IT Service Management

Monitoring and Log Management in Hybrid Cloud Environments
Agenda

- Overview Hybrid Service Management
- Monitoring
- Log Management
- Closing
Agenda

- Overview Hybrid Service Management
- Monitoring
- Log Management
- Closing
What is IT Service Management?

IT Service Management encompasses:

- the methods, tools and processes by which IT departments *support and enable* their ecosystem to deliver *business services*
- the framework by which *effectiveness and value of IT services* are measured
- support for *Agile, DevOps and Waterfall* methodologies
- both *engineering and operations* domains
- both *pre-production and production* phases/environments

Key ITSM domains and capabilities include, but are not limited to:

- Hosting a *catalog of IT services*, facilitating and coordinating the efficient *request* for and *fulfilment* of those services
- Managing *Business Process Availability & Resiliency* through the enabling technology
- *IT Service Assurance* – including Health/Performance of as well as Identification, Analysis and Resolution of issues associated with technology-enabled services
- *Full life-cycle management of IT* assets – be them hardware, software, application or virtual (e.g. cloud)
ITSM disciplines

- Increase delivery velocity and quality of new business services
- Resolve problems faster for increased quality of service and reduced costs
- Predict & prevent issues before they impact end users
- Drive efficiencies in business processes and asset utilization
The nature & requirements of Applications are evolving...

The era of Cloud requires digital engagement, rapid delivery of client facing applications, and new consumption models with focus on business outcomes and end user experience. Monitoring and analytics are no longer an option but an assumed requirement.
Two-Speed IT is Today’s Reality

1: Transform

- Systems of Record
- 1: Transform
  - Develop
  - Build
  - Test
  - Deploy
  - Production

2: Integrate

- Systems of Engagement
- 2: Integrate
  - Develop
  - Build
  - Test
  - Deploy
  - Production

3: Accelerate

- Rapid iterations
  - Develop
  - Build
  - Test
  - Deploy
  - Production

- Slower iterations
  - Develop
  - Build
  - Test
  - Deploy
  - Production

- Virtualize
  - Virtualize

- Accelerate
  - Integrate
  - Transform

Two-Speed IT is Today’s Reality

Systems of Record

- Transform
- Integrate
- Accelerate

Systems of Engagement

- Transform
- Integrate
- Accelerate

© 2015 IBM Corporation
Organizations are faced with challenges as they embrace Cloud Enabled and Cloud First Delivery Models

**Challenges and Shifts**

- Improve utilization of services to reduce costs
- Shifting to cloud models and new rental economy to accelerate delivery of services
- Optimize operations to drive efficiencies and improve quality of service

**Challenges and Shifts**

- Speed innovation and continuous delivery of applications
- Exploit new programming models, social, mobile
- Business and technology models that can react dynamically to end user demand
Agenda

- Overview Hybrid Service Management

- Monitoring
  - Log Management

- Closing
Performance Management in the new IT Demand Environment

A new level of performance requirements for traditional Operations….

Service Delivery

E-commerce 24/7 Business Model
How business is done today with customers are demanding even more…

Customer Retention

New technology and mobile applications
Keeping pace with consumer trends is challenging

Mean Time To Repair (MTTR)

Financial Impact
Immediate transactions and execution from any device is expected.

CIO

Line of Business Executive

IT Operations Manager
Who Uses APM & Why do they Care

Olivia the Application Owner
Talks to end users, ensuring they have a great experience and that the application succeeds.

End users

Devices

Web Servers

App Servers

Databases

Eric the Application Developer
Writes the code that runs on web and app servers and delivers value to the end users.

Kevin the IT Operations specialist
Manages the infrastructure that runs the applications.

APM = Application Performance Management
Application Performance Management
Reducing & Preventing Outages and Slowdowns for the 24/7 Application World

Applications consist of many parts, understanding issues can be complex

1. **Identify performance issues beforehand**
   - Unified user interface provides a single view across on-premise, public, and private cloud applications.
   - Best in class monitoring coverage: operating systems, middleware, packaged applications, transaction tracking and mainframe systems.
   - Simplified problem resolution with dashboards that identify applications and application components with issues.

2. **Isolate where the problem is occurring**
   - Visibility to end user experience of proprietary applications, identifies problems before SLAs are impacted.
   - Quickly isolate bottlenecks affecting application performance by tracking 100% of application transactions through the entire application domain.
   - Navigate from application status to application components to code level details in context using the same UI.

