CHAPTER 1

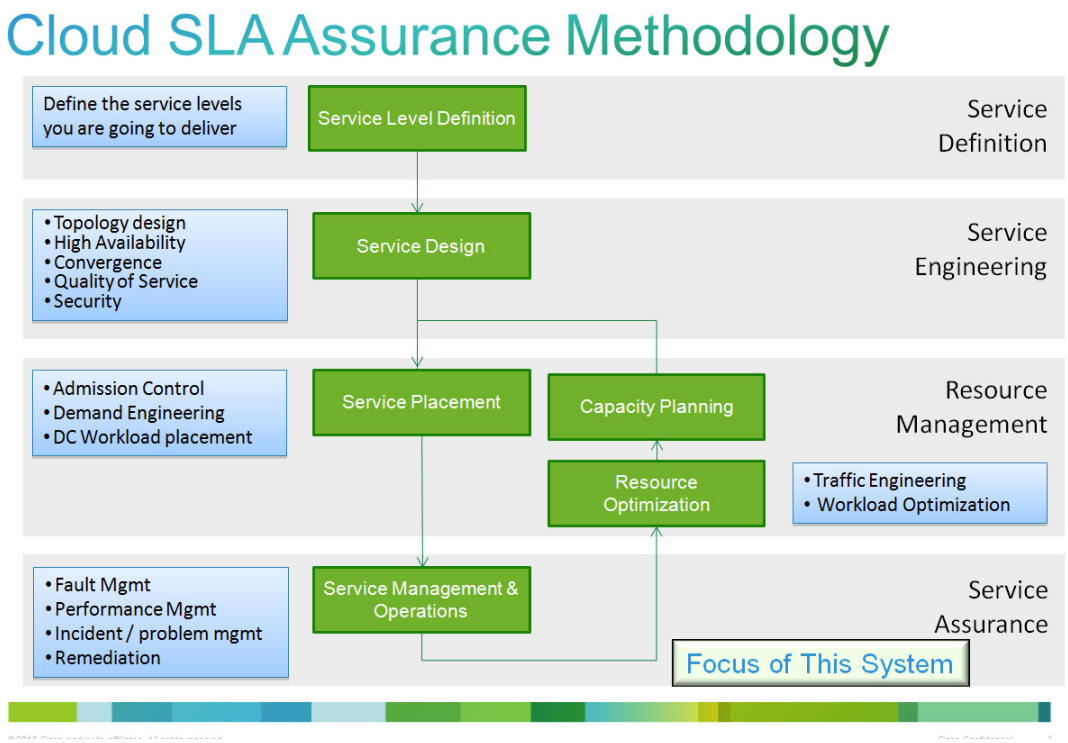
Introduction

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 the key barriers for Enterprises to purchase cloud services. 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.

SPs have to take measures both in engineering the service and in operating the service to offer their customers the SLAs necessary to realize the potential of virtual private cloud differentiation. 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.

The 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 the virtual private cloud opportunity, service assurance also plays a role in Enterprise 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 Virtualized Multiservice Data Center (VMDC) architecture. The Cloud Service Assurance for VMDC (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), Cisco Virtualization Experience Infrastructure (VXI), and SP TelePresence.

This chapter presents the following topics:

- System Purpose, page 1-2
- System Objectives, page 1-3
- Key Benefits of Cloud Service Assurance, page 1-4
- CLSA VMDC 2.3 Summary of Changes, page 1-7
- CLSA VMDC 3.0 Summary of Changes, page 1-8

System Purpose

This document describes design guidelines for Cloud Service Assurance for VMDC (CLSA VMDC). This version of the system supports VMDC 3.0, VMDC 2.2, VMDC 2.3, and earlier infrastructure architectures. CLSA VMDC is based on Zenoss Cloud Service Assurance (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.

