

Monitoring Heterogeneous Environments

Darren Mar-Elia
President & CTO
SDM Software, Inc.

Agenda

- Heterogeneous monitoring historically
- Solutions for heterogeneous monitoring
 - Demo
- Systems versus application monitoring
 - .NET and Java
- What's next?
 - State-based monitoring
 - True Business Service Management
 - The impact of Web services & SOA

Heterogeneous Monitoring Historically

- Cross-platform monitoring has been around since Windows became a viable enterprise platform in the mid-90s
- Historically implemented on Unix-based monitoring frameworks
- The history of these was to bring Unix-like tools to Windows

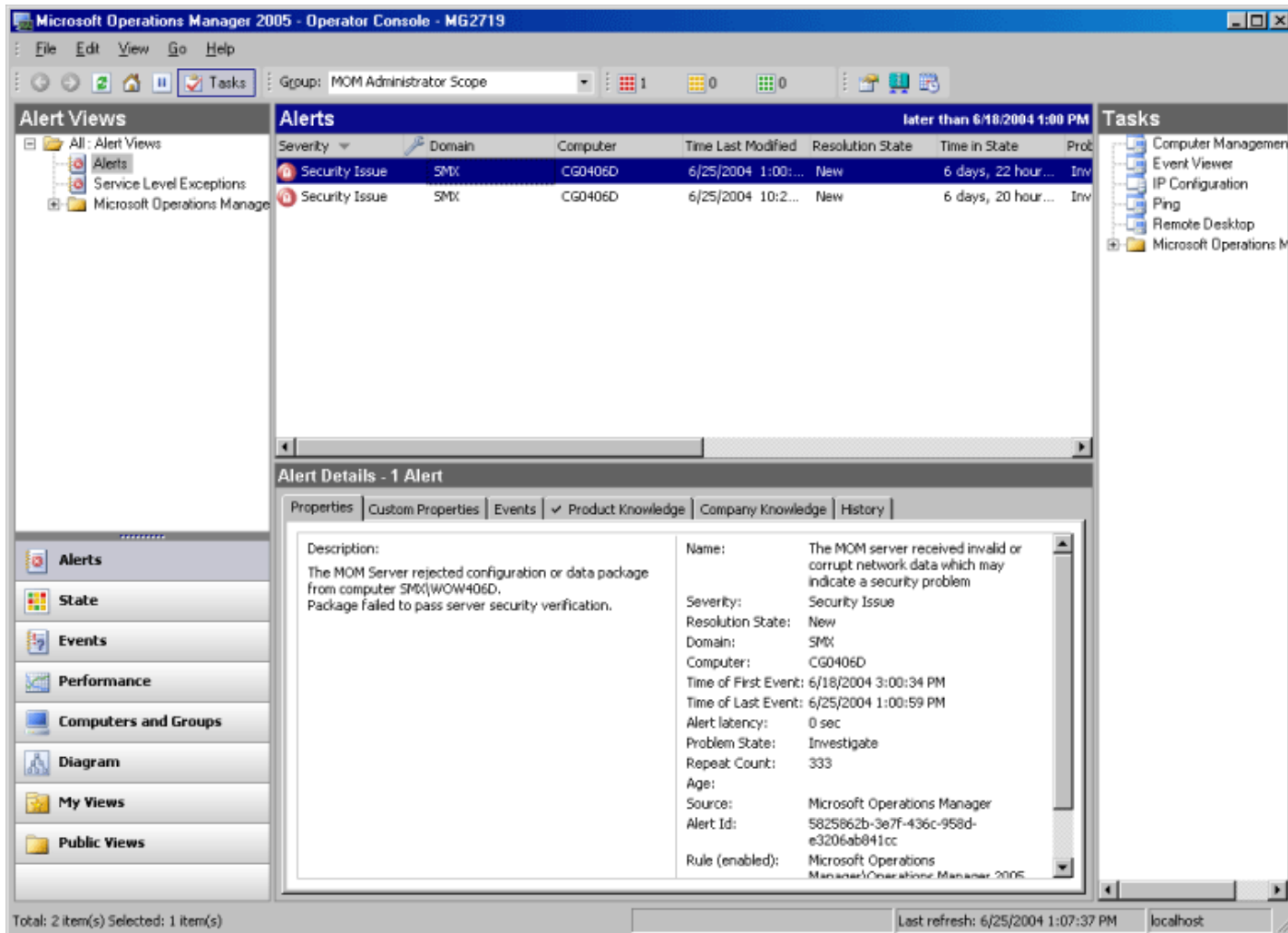
Heterogeneous Monitoring Historically

- Early solutions were “least-common denominator” instrumentation for Windows
 - SNMP
 - Didn’t “understand” Windows-specific platform issues
 - E.g. early versions of Tivoli used Windows-based BASH shell scripts to query counters
- Unfamiliar management interface for Windows admins

Heterogeneous Monitoring Historically

- NetIQ AppManager and Microsoft Operations Manager (MOM) raised the bar for Windows monitoring
- In many enterprises, Unix-based frameworks like Tivoli and HP OpenView were and are still the “monitor of monitors”

Microsoft Operations Manager



The screenshot displays the Microsoft Operations Manager 2005 Operator Console. The main window shows a list of alerts under the 'Alerts' tab, filtered for 'later than 6/18/2004 1:00 PM'. Two alerts are visible, both categorized as 'Security Issue' on computer 'CG0406D' in domain 'SMX'. The first alert occurred on 6/25/2004 at 1:00:59 PM, and the second at 10:2:33 AM. Both are in a 'New' state and have been in that state for over 6 days.

The 'Alert Details - 1 Alert' pane is expanded, showing the following information:

- Description:** The MOM Server rejected configuration or data package from computer SMX(\WOW406D). Package failed to pass server security verification.
