

Overview

The Cisco® Virtualized Multiservice Data Center (VMDC) is a set of specifications and guidelines for creating a scalable, secure, and resilient infrastructure that addresses the needs of cloud computing. Cloud Service Assurance for VMDC enables reliable service delivery in a VMDC, FlexPod, Vblock or Cisco Unified DC deployment, providing the following benefits:

- **Reduced Time to Deployment**—Provides a fully tested and validated service assurance solution for VMDC-architected data centers.
- **Improved Operational Efficiency**—Automated discovery and continuous relationship modeling ensures operation teams can work with customers instead of administering software.
- **Improved Customer Service**—Cloud Service Assurance for VMDC helps identify services most affected by availability or performance issues in underlying infrastructure, speeding root cause identification and reducing mean-time-to-repair.
- **Reduced Risk**—Enterprises and Service Providers deploy new architectures with confidence.

Cloud Service Assurance for VMDC Solution Highlights

Cloud Service Assurance for VMDC is provided by Cisco Partner Zenoss, Inc. through the Solution Plus program. Zenoss Cloud Service Assurance (Zenoss CSA) is an advanced software solution for Cisco Data Center Cloud converged infrastructure deployments. It enables reliable service delivery by providing an essential platform for resource monitoring, relationship modeling, adaptive dependency discovery, and continuous delivery of quantitative impact and root cause analysis.

- Customers deploying converged infrastructure solutions gain efficiencies from a the ability to understand and work with converged infrastructure as a unified solution instead of disparate technology stacks.
- As customers transition to cloud operations with the addition of service catalogs, customer portals, and orchestration solutions, the value of Zenoss CSA grows with automated service monitoring for cloud tenant users and business applications.

Cisco and Zenoss have jointly validated the Zenoss Cloud Service Assurance product, extending and customizing it to work with the VMDC architecture and Cisco Unified Data Center.

Figure 1 Zenoss Cloud Service Assurance System Architecture

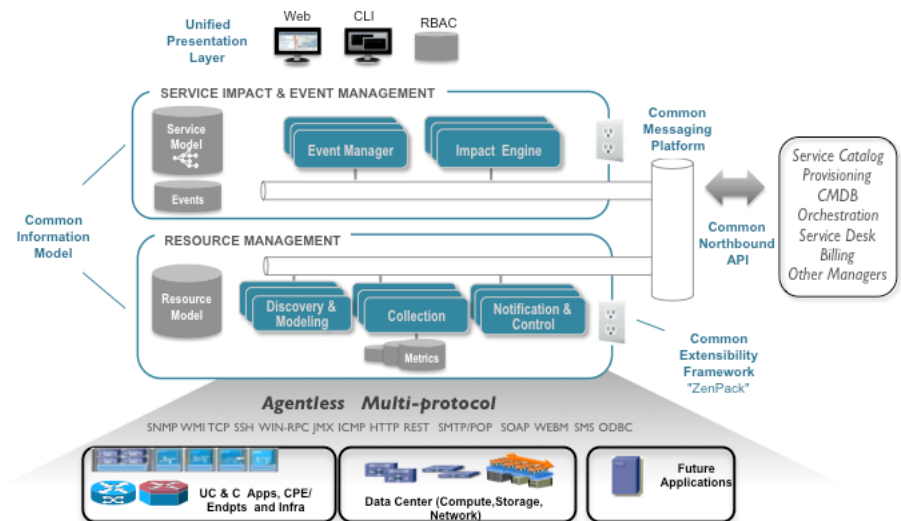
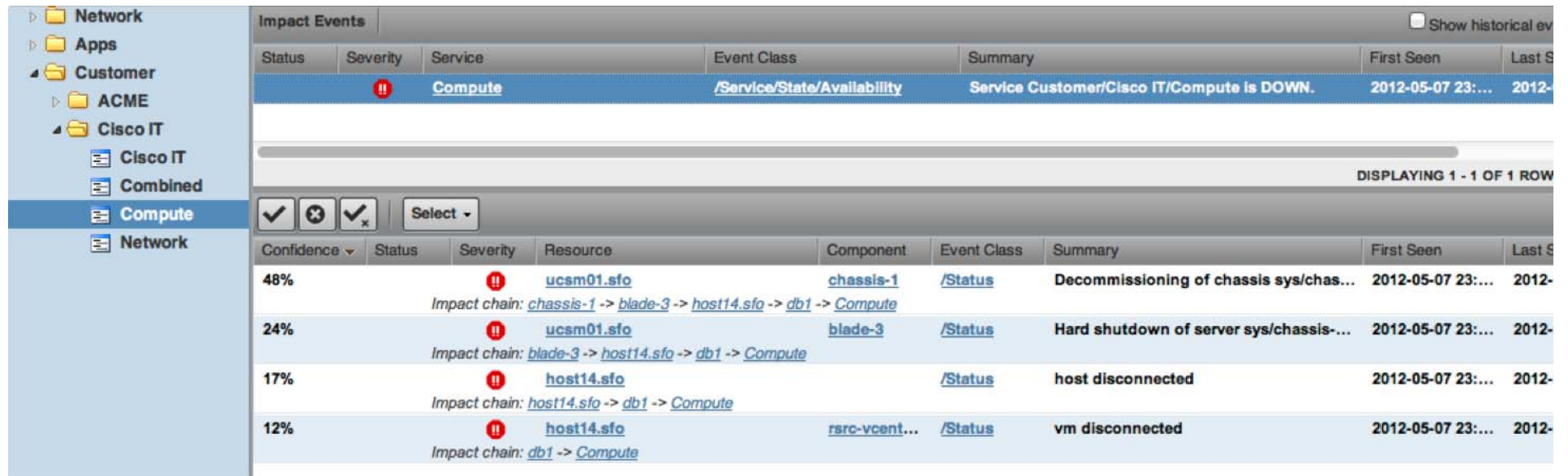