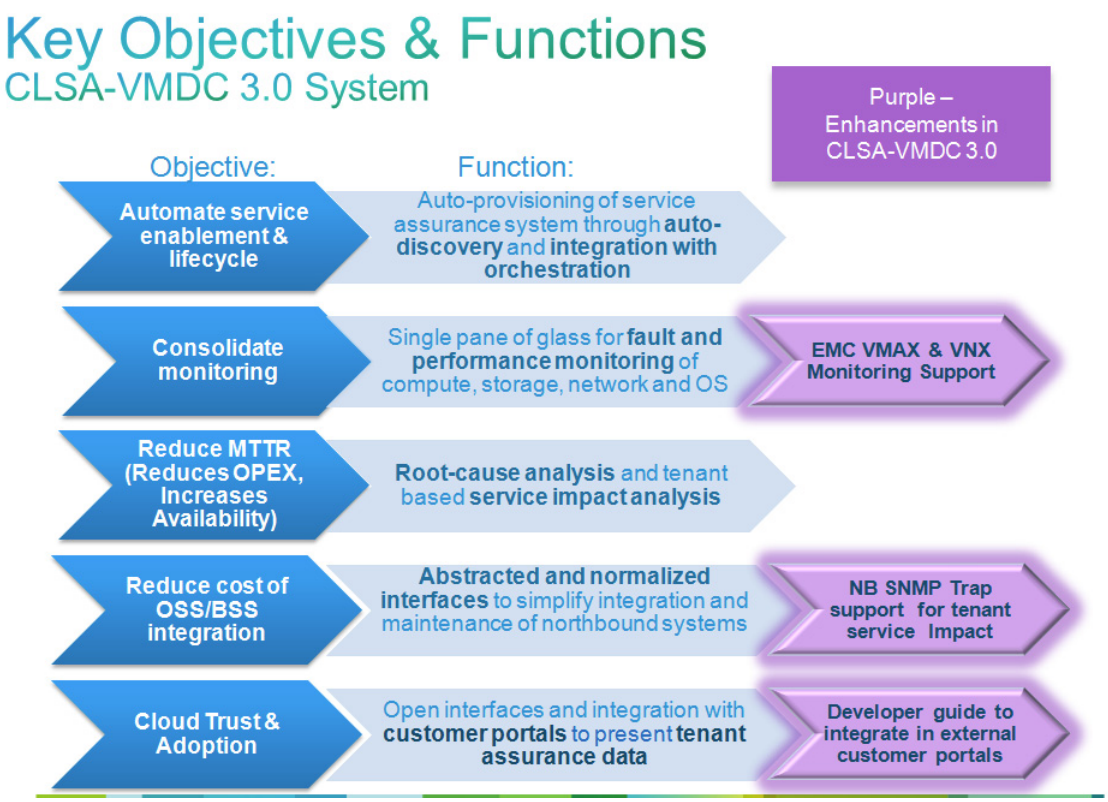
Note While the CLSA VMDC Design and Implementation Guide (DIG) references specific VMDC systems, previous versions of the VMDC system are also supported. The CLSA VMDC system also supports other Data Center (DC) designs, as well as the VCE Vblock and NetApp FlexPod stacks.

Zenoss CSA is a multiservice system that offers real time aggregated dashboards as well as reporting capabilities. The system 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.

