TIVOLI NETCOOL USER SYMPOSIUM

Enterprise Event Management for the Defense Intelligence Agency

Roberta Hilton

Defense Intelligence Agency

-and-

James Brunke

Crystal Technology Solutions Group Inc

jbrunke@ctsgi.com

ALIGN. ACCELERATE. INNOVATE.

Agenda

- Current State
- Problem Statement
- Business Impact
- End State Vision
- Solution Set
- Approach & Guidelines
- High Level Architecture
- Design Details
- Transitional Challenges

Current State

- Globalizing Enterprise Management
  - Regional Service Center (RSC) represents the transformation of the Department of Defense (DoD) Intelligence Information System (DoDIIS) architecture to a centrally managed, regionally executed, delivery of information technology (IT) services.
    - Culture that supports and stimulates an open exchange of ideas across the workforce
- Multiple RSCs manage IT infrastructure independently

Numerous disparate “mini-enterprises”

- No consolidated view of the entire enterprise or common operational pictures
- No means to view support services and capabilities and their dependencies (most monitoring currently being accomplished from a an IT centric, functional perspective)
- Many capabilities, but most are not “visible”
  - Significant gap in current monitoring/management capabilities of core services and capabilities/services
  - Some global capabilities being monitored regionally
- Various monitoring/management maturity levels across a un-joined enterprise
- No centralized (hierarchical) reporting structure
- No global service management process

Lack of understanding of the performance, cost, and effectiveness of the enterprise

- Lack of common processes, criteria, and capabilities
- Requires a common measurement methodology AND common tools
- The hard work of establishing realistic and achievable performance metrics has not begun.
  - Establish Operational Level Agreement (internally) first.
  - Use existing proven SLA's as the benchmark
  - Determine how external dependencies will be addressed (i.e. what about the elements we don't control such as the DISA backbone)
- Common, global RSC Service Management (incident, problem and change management for example) processes essential
- CMDB scalability required for event enrichment
- Determining what we will measure

Various interpretations of what constitutes a service

- No authoritative source of global services
- No means to classify existing services as regionally hosted applications
- Service management requires service modeling and mapping

Business Impact

- Critical war-fighting intelligence support capabilities remain “invisible” until the phone rings
- Inconsistency in service performance and accountability of the services offered
- Transitional efforts to improve the characteristics of the enterprise become too loosely defined to measure successes

End State Vision

- Become an integrated enterprise with one team, one vision, one strategy, and one mission
- Be customer driven in every effort and with every investment
- Create and drive a strategic process that creates and maintains a sustainable and renewable enterprise
- Create and manage a single and integrated services delivery infrastructure across the IT enterprise
- Improve customer, partner and employee relationships by aggressive participation in, and by leveraging data from, this common infrastructure by all members
- Provide well managed and respected stewardship of all IT resources, budget and assets

Enterprise Management Took Kit (EM/tk)

- Design an enterprise approach that evaluates the health of the enterprise
- Design an enterprise solution and recommend tools to assure enterprise entities are performing and providing proactive service
- Provide policy and standards to assure all components entering the enterprise are monitored and/or managed

EM/tk - Mission Statement

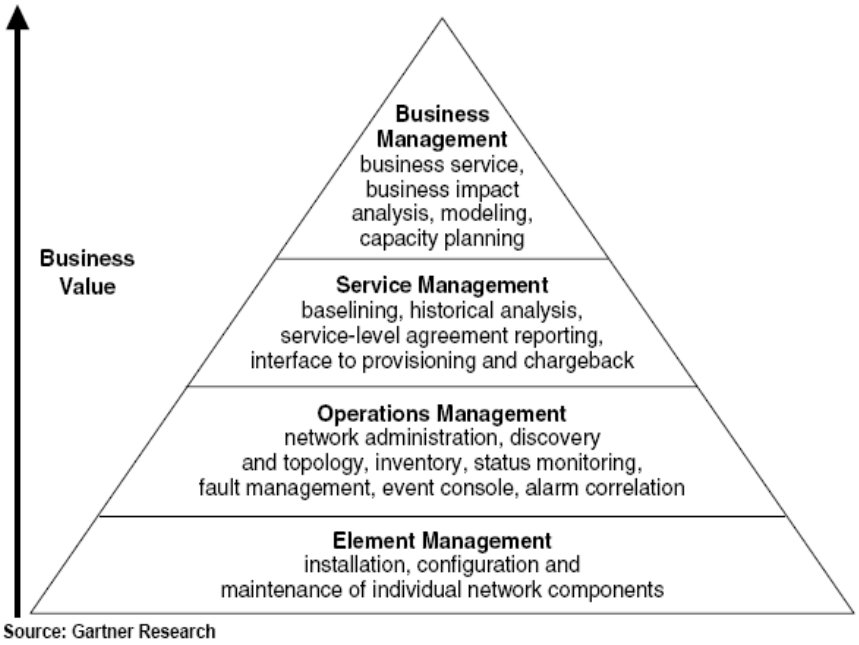
Design, integrate, and implement the ability to collect and correlate events from the IT infrastructure to analyze, predict, and react to mission and service impacts

- Improve end-to-end availability of services
- Improve user satisfaction with the services received
- Service availability rather than component availability
- Proactive vs. Reactive
- Vehicle to establish performance and reliability matrix
- Improve understanding of the components within the infrastructure responsible for the delivery of end-to-end services

Approach & Guidelines

- Outside looking in: Customer focused
- Use an end-to-end enterprise service management approach
- Use established *Industry Best Practice* models such as ITIL as the operational enterprise service delivery framework
- Acknowledge missing critical path processes and capabilities
- Use existing capabilities to the extent possible
- Use best of breed monitoring tools in each of the functional areas
- Apply solutions to all layers on the enterprise (Applications, middleware, OS's, hardware, LAN, and facilities)
- Maintain long term integration objectives in initial capability solution sets
- Provide regional, supporting, and global enterprise views
- Limit scope and initial capabilities

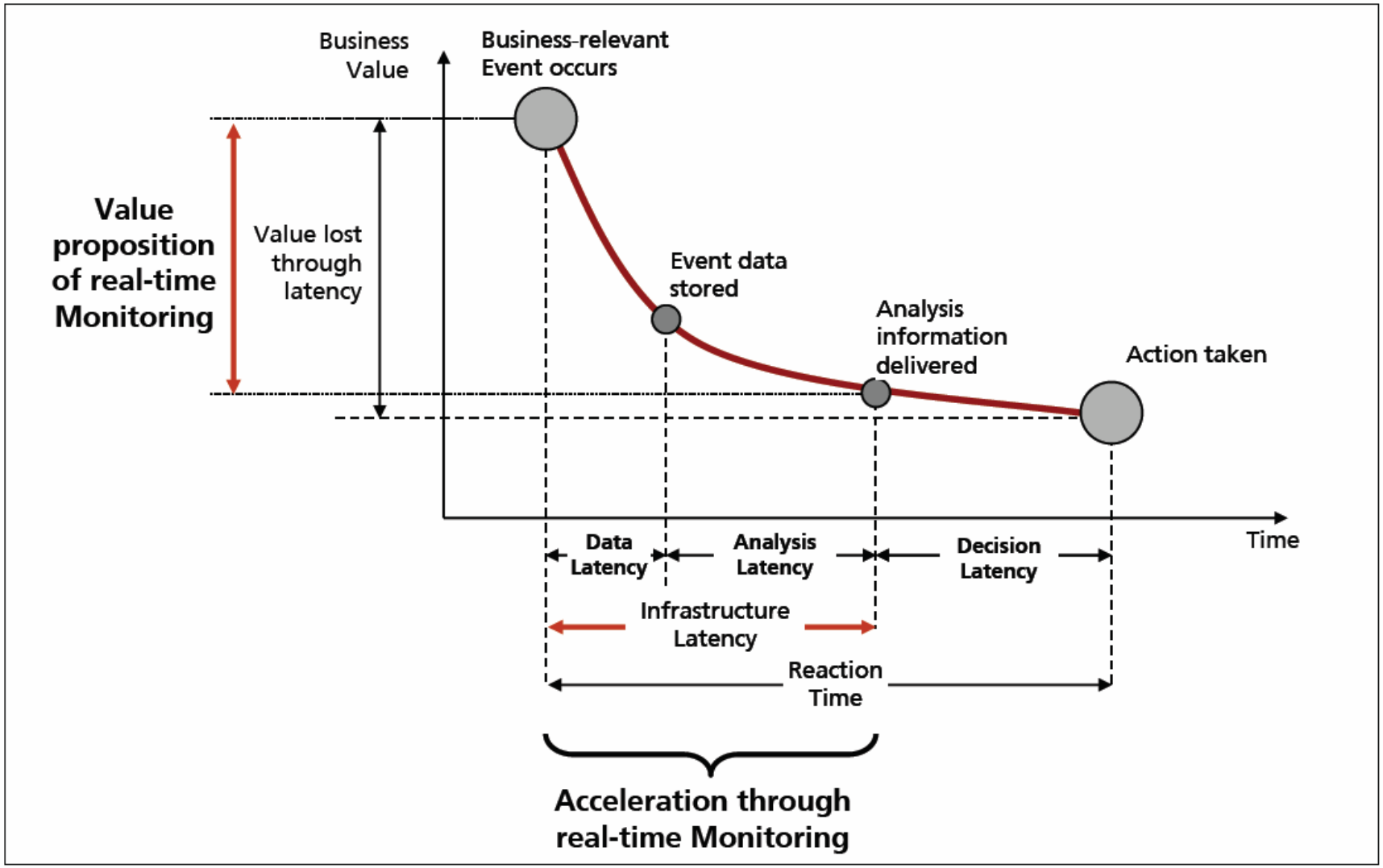
Tiered Approach



Source: Gartner Research

- Segmenting network management tools provides enterprises with a framework to target investments
- Investing in tools addressing higher layers of the framework is important
- **Implementing lower-layer tools should take precedence so that a strong foundation can be built**
- No one vendor can provide the total solution
- Include criteria representing the strength of vendor partnerships, synchronization and re-use of data across management layers, and the degree of integration among tools

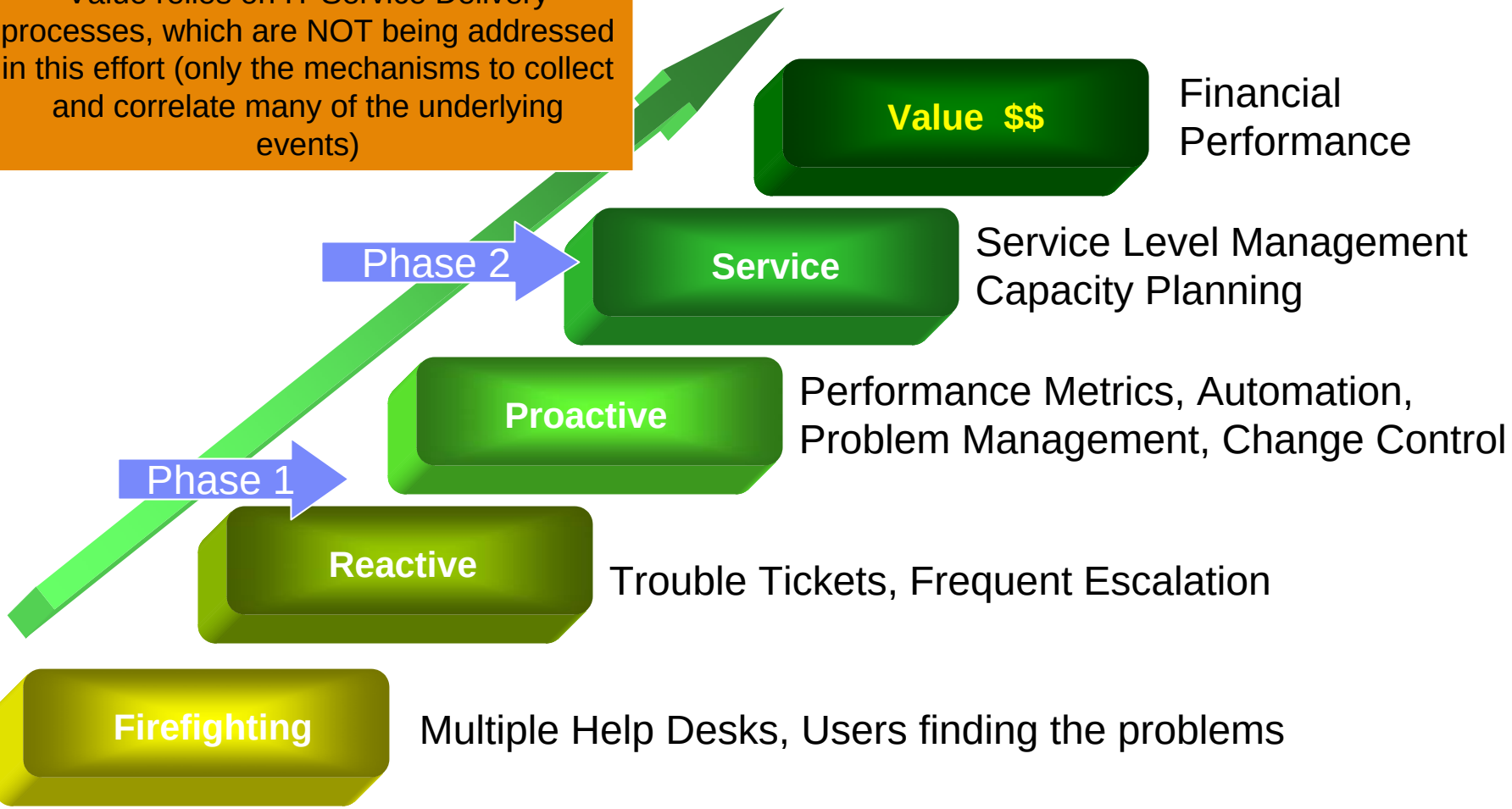
Scope of Effort



Source: compare Hackathorn, 2002

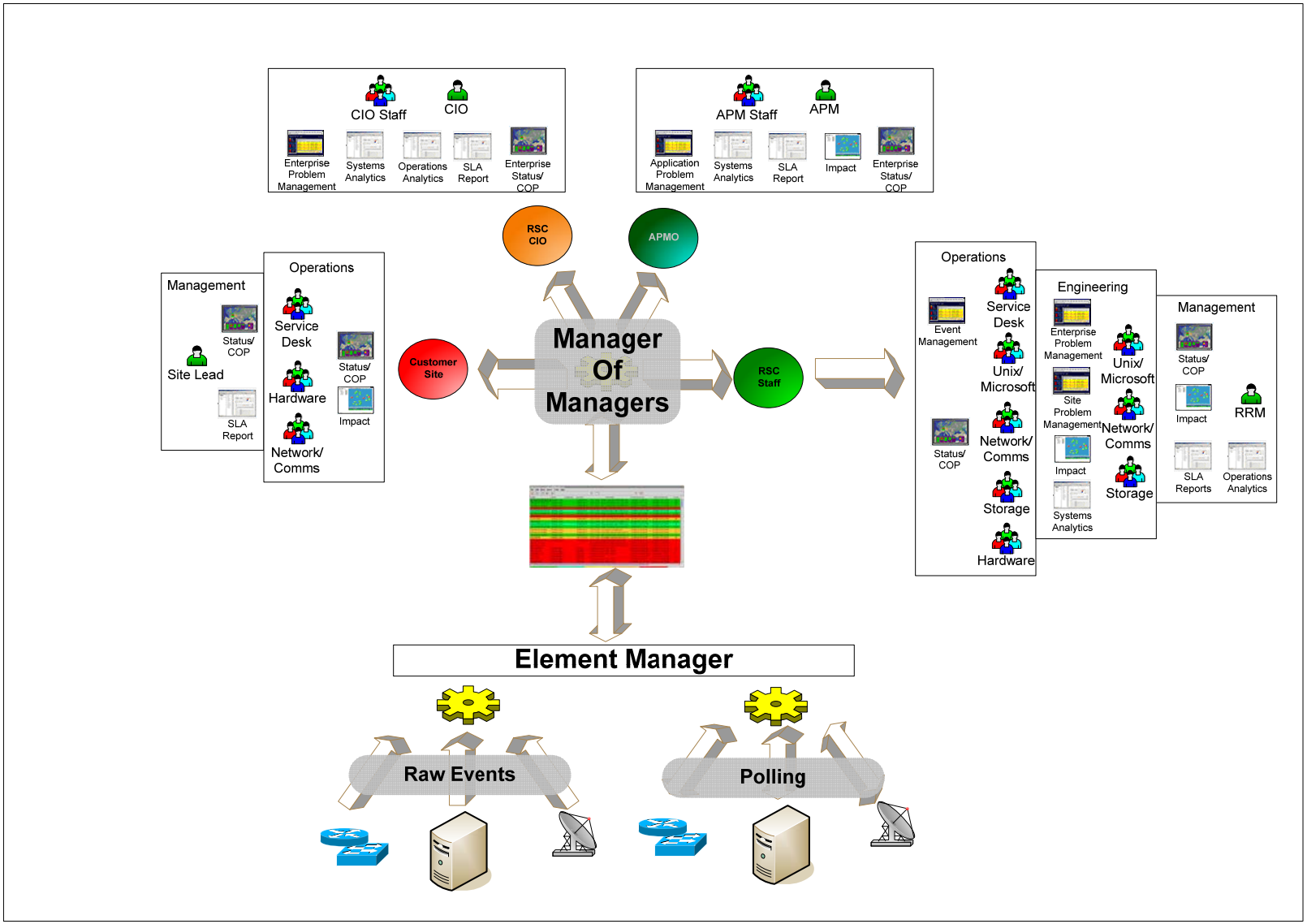
Phased Approach

Value relies on IT Service Delivery processes, which are NOT being addressed in this effort (only the mechanisms to collect and correlate many of the underlying events)



Source: The Gartner Group Capability Maturity Model

High Level Architecture



Software Products

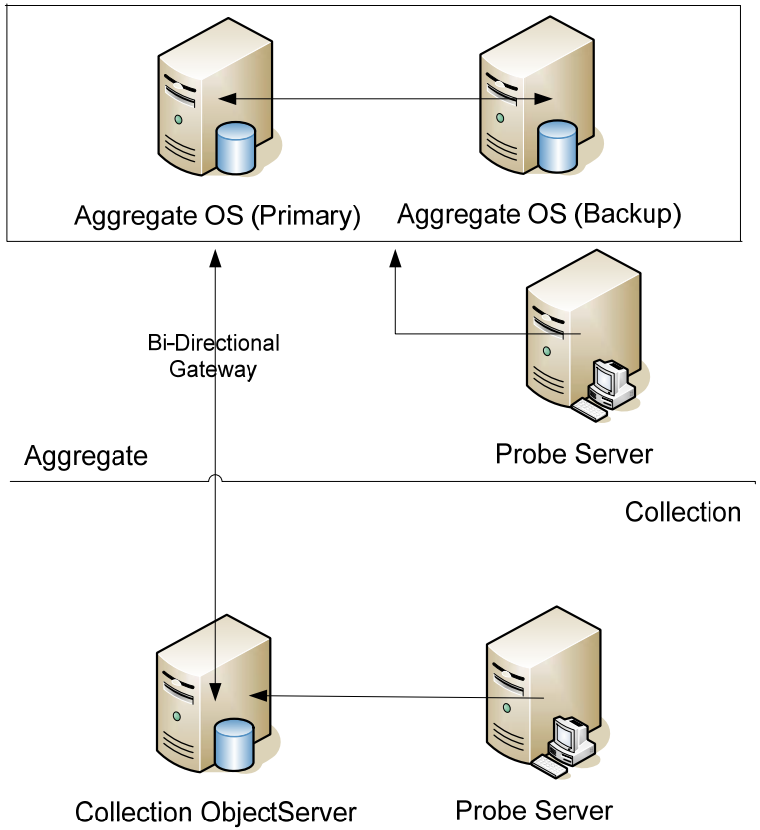
- Manager of Manager – Tivoli Netcool (OMNIbus, RAD)
- Microsoft Element Manager – Microsoft Operations Manager
- Unix Element Manager – CA System Edge
- Network Element Manager – Tivoli Netcool/Precision
- Voice over IP Manager – TBD
- Others…

Requirements Driving the Design

- Utilize existing product investment
- Provide most functionality at lowest possible cost
- Immediate failover not required for Phase 1
- Must distinguish local site events from global events

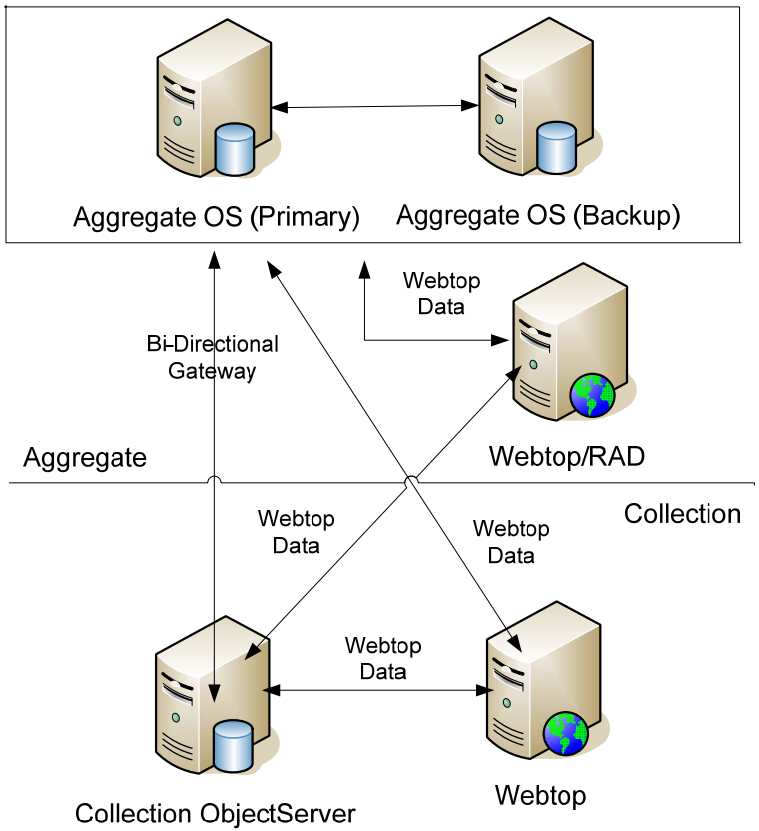
ObjectServer Configuration

- “Modified” 3-tier architecture
- Multiple Collection layer OS feeding into a redundant pair of Aggregate OS
- Aggregate OS located in different sites
- No Display Layer OS
- No redundancy in Collection layer OS
- Probes/Gateways will be failed over directly to Aggregate layer OS (scripted)
- Aggregate OS also perform duty as Collection OS for their local site



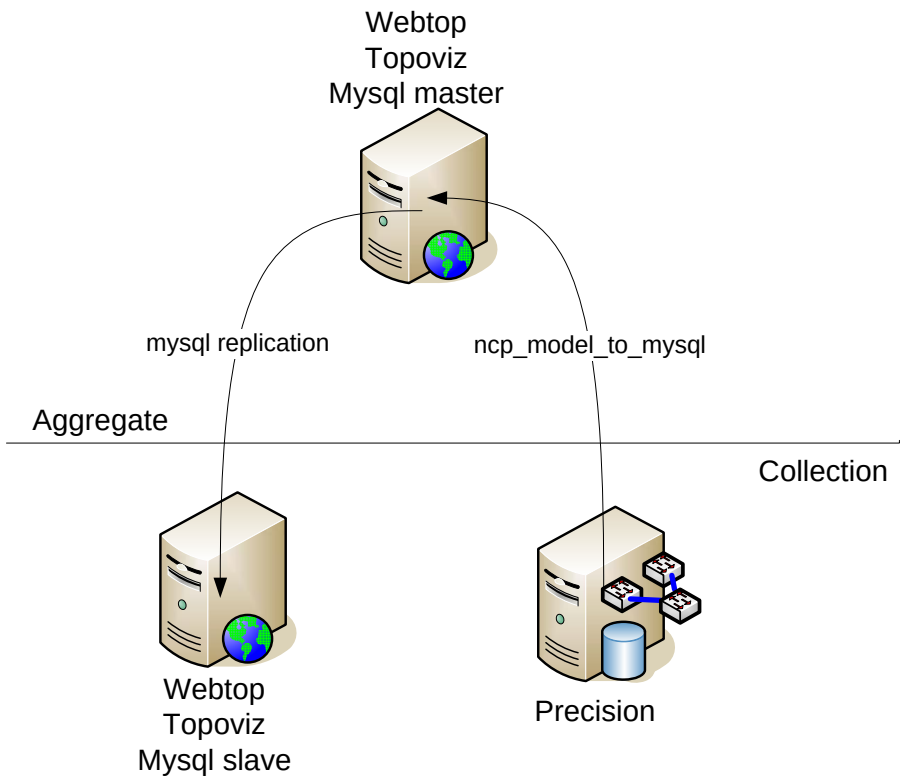
Webtop Configuration

- Webtop/Topoviz (NGF) servers at each Collection site
- Webtop/Topoviz/RAD (NGF) servers at each Aggregate site
- Each RAD server connects to Aggregate OS and Collection OS
- Each Webtop server connects to local Collection OS and Aggregate OS pair
- Users can login to Webtop at Aggregate layer if local Webtop server fails



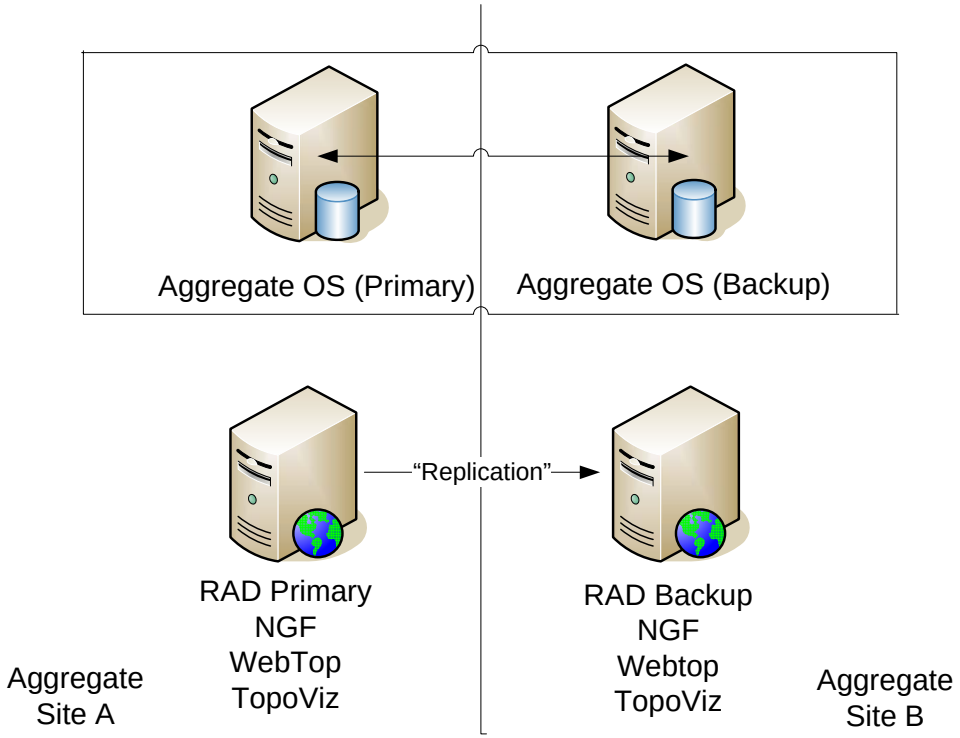
Precision Configuration

- Precision server setup to discover manage objects in each site
- RCA performed with local Collection ObjectServer
- All domain model saved in centralized master mysql database
- Network topology for visualization “pushed” to each local Webtop server via mysql replication



RAD Configuration

- Both display servers will be available for event/topology views
- Aggregate Site A runs Primary RAD Server
- Periodically configuration data will be “replicated” to server in Aggregate Site B



Other Design Details…

- Probes
- Netcool Knowledge Library
- Gateways
- Internet Service Monitors
- Impact
- AppDisco / TADDM
- SyslogNG
- Subversion
- Active Directory
- Operating System

Transitional Challenges

- $$$
- Disparate event management architectures
- Managing the final enterprise solution
- Managing change
- Lack of authoritative CMDB
- Service Catalog
- Absence of enterprise IT service delivery processes
- Resource allocation

IBM

Questions?

Thank you!