Maintaining PJM Tool Availability

Foluso Afelumo
Tech Change Forum
Application Availability

Ensure safety of operation
- Security updates
- Security patching

Ensure uptime of the applications
- Realtime monitoring
- Availability testing
- Protection from unsupported usage patterns
Protection from Unsupported Usage Patterns

Why

– Ensure equitable access to PJM systems
– Allow users to address potentially unauthorized account usage
Concurrent Sessions

- Limit the number of concurrent authenticated sessions (tokens)

Usage Rates

- Limit the request rates against the PJM tools
Concurrent Sessions

• Limit the number of concurrent authenticated sessions (tokens)

Usage Rates

• Limit the request rates against the PJM tools
Approach 1: Concurrent Authenticated Sessions

Details
- User sessions limited to 25 sessions per user

Impact
- Automated processes/scripts/tools that create sessions

Action required
- Log out of sessions when not in use
- Re-use existing sessions
1. Deny access
   • 26\textsuperscript{th} attempt is unsuccessful
2. Invalidate next expiring session
   • Session with longest inactivity time is destroyed on 26\textsuperscript{th} attempt
3. Invalidate oldest session
   • 1\textsuperscript{st} created session is destroyed on 26\textsuperscript{th} attempt
• October
  – Connect with users who are over threshold
  – Mid-October – enable in sandbox
  – Finalize approach – communicate at October TCF
• November
  – Implement on 11/21
• **Covered now**
  Account Manager, Billing Line Item Transfer, Bulletin Board, Data Miner, Emergency Procedures, ExSchedule, FTR Center, Gas Pipeline, InSchedule, Markets Gateway, Messages, Planning Center, Post Contingency Local Load Relief, Power Meter, Resource Tracker, Voting

• **Covered in the future**
  eCredit, eRPM, MSRS, OASIS

• **Not in scope**
  eDataFeed
Concurrent Sessions

• Limit the number of concurrent authenticated sessions (tokens)

Usage Rates

• Limit the request rates against the PJM tools
Approach 2: Usage Rates

Details
- Request rates to tools to be enforced.

Impact
- Automated scripts that interact with APIs
- Screen scrapers

Action required
- Adjust usage pattern to meet published usage rates
## Applications allowing 600 requests per minute

<table>
<thead>
<tr>
<th>Applications with APIs</th>
<th>Applications without APIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Miner</td>
<td>Account Manager</td>
</tr>
<tr>
<td>EdataFeed</td>
<td>Billing Line Item Transfer</td>
</tr>
<tr>
<td>ExSchedule</td>
<td>Bulletin Board</td>
</tr>
<tr>
<td>Gas Pipeline</td>
<td>Planning Center</td>
</tr>
<tr>
<td>InSchedule</td>
<td>Post-Contingency Local Load Relief</td>
</tr>
<tr>
<td>Power Meter</td>
<td>Resource Tracker</td>
</tr>
<tr>
<td></td>
<td>Voting</td>
</tr>
</tbody>
</table>
## Applications allowing greater usage

<table>
<thead>
<tr>
<th>Application</th>
<th>Requests/minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Procedures</td>
<td>1200</td>
</tr>
<tr>
<td>oasis.pjm.com standalone pages</td>
<td>1200</td>
</tr>
<tr>
<td>Markets Gateway</td>
<td>1800</td>
</tr>
</tbody>
</table>
• oasis.pjm.com standalone page restrictions cover
Implementation Plan

• September / October
  – Reach out to users currently exceeding threshold
  – Identify usage rates for other applications

• November
  – Communicate next steps
Start monitoring

Alert when usage rate is exceed

Block access to application

Notify client managers
If you believe your access is being blocked, please contact your client manager OR PJM’s customer service hotline.