Table 1 *Solution Highlights*

Highlight	Details
Unified service assurance for Cisco Data Center solutions components	Single product with out-of-the-box coverage for compute, virtualization, storage, and networking devices provides service assurance for cloud tenants, business applications, and converged infrastructure deployments.
Validated data center design for enterprise or service provider scalability	Zenoss Cloud Service Assurance is validated for the VMDC 2.2, and 3.0 data center architectures.
Comprehensive VMDC device coverage	Out-of-the-box support for compute, virtualization, storage, and networking services.
Dynamic cloud infrastructure model	Automatically discover and maintain identify components devices and relationships eliminating the need to develop, and maintain, ever changing service-specific rules.
Service impact awareness and root cause analysis	Identify service-impacting events across multiple technology stacks, rapidly focusing resources on incident root cause. Initial release focusing on compute, then adding network service impact coverage in upcoming releases.
High availability	HA deployment option provides automated protection against multiple failure scenarios.
Enhanced SLA reporting	Provides tenant-service fault & performance reporting.
Automatic discovery with optional orchestration integration	Integrates with orchestration solutions such as Cisco Intelligent Automation for Cloud to provide cloud user-focused service assurance and per-tenant visibility of resource usage. Automated data center network discovery, Cisco Unified Computing, and virtual machines reduces deployment costs. Orchestration software integration, including Cisco Intelligent Automation for Cloud (CIAC), to automate service impact.

Figure 2 *Zenoss Cloud Service Assurance Product Service Impact*



Zenoss CSA assesses performance and availability failures for each customer, providing reliably quantified root cause identification