- Name:** The MOM server received invalid or corrupt network data which may indicate a security problem
- Severity:** Security Issue
- Resolution State:** New
- Domain:** SMX
- Computer:** CG0406D
- Time of First Event:** 6/18/2004 3:00:34 PM
- Time of Last Event:** 6/25/2004 1:00:59 PM
- Alert latency:** 0 sec
- Problem State:** Investigate
- Repeat Count:** 333
- Age:**
- Source:** Microsoft Operations Manager
- Alert Id:** 5825862b-3e7f-436c-958d-e3206ab041cc
- Rule (enabled):** Microsoft Operations Manager\Operations Manager 2005

The interface includes a left-hand navigation pane with options like 'Alerts', 'State', 'Events', 'Performance', 'Computers and Groups', 'Diagram', 'My Views', and 'Public Views'. A right-hand pane shows 'Tasks' such as 'Computer Management', 'Event Viewer', 'IP Configuration', 'Ping', and 'Remote Desktop'. The status bar at the bottom indicates 'Total: 2 item(s) Selected: 1 item(s)' and 'Last refresh: 6/25/2004 1:07:37 PM'.

Separation of Duties

- Windows-only monitors control monitoring of Windows
 - Often report up to a framework
- Made sense -- Windows admins and *nix admins rarely mixed duties
 - Data center reporting and trouble handling is usually platform agnostic

Platform-Agnostic Management

- The trend to platform-specific management is reversing
 - Strapped IT shops lower the “religious” boundaries
 - Admins becoming general purpose
- Ultimate goal is that, regardless of Windows, Linux, Unix, MacOS, management is seamless
 - We’re not there yet but moving in the right direction

Heterogeneous Monitoring from Windows

- MS-MOM (System Center Operations Manager)
 - A major platform for extending Windows monitoring to non-Windows environments
- **NetIQ** and other “low-cost” monitoring solutions such as **What’sUp Gold** (www.ipswitch.com) and **Big Brother** (www.bb4.com) introduced cross-platform monitoring from Windows