System Objectives

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

Figure 1-2 Key Objectives and Functions of CLSA VMDC

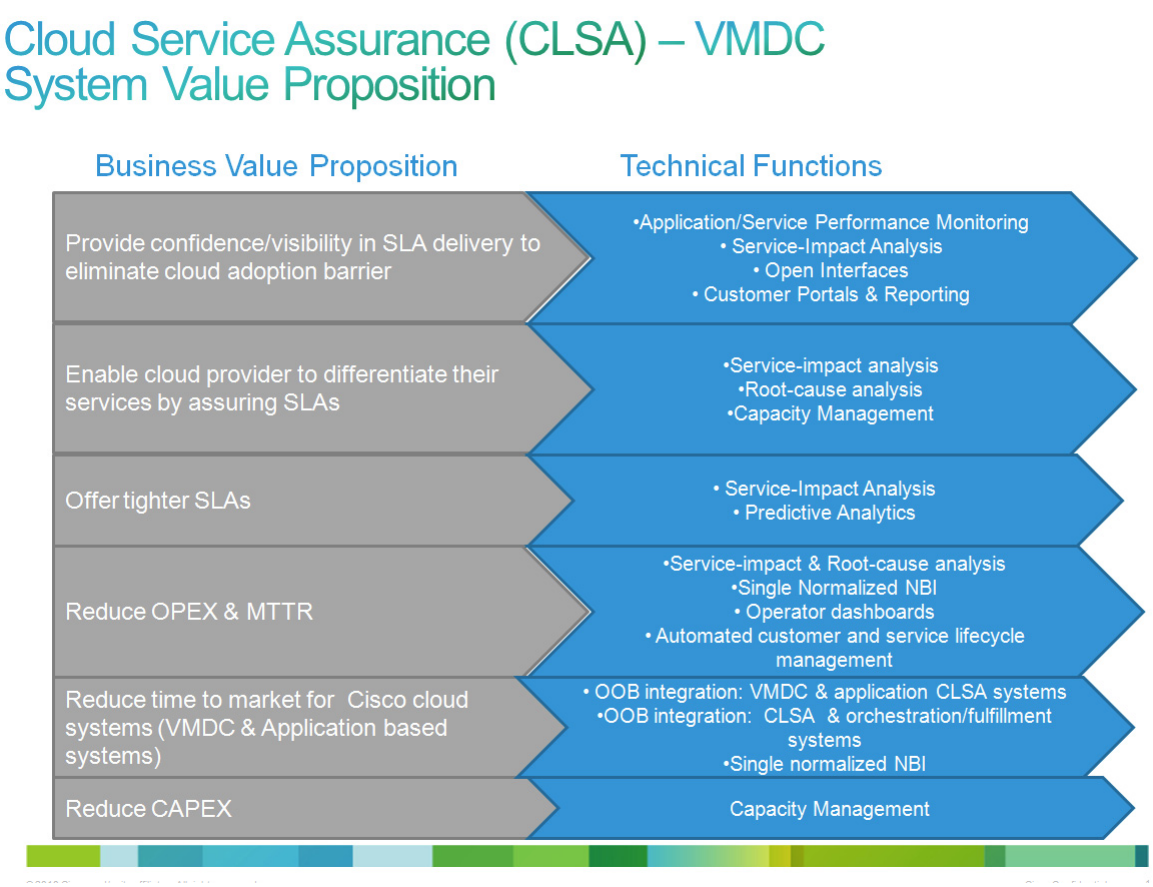


Key Benefits of Cloud Service Assurance, page 1-4 provides more in-depth discussion on the benefits of cloud service assurance.

Key Benefits of Cloud Service Assurance

Figure 1-3 outlines the key business value propositions of cloud service assurance and the technical functions that help realize these value propositions.

Figure 1-3 Key Benefits of Cloud Service Assurance



Cloud service assurance focuses on solving the following four key customer problem statements:

- Automating Service Enablement, page 1-4
- Consolidated Monitoring, page 1-5
- Reducing Mean Time to Repair (MTTR), page 1-6
- Northbound OSS/BSS integration, page 1-7

Automating Service Enablement

As previously noted, assurance services are a key component of the overall cloud service offering. In order to enable and manage the lifecycle of assurance services, a significant amount of manual configuration may be required. In cloud environments that call for self-service and large scale, automatic

enablement of service assurance is required. Automatic enablement of service assurance can be achieved in a couple of different ways. Fundamentally, the following approaches can be taken to automate service enablement and life cycle:

1. Reduce necessary amount of configuration (by using technology that is self learning (e.g., self learning thresholds).
2. Automatic discovery (by assurance system).
3. Programmatic orchestrated provisioning (via integration with orchestration system).

CLSA VMDC utilizes all of the above methods to automate service enablement with specific emphasis on automatic discovery.

The following types of objects are automatically discovered in CLSA VMDC:

- Monitored devices (e.g., UCS, Nexus 7000, MDS 9000, etc.).
- Sub-components of devices and their relationships (e.g., UCS chassis, blades, fabric interconnect, etc.).
- Tenant-based Service Impact Analysis (SIA) models for the compute (e.g., tenant Virtual Machine (VM) mapping to service impacting dedicated and shared vCenter and UCSM managed resources).

Consolidated Monitoring

Due to the large number of components and technologies in many of the SP and IT systems, operations staff are typically segmented and specialized, and they utilize a number of customized tools. This operations staff division of labor results in a monitoring approach that involves observing multiple screens and interaction between a number of organizations when trying to solve even the simplest problems. For example, there are storage operations that are responsible for storage only using their favorite tool, and similarly, there are compute operations with their staff and tools, network operations, and applications operations, and so on. This approach not only increases Mean Time to Repair (MTTR), and thus customer dissatisfaction, but it will also be unmanageable for cloud systems that are extremely dynamic and deployed at extreme scale. While there will always be a need to have specialized staff with focused expertise, there must be some consolidation of monitoring products to provide a single pane of glass that will simplify Tier 1 and 2 operations.