3. **Resolve issues before your business is impacted**
   - Method level statistics triggered automatically provides visibility and details into source code problems at the exact moment of an issue.
   - Search and diagnose problems using an integrated search facility which can quickly determine recommended actions to resolve issues.
   - Integrated Predictive Insights predicts potential outages when metrics exhibit anomalous behavior.
What is Application Performance Management?

Visibility, control and automation to intelligently manage critical applications in cloud, physical and hybrid environments.

- **Discovery**: Quickly find application resources
- **End User Experience**: Ensure SLA compliance
- **Transaction Tracking**: Rapid problem isolation
- **Diagnostics**: Domain-specific deep-dive and repair
- **Predictive Analytics**: Reduce outages & improve business performance

**shared data & common services**

- Understand the end-user experience
- Follow changing workloads
- See steps across the cloud

*Mobile devices & smart endpoints*  
*Highly virtualized applications, storage & networks*  
*Private, public & hybrid clouds*
Walk Through Example

- Transaction tracking isolates application level performance bottlenecks for WebSphere and .NET application environments

Application transaction monitoring
Detect which transactions (types) are contributing to a bad user experience.

Query the TopN list of transaction instances

Problem determination
View the TopN problematic transaction instances for this type.

Start an instance trace to correlate the end-to-end pieces

Identify root cause
Use the method trace to identify the line of code.

Launch into deep dive for the bottleneck

Isolate bottlenecks
Visualize where time is spent in the transaction.
What's in your application?

Ensure that you can cover their “stack” using the coverage catalog

The Network

Web Servers → App Servers → Databases +

Coding languages, Frameworks, Messaging, Packaged apps, Hypervisors, etc.

This is just a sample of IBM’s coverage

Go here for the list

Link to coverage catalog:
https://www.ibmserviceengage.com/application-monitoring/articles/supported-systems
Broad Support across the IT Landscape

https://ibm.biz/BdXtZh
Monitoring WebSphere Application Server instances

- Node name
- Server status
- Slowest response time (ms)
- JVM memory usage
- Logs status
- Connection pool status
- Heap usage
Details dashboards: Examining garbage collection statistics

More detail dashboards available:
- WebSphere queries
- EJB containers
- Messaging and messaging engines
- Thread pools
- Database connection pools
- Web services

1. Increased CPU usage
2. Increased heap usage
3. Spike in average response time
24x7 Global Website Monitoring – Points of Presence

Application Dashboard

Transaction Availability Over Time

Transaction Details

Subtransactions

Playback Locations

Location | Latest Status | Last Run At | Latest Response Time | Unavailable (%) | Slow (%) | Average Response Time
---|---|---|---|---|---|---
Washington | | Dec 02, 2014, 13:26 | 33.39 | 0.00 | 100.00 | 27
Singapore | | Dec 02, 2014, 13:28 | 21.07 | 24.32 | 75.68 | 37
End-to-End Monitoring, Tracking and Diagnosis

1. **End User Monitoring**
   Start by monitoring transaction performance and end-user problems.

2. **Transaction Tracking**
   Correlate data from app server, MQ, CICS, IMS, custom instrumentation, etc. to show topology and isolate problems.

3. **Deep Dive Diagnostics**
   Launch in context to SME tools where appropriate.
   In this scenario, the problem is a WebSphere JEE memory leak.

---

### Transaction Root Cause Analysis

<table>
<thead>
<tr>
<th>1. <strong>Sense</strong></th>
<th>2. <strong>Isolate</strong></th>
<th>3. <strong>Diagnose and repair</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Experience and alert on threshold violation</td>
<td>by measuring performance data against baseline through entire infrastructure</td>
<td>through launch-in-context into deep-dive diagnostics</td>
</tr>
</tbody>
</table>
Advanced Monitoring Topics

IT infrastructure monitoring solutions stream millions of health metrics with hidden symptoms.

IT Infrastructure streams terabytes of log data with hidden error messages.

... plus Dynamic Environments; Hybrid Environments, DevOps, etc.
**IBM Operations Analytics – Predictive Insights**

**Challenge:** Reacting to performance thresholds is not enough. IT Staffs must become proactive to ensure mission critical applications never go down.

