Proactive Oracle Database Monitoring And Capacity Planning With Splunk

Tyler Muth
Analytics Architect, Splunk Public Sector
Collateral - bit.ly/conf16-tmuth
Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

bit.ly/conf16-tmuth
Who Am I?

• Oracle – 16 years
  – APEX Development Team
  – Chief Database Engineer, Public Sector
  – Lead many Exadata POCs
  – Wrote AWR-Miner for Sizing and Capacity Planning, Logger, AWR Formatter
Why Splunk for Oracle?

- Security
- Performance Monitoring
- Capacity Planning
- Configuration Management
- Error Analysis
- Single-Pane View of “Application”
What Can You Splunk?

Oracle Database

- alert.log
- listener log
- trace files
- Audit
- Tables
- syslog
- Files
- OS
- Dictionary
- Custom
- OSWatcher / ExaWatcher
- TA Unix
- Exachk
- Exadata & SuperCluster
- Cell metrics
How Can You Splunk It?

- Add-on for Unix
- DB Connect (DBX)
- Splunk Add-on for Oracle DB
- Modular Input (in-progress)
- Standard File Monitor
## Why Would You Splunk These?

<table>
<thead>
<tr>
<th></th>
<th>Security</th>
<th>Performance</th>
<th>Capacity Planning</th>
<th>Configuration Management</th>
<th>Error Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert.log</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓  ✓</td>
</tr>
<tr>
<td>trace files</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Audit Files</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit syslog</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Tables</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dictionary Tables</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Custom Tables</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>OS – TA Unix</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS – OSWatcher / Exawatcher</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exadata - exachk</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exadata – Cell metrics</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

bit.ly/conf16-tmuth
Demo Architecture
Demo – Average Active Sessions

Using DB Connect (DBX) to pull DB metrics stored in tables / views

Most Databases

DB Connect App

JDBC
Demo – Average Active Sessions
Demo – DB Memory & CPU

Exadata Virtual

Unix Plugin

* nix

ps
vmstat
netstat
iostat

* nix

splunk
Demo – DB Memory & CPU
Demo– Logger Plugin

Logger Package

Error Logged ➔ REST Call (push)

HTTP Event Collector (HEC)
Demo – Logger Plugin
Demo– Logger Plugin

An unexpected internal application error has occurred. Please get in contact with your system administrator and provide reference# for further investigation.

Technical Info (only visible for developer)
Demo – Cell Metrics
Demo - Swingbench
Demo jMeter
Conclusion

- **Oracle Databases**
  - Are part of many high-visibility systems
  - Are highly instrumented
  - Lack good tools to aggregate and visualize this data

- **Splunk**
  - Can consume, visualize and aggregate this data
  - Can correlate this data with other parts of the “system”
  - Can add tremendous value to Oracle customers