In addition, to fully automate some of operations tasks through value add assurance functions such as Root Cause Analysis (RCA) and SIA, assurance products need to have visibility of all of the components that work together to deliver the service. While segmented visibility will always exist and present challenges in the cloud environment due to business and ownership boundaries, the effort needs to be made to provide as much visibility as possible. More visibility means more value add from the assurance system.

To solve visibility challenges, consolidated monitoring and data collection is one of the fundamental functions of any cloud service assurance system. Consolidated monitoring and data collection needs to be done in the following ways:

- Various domains (applications, compute, storage, network). The cloud assurance system needs to provide a single pane of glass to monitor components from various domains.
- Fault and performance data. The cloud assurance system needs to consolidate fault and performance data and leverage both for all of its higher order functions like RCA and SIA.
- Various data sources, interfaces, and protocols. The cloud assurance system needs to collect data from multiple data sources and protocols and consolidate this data into unified device and service models. Some examples of different data sources and protocols are SNMP, syslog, WS API, Netflow, customer opened tickets, and so on.

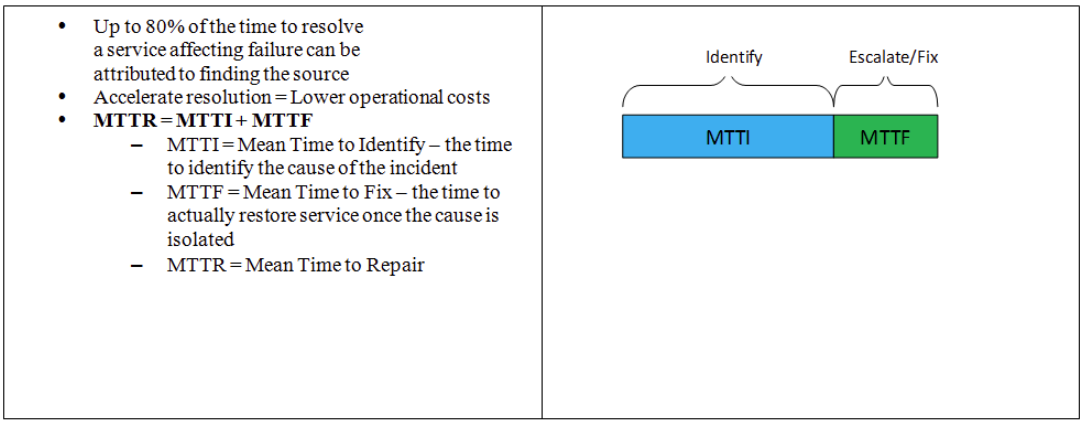
Consolidated monitoring provides the visibility necessary to enable the assurance system to provide more value add, while it can still achieve segmentation of operations through Role-based Access Control (RBAC) and flexible and configurable filtering capabilities.

Reducing Mean Time to Repair (MTTR)

In high pressure Network Operations Center (NOC) environments, operators handle various types of faults, isolate the issues, troubleshoot the problems, or escalate the problem to experts. To reduce the end-customer impact, it is very important to continuously improve MTTR. In traditional systems, general guidance for MTTR is less than 30 minutes from problem detection to problem resolution. For the cloud system, there is no generally accepted criteria, but expectations are that it will perform at least no worse than traditional systems.

Figure 1-4 illustrates the concept of MTTR.

Figure 1-4 Reducing Mean Time to Repair



The VMDC system consists of multiple technologies and components such as compute, storage, network, and network services components. The VMDC system is integrated to leverage these multiple technologies to create a platform for SPs and Enterprises to offer cloud services. Due to the interdependence of the components in the VMDC system, fault and performance issues in these components impact the services offered. The large number of components and technologies necessary to deliver cloud services increases the challenge of identifying the root cause and normalizing and correlating the faults that are generated by each of the individual components.

