CHAPTER 1

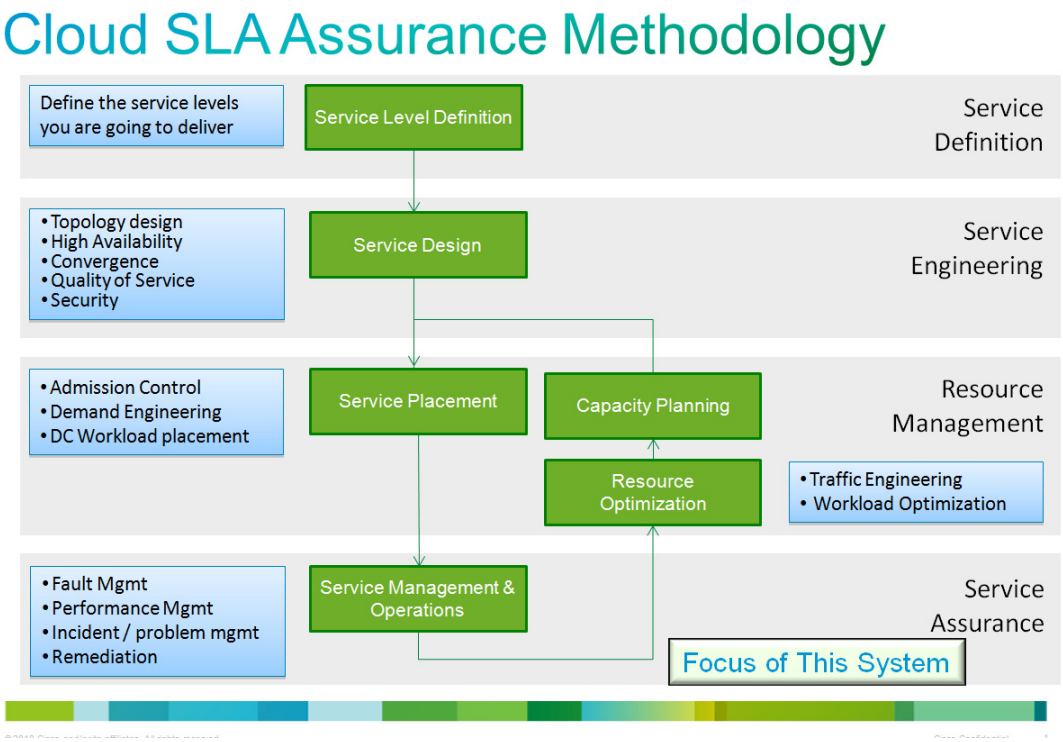
Introduction

In recent years, there has been a race by both traditional Service Providers (SPs) and public cloud providers such as Amazon to capture the cloud services market. SPs have identified the capability to offer Service Level Agreements (SLAs) as their key differentiator in the race for the cloud. In response, SPs are deploying virtual private cloud services accessed by Enterprises (cloud consumers) over the SP's IP/MPLS VPN network infrastructure. In addition, lack of trust had been identified as one of key barriers for Enterprises to purchase cloud services. In order to gain end customer trust of cloud services, it is important that a cloud provider offer customers visibility in the performance of their applications hosted in the cloud.

To offer SLAs necessary to realize the potential of virtual private cloud differentiation, SPs have to take measures both in engineering the service and in operating the service. The term "service assurance" is commonly used to refer to performance management and fault management, i.e., monitoring and reporting that the service levels are met and identifying/resolving service impacting faults. More generally, assurance means providing a high level of confidence that a commitment can be met; this encompasses more than just operation and management aspects, but also includes service engineering aspects.

Broader SLA assurance framework with all necessary functions to offer SLAs is illustrated in Figure 1-1. This framework includes service assurance as one of its building blocks, which is the focus of this system and this document. In addition to virtual private cloud opportunity, service assurance also plays a role in private clouds to enable efficient Day 2 operations and gain visibility necessary to optimize resources utilization.

Figure 1-1 Cloud SLA Assurance Methodology



Both Infrastructure as a Service (IaaS) and Software as a Service (SaaS) private and virtual private cloud services can be offered on top of the Cisco Virtualized Multi-Services Data Center (VMDC) architecture. The Cloud Service Assurance for Virtualized Multi-Services Data Center (CLSA-VMDC) system provides service assurance capabilities for VMDC, as well as private and virtual private cloud IaaS. This system can also be leveraged as a building block of application-based cloud services such as Cisco Hosted Collaboration Solution (HCS).

System Purpose

This document describes design and implementation guidelines for Cloud Service Assurance for Virtualized Multi-Services Data Center 2.2 (CLSA-VMDC 2.2), which is the first release of CLSA-VMDC and IaaS-based offers. This version of the system supports VMDC 2.2, VMDC 2.1, and earlier infrastructure architectures. CLSA-VMDC 2.2 is based on Zenoss Cloud Service Assurance (Zenoss CSA), which was built from the ground up for cloud technology management. Zenoss CSA is a service impact model-based system that allows for rapid new service introduction, tenant-based service assurance, consolidated monitoring of the VMDC infrastructure, and simple customizations that can be deployed without service down time via plugins called ZenPacks. Chapter # VMDC System Overview provides a brief review of the VMDC 2.2 system and its components. Chapter # CLSA-VMDC System Architecture provides an overview of the CLSA-VMDC system architecture.

Note While this CLSA-VMDC design and implementation guide references the VMDC 2.2 system, other versions of the VMDC system are supported. The CLSA-VMDC system also supports other Data Center (DC) designs, as well as the VCE VBlock and NetApp FlexPod stacks.

Zenoss CSA is a multi-tenant services system, and it offers real time SP aggregated dashboards as well as reporting capabilities. It can be deployed both in centralized and distributed architecture, and allows for incremental deployment growth. While it offers rich functionality for IaaS domains, the solution is lightweight and has open interfaces to allow for simple integration into existing Operations Support System (OSS) and ticketing systems with minimal cost. As such, this solution is positioned not as a replacement, but as a complement to existing Manager-of-Manager (MOM) systems (e.g., IBM Netcool), ticketing systems (e.g., BMC Remedy), and so on. Chapter # Zenoss Cloud Service Assurance Overview discusses the product architecture and provides an overview of the capabilities of the core assurance platform. Chapter # System Design Constraints discusses the system design constraints of CLSA-VMDC and describes the specific capabilities of the products used. Chapter # System Deployment provides details of a CLSA-VMDC deployment centered around a Zenoss CSA platform. Chapter # Operational Use Cases illustrates the service assurance use cases for VMDC device discovery, monitoring, service impact, and root cause analysis.

System Benefits

The key business benefits of CLSA-VMDC 2.2 and the respective technical functions that realize these benefits are illustrated in Figure 1-2 and discussed throughout this document.

Figure 1-2 Key Business Benefits of CLSA-VMDC 2.2