Protocols Make It Work

- Least-Common Denominator is common
 - SNMP
 - SSH/Shell Scripts
- Some are getting more sophisticated however
 - Quest/Vintela implements a native “WBEM” stack on *nix to fully instrument those systems
 - Platform vendors are beginning to incorporate better instrumentation
 - (e.g. Novell’s adoption of OpenWBEM)
 - Check out <http://sourceforge.net/projects/openwbem/> for more details

Windows-based Products

- MOM extensions from vendors like Quest Software and eXc (www.excsoftware.com) bring non-Windows monitoring into the MOM console seamlessly.
 - Unix & Linux systems look like Windows boxes
- Each takes a different approach
 - Quest implements native agents on *nix using WBEM
 - eXc uses shell script based proxy agents from Windows (no code runs on *nix platforms)

Monitoring non-Windows from MOM –eXc Software

System Center Operations Manager 2007 - EXCRC2

File Edit View Go Actions Tools Help

Search Scope Find Actions

Monitoring

- Monitoring
 - Active Alerts
 - Computers
 - Discovered Inventory
 - Distributed Applications
 - Task Status
 - Agentless Exception Monitoring
 - Microsoft Windows Client
 - Microsoft Windows Server
 - Network Device
 - non-Windows system/devices
 - non-Windows Alerts
 - non-Windows Events
 - non-Windows Performance
 - non-Windows Proxy Computers State
 - non-Windows State
 - Operations Manager
 - Synthetic Transaction
 - Web Application

Show or hide views...
New view ▶

- Monitoring
- Authoring
- Reporting
- Administration
- My Workspace

non-Windows Performance

Legend

| Show | Color | Path | Target | Object | Counter |
|-------------------------------------|--------------|-----------------|-------------|--------------------|---|
| <input type="checkbox"/> | purple | OM2007RC2.mm... | Linux1 | lo Ipkts | Ipkts |
| <input type="checkbox"/> | light blue | OM2007RC2.mm... | Linux1 | DISK: /dev/hda5 | space used % |
| <input checked="" type="checkbox"/> | green | OM2007RC2.mm... | Linux1 | CPU | idle% |
| <input type="checkbox"/> | dark green | OM2007RC2.mm... | Linux1 | MEM | free |
| <input checked="" type="checkbox"/> | blue | OM2007RC2.mm... | Linux1 | network connect... | login latency (sec.) |
| <input type="checkbox"/> | pink | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/1... | CISCO SWITCH OUTBOUND buffers swapped out (E |
| <input type="checkbox"/> | light green | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/1... | CISCO SWITCH OUTBOUND KB/sec |
| <input type="checkbox"/> | light blue | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/4... | CISCO SWITCH INTERFACE RELIABILITY % |
| <input type="checkbox"/> | yellow-green | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/2... | CISCO SWITCH OUTBOUND packets/sec |
| <input type="checkbox"/> | dark green | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/2... | CISCO SWITCH OUTBOUND buffer failure (Errors) |
| <input type="checkbox"/> | dark blue | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/1... | CISCO SWITCH OUTBOUND Output Errors |
| <input type="checkbox"/> | blue | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/8... | CISCO SWITCH INBOUND runts (Errors) |
| <input type="checkbox"/> | cyan | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/2... | CISCO SWITCH INTERFACE RXLOAD % BUSY |
| <input type="checkbox"/> | yellow | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/7... | CISCO SWITCH OUTBOUND lost carrier (Errors) |
| <input type="checkbox"/> | yellow-green | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/1... | CISCO SWITCH OUTBOUND KB/sec |
| <input type="checkbox"/> | orange | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/1... | CISCO SWITCH OUTBOUND Output Errors |
| <input type="checkbox"/> | purple | OM2007RC2.mm... | CiscoSwitch | FastEthernet0/3... | CISCO SWITCH INTERFACE RXLOAD % BUSY |

Actions

Performance Actions

- Save image as...
- Copy image to clipboard
- Copy data to clipboard
- Select time range...
- Personalize view...

Baseline

- Resume the baseline
- Pause the baseline
- Reset the baseline

eXcSoftware.nonWindows.non...