Table 2 Business Benefits

Dramatically improves IT agility, enabling new applications to be delivered rapidly and providing immediate awareness of cloud tenant application performance	<ul style="list-style-type: none"> • Dynamically and automatically tracks relationships across technology stacks to ensure continuous dependency awareness. • Immediate real time monitoring of newly provisioned cloud services with orchestration integration. • Fully integrated with hardware managers (i.e. UCS Manager) and Virtualization Managers (i.e. VMware vCenter) to automatically adapt to additional compute, virtualization, and storage resources.
Connect IT operations to the business with service awareness	<ul style="list-style-type: none"> • Provides IT awareness of the service health of business services and cloud tenants. • Service dependency tracking to identify which tenant services are affected by an infrastructure outage and whether the outage has degraded the service or caused it to fail. • Continuous analysis of service-impacting availability and performance events quantifies root cause probability and enables quick issue correction.
Deliver higher customer service availability (SLAs) and performance with improved Mean Time to Repair (MTTR)	<ul style="list-style-type: none"> • Tracks service-specific availability and performance status, enabling infrastructure engineers to focus on customer issue resolution. • Provides root cause analysis combining multiple technology stacks, enabling faster and more accurate incident assignment. Initial release focusing on compute and then adding network service impact coverage in upcoming releases. • Extensible integration with orchestration permits automation of routine recovery tasks. • Supports and tracks success of cloud-specific recovery operations such as vMotion.
Increase return on IT investment	<ul style="list-style-type: none"> • Realize the full benefit of converged infrastructure by increasing economies of scale. • Increase overall asset utilization without affecting performance by identifying areas of high and low resource utilization. • Increase server-to-staff ratio by implementing replicable, automated processes.
Keeps IT in control through standards and policies	<ul style="list-style-type: none"> • Monitoring-by-policy, so that newly provisioned workloads receive consistent implementation of best-practice monitoring and policy-compliant impact service management and root cause analysis. • Maintain continuous awareness across the dynamically-changing environment.

Table 3 IT Benefits

Complete coverage for Cisco VMDC infrastructure	<ul style="list-style-type: none"> • Out-of-the-box monitoring policies for Cisco UCS compute, VMware vCenter virtualization, Nexus networking, and NetApp and EMC storage resources. Supports FlexPod and vBlock solutions.
Automated discovery	<ul style="list-style-type: none"> • Change-driven and scheduled discovery ensures accurate understanding of cloud infrastructure.
Accurate relationship model	<ul style="list-style-type: none"> • Maintains an up-to-date model of the relationships between compute, virtualization, storage, and networking components using context provided by component configuration.
Event, availability, and performance management	<ul style="list-style-type: none"> • Single pane of glass eliminates the need to integrate separate management applications.
Cloud scalability	<ul style="list-style-type: none"> • Distributed architecture supports deployment models from proof of concept to multi-data center production operations.
Customizable, extensible, integrate-able	<ul style="list-style-type: none"> • Extensive set of APIs.
Automated configuration discovery	<ul style="list-style-type: none"> • Change-driven and scheduled configuration discovery ensures accurate understanding of the cloud infrastructure.
Accurate relationship model	<ul style="list-style-type: none"> • Maintains an up-to-date model of the relationships between compute, virtualization, storage, and networking components using context provided by component configuration.
Relationship visualization	<ul style="list-style-type: none"> • Administrators can see the current relationships between compute, virtualization, storage, and networking components to better understand issues and potential issues.
Automatic creation and maintenance of tenant and business application end-user services	<ul style="list-style-type: none"> • Service definition is created and modified concurrently when the Cloud Portal is used to create or modify services and cloud resources are provisioned.
Continuous understanding of service dependencies	<ul style="list-style-type: none"> • Tracks and maps the compute, virtualization, network, and storage resources used by each end user service into a service dependency model. The model is dynamically and automatically maintained with changes to cloud infrastructure.
Service Impact identification and quantitative root cause analysis	<ul style="list-style-type: none"> • When infrastructure availability and performance events occur, Zenoss CSA identifies affected end user services using the relationship model. The service dependency model is analyzed to determine impact level. A continuous quantitative root cause analysis process suppresses event floods and identifies potential impact chains in order of probability. • Zenoss CSA provides out-of-the-box service impact support for Windows and Linux workloads, VMware vSphere, Cisco UCS, NetApp filers, EMC storage arrays, and a limited set of network components. Service impact support can be extended to provide additional coverage.
Event flood suppression	<ul style="list-style-type: none"> • When multiple technology stacks are combined in a private cloud, single incidents generate a flood of sympathetic events. Zenoss crosses technology boundaries to provide a quantitative ranking of potential points.

Cloud Service Assurance Use Case Coverage

Zenoss Cloud Service Assurance supports the following CSA scenarios.