System scale plays a key role in creating the need for specific notifications about system failures and a reduced set of faults on the NOC operator dashboard. For example, due to the large size of a VMDC system that serves multiple end-customers, the assurance system can potentially generate thousands of events/faults on the NOC dashboard. If the NOC operator has to look at every fault generated by each domain manager, then the NOC operator may become overwhelmed. This can result in a time-consuming task for the NOC operator, who has to review hundreds of events/faults to identify the actionable events and then escalate those to the experts. This fault isolation time period results in higher mean-time-to-investigate/identify, and hence longer MTTR. This all equates to longer downtimes and unsatisfied end customers.

To reduce the MTTR, it is very important that the NOC operators receive specific notifications identifying the root cause of a failure. To achieve this, CLSA VMDC provides fault processing capabilities across components and domain managers and improves the correlation within the components and domains. CLSA VMDC refers to RCA that spans across multiple domains as X-domain RCA.

Northbound OSS/BSS integration

Almost every SP and many large Enterprises have existing OSS/Business Support Systems (BSS) deployed and operational (e.g., ticketing systems, MoM systems, problem and incident management systems, etc.). The SP staff and processes are generally aligned with the existing OSS/BSS workflows. VMDC is a new solution for SPs, however, SPs expect the VMDC assurance solution to integrate with their existing OSS/BSS.

The individual VMDC system components do offer interfaces to integrate with the OSS systems via SNMP Traps, syslogs, and emails, however, since each device and domain manager is an independent application, the integration interfaces are not consistent, and the number of integration points would be large (on the order of dozens of interfaces for VMDC system). Although the assurance domain manager integration northbound with the SP OSS is a one-time task, it needs ongoing maintenance due to:

- Need for ongoing fine-tuning.
- Changes in the underlying system and interfaces (e.g., API changes on southbound devices and domain managers).
- Deployment of additional instances of domain managers.
- Addition of new components and domain managers in future service assurance enhancements.

In order to ease the integration of the VMDC system in existing OSS/BSS systems, and thus SP adoption of the VMDC system, the number of integration points between VMDC and the SP's OSS/BSS needs to be reduced. The SP needs to be shielded from all maintenance and changes in the underlying VMDC system and interfaces unless the change is introducing significant new functionality to the SP. This can be achieved by providing single normalized interfaces from CLSA VMDC.

CLSA VMDC 2.3 Summary of Changes

CLSA VMDC 2.3 extends the VMDC assurance solution to provide support for several advanced features and to expand coverage of VMDC device discovery and monitoring. The list below identifies the major new features supported in this release.

- ASA 5555
- ACE 4710
- Nexus 7004 with SUP2 and F2 FabricPath Line Cards
- VMware VM to EMC VNX Impact Graphing

Table 1-1 lists the document updates associated with these enhancements for ease of reference.

Table 1-1 CLSA VMDC 2.3 Summary of DIG Updates

Section Title	Section Description
CLSA VMDC 2.3 Summary of Changes, page 1-7	Identifies CLSA VMDC 2.3 DIG updates (this section)
VMDC System Overview, page 2-1	Updated overview of VMDC System to include VMDC 2.3
CLSA VMDC System Architecture, page 3-1	Added VMDC 2.3 architecture and new hardware coverage

CLSA VMDC 3.0 Summary of Changes

CLSA VMDC 3.0 extends the VMDC assurance solution to provide support for several advanced features and to expand coverage of VMDC device discovery and monitoring. The list below identifies the major new features supported in this release:

- Zenoss High Availability Support
- New Zenoss Northbound Service Impact Trap
- New device support for both EMC VMAX and VNX block storage
- Cisco VMDC device families support extended (Nexus, ASA, UCS)
- New Zenoss Sample Tenant Portal

Note CLSA VMDC version numbering is closely tied to VMDC IaaS releases. As new devices are added to the VMDC infrastructure, CLSA VMDC will include new device support for discovery and monitoring in follow-on releases. Subsequent CLSA VMDC releases will also continue to enhance support for SIA and RCA, expanding coverage out-of-the-box for network infrastructure.

Table 1-2 lists the document updates associated with these enhancements for ease of reference.

Table 1-2 CLSA VMDC 3.0 Summary of DIG Updates

Section Title	Section Description
CLSA VMDC 2.3 Summary of Changes, page 1-7	Identifies CLSA VMDC 3.0 DIG updates (this section)
VMDC System Overview, page 2-1	Updated overview of VMDC System to include VMDC 3.0
Zenoss Service Impact SNMP Trap, page 3-21	New section providing details for the Zenoss Service Impact Trap