**Automated Threshold Maintenance**
No complex manual intervention to setup & maintain with 5 times faster processing

**Anomaly Detection**
Alerting before potential issues become service impacting, enabling IT to shift from reactive to proactive

**On-Prem and SaaS**
Predictive Insights now available as a Service, providing additional value to our Performance Management solutions

**Supports Heterogeneous Environments**
Out-of-the-box integrations to IBM APM/ITM or 3rd-party monitoring solutions
Multivariate Analytics
Statistical models can discover mathematical relationships between metrics

The extent this can be achieved depends on a number of factors, such as: range and type of data, availability of data, and stability of environment. Analytics falls back to a single metric if metrics are unrelated.
Example Scenario: Internet Banking Application
Granger based analytics learns the mathematical relationship between metrics

- Learns ‘Web Response Time’ has a normal causal relationship with ‘User Requests’ - WRT gets slower as user load gets higher.
- If this healthy historical relationship breaks down, say due to a memory leak, an anomaly is raised immediately.
- The problem is detected even while WRT service is “good”.

Emerging problems can be detected even while service level are good in absolute term.

Internet Banking

A
User Requests

B
Web Response Time

D

E

F

G

H

I

Web Response Time

Anomaly Event
Business Impacted
WRT Bad
WRT Good

User Requests

Time

Early Warning
Simplify view into the health of the Application Environment

State of the Art Dashboard

- Take guesswork out of end user experience with smart drill downs
- Easy to understand dashboards
- Quickly renders data
- Customizable with a wide variety of charts and graphs and data sources
- Runs on mobile devices
Contextual Service Visibility

Balanced Scorecards & KPIs

Realtime Event & Root Cause Views

Realtime Service Dependency Views

SLA Performance Tracking

Contextual Views of Federated Data/Intelligence
Agenda

- Overview Hybrid Service Management
- Monitoring
- Log Management
- Closing
IT Operations is a Big Data challenge

- Typical Large Enterprise: 5000 servers + network + storage + middleware generates ~1.3 TB of availability & performance management data per day
- Multi-national / xSP with 20,000 servers + ... generates ~4.5 TB per day
- DevOps & Agile Development required by web- & mobile applications leading to frustration
- APM Digest 2012: 75% of Senior IT Execs dissatisfied with traditional management approaches, 30% claim they cannot predict potential outages

Operations & Line of Business demands insights to ...


Smarter Infrastructure becoming a Big Data opportunity

- Typical Enterprise generates 27 million tickets and 20 million work orders to manage 15 million unique assets – 1 TB of unstructured data a day
- Intelligent networked assets themselves produce data: voltage, power, temp, flow ... example: CEPCO managing 11 million residential smart-meters
- Opportunities to provide insights & trends on asset performance, reliability, & cost management
Operational IT Analytics Solution

**Optimized Performance**
- Optimize across your IT app infrastructure

**Proactive Outage Avoidance**
- Proactively avoid problems before they occur

**Faster Problem Resolution**
- Search quickly across massive amounts of data

---

IBM Operations Analytics

- Streams
- Apache Solr
- InfoSphere BigInsights
- Rave
- DB2

---

**Application Performance**
- Documentation

**System & Log Monitoring**
- Transactions

**Assets & Workorders**
- Alerts, Alarms & Events

---

**Operational Environment**
- Applications
- Systems
- Workloads
- Wireless
- Network
- Voice
- Security
- Mainframe
- Storage
- Assets
Challenge: To diagnose service problems in applications and the infrastructure supporting them involves analyzing incredible amounts of data.
Data Collection Technology

Application/system

Business Users

Application Components

App Developer/IT Ops Engineer

Push logs (Log File Agent, REST interface, Log stash)

Pull logs using remote monitoring (agent less option)

Log Analysis Server

© 2015 IBM Corporation
Log Monitoring Capabilities

- **Log Collection and Parsing**
  - Log agents for collection
  - Automated pattern discovery with generic annotation
  - Tooling to add annotations

- **Visualisation**
  - Quickly isolate the problem with dashboards
  - Complement the search investigation with integrated charting

- **Search Interface**
  - Rapidly search and correlate multiple logs to determine why a problem is occurring. Search in context of events, apps, tickets.
  - Save searches and charts to dashboards to speed future investigations

- **Expert Advise**
  - Search expert advice to resolve the problem

- **Insight Packs and Extensibility**
  - Pre-packed insights on key technologies such as WebSphere.
  - Ability to create and extend insight packs

- **Embedded Analytics**
  - SmartCloud Analytics embedded in Web API Management, Worklight, and more
Extraction of Meaning

