Preface

The Cisco® Virtualized Multi-Tenant Data Center (VMDC) solution provides design and implementation guidance for enterprises deploying private cloud services and service providers building virtual private and public cloud services. The Cisco VMDC solution integrates various Cisco and third-party products that are part of the cloud computing ecosystem.

VMDC 2.2 is an incremental release, leveraging and only slightly modifying the architecture defined in the preceding parent 2.0 release. In this phase of the VMDC solution, we present incremental enhancements to the multi-tenant security models outlined in the previous 2.0 system release, introducing defense-in-depth firewalling utilizing the new Cisco Virtual Security Gateway in combination with the ASA appliance and reworking the end-to-end QoS framework to accommodate multimedia SaaS applications such as the Cisco Collaboration solutions. We also begin to examine issues of hybrid (public/private) interworking from the aspect of VM migration, and look at Service Provider (i.e., intra-organizational) Data Center Interconnect in the context of VPLS transport, focusing on Nexus 7000/ASR 9000 interoperability.

Product screen shots and other similar material in this document are used for illustrative purposes only and are VMAX (EMC Corporation), NetApp FAS3240 (NetApp), vSphere (VMware, Inc.), respectively. All other marks and names mentioned herein may be trademarks of their respective companies. The use of the word "partner" or "partnership" does not imply a legal partnership relationship between Cisco and any other company.

Introduction

Interest in cloud computing over the last several years has been phenomenal. For cloud providers, public or private, it will transform business and operational processes, streamlining customer on-ramping and time to market, facilitating innovation, providing cost efficiencies, and enabling the ability to scale resources on demand.

Cisco's Virtualized Multi-tenant Data Center (VMDC) system defines an end-to-end architecture, which an organization may reference for the migration or build out of virtualized, multi-tenant data centers for new cloud-based service models such as Infrastructure as a Service (IaaS).

The system builds upon these foundational pillars in terms of architectural approach:

- **Secure Multi-tenancy—**Leveraging traditional security best practices in a multi-layered approach to secure the shared physical infrastructure and those logical constructs that contain tenant-specific resources, while applying new technologies to provide security policy and policy mobility to the virtual machine level insures the continued ability to enforce and comply with business and regulatory policies, even in a highly virtualized multi-tenant environment.
- **Modularity—**A pod-based modular design approach mitigates the risks associated with unplanned growth, providing a framework for scalability that is achievable in manageable increments with predictable physical and cost characteristics, and allowing for rapid time-to market through streamlined service instantiation processes.
- **High Availability—**Building for carrier-class availability through platform, network, and hardware and software component level resiliency minimizes the probability and duration of service-affecting incidents, meaning that Private IT and Public Cloud administrators can focus on supporting the bottom line rather than fighting fires.
- **Differentiated Service Support—**Defining logical models around services use cases results in a services-oriented framework for systems definition, insuring that resources can be applied and tuned to meet tenant requirements.
- **Service Orchestration—**Dynamic application and re-use of freed resources is a key aspect of a Cloud-based operations model, thus the ability to properly represent abstractions of the underlying tenant-specific resources and services is a fundamental requirement for automated service orchestration and fulfillment; this is accomplished in the VMDC architecture through continued evolution of network container definitions which can be leveraged by in-house middleware and partner management solutions.

Intended Audience

This document is intended for, but not limited to, system architects, network design engineers, systems engineers, field consultants, advanced services specialists, and customers who want to understand how to deploy a public or private cloud data center infrastructure. This design guide assumes that the reader is familiar with the basic concepts of IP protocols, QoS, DiffServ and HA. This guide also assumes that the reader is aware of general system requirements and has knowledge of enterprise or service provider network and Data Center architectures.

Related Documents

The following documents are available for reference:

- Cisco Virtualized MultiTenant Data Center Design Guide Release 1.1
- Cisco Virtualized Multi-Tenant Data Center 2.0 Design and Implementation Guide
- Cisco Virtualized Multi-Tenant Data Center, Version 2.1, Implementation Guide
- Design Considerations for Classical Ethernet Integration of the Cisco Nexus 7000 M1 and F1 Modules
- Virtualized Multi-Tenant Data Center New Technologies - VSG, Cisco Nexus 7000 F1 Line Cards, and Appliance-Based Services

- Cisco Virtualized Multi-Tenant Data Center Implementation Guides, Releases 1.0-2.2 (available under NDA) are located at: http://sdu.cisco.com/systems/system.php?sysid=22
- Data Center Interconnect over MPLS, Ethernet or IP Transport documents are located at: http://www.cisco.com/en/US/netsol/ns749/networking_solutions_sub_program_home.html and at: http://www.cisco.com/en/US/netsol/ns975/index.html

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 http://www.cisco.com/go/validateddesigns.