CHAPTER 4

Zenoss Cloud Service Assurance Overview

Zenoss Cloud Service Assurance (CSA) is used as the Service Assurance Manager (SAM) for Cloud Service Assurance for Virtualized Multiservice Data Center (CLSA VMDC). Zenoss CSA consists of the following two elements:

- Core assurance platform
- VMDC ZenPacks that include VMDC specific device plugins that provide out-of-the-box support for VMDC components on the core assurance platform

This chapter discusses the product architecture and provides an overview of the capabilities of the core assurance platform and presents the following topics:

- Zenoss Cloud Service Assurance Functional Overview, page 4-1
- Zenoss Cloud Service Assurance Architecture Highlights, page 4-7

Zenoss Cloud Service Assurance Functional Overview

Zenoss CSA focuses on the assurance and optimization category of cloud operations. The console provides a unified view of assurance and operations. Cloud operations consoles meet a combination of Enterprise role-based security and Service Provider (SP) multiservice needs. Enterprises have traditionally defined multiple organizational roles limiting the actions a user in the role can perform. SPs have traditionally provided each customer a view of just their given resources as a paid service. In cloud-enabled organizations, both needs must be met simultaneously.

As far as customers are concerned, the ability to deliver against the service level they chose from the Service Catalog is paramount. Whether characterizing this mutual understanding as an expectation or a formal agreement, there is a need to track and report against the agreed to metrics in a manner that is easy to understand. This means providing separate views for each customer and workload, and operating as if there are multiple distinct tenants using common cloud resources.

To provide the service level metrics and meet the expectations, the workloads and the supporting infrastructure must be monitored to detect issues that may impact the customer. The Impact and Event and Management collects device, application, and infrastructure information that identifies potential issues and evaluates it to determine which issues are critical. Performance Monitoring collects vital performance statistics at every layer of the infrastructure, evaluates it to determine whether anything should be fed into the Impact Management process, and stores it for long term analytics. These two functions provide reactive management to application, device, and infrastructure issues.

For some issues such as a sudden failure of a power supply, there is no advanced warning. For other issues, there are trends that can be collectively understood and provide early warning of an impending issue. Predictive Analytics attempts to provide proactive analysis of data, searching for identification and remediation of issues before they reach a critical state.

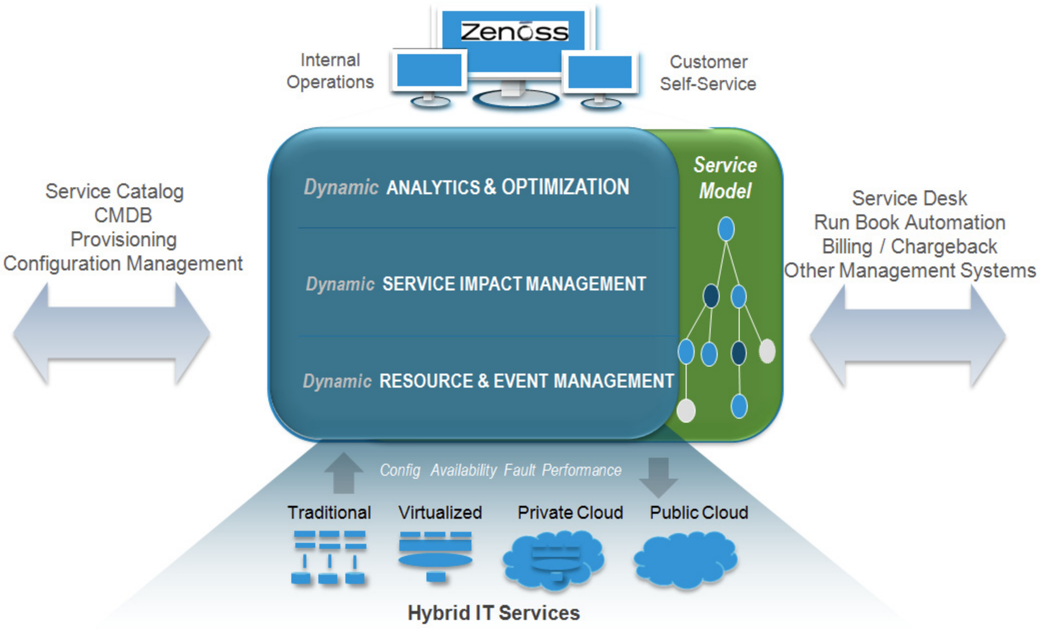
In cloud operations, the discipline of Capacity Analytics changes roles from an assessment of workload-driven resource requirements against the fixed amount available from a dedicated hardware platform. Reacting to the assessment can take weeks as new hardware is provisioned. Within the cloud Data Center (DC), resource allocations can be altered in minutes, and the reaction to changing workload needs should be just as fast. Administrators need to communicate to customers the needs of their workloads and get confirmation that they are willing to bear any increased costs, or allow the resource needs to go unmet and application performance to suffer. Administrators also need to provision enough resources for the overall DC to ensure that peak load commitments can be met, which means understanding capacity at an aggregated level.