Table 4 *Cloud Service Assurance Support*

Scenario	Zenoss CSA Function
Unified monitoring data collection platform for VMDC components	<ul style="list-style-type: none"> Collects fault, availability and performance data from all VMDC components. Generates availability and performance data using synthetic transactions. Supports physical, virtual, and cloud devices Supports multiple data collection protocols.
Supports multiple data collection protocols and APIs	<ul style="list-style-type: none"> SNMP, Syslog, XMLRPC, JSON/API, AMQP, SSH, JMX, WMI, Windows Perfmon, SMI-S, ICMP, Telnet, UCSM XML API, NetConf, vSphere SOAP API, vCloud Director, Amazon EC2 CloudWatch, Cisco CallManager AXL, HTTP, ODBC, SMTP, POP, DNS, LDAP, NTP, FTP, IRC, XMPP, RPC, NNTP. Extensible with scripting.
Agent-less data collection Resilient, distributed deployment	<ul style="list-style-type: none"> Leverages native agents (no need for installing extra agents). Scales horizontally to support very large environments. Supports proof-of-concept and small environments with a single virtual machine. High availability configuration enables operation with no single point of failure.
Automated discovery of VMDC network and network service devices	<ul style="list-style-type: none"> Within an IP address range, discovers and identifies supported VMDC networking devices. Classifies devices, applies device-specific monitoring templates, and begins data collection. Collects fault events and performance KPIs. Tracks configuration changes such as establishment of new network services. Advanced coverage for Nexus 1000v and VSG, 2000, 3000, 5000, and 7000 series; Catalyst 6500 and VSS with FWSM, ASA, and ACE modules, ASA 5500, ASR 1000 and 9000, and MDS 9000 devices.
Automated discovery of Cisco UCS components	<ul style="list-style-type: none"> Uses Cisco UCS XML API to automatically track newly added components in a UCS complex. Tracks assignment of service profiles to blades. Uses UCS-specific monitoring templates to collect fault events, configuration changes, and performance KPIs. Tracks association between service profiles and the operating system running on the blade, providing automatic impact relationship management.
Automated discovery of VMware guests	<ul style="list-style-type: none"> Uses VMware vSphere API to automatically discover and track changes to virtual machines, hosts, datastores, clusters, and resource pools. Uses VMware-specific monitoring templates to collect fault and task events, relationship changes such as vMotion events, and performance KPIs. Tracks association between virtual machines and operating systems, ESX/ESXi hosts and UCS service profiles, datastores and NetApp LUNs, providing automatic impact relationship management.
Monitoring of NetApp FAS filers	<ul style="list-style-type: none"> Uses NetApp APIs to automatically discover and track changes to LUNs, file systems, Qtrees, etc. Uses NetApp-specific monitoring templates to collect fault and task events and performance KPIs. Tracks association between LUNs, filesystems, and VMware datastores, providing automatic impact relationship management.
Monitoring of EMC VNX and VMAX storage systems	<ul style="list-style-type: none"> Connects to EMC SMI-S Provider to automatically discover and track changes to storage pools, hard disks, arrays, enclosures, link control cards, power supplies, batteries, storage processors, and storage processor ports. Supports block mode devices with EMC-specific monitoring templates for performance KPIs and fault events.
Monitoring of Windows and Linux workloads	<ul style="list-style-type: none"> Uses multiple operating system-provided APIs to automatically discover and track changes within each operating system, such as additional file systems or new Windows services. Uses operating-specific monitoring templates to collect system events and performance KPIs and verify availability of device and components. Tracks association between operating system and virtual machine or operating system and UCS service profile, providing automatic impact relationship management.
Consolidated visibility for events, availability, and KPIs	<ul style="list-style-type: none"> Web console provides single user interface with access to monitoring data for all VMDC components. Consistent device model crosses VMDC technology stacks to common data presentation for infrastructure engineers.
Identifies error conditions with threshold analysis of performance KPIs	<ul style="list-style-type: none"> Generates events when performance KPIs are outside of desired range. Applies Holt-Winters algorithm to provide predictive thresholds.

Scenario	Zenoss CSA Function
Stores events and performance KPIs for historical reporting	<ul style="list-style-type: none"> • Performance KPIs are stored by default for 90 days. • Events are stored by default for up to one year. • Defaults can be modified to meet individual needs.
Provides event management facilities	<ul style="list-style-type: none"> • Identifies and suppresses duplicate events by incrementing event count and updating most recent event date and time. • Identifies and suppresses non-critical events from the event console and optionally from the event database. • Recognizes "clear" events indicating a fault condition has improved and automatically closes the original fault event. • Automatic event enrichment adds affected business applications and tenant services to relevant events Enables event enrichment by leveraging knowledge of components and relationships.
Integrated action and notification framework	<ul style="list-style-type: none"> • Out-of-the-box actions library. • Open and extensible. • Escalation and calendaring support. • Maintenance window support.
Simplified integration with OSS/BSS existing management systems and processes	<ul style="list-style-type: none"> • Abstracted and normalized integration interface for all VMDC devices using a single northbound API delivers select events for all converged infrastructure devices as well as business applications and tenant services. • API provides for device event integration using any combination of SNMP traps, Email, JSON API, Page, AMQP, and scripted integration such as calls to REST interfaces. • Integration with BMC Remedy and Service Now ticketing systems is provided. • Unlimited number of northbound destinations.
Integration with Orchestration/Service Fulfillment	<ul style="list-style-type: none"> • Published interfaces for device discovery and classification, impact service creation, management, and policy creation. • Data extraction interfaces for business application and tenant service status, KPIs, and events. • Tenant Service Impact integration with CIAC is available. • Orchestration vendor- independent implementation. • Tenant service and VM association can be loaded to Zenoss CSA without an automated orchestration system.
Open and extensible	<ul style="list-style-type: none"> • JSON API provides access to device model and attributes, performance data, event data, and service data. • JSON API can also be used to manage events (acknowledge, clear, close), add and remove monitored devices, set production/maintenance state for devices, initiate discovery and modeling, manage thresholds, and more.
Automatic discovery of tenant based service impact model	<ul style="list-style-type: none"> • Service impact model for compute maps tenant VMs to s dedicated and shared vCenter and UCS managed resources.
Tenant root cause	<ul style="list-style-type: none"> • Prioritized events by business relevance and urgency. • Identifies service impacting technical risk, enabling future failures to be addressed prior to tenant impact. • Visual confirmation of whether redundancy is protecting service availability.
Root cause analysis	<ul style="list-style-type: none"> • Classifies events as probable root cause vs. symptomatic events. • Combines event correlation rules with service topology models.
Impact analysis	<ul style="list-style-type: none"> • Dynamically maintains a graph of relationships between physical and virtual resources. • Propagates fault and performance degradation through graph to infer business service impact and probable root causes. • Reduces event console to a few root causes.
Service impact	<ul style="list-style-type: none"> • Focus on service state vs. resource state. • Notify only on change in service state. • Provides root cause analysis focused on individual services.

Zenoss Cloud Service Assurance Converged Infrastructure Support

Compute	Cisco UCS, including Fabric Interconnect, Chassis, and B-series blade servers.
Virtualization	VMware vSphere.
Storage	NetApp FAS series, EMC VNX, EMC VMAX.
Network	Nexus 1010, 1000v and VSG, 2000, 3000, 5000, and 7000 series; Catalyst 6500 and VSS with FWSM, ASA, and ACE modules, ASA 5500, ASR 1000 and 9000, and MDS 9000.
Workload OS	Windows, Linux.
Workload applications	Microsoft Active Directory, Microsoft Exchange, Microsoft Internet Information Server, Microsoft SQL Server, Apache Tomcat, BEA Weblogic, JBoss Application Server.
Extensibility	Additional capabilities available from partner Zenoss.

Zenoss Cloud Service Assurance Scale

Total Number of Monitored Components	1,500,000 with 5 KPIs per component
Continuous Event Rate	5,000 events per second

For More Information

To learn more about Cloud Service Assurance for VMDC, download the Cisco Validated Design Guide from www.cisco.com/go/cloudassurance

Cisco Design Zone

Design Zone for [Virtualized Multi-Services Data Center \(VMDC\)](#)