Log file:

com.ibm.ws.webcontainer.servlet.ServletWrapper service SRVE0068E:
Uncaught exception created in one of the service methods of the servlet
TradeAppServlet in application DayTrader2-EE5. Exception created:
javax.servlet.ServletException: TradeServletAction.doSell(...) exception
selling holding 3111 for user =uid:43 at
org.apache.geronimo.samples.daytrader.web.TradeServletAction.doSell(Trad
eServletAction.java:708)

Log Analytics Server

- Thread ID
- Error Code

Text analytics and Regular expressions

Generic annotations or Insight Packs

<table>
<thead>
<tr>
<th>logRecord</th>
<th>timestamp</th>
<th>traceBlockAll</th>
<th>exceptionMethodName</th>
</tr>
</thead>
<tbody>
<tr>
<td>[10/9/12 5:51:37:181 GMT+05:30] 00000059 SystemOut 0 at o...</td>
<td>2012-10-09T05:13:37+05:30</td>
<td>at org.apache.geronimo.samples.daytrader....</td>
<td>performTask</td>
</tr>
<tr>
<td>[10/9/12 5:51:37:181 GMT+05:30] 00000059 SystemOut 0 at o...</td>
<td>2012-10-09T05:13:37+05:30</td>
<td>at org.apache.geronimo.samples.daytrader....</td>
<td>doGet</td>
</tr>
<tr>
<td>[10/9/12 5:51:37:181 GMT+05:30] 00000059 SystemOut 0 at ja...</td>
<td>2012-10-09T05:13:37+05:30</td>
<td>at javax.servlet.http.HttpServlet.service(HttpServletRequest...</td>
<td></td>
</tr>
<tr>
<td>[10/9/12 5:51:37:181 GMT+05:30] 00000059 SystemOut 0 at ja...</td>
<td>2012-10-09T05:13:37+05:30</td>
<td>at javax.servlet.http.HttpServlet.service(HttpServletRequest...</td>
<td></td>
</tr>
<tr>
<td>[10/9/12 5:51:37:181 GMT+05:30] 00000059 SystemOut 0 at c...</td>
<td>2012-10-09T05:13:37+05:30</td>
<td>at com.ibm.ws.webcontainer.servlet.Servlet...</td>
<td></td>
</tr>
<tr>
<td>[10/9/12 5:51:37:181 GMT+05:30] 00000059 SystemOut 0 at c...</td>
<td>2012-10-09T05:13:37+05:30</td>
<td>at com.ibm.ws.webcontainer.servlet.Servlet...</td>
<td></td>
</tr>
<tr>
<td>[10/9/12 5:51:37:181 GMT+05:30] 00000059 SystemOut 0 at c...</td>
<td>2012-10-09T05:13:37+05:30</td>
<td>at com.ibm.ws.webcontainer.servlet.Servlet...</td>
<td></td>
</tr>
<tr>
<td>[10/9/12 5:51:37:181 GMT+05:30] 00000059 SystemOut 0 at c...</td>
<td>2012-10-09T05:13:37+05:30</td>
<td>at com.ibm.ws.webcontainer.servlet.Servlet...</td>
<td></td>
</tr>
</tbody>
</table>
Search Interface

- Saved Searches
- Free Form Search
- Search Parameters (Time, Logsource)
- Search Results over Time
- Configured Patterns (Annotations)
- Raw Log Records
Visualization

Inference: Server 2 shows a very high number of incoming messages on Saturday (30th Nov) and Sunday (1st Dec). Administrator need to check the hourly message inflow on Server 2 for further analysis.
Agenda

- Overview Hybrid Service Management
- Monitoring
- Log Management
- Closing
Summary

- Resource Monitoring is "table stakes", all monitoring aspects need to be considered
  - Response time tracking from multiple PoP's
  - Transaction Tracking
  - Application Diagnostics
  - Logfile Monitoring and Search

- Characteristics of the Cloud impose new requirements for Service Management
  - Dynamics, Scale
  - DevOps Culture

- Today's Service Management needs to bring traditional datacenter ("SoR") and cloud-first environments ("SoE") together: **Hybrid Management**
  - Composite Applications spanning SoR and SoE
  - Service Integration, Multi-vendor

- Understand the different users ("personas")
  - Operations
  - Development (DevOps, EnvOps)
  - Service Managers, Account Managers
Food for thought

- With Redundancy, Chaos Monkeys, Circuit Breaker, do you still need monitoring?

- With Dynamics of a cloud operating environment, are Configuration Management Databases (CMDB) / Configuration Management Systems (CMS) still valid?

- Is there a fundamental difference between Metrics, Logfiles, and Events?