Figure 4-1 shows the key functions that are available within Zenoss CSA. There are three key categories of the functions implemented in three software sub-components:

1. Resource Management, which provides discovery, data collection, performance, and event monitoring and notification capabilities.
2. Impact and Event Management, which provides full event management lifecycle, Root Cause Analysis (RCA), and Service Impact Analysis (SIA).
3. Analytics and Optimization, which provides a data warehouse for long term data trending, analytics engine, and reporting capabilities.

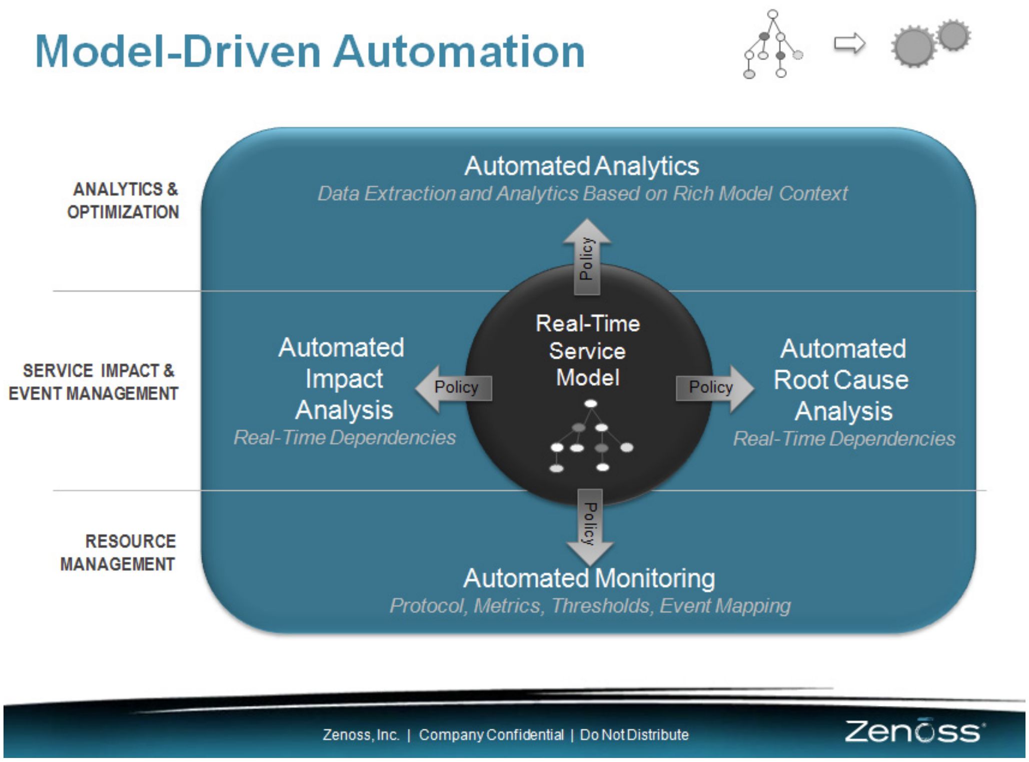
Note Resource Management and Impact and Event Management are the focus of CLSA VMDC. The Analytics and Optimization functions were only evaluated on a best effort basis, but are not fully customized nor validated for VMDC environments.