- Issue Command

eXcSoftware.nonWindows.non...

- Alert Logging Latency
- Alerts
- Availability
- Configuration Changes
- Custom Configuration
- Custom Event
- Event Analysis
- Most Common Events

Resources

- Microsoft Operations Manager Help
- Microsoft Operations Manager Online

Ready

Advantages of Monitoring *nix from Windows

- Familiar Windows interface
- Lower cost
- Reduced complexity

Windows Monitoring Challenges

- Least-common denominator instrumentation
 - Better cross-platform management standards begin to help this
- Unfamiliar interface for Unix admins
- Licensing costs versus open-source solutions

HETEROGENEOUS MONITORING DEMO

System vs. Application Monitoring

- Health of a component (e.g., server) versus health of application
- Component monitoring is a commodity now!
- Pricing pressures for component monitoring
 - Good for customers, bad for vendors

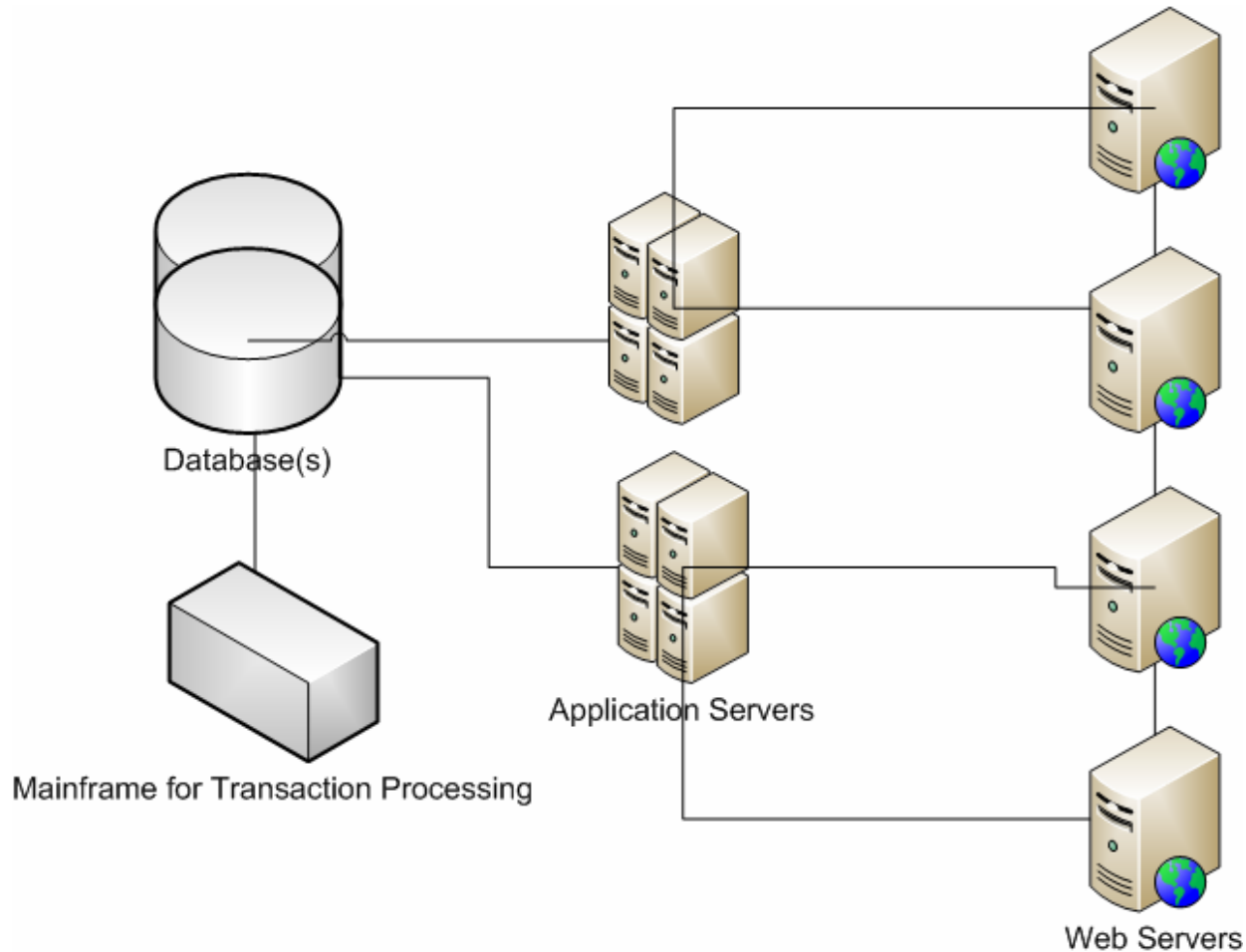
System vs. Application Monitoring

- Application monitoring presents bigger challenges
 - Enterprise applications live in multiple tiers across multiple servers
- “Up” and “Down” are less obvious
- What is the state of my applications?
 - From client to database

End-to-End Application Monitoring

- Health of an application requires complex instrumentation
- And an end-to-end view of application performance
 - Client application response times (Web-based and rich-client)
 - Network latencies
 - Front-end Web servers, business logic tiers, back-end databases

Application Landscape Today



End-to-End Application Monitoring

- Growing need for application transaction profiling
 - Understand the context of a transaction
- Vendors are not delivering on the dream yet
- Most customers are still trying to get their hands around the silos that compose an application
- Application monitoring is now a must-have

.NET and Java

- Java application monitoring solutions have been around for a while
- .NET is just now starting to find the enterprise traction
 - Vendors are starting to catch up
- But most customers have these environments silo'd

.NET and Java

- Vendors still focus on the silos
- Very few “composite” apps
- Will probably remain that way for a while
 - Service Oriented Architectures (SOA) will probably move this change along
- Monitoring Java apps versus .NET apps – similar challenges

