Simplify Security Compliance and Systems Administration with Db2 Web Query

Doug Mack, Rob Bestgen
IBM Lab Services
mackd@us.ibm.com,
bestgen@us.ibm.com

Db2 Web Query Team:
QU2@us.ibm.com

POWERUp18 Session ID:
Agenda Key:

Agenda

• IBM i “Services”

• What is Db2 Web Query for i

• Combining the two
  – Sample reports/dashboards for the Systems Administrator
  – PowerSC Compliance Assessment and Reporting Solution

© 2018 IBM Corporation
The Reports Leverage IBM i Services

• What are IBM i Services?
  – SQL Based interfaces to common CL or API type commands
  – Delivered as SQL Views, User Defined Functions or Stored Procedures
    • All of which can be made readily available for use in DB2 Web Query reports
    • SQL Script examples provided in iNav and ACS Run SQL Scripts
  – Easier to get system information via SQL Based visualization tools like….DB2 Web Query

• Services are there today
  – Depending on TR and IBM i OS level

• DB2 Web Query can be leveraged to build reports, charts/graphs, dashboards or populate spreadsheets
  over the data returned from the various services

SQL Examples over IBM i Services are included in Access Client Solutions

• Using Run SQL Scripts
• Insert from Examples…
For More Information on Services and Delivery Dates

Enhancements in TR4
- Inlined UDTFs
- Trigger (re)deployment
- More IBM i Services
- New DB2 built-in Global Variables
- Enhanced SQL Scalar functions
- Evaluation option for DB2 SMP & DB2 Multisystem

Enhancements in 7.3:
- Temporal Tables
- Generated columns for auditing
- New OLAP built-ins
- Raised architecture limits
- New support for partitioned tables
- More IBM i Services
- And much more

Enhancements in TR5 & TR1
- JSON_TABLE()
- INCLUDE for SQL Routines
- Visual Explain in ACS
- Inlined Scalar Functions
- More IBM i Services
- New DB2 for i Services
- And much more…

www.ibm.com/developerworks/ibmi/techupdates/db2

© 2018 IBM Corporation

Monitoring System Utilization Metrics:
Sample Reports and Dashboards

© 2018 IBM Corporation
Sample System Admin Reports

- Once installed, Run the “Get Status of Sys Admin Reports” by double clicking or right click and “RUN”

- Run the report if desired by clicking on the links in the Full Path column

CPU Utilization Dashboard

- Supports one or multiple LPARs/Servers
  - System CPU Utilization
  - Can be easily extended to other system metrics
- Auto Refresh Enabled
  - Remote data collection requires remote system connections to be set up (RDB directory entries and SVRAUTE entries)
- Continues to collect and store historical data using a Stored Procedure once the report is initially run
  - Stops collecting if ‘no one is watching’ for an extended period of time
Monitoring Output Queues and Spool Files

- Are you cleaning up your spool files?

![Top 10 output queues by # of spool files]

System Status

- Various metrics across all LPARs/Servers
  - Not set up as auto refresh but could be easily enough
  - Traffic lighting to highlight potential problems
  - You could easily change the report to include your own thresholds to monitor

### System(s) Status

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Total Jobs in System</th>
<th>Active Jobs in System</th>
<th>Interactive Jobs in System</th>
<th>Active Threads in System</th>
<th>Elapsed Time</th>
<th>Utilized CPU Used</th>
<th>Current CPU Capacity</th>
<th>Average CPU Utilization</th>
<th>Minimum CPU Utilization</th>
<th>Maximum CPU Utilization</th>
<th>System A/S Total Storage</th>
<th>Total Auxiliary Storage</th>
<th>System A/S Used</th>
<th>Current Temporary Storage</th>
<th>Maximum Temporary Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE30E1</td>
<td>310</td>
<td>250</td>
<td>00</td>
<td>1111</td>
<td>1</td>
<td>2.00</td>
<td>2.00</td>
<td>0.21</td>
<td>0.00</td>
<td>0.00</td>
<td>1469002</td>
<td>1469002</td>
<td>61.04</td>
<td>7523</td>
<td>7550</td>
</tr>
<tr>
<td>DE30E2</td>
<td>644</td>
<td>244</td>
<td>00</td>
<td>1112</td>
<td>1</td>
<td>2.00</td>
<td>2.00</td>
<td>0.21</td>
<td>0.00</td>
<td>0.00</td>
<td>954437</td>
<td>954437</td>
<td>50.21</td>
<td>7778</td>
<td>7846</td>
</tr>
<tr>
<td>DE30E3</td>
<td>953</td>
<td>282</td>
<td>00</td>
<td>1218</td>
<td>1</td>
<td>7.00</td>
<td>4.00</td>
<td>0.11</td>
<td>0.00</td>
<td>0.00</td>
<td>6242036</td>
<td>6242036</td>
<td>27.63</td>
<td>8215</td>
<td>8290</td>
</tr>
<tr>
<td>DE30E4</td>
<td>465</td>
<td>242</td>
<td>00</td>
<td>925</td>
<td>1</td>
<td>2.80</td>
<td>2.00</td>
<td>0.11</td>
<td>0.00</td>
<td>0.00</td>
<td>6242036</td>
<td>6242036</td>
<td>15.73</td>
<td>6976</td>
<td>7833</td>
</tr>
</tbody>
</table>

Run on May 4, 2017 at 13:46:47

© 2018 IBM Corporation
Subsystem Status and Top 10 Jobs by CPU, I/O, and Temp Storage

- Subsystem Summary “Active” Report
  - Sort, filter, add a comment and email, etc.

Summary info by subsystem

Top xx Jobs by:
- CPU time
- I/O count
- Temp. Storage

How Up to Date are your Group PTFs?

- Checks installed level against available level
- Available levels obtained from the web
  - Note: your system must have a connection to the web
Storage Utilization Reports

- Information can be aggregated across ASPs to get totals
  - Rank by total storage (top xx users)
  - Temp Storage by JOB
  - Could start keeping history to track trends

What is the process?

- Prepare the service for DB2 Web Query
  - Services shipped as stored procedures (SP) need a simple wrapper SP to turn the output into a result set
  - Services shipped as User Defined Table Function (UDTF) simply need an SQL VIEW over the function
  - Services shipped as a VIEW (which most are) – move onto the next step!
What is the process?

• Create (one time) a DB2 Web Query Synonym (meta data) over the prepared service
  - View or SP
    • A two minute (if that) exercise

What is the process?

• The Synonym is a representation of the underlying file (or view in this case). It does not contain data, but is a layer in between report authoring tool and the data in the tables/files to simplify report authoring
• You could:
  – Add additional calculated fields
  – Change field names/data types
  – Join this file to another in the same synonym
  – Add date attributes (e.g., Day of week)
• “Sample Data” allows you to see the results
Once the Synonym is in Place, Start Building your Report

• Start building your report over the new Synonym
  – Standard report or chart, or other visualizations
  – Output could be HTML, Excel, Active Reports (good for mobile devices), PDF, PowerPoint
  – Could schedule the reports to run in the background and email or store in IFS
  – Add desired reports to dashboard
    • Could even set up a timed refresh for an interactive dashboard

What about History and Trending?

• Today, most of the reports are point in time
  – With the exception of the CPU Utilization Dashboard, which does store historical data as it goes
• If you’re at 7.3, it would be very easy to set up a timed job to collect data via IBM i Services and dump the data into a temporal table

Or....

• No matter what release you’re at, use DB2 Web Query’s DataMigrator to automate that process of collecting and loading a history table

• Reports/dashboards could be updated then to include trending information based on timestamps in collections
• If you’d like some help with this, let us know: qu2@us.ibm.com
How Do I Acquire these Sample Reports?

Db2 Web Query Installation and Setup
(in 15 minutes)

With the NEW EZ-Install Package

Request by sending email to QU2@us.ibm.com w/ serial number of system you plan to install on
What is the EZ-Install Package

- A single downloadable image that you can request that includes:
  - Db2 Web Query Version 2.2
    - Express and Standard Edition
    - Data Migrator and Developer Workbench
  - Sample IBM i System Administration Reports
  - Db2 Web Query Auditing/Monitoring Reports
  - Query/400 Discovery Tool
  - All of the Tutorial Reports already completed
    - (but this would be cheating if you didn’t do the tutorials yourself)

- Installation Process Walks You through the Installation
  - Add a user you designate as a Db2 Web Query Administrator (don’t use QSECOFR please)
  - Restore of Db2 Web Query Sample Database and Meta data (needed for self guided tutorials)
  - Restore of Audit and Sample IBM i System Admin reports
  - Discovery Tool and completed tutorial reports are included but enabled optionally

Security Compliance Monitoring
Compliance Assessment and Reporting Tool – Enterprise Edition

- Covers:
  - Password management
  - Profile administration
  - Special authorities
  - Group inheritance
  - Network configuration
  - NetServer attributes
  - Operational security
  - PTF currency
  - Event monitoring
  - Customer define items
  - Security risks and more

- Daily compliance dashboard reports at LPAR, system or enterprise level

- Enables compliance officer to demonstrate adherence to pre-defined or customer-defined security polices.
- System and Security reporting made easy!

http://ibm.biz/IBMiSecurity or contact Terry Ford at TAFORD@us.ibm.com

“T just want to arrive in the morning, get a cup of coffee, and have a view of what systems are in compliance and which are not.”
High Level Dashboards

- Toggle through Different Views
  - IBM’s recommended best practice
  - Your Policy
    - Might be different than the IBM recommendations
  - Policy Exceptions
    - Exceptions might be something that is a defined temporary exception or a system that might have different policies
    - Examples might be a system that is being brought up, or an H/A or DEV system
  - Traffic Lighting for easy visualizations of where you are in or out of compliance
    - Drill downs to view details
- Views by Region, Country, OS Version, System purpose (prod, dev, ha/dr), etc.

Compliance Assessment and Reporting Tool

By System Dashboard
- Key system and data collection information
- Status of last collection attempt (Success or Fail)
- Key system attributes – VRM, Location, etc.
- Overall and detailed system grading based upon last successful collection
Cross System Analysis
Horizontal or vertical presentation of risk indicators across LPARs

Monitoring Vulnerabilities Across Systems
Cross System Analysis

PTF Inventory...

Profile Analysis

Horizontal or vertical presentation of user profiles across LPARs
Profile Analysis
Aggregation of user profiles across LPARs

Compliance Assessment and Reporting Tool

Profile Analysis
Drill down into user profiles as configured across LPARs
Compliance Assessment and Reporting Tool

New! Event monitoring capability. Monitor actions as they happen!

Covers:
- Password management
- Profile administration
- Special authorities
- Group inheritance
- Network configuration
- NetServer attributes
- Operational security
- PTF currency
- Event monitoring
- Customer define items
- Security risