Maintaining PJM Tool Availability

Foluso Afelumo
2 Separate Approaches

Concurrent Sessions

- Limit the number of concurrent authenticated sessions (tokens)

Usage Rates

- Limit the request rates against the PJM tools
Concurrent Sessions - Implementation Options

1. Deny access
   - 26th attempt is unsuccessful

2. Invalidate next expiring session
   - Session with longest inactivity time is destroyed on 26th attempt

3. Invalidate oldest session
   - 1st created session is destroyed on 26th attempt
Concurrent Sessions - Implementation

- **October**
  - Begun connecting with users
  - 10/24 - Implemented in Train

- **November**
  - 11/29 – Implementation delayed
* Whenever a user goes over the maximum request rate, the response will be an http-503 error
** We will contact affected users when we are able to identify them
• Monitoring will be for a request rate of 20 requests/second over a 10-15 second rolling window.
• Any request rates that go over 20 requests/second will have data transfers throttled.
• The impact of throttling will be a response code of HTTP-503 instead of the expected data.
• Once the system’s monitoring window has cleared, data transfer will resume.
• On a daily basis our system will provide a report to our client managers
• Client managers will reach out to users in cases where IP addresses can be tied to usernames (due to accessing other tools)
• The reaching out is to inform folks that they were impacted by the throttling system.
• Once implemented, if you have questions, please call your client manager and provide the exact error you’re seeing – it will help determine if you’re being throttled by the system or not.
Usage Rates – Implementation Update

• **November**
  – Working to implement an automated solution to manage usage for oasis.pjm.com
    • Targeting 20 requests per second (as opposed to 1200/min)

• **December**
  – Seek to implement on December 15th for oasis.pjm.com only