Figure 4-1 Key Functions of Zenoss CSA



The core issue in the cloud DC is keeping up with its rapid rate of change. When a customer's order for a new IT service is automatically fulfilled and placed into production, there is no time to manually update tools or components. At the heart of Zenoss CSA is a unified, real-time understanding of the entire IT environment, including resources, services, relationships, dependencies, state, and configuration. With this understanding, Zenoss is able to simplify the service assurance process with template-driven resource monitoring and automated impact and RCA. Unlike traditional systems that rely on configuration databases that are updated in batch mode, the Zenoss model is maintained in near real time through a series of discovery and modeling techniques that tap into the stream of configuration changes as they happen across the physical, virtual, and cloud-based infrastructure. As with every other aspect of the product, this model can be extended through its open API (Figure 4-2).

Figure 4-2 Model-Driven Automation



Model-Driven Automation

ANALYTICS & OPTIMIZATION

SERVICE IMPACT & EVENT MANAGEMENT

RESOURCE MANAGEMENT

Automated Analytics

Data Extraction and Analytics Based on Rich Model Context

Automated Impact Analysis

Real-Time Dependencies

Real-Time Service Model

Policy

Automated Root Cause Analysis

Real-Time Dependencies

Automated Monitoring

Protocol, Metrics, Thresholds, Event Mapping

Zenoss, Inc. | Company Confidential | Do Not Distribute

Zenoss

The following sections provide more details on the key functions of Zenoss CSA.

- Dynamic Resource Management, page 4-3
- Dynamic Impact and Event Management, page 4-4
- Dynamic Analytics and Optimization, page 4-6

Dynamic Resource Management

The foundation of service assurance in the hybrid cloud DC is unified, cross-domain resource monitoring and control that brings together configuration, performance, availability, fault, event and log information across the physical, virtual and cloud-based infrastructure and applications, and enables automated actions to be performed at the resource level. Zenoss CSA delivers this capability on a scalable, open platform that is easy to extend, and is able to track dynamic elements and relationships as they evolve in near real time.

Key feature areas include the following:

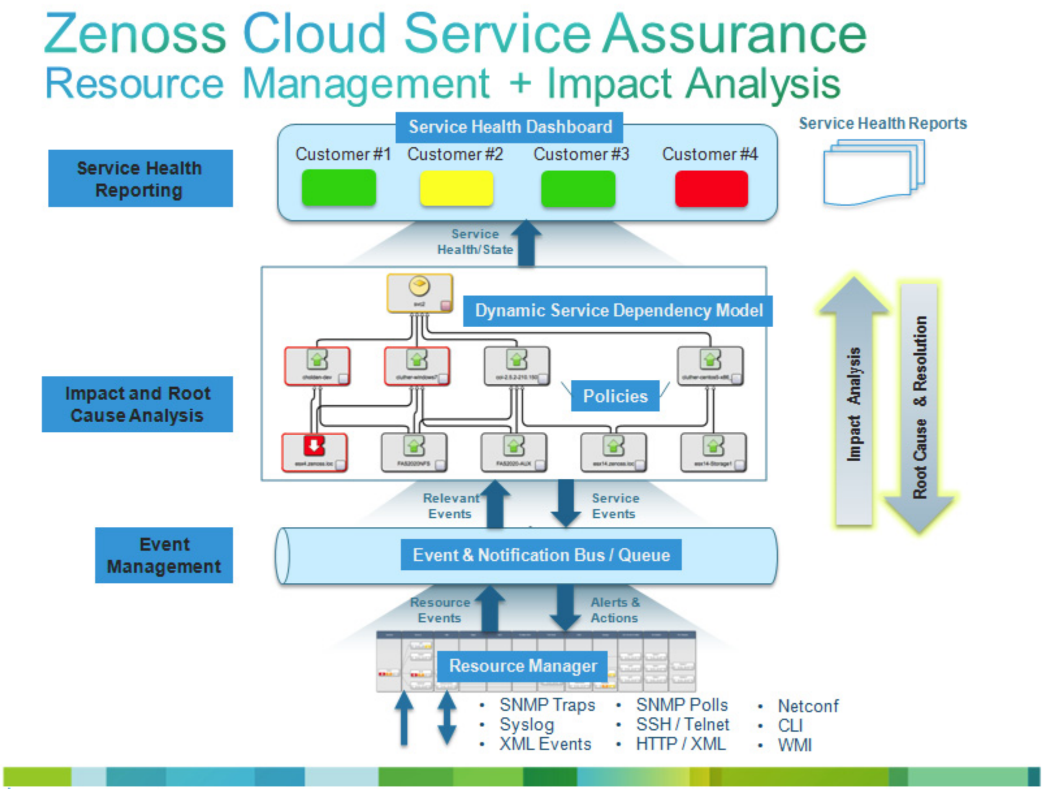
- **Discovery and Modeling**. Automatically maintain real-time inventory and configuration details for the entire IT environment; includes real-time relationship tracking of dynamic relationships common in virtualized and cloud-based infrastructures.
- **Full-stack Monitoring**. Unify and automate performance, availability, and event monitoring of networks, servers, storage and applications across physical, virtual, and cloud-based environments with a single, model-driven, horizontally-scalable, extensible collection platform.
- **Notification and Control**. Rich alerting and remediation framework allows the user to be notified via email, text, or pager based on user-specified policies, or to take direct automated action to address a problem in real time.

Dynamic Impact and Event Management

Maintaining a real-time perspective on service health, and linking health issues to the underlying infrastructure in a reliable, simple, and cost-effective way can be challenging in hybrid data centers. In particular, legacy approaches to impact management and RCA simply break down due to the shared and dynamic nature of virtualized and cloud-based infrastructures.

Figure 4-3 illustrates how Zenoss CSA transforms state information from the resource manager into a stream of events that are processed in near real time by its SIA and RCA engine, leveraging the real-time service model. This processing feeds a service health dashboard and generates service events that are used for alerting, troubleshooting, and to initiate real-time automation and service remediation. The result is real-time service level awareness, rapid triage, and closed-loop automation that thrives in the dynamic, hybrid cloud environment.

Figure 4-3 Service Health Dashboard



Dynamic Service Modeling

Zenoss CSA maintains a real-time service model, and automatically discovers infrastructure dependencies. Service constructs can be easily defined based on logical business constructs to define the infrastructure groupings supporting a specific application service. For example, a Customer Relationship Management (CRM) application service might require e-mail, web, and database services to be present in order to operate. These logical definitions define the collection of services required for the CRM service to be considered functional. Once this logical service hierarchy is defined, the application or OS instances delivering the service functions are associated and Zenoss CSA takes care of the rest. Using advanced dependency modeling capabilities, Zenoss CSA pulls in all relevant infrastructure elements. Virtual Machine (VM) partitions, blades, chassis, storage, network interfaces, and a wide variety of device components are all automatically discovered and mapped into the relevant service dependency graphs.

Dynamic Impact Analysis

Dynamic Impact Analysis identifies which services are affected by conditions in supporting components or infrastructure. For example, a failing fan in a Cisco UCS chassis might result in dozens of virtual machines being moved to new virtual hosts. With Zenoss impact analysis, IT operations can determine which business services will be affected by the fan failure and can plan corrective actions to minimize service level disruptions.

Dynamic RCA

Dynamic RCA allows IT operators to quickly identify the specific events most likely to be the cause of a service impacting condition. In complex IT environments, it is not uncommon for a single component failure to cause a cascade of failures, resulting in an event storm totaling thousands of individual events.

Zenoss CSA includes a proprietary Confidence Ranking Engine built on top of Impact Analysis to quickly triage these events and identify where IT resources should be applied to correct these types of situations. This algorithm filters impact events based on a variety of criteria including severity of the event, service graph depth, and the number of graph branches affected by an event. This ranking algorithm allows IT operators to target resources to address events deemed the most likely cause of a service failure or degradation. Real world deployments of Zenoss CSA have validated the effectiveness of the service impact framework by demonstrating significant event reduction and highly accurate identification of root cause events.

Simple, Modular Policy - "Policy Gates"

Traditional impact managers require complex, top down rule sets to be defined, which require either a static IT infrastructure or a detailed understanding of all possible infrastructure configurations to identify service impact or determine root cause. This approach fails in dynamic virtualized or cloud data centers due to the need to maintain hard dependencies on named infrastructure elements. In contrast, Zenoss CSA uses Policy Gates to define impact rules on an element-by-element basis, and rolls up impact results through the current service model to reach conclusions. The design premise of this system is that the state of any given element in a service graph is determined by analyzing the state of the immediate children of that element. A change in the state of a given element is propagated to the parents of that element, causing the parents to evaluate their own state using their own Policy Gate configurations. The net result of this approach is that functions such as event aggregation, filtering, de-duplication and masking are provided automatically, eliminating the need for highly specialized skills to write impact rules and dramatically reducing human effort in event processing.

Unified, Scale Event Management

Aggregate and manage events for an entire IT environment with a next generation event management system that provides automated event normalization and enrichment, and is easily extended, integrated, and scaled through an embedded message bus. Zenoss CSA is capable of processing in excess of 1,500 events per second with a single event processor. Field deployments have shown that the system is capable of quickly parsing through event storms scaling to thousands of events in seconds, resulting in just a handful of events after processing through the Service Impact and Confidence Ranking.

Dynamic Analytics and Optimization

The final step of the service assurance lifecycle is historical analysis and planning. Deep, cross-domain analytics are needed to perform capacity planning and drive optimization of the environment. Zenoss CSA enables this through its integrated analytics capabilities that directly leverage the real-time service model and all state information from the Resource, Impact, and Event Management modules. Leveraging a powerful, open business intelligence engine, the Zenoss analytics capability provides a scalable and rich analytics platform that addresses tenant reporting needs, management dashboards, capacity planning, and insight for optimization. Specific capabilities include:

- **Turnkey Operations Data Warehouse**. Automatically aggregates and normalizes configuration, performance, and event history for the entire IT environment across physical, virtual, and cloud-based infrastructure and applications.
- **Unified Historical Analytics**. Understand utilization and health trends across an IT's entire infrastructure including tenant-based consumption and availability reporting; gain deep, timely insight through drag-and-drop dashboards, out-of-the-box reports, and powerful ad-hoc analytics all available through a multiservice web portal. The Zenoss Analytics software module is not validated or included as part of CLSA VMDC, however, this software module can be obtained directly from Zenoss, Inc.

- **Predictive Analytics**. Forecast capacity needs and anticipate availability problems through predictive trending that allows for visualization and proactive management of upcoming operational issues and infrastructure requirements

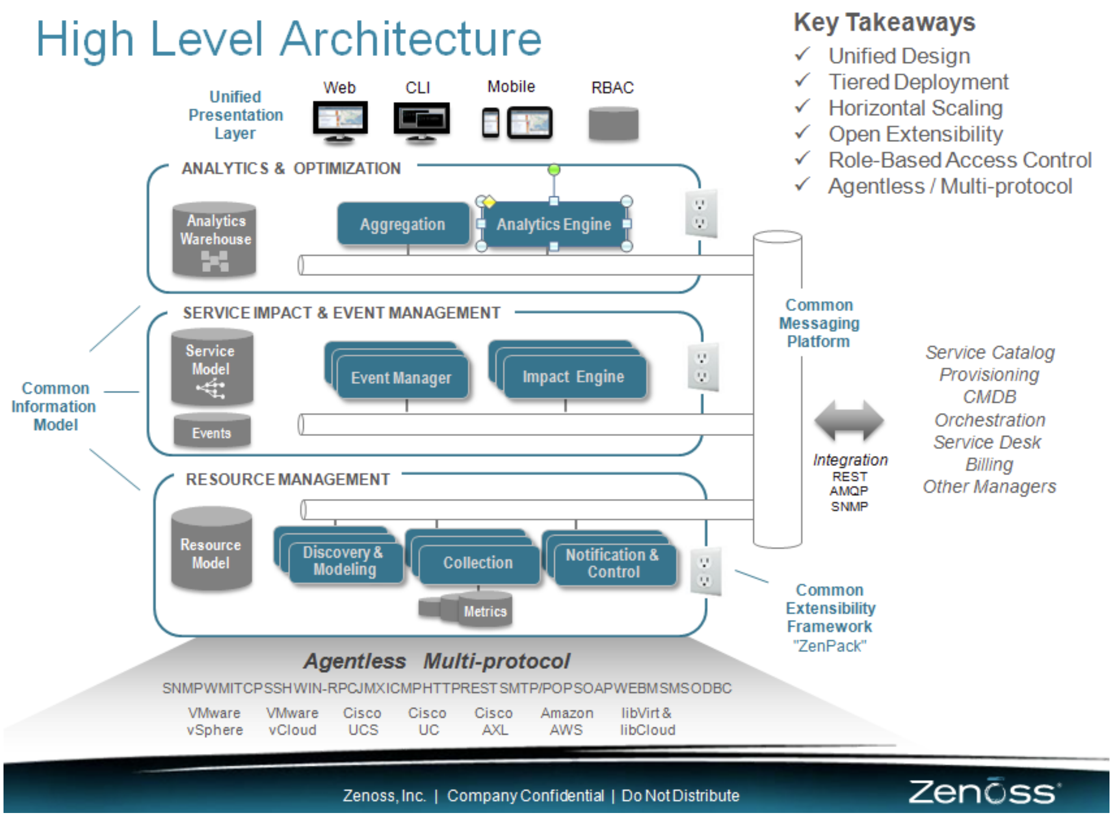
Zenoss Cloud Service Assurance Architecture Highlights

This section highlights the key aspects of the Zenoss CSA architecture that distinguish it from other platforms. Some of the key architecture characteristics are listed below.

- **Unified Design**. End-to-end service assurance and analytics capability designed from the ground up as one product on a common architecture.
- **Horizontal Scaling**. Scale the deployment to manage hundreds of nodes from a single server to 100K nodes in a globally distributed configuration, leveraging low-cost hardware. Scale as needed to manage elastic infrastructure.
- **Agentless, Multi-Protocol**. Agentless collection and control platform that leverages a suite of secure access methods, management APIs, and synthetic transactions to instrument the full stack at scale without the need for proprietary agents.
- **Open Integration and Extensibility Framework**. Rapidly extend, customize, and integrate with other management tools, leveraging open architecture and "ZenPack" plug-in framework. Leverage a global community of extension developers and partners.
- **Integrated RCA and SIA**. RCA is performed as a side product of the SIA, as opposed to traditional systems, which perform two functions using two different sets of rules, models, or even products. This simplifies development of customizations, as well as provides direct relationship between root cause events and service impact events caused by the root cause events.

Figure 4-4 and Figure 4-5 highlight the key aspects of the Zenoss CSA architecture.

Figure 4-4 High-Level Architecture

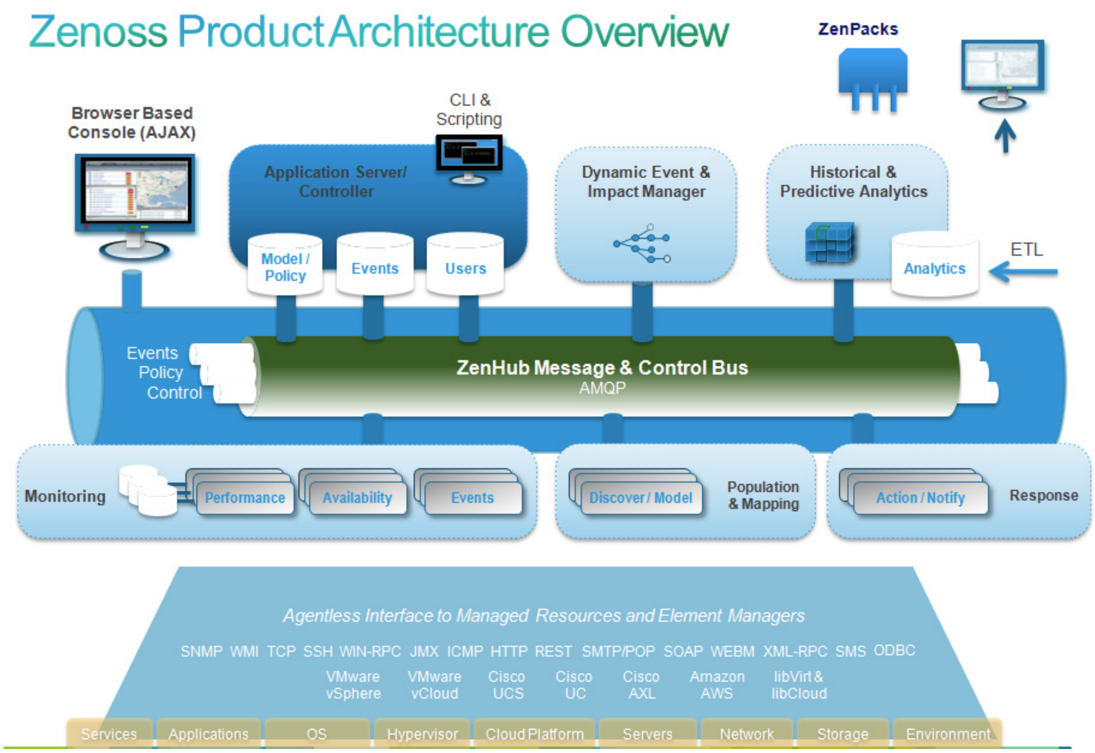


High Level Architecture

Key Takeaways

- ✓ Unified Design
- ✓ Tiered Deployment
- ✓ Horizontal Scaling
- ✓ Open Extensibility
- ✓ Role-Based Access Control
- ✓ Agentless / Multi-protocol

Figure 4-5 Zenoss Product Architecture Overview


Zenoss Product Architecture Overview
ZenPacks
Browser Based Console (AJAX)
CLI & Scripting
Application Server/ Controller
Model / Policy
Events
Users
Dynamic Event & Impact Manager
Historical & Predictive Analytics
Analytics
ETL
Events
Policy
Control
ZenHub Message & Control Bus
AMQP
Monitoring
Performance
Availability
Events
Discover / Model
Population & Mapping
Action / Notify
Response
Agentless Interface to Managed Resources and Element Managers
SNMP WMI TCP SSH WIN-RPC JMX ICMP HTTP REST SMTP/POP SOAP WEBM XML-RPC SMS ODBC
VMware vSphere
VMware vCloud
Cisco UCS
Cisco UC
Cisco AXL
Amazon AWS
libVirt & libCloud
Services
Applications
OS
Hypervisor
Cloud Platform
Servers
Network
Storage
Environment