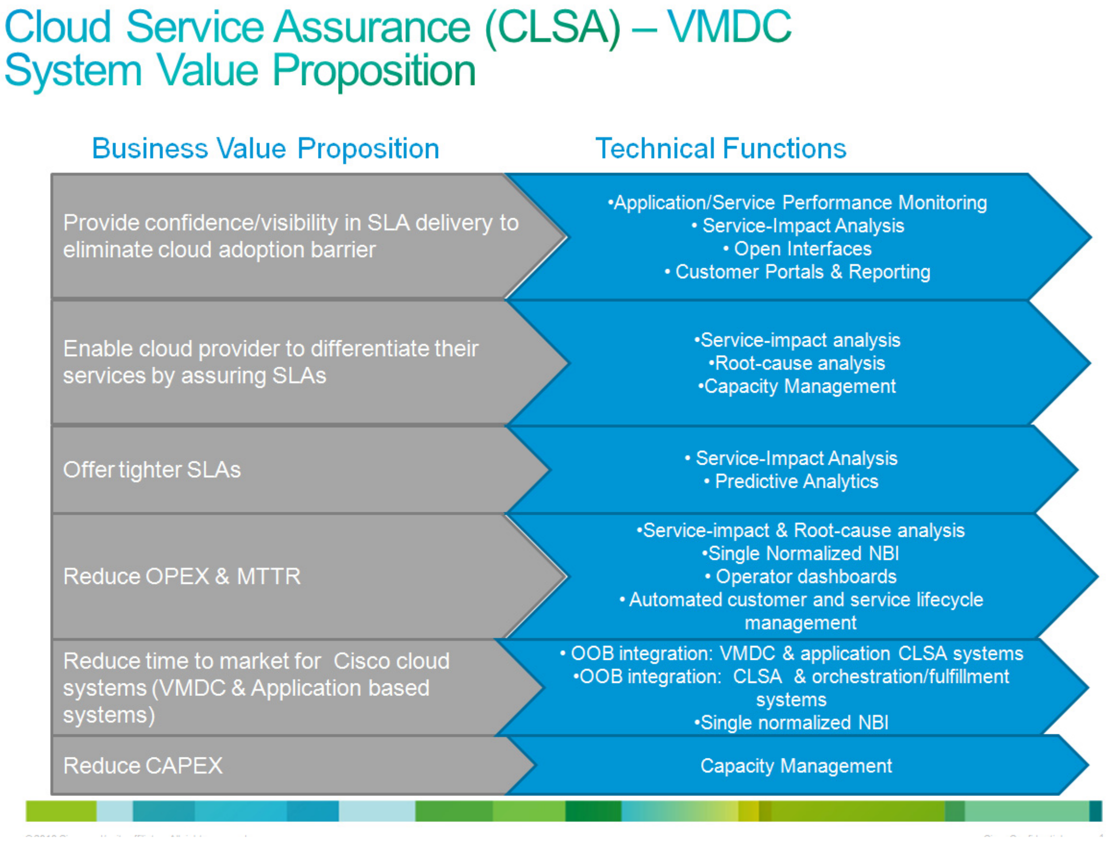
CHAPTER 2

Key Benefits of Cloud Service Assurance

Figure 2-1 outlines key business value propositions of cloud service assurance and the technical functions that help realize these value propositions.

Figure 2-1 Key Benefits of Cloud Service Assurance



Cloud Service Assurance (CLSA) – VMDC System Value Proposition

Business Value Proposition	Technical Functions
Provide confidence/visibility in SLA delivery to eliminate cloud adoption barrier	•Application/Service Performance Monitoring • Service-Impact Analysis • Open Interfaces • Customer Portals & Reporting
Enable cloud provider to differentiate their services by assuring SLAs	•Service-impact analysis •Root-cause analysis •Capacity Management
Offer tighter SLAs	• Service-Impact Analysis • Predictive Analytics
Reduce OPEX & MTTR	•Service-impact & Root-cause analysis •Single Normalized NBI • Operator dashboards • Automated customer and service lifecycle management
Reduce time to market for Cisco cloud systems (VMDC & Application based systems)	• OOB integration: VMDC & application CLSA systems •OOB integration: CLSA & orchestration/fulfillment systems •Single normalized NBI
Reduce CAPEX	Capacity Management

Cloud Service Assurance focuses on solving the following four, key customer problem statements:

- Automate Service Enablement, page 2-2
- Consolidated Monitoring, page 2-2
- Reducing Mean Time to Repair, page 2-3
- Northbound OSS and BSS Integration, page 2-4

Automate 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. Auto enablement of service assurance can be achieved in a couple of different ways. Fundamentally, the following are approaches that 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. Auto-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 auto-discovery.

The following types of objects are auto-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) model 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, SP and IT operations are typically segmented and specialized, and they typically utilize a number of specialized tools resulting 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, in order 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.

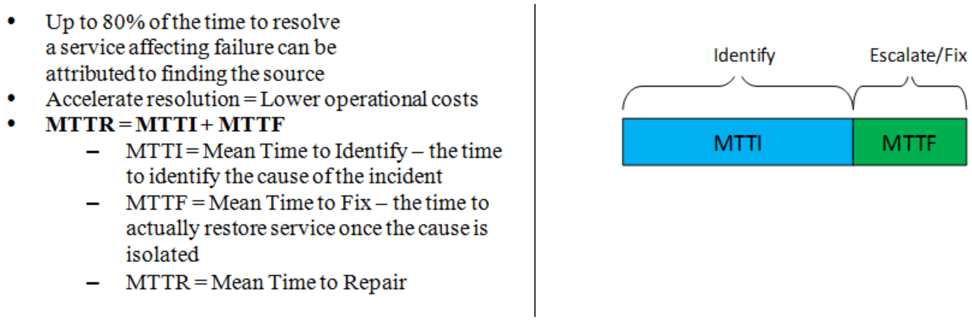
- Fault and performance data. The cloud assurance system needs to consolidate fault and performance data and leverage both for all of its higher order functions like RCA and SIA.
- Various data sources, interfaces, and protocols. The cloud assurance system needs to collect data from multiple data sources 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

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 the Mean Time to Repair (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 2-2 Reducing Mean Time to Repair



- Up to 80% of the time to resolve a service affecting failure can be attributed to finding the source
- Accelerate resolution = Lower operational costs
- **MTTR = MTTI + MTTF**
  - MTTI = Mean Time to Identify – the time to identify the cause of the incident
  - MTTF = Mean Time to Fix – the time to actually restore service once the cause is isolated
  - MTTR = 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 interdependencies of the components in the VMDC system, the issues in components impacts the services offered by the dependent components. Usage of a larger number of components and technologies necessary to deliver the service brings the challenge of identifying the root cause and normalizing and correlating the faults that are generated by each of the individual components.

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 the 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 may result in a time-consuming task for the NOC operator, who has to review hundreds of events/faults in order to identify the actionable events and then escalate those to the experts. This will result 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 and BSS Integration

Almost every SP and many large Enterprises have existing Operations Support Systems (OSS)/Business Support Systems (BSS) deployed and operational (e.g., ticketing systems, Manager-of-Managers (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 VMDC assurance solution to integrate with the 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 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 on-going maintenance due to:

- Need for on-going 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

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.