Designing a requirements based packet capture infrastructure

John Pittle
Distinguished Performance Consultant, Riverbed Professional Services

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017
• Which IT teams / disciplines are represented in the session today?

• What industries are represented?
Speaker Introduction

• App911 Emergency Troubleshooting Team Lead
• Technology Adoption Services Team Lead
• Consulting Practice Mentor
• Best Practices Contributor
• Program Owner – Riverbed Performance Management Workshop Series
• We Love Packets!
• Many performance / availability issues can only be solved with packets and expert analysis
• Analysis is often delayed or deferred because we don’t have the packets or the context we need at the time we need them
• Requirements based design of packet capture and analysis solutions can help ensure you get the funding needed to adequately support the business
My Ask for This Session

- Engage and Participate
- Share your experience
- Learn from your Peers
- Improve your Craft
Agenda

• Performance Management Landscape
• Packet Related Workflows & Technologies
• Requirements & Business Case Mechanics
• Gap & Risk Heat Maps
• Recommendations and Wrap-up
Performance Management Landscape

- End User Experience
- User End Point Monitoring
- Packets
- Flow (NetFlow, Jflow, Sflow, NBAR, etc)
- SNMP
- Application Metrics
- Application Logging
- Javascript Injection
- Host Metrics
- Infrastructure Metrics
Hybrid Enterprise
User End Experience Monitoring

EUE Performance
Before / After Analysis
Device Health
Utilization Monitoring
Browser EUE - Javascript Injection

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017
Infrastructure Devices / Servers

SNMP
WMI
Vendor Agents
Flow Records

Netflow
Enhanced Flow
S-Flow, J-Flow
NBAR/NBAR2
Packet Capture / Collection

Host Captures
SPAN/TAP
Passive Appliances
Traffic Aggregators
Full End to End Visibility

- Packets
- End Point Device
- Infrastructure

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017
• Link utilization is 80%, who’s using the bandwidth?
• Server utilization is 85%, who’s generating the load?
• Is user experience impacted?
• How long has it been going on?
• App ABC is slow, what infrastructure does it use?
• Who owns the fix?
• If device XYZ goes down, who’s impacted?
Heard in the CIO Staff Meeting

- Are we meeting our SLAs?
- Are customers happy?
- Is IT measurably contributing to company success?
- Are we investing in the right areas? How do we know?
- What’s the impact if we ___________?
A comprehensive, synergistic, holistic Performance Management strategy is needed to fully answer these questions.

Packet based performance monitoring is a key part of that strategy.
Questions / Discussion
Packet Related Workflows & Technologies

• Capture
• Monitoring
• Triage and Troubleshooting
• Performance Analysis / Protocol Analysis
• Planning
Packet Capture

- Host Based Captures
- Network Devices with Capture Capability
- Passive Appliances
- SPAN/TAP Design
- Packet Aggregation Design
- Packet Aggregation Appliances
### Manage Multiple Host Capture Agents

<table>
<thead>
<tr>
<th>Agent Name</th>
<th>Description</th>
<th>TCP Port</th>
<th>Agent Network Adapter</th>
<th>Filter</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>server-dev-01</td>
<td>[ ] Description</td>
<td>27401</td>
<td>eth0</td>
<td>Default</td>
<td>1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux 3.13)]</td>
</tr>
<tr>
<td>apache-dev-01</td>
<td>[ ] Description</td>
<td>27401</td>
<td>eth0</td>
<td>Default</td>
<td>0 currently active captures [Version 3.9 (Build 450), Linux/x86 (Linux 3.13)]</td>
</tr>
<tr>
<td>face-tcserver-dev-01</td>
<td>[ ] Description</td>
<td>27401</td>
<td>eth1</td>
<td>Default</td>
<td>1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux 3.13)]</td>
</tr>
<tr>
<td>face-tcserver-dev-02</td>
<td>[ ] Description</td>
<td>27401</td>
<td>eth0</td>
<td>Default</td>
<td>1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux 3.13)]</td>
</tr>
<tr>
<td>strip-apache-dev-01</td>
<td>[ ] Description</td>
<td>27401</td>
<td>eth0</td>
<td>Default</td>
<td>1 currently active capture [Version 3.9 (Build 450), Linux/x86 (Linux 3.13)]</td>
</tr>
<tr>
<td>tcserver-dev-01</td>
<td>[ ] Description</td>
<td>27401</td>
<td>eth1</td>
<td>Default</td>
<td>0 currently active captures [Version 3.9 (Build 450), Linux/x86 (Linux 3.13)]</td>
</tr>
</tbody>
</table>
Preview before downloading
Navigate to most relevant traffic before download
• Always on, always analyzing performance
• All conversations, all the time, based on the traffic presented
• Capture packets into very large, indexed repository
• Packet Slicing and Filtering
• Byte Pattern Recognition
• Focused preview and selection of relevant conversations before download
Passive Appliance - Continuous Capture

High Speed Capture Summary

Rolling Buffer range: 4 days, 2 hours, 24 minutes (2017-06-15 15:35:00 to 2017-06-19 17:59:00)
Rolling Buffer size: 23.5 TB
Snapshot Buffer range: 0 days, 0 hours, 0 minutes (0000-00-00 00:00:00 to 0000-00-00 00:00:00)
Snapshot Buffer size: 5.0 MB
Snapshots: 0

Detailed Information

The following table shows packet capture metrics for each individual interface and for all interfaces on the appliance (last row). Each metric is updated every minute. The graph shows the variation in average throughput over the total time window in five minute increments.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0</td>
<td>0.0</td>
<td>N/A</td>
<td>N/A</td>
<td>0.0</td>
<td>0.0</td>
<td>650.8</td>
<td>1524</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>927798.1</td>
<td>1407386.6</td>
<td>N/A</td>
<td>N/A</td>
<td>176720.1</td>
<td>259863.1</td>
<td>650.8</td>
<td>1524</td>
<td>N/A</td>
</tr>
<tr>
<td>All</td>
<td>927798.1</td>
<td>1407386.6</td>
<td>712101.8</td>
<td>1160830.0</td>
<td>176720.1</td>
<td>259863.1</td>
<td>650.8</td>
<td>1524</td>
<td>0.0</td>
</tr>
</tbody>
</table>
**SPAN & TAP**

- **Engineered traffic feeds for performance and security tools**
- **SPAN design challenges**
  - Device / traffic impacts
  - Full duplex over half duplex
  - Oversubscription
- **TAP design challenges**
  - Full duplex over half duplex
  - Managed vs. unmanaged TAPs
- **Virtual TAPs for ESX**
Packet Aggregators

- Essential in large environments
- Key Features:
  - Filtering, Splitting, Aggregating
  - Header modification
  - Scalability
  - De-dup
  - Flow generation
Monitoring - Passive Appliances

- Always on, always analyzing performance
- All conversations, all the time, based on the traffic presented
- Proactive alerting
- Baselining and historical trends
- Quickly determine problem domain and download relevant packets when deeper dive is needed
Real Time Views - Sample

Each chart is for a different DB

MW-DC to West (blue line) not impacted during this time period
Triage & Troubleshooting

- Automated Expert Analysis
- Key stats with traffic overlay
- Protocol Decodes
- End to End Transaction Views
Expert Analysis Sample

• 1 minute sample
• Automated Summary of Delays Analysis
• Some minor packet loss detected as reported by the 73ACK indicators

• Out of sequence packets are not necessarily expected, but we are using Internet transport so we should expect the unexpected
Relevant Statistics

Throughput

Bytes in Flight

Out of Sequence

Microbursts of 18-23Mbps
Packet Exchange vs. Bytes in Flight
399ms burst drill down - 2.2 MB
• Diagnosed TCP Slow Start on Idle without looking at decodes

• One more quick sample of visualization before we move on....
1.3 sec RTO
TCP RTO Visualization 2 of 4

4.0 sec RTO
TCP RTO Visualization 3 of 4

12 sec RTO
TCP RTO Visualization 4 of 4

30 sec between loss and RST
Performance Analysis Workflows

- Dev Team Unit Testing
- Load Testing
- Pre-Deployment
- New Technology Assessments
- 3rd Party Software Qualification
• Capacity Planning
• Migration Planning
• Technology Assessments
• Bandwidth Impact Assessment
• End to End Modeling
Migration Planning - Latency Sensitive Conversations
Impact of 40ms Round Trip Latency

Response time increases from 1 minute to 6 minutes
Questions / Discussion
• Packets are an essential data source for Performance Management workflows
• Business leaders / budget owners seldom understand the importance
• They need your help to understand how visibility gaps are actually a risk to the business
Troubleshooting in the Wild

• DB Replication Delays impact customer data visibility
• Claims Management Down
• Load Testing brings down production data center
• Call Center Stability Disruption
• eCommerce web page crash during checkout
• 2 hour outage of global eCommerce website
• Finance website crashes after super bowl commercial
• Global DNS Failover Troubleshooting
Tie your requirements for packet based capabilities to key apps and key infrastructure services
Characterize the business risk to your key apps & infrastructure
Capture current state capabilities
Identify gaps
Identify risk to the business

Business Case
Types of Service Delivery Risks

• Poor app performance overall, can’t meet SLAs
• App / Service is non-responsive
• Dependent system is down
• Can’t complete key transactions
• Incomplete visibility
• Poorly performing infrastructure services are impacting everything
Business Impact

- Customer Churn
- Lost Revenue
- Lost Productivity / Overtime Costs
- Penalties / Fines
- Missed Market Opportunities
Key Apps

• The most important apps to the business
• Characterize scope, scale, user community
• Identify business disruption when these apps are down or performing poorly
• Simple spreadsheet to capture key attributes
### Key App Attributes

<table>
<thead>
<tr>
<th>App #</th>
<th>App Name</th>
<th>App Technology</th>
<th>Primary BU</th>
<th>Business Use</th>
<th>Hosting Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enter details for up to 10 applications considered critical to the business.
<table>
<thead>
<tr>
<th>App #</th>
<th>Hosting Location</th>
<th>Est. total minutes outage last 90 days</th>
<th>Count of Registered Users</th>
<th>Peak Concurrent Users</th>
<th>Est. cost of outage /Hr (Low)</th>
<th>Est. cost of outage /Hr (Med)</th>
<th>Est. cost of outage /Hr (High)</th>
<th>Lost Revenue (Y/N)</th>
<th>Higher Costs (Y/N)</th>
<th>Lost Mktk Opportunity (Y/N)</th>
<th>Customer Sat (Y/N)</th>
<th>Other (Specify)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Who has these details?

- Service Delivery Managers
- IT Business Office
- BU Owners
- Operations
Current State Capture / Visibility Capabilities

• For each Key App - what is the most essential traffic to capture?
• What metrics / capability would this give you?
• If you had “full coverage”, how would you describe it?
Heat Map Overview

• Simple Excel Spreadsheets with conditional formatting
• Visualize where we need coverage vs. where we have coverage
• Use color scheme to indicate risk
• Iterations of the heat map can be used to communicate a plan & cost estimates
## Current State – Packet Capture Coverage

<table>
<thead>
<tr>
<th>Views</th>
<th>Oracle</th>
<th>Tibco</th>
<th>Powerstrip</th>
<th>OBI</th>
<th>ERP</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Experience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web to App Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to DB Performance</td>
<td></td>
<td></td>
<td><img src="image" alt="Yellow" /></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to Partner Systems</td>
<td><img src="image" alt="Gray" /></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to SSO Performance</td>
<td><img src="image" alt="Gray" /></td>
<td></td>
<td><img src="image" alt="Gray" /></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Complete**: Represents full coverage.
- **Partial**: Represents partial coverage.
- **Some Risk**: Represents some risk.
- **Significant Risk**: Represents significant risk.
- **Not Applicable**: Represents not applicable.
Current State / Future State Roadmap

• Where are my gaps / risks today?
• What do I address first?
• …second?
• …third, and so on?

• What would it take to reduce unplanned downtown for this app by 120 minutes per year?
• What would that be worth to the business?
## Phase 1 – This Quarter

<table>
<thead>
<tr>
<th>Views</th>
<th>Oracle</th>
<th>Tibco</th>
<th>Powerstrip</th>
<th>OBI</th>
<th>ERP</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Experience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web to App Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to DB Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to Partner Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to SSO Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- **Complete**
- **Partial**
- **Some Risk**
- **Significant Risk**
- **Not Applicable**
## Phase 2 – Next Quarter

<table>
<thead>
<tr>
<th>Views</th>
<th>Oracle</th>
<th>Tibco</th>
<th>Powerstrip</th>
<th>OBI</th>
<th>ERP</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Experience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web to App Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to DB Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to Partner Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to SSO Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- **Green**: Complete
- **Yellow**: Partial
- **Red**: Some Risk
- **Orange**: Significant Risk
- **Gray**: Not Applicable
## Phase 3 – two Quarters out

<table>
<thead>
<tr>
<th>Views</th>
<th>Oracle</th>
<th>Tibco</th>
<th>Powerstrip</th>
<th>OBI</th>
<th>ERP</th>
<th>Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Experience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web to App Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to DB Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to Partner Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App to SSO Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- **Complete**: Green
- **Partial**: Yellow
- **Some Risk**: Red
- **Significant Risk**: Red
- **Not Applicable**: Grey

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017
### Alternate Phase 1

<table>
<thead>
<tr>
<th>Views</th>
<th>Key Applications Roadmap Phase 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Oracle</td>
</tr>
<tr>
<td>End User Experience</td>
<td></td>
</tr>
<tr>
<td>Web to App Performance</td>
<td></td>
</tr>
<tr>
<td>App to DB Performance</td>
<td></td>
</tr>
<tr>
<td>App to Partner Systems</td>
<td></td>
</tr>
<tr>
<td>App to SSO Performance</td>
<td></td>
</tr>
</tbody>
</table>

- **Complete**
- **Partial**
- **Some Risk**
- **Significant Risk**
- **Not Applicable**
Key Infrastructure – Shared Services

• What are some key shared services in your environment?

• Degradation in these services will impact the entire environment
Key Infrastructure – Shared Services

• DNS
• NTP
• Active Directory / LDAP
• Single Sign-on
• Email
• Sharepoint Servers
• VPN / Token Gateways
• NAS Storage
• VoIP and related infrastructure
• Etc…
## Current State – Critical Shared Services

<table>
<thead>
<tr>
<th>Critical Infrastructure Services</th>
<th>DNS</th>
<th>Global Load Balancer</th>
<th>AD/LDAP</th>
<th>Single Sign On (SSO)</th>
<th>Prod NetApp Filers</th>
<th>Local Load Balancers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Rates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection Rates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Utilization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Throughput Rates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet Loss / Retrans</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet Captures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Green** = Complete
- **Yellow** = Some Risk
- **Red** = Significant Risk

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017
General Recommendations

• Use passive appliances to get coverage for infrastructure shared services and all application edge traffic (EUE)
• Identify key apps where inter-tier packets are most beneficial and expand traffic feeds
• Leverage host based captures everywhere
• Add supplemental analysis capabilities on top of Wireshark
Wrap-Up

• Packets are an essential component of your overall Performance Management capabilities
• Most companies have significant gaps in their packet capture and analysis workflows
• These gaps represent business risk and can be identified with a rationalized current state assessment tied to key apps and shared services
• Create a future state roadmap that shows the improvements and benefits of addressing gaps
Thank You for your Participation!