi-media application support	Extends and validates the campus quality of service (QoS) model to the data center, enabling higher quality of experience for multi-media applications such as VoIP, video, and hosted collaboration.
Layer 2 data center interconnect	Validates Virtual Private LAN Services (VPLS) and Ethernet over Multiprotocol Label Switching (EoMPLS) on the Cisco Aggregation Series Router 9000 (ASR 9000) for data center interconnect, enabling SPs to seamlessly connect their data centers through their IP-NGN networks for intra-data center connectivity as well as hybrid cloud support for connecting enterprise data centers.
Scalability	Builds on top of the release 2.0 baseline and revalidates the scalability of the large pod model for parameters such as VLANs, MAC addresses, Hot Standby Router Protocol (HSRP), routes, contexts, and virtual machines.
End-to-end security	Revalidates the end-to-end security validation that was designed in release 2.0 and extended with enhanced security services for secure multi-tenancy.
High availability	Revalidates failover scenarios and the high availability of the system as designed in release 2.0.
Platforms	Validates new platforms such as the ASR 9000 for data center edge, Cisco ACE30 Application Control Engine Module for virtual Server Load Balancing (vSLB), ASA5585X for virtual firewall (vFW), and VSG for virtual machine (VM) security.

Solution Scale

The following table summarizes the Cisco VMDC 2.2 scalability validation.

Feature	Compact Pod Design	Large Pod Design
Tenants	32	152
Servers per pod	64	512
Virtual machines per pod	1440	11,520
VLANs per pod	180	520
Virtual firewall contexts	6	8
Virtual load balancers	16	24
Server VLANs	180	200
MAC addresses	12,000	24,000
HSRP gateway instances	196	504
Routing protocol scale	256 Open Shortest Path First (OSPF) neighbors	480 Border Gateway Protocol (BGP) peers

Solution Topology



Solution Components

Features	Components
Network	• Cisco Nexus® 7010, 7018, NXOS 5.2.1 • Data center services node—Cisco Catalyst® 6509-E Switch (with Virtual Switching System [VSS]), IOS 12.2(33)SXJ • Cisco ASR 9000, XR 4.1.0 • Cisco ASR 1006, XE 3.4.0 15.1(3)S
Services	• Cisco Nexus 1000V switch, NXOS 4.2.1 SV1(1.4a) • Cisco Virtual Security Gateway, 4.2(1)SV1(2) • Cisco Virtual Network Management Center: 1.2(1b) • Cisco Adaptive Security Appliance 5585-60X, 8.4.2 • Cisco ACE30 Application Control Engine Module, A 4.2.1
Compute	• Cisco Unified Computing System™ (UCS™), 1.4(2b) • Cisco UCS 5108 Blade Server Chassis • Cisco UCS 6140 Fabric Interconnect • Cisco UCS B200 M1 Blade Server • Cisco UCS M71KR-E Emulex Converged Network Adapter (CNA) • Cisco UCS M81KR Virtual Interface Card (VIC)
Virtualization	• VMware® vSphere™ 4.1 U1 • VMware ESXi 4.1U1 Hypervisor • Cisco Nexus 1000V switch (virtual access switch)
Storage	• Cisco MDS 9513 Multilayer Directors, NXOS 5.0.4d • EMC® Symmetrix® VMAX™ with Engenuity 5874 • NetApp® FAS3170 and NetApp FAS6080 with ONTAP® 8.0.2

Layered Security Strategy

Layer	Security Options
Data center edge	• Secured access and perimeter firewall • MPLS • Layer 2 and Layer 3 VPNs • SSL and IP Security (IPsec) VPNs • Infrastructure security to protect device, traffic plane, and control plane
Core and aggregation	• Device virtualization for control-, data-, and management-plane segmentation • Infrastructure security to protect device, traffic plane, and control plane services
Services	• Server load balancing to mask servers and applications • Application firewall to mitigate cross-site scripting (XSS), HTTP, SQL, and XML attacks • Infrastructure security to protect device, traffic plane, and control plane
Aggregation and access	• Secure, authenticated connections • Dynamic Address Resolution Protocol (ARP) inspection • Dynamic Host Configuration Protocol (DHCP) snooping • IP source guard • Zone security (private VLANs, port switching, and port profiles with access control lists) • Infrastructure security to protect device, traffic plane, and control plane
Virtual access	• Policy-based virtual machine connectivity • Mobile virtual machine security and network policies • Virtual firewall integration with Cisco Nexus 1000V switch
Compute	• Role Based Access Control • Application security
Storage and storage aggregation	• Fibre Channel Zoning

Differentiated Services—Example Service Tiers

Service	Bronze	Silver	Gold	Palladium
Tenant-specific network services	No additional services	Load-balancing services	Firewall and load-balancing services	Firewall and load-balancing services
Segmentation	One VLAN per client and a single virtual routing and forwarding (VRF) instance	Multiple VLANs per client and a single VRF instance	Multiple VLANs per client and a single VRF instance	Multiple VLANs per client with both a a public and private VRF instance
Data protection	None	Snap: Virtual copy (local site)	Clone: Mirror copy (local site)	Clone: Mirror copy (local site)
Disaster recovery	None	Remote replication (with specific recovery-point objective [RPO] or recovery-time objective [RTO])	Remote replication (any-point-in-time recovery)	Remote replication (any-point-in-time recovery)
Workload sizing (number of virtual machines per core)	4:1, 2:1, or 1:1	4:1, 2:1, or 1:1	4:1, 2:1, or 1:1	4:1, 2:1, or 1:1

Management and Automation

VMDC 2.2 is complemented by a set of orchestration, automation, and management software. For details contact your Cisco account representative.

For More Information

For more information about Cisco VMDC, visit http://www.cisco.com/go/vmdc and consult your Cisco account representative.