Proactive Oracle Database Monitoring And Capacity Planning With Splunk

Tyler Muth  |  Analytics Architect

September 2017  |  Washington, DC
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
• tmuth@splunk.com
Introduction

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
Why Splunk For Oracle?

Security

Performance Monitoring

Capacity Planning

Configuration Management

Error Analysis

Single-Pane View of “Application”
How Can You Splunk It?

- Add-on for Unix
- DB Connect (DBX)
- Splunk Add-on for Oracle DB
- Standard File Monitor

Oracle Database

- alert.log
- listener log
- trace files
- Files
- syslog
- Audit
- Tables

- Exadata & SuperCluster
- Exachk
- OSWatcher / ExaWatcher
- TA Unix
- OS
- Dictionary
- Custom

How Can You Splunk It?
# 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 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>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>
Getting Oracle Data Into Splunk
Demo – Average Active Sessions

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

Most Databases

DB Connect App

DB

JDBC
Demo – DB Memory & CPU
Demo Alert Log

- Demo of pulling alert.log data into splunk
Demo Audit Logging

- Demo of bringing audit log data into Splunk
Demo Capacity Planning

- Capacity planning demo using AWR data from many databases.
Demo – Logger Plugin

Error Logged → REST Call (push) → HTTP Event Collector (HEC) → Logger Package
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
Thank You

Don't forget to rate this session in the .conf2017 mobile app