Preface

Revised: October 20, 2010

Overview

The Cisco Virtualized Multi-Tenant Data Center (VMDC) is a reference architecture that brings together core products and technologies from Cisco, NetApp, EMC, VMware, and BMC to deliver a comprehensive cloud solution. The Cisco VMDC 2.0 solution expands on the VMDC 1.1 solution. Key additions in 2.0 are integrated compute stacks as compute and storage building blocks and the validation of two scale points: Compact Pod and Large Pod. The solution also includes two additional implementation modules: a service portal and orchestration component and business continuance (disaster recovery) component. The VMDC 2.0 solution is described in a range of documents:

- Solution and Architecture Overview
- Design and Implementation Guides
  - Compact Pod Design
  - Compact Pod Implementation
  - Large Pod Design
  - Large Pod Implementation
  - Business Continuance Design
  - Service Orchestration Design

This preface contains the following topics:

Purpose of This Document

This document will help you design deployments of a private or public IaaS cloud data center based on the VMDC architecture. This Cisco-driven, end-to-end architecture defines how to create and manage flexible, dynamic pools of virtualized resources that can be shared efficiently and securely among different tenants. An orchestration solution creates a service portal that reduces resource provisioning and improves time-to-market (TTM) for IaaS-based services.

The Compact Pod design focuses on small to medium deployments with up to 32 tenants and up to 4,000 VM instances.

Audience

This document is intended for, but not limited to, network architects, systems engineers, field consultants, advanced services specialists, and customers who want to understand how to deploy a public or private cloud data center infrastructure.

Solution Objectives

The Cisco VMDC 2.0 solution addresses the following problems:

- **Resource utilization**. Traditionally, enterprises design their data centers using dedicated resource silos. These siloed resources include access switches, server racks, and storage pools assigned to specific applications and business units. This siloed approach results in inefficient resource use, where resource pools are customized per application, resulting in few shared resources. This design also cannot harness unused or idle resources, is complex to administer, and is difficult to scale, which results in longer deployment times. For enterprises and public cloud service providers, inefficient resource use increases capital and operational expenses, decreasing revenue margins.
- **Security guarantees**. In a multi-tenant environment, resource access must be controlled among tenants. This control is more challenging when resources are shared. Tenants need to be assured that their data and their applications are secure in highly virtualized systems.
- **Resource provisioning**. Manual provisioning often takes longer than four weeks to provision new resources. In many cases, this lengthy provision time fails to meet business agility and TTM requirements of enterprises and service providers.
- **Complex and expensive administration**. Today, network, server, security, and application administrators must collaborate to bring up new resources for each new or expanding tenant. In highly virtualized systems, collaboration based on manual methods does not scale, resulting in slow responses to business needs. It is complicated and time consuming to streamline tasks, such as manual configuration and resource provisioning. Also, resource churn increases capital and operating expenditures and overhead.

As enterprise IT departments evolve, they want a data center solution that supports rapid provisioning of resources that are efficiently shared and secured. Similarly, service providers want solutions that enable them to reduce TTM for new revenue-generating services and to improve ongoing operational expenses (OpEx). This document introduces an architecture that offers the flexibility to share common infrastructure among tenants while securely separating those tenants and data and enabling per-tenant differentiated services.

Related Documentation

The Cisco VMDC design recommends that general Cisco data center design best practices be followed as the foundation for IaaS deployments. The following Cisco Validated Design (CVD) companion documents provide guidance on such a foundation:

Data Center Design—IP Network Infrastructure

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html

Data Center Service Patterns

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_serv_pat.html

Security and Virtualization in the Data Center

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_sec_design.html

Designing Secure Multi-Tenancy into Virtualized Data Centers

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_dcVDDC.html

Enhanced Secure Multi-Tenancy Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/securecldg_V2.html

The following VMDC solution document provide additional details on the solution:

Cisco VMDC 1.1 Design and Deployment Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/vmdcDdg11.pdf

Cisco VMDC Solution Overview

http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/solution_overview_c22-602978.html

Cisco VMDC Solution White Paper

http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns836/white_paper_c11-604559.html

Vblock Infrastructure Solutions

http://www.acadia.com/solutions/vblock/index.htm

About Cisco Validated Designs

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.