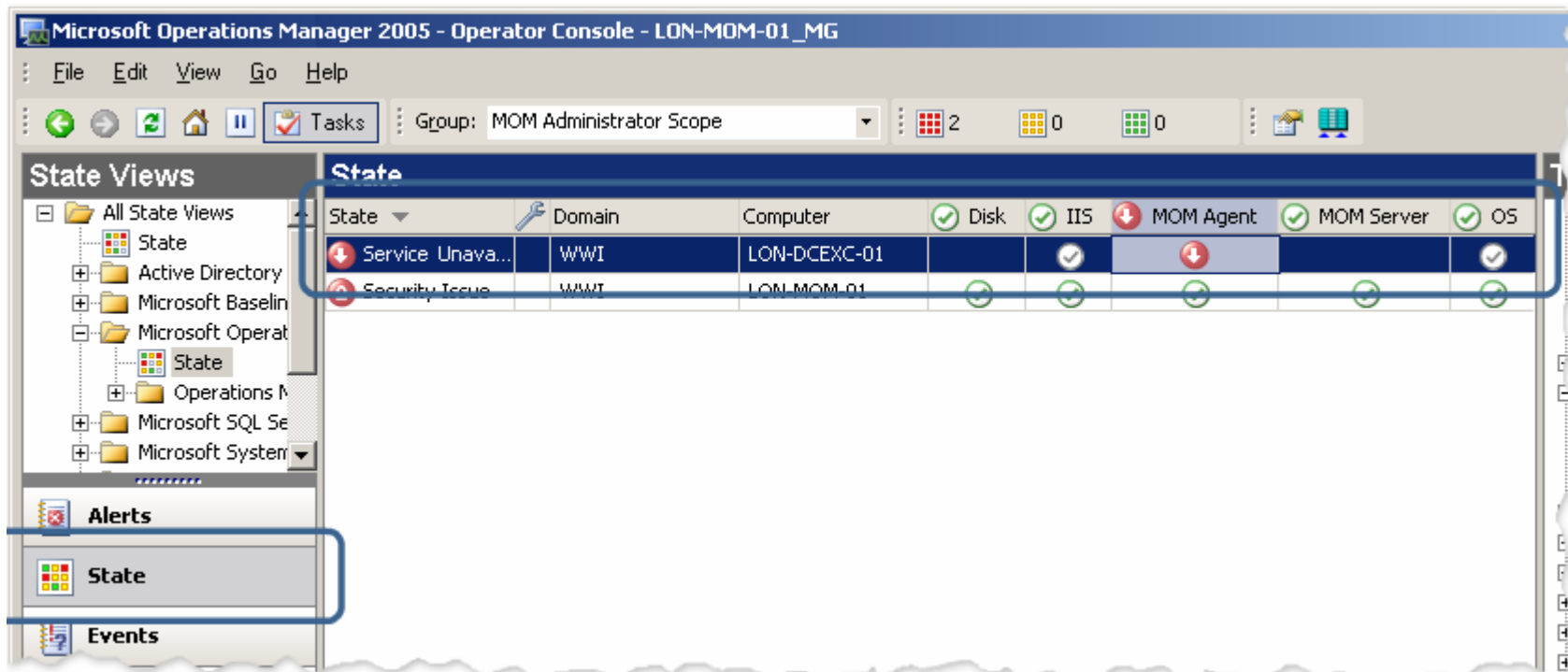
Application Monitoring Vendors

- Most of the small monitoring solutions have been gobbled up—only the “big” guys a few tier-two players remain:
 - HP/Mercury
 - IBM/Tivoli
 - CA/Wily
 - BMC
 - Symantec/Veritas/Precise
 - Quest/Foglight

The Future

- Monitoring “state” of a service is a maturing of the component model
 - Close to end-to-end monitoring but different
- A service has a set of interdependent components with known healthy states
- State monitoring looks for unhealthy conditions amongst a set of interdependent components
- A good example is MS-MOM

MOM State-Monitoring



Microsoft Operations Manager 2005 - Operator Console - LON-MOM-01_MG

File Edit View Go Help

Tasks Group: MOM Administrator Scope

State Views

- All State Views
 - State
 - Active Directory
 - Microsoft Baselin
 - Microsoft Operat
 - State
 - Operations M
 - Microsoft SQL Se
 - Microsoft System
- Alerts
- State
- Events

State

| State | Domain | Computer | Disk | IIS | MOM Agent | MOM Server | OS |
|------------------|--------|--------------|------|-----|-----------|------------|----|
| Service Unava... | WWI | LON-DCEXC-01 | ✓ | ✓ | ✗ | ✓ | ✓ |
| Security Issue | WWI | LON-MOM-01 | ✓ | ✓ | ✓ | ✓ | ✓ |

Business Service Management

- BSM has been around for a while
- Tying IT to the business more closely
 - Gets IT thinking about components as business services
- Up until now, just a pipe dream for most vendors and customers
 - Because it's hard!

Business Service Management

- Biggest drivers
 - Lower IT costs
 - Improve business relevance
- Vendors are starting to figure this out as well (BMC is a good example here)

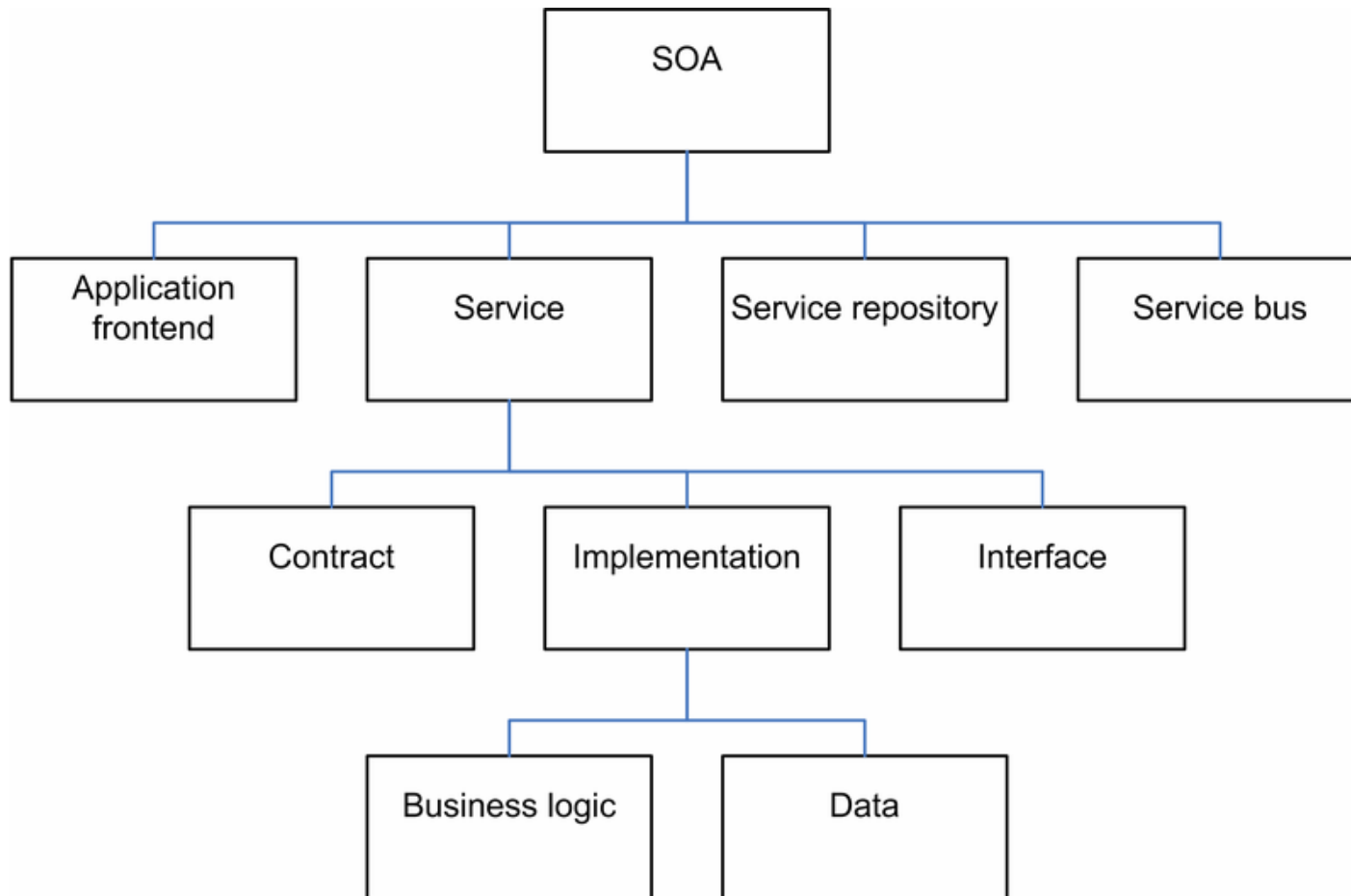
BSM

- A function of maturity for IT shops
 - Silos have evolved into managing of business services
- Still the holy grail for a lot of organizations

SOA & Web Services

- SOA is a hot topic for many organizations
- Reality is that many are early, if at all, down this road
- SOA does change the monitoring landscape
- Monitoring loosely coupled, asynchronous services communicating with each other is hard!

SOA Architecture



SOA & Web Services

- Most current SOA implementations are familiar request-reply types of services
 - Lends itself to traditional application monitoring
- Service-bus oriented SOA is starting to get traction
 - Will change the monitoring needs and landscape

SOA & Web Services

- WS and SOA are platform-agnostic
 - Composite .NET/Java services more common as SOA implementations increase
- The silos will have to crumble!

SOA Monitoring Vendors

- The big guys are in this market
- But also some smaller vendors
 - Certagon (www.certagon.com)
 - Symphoniq (www.symphoniq.com)
 - Tidal Software (www.tidalsoftware.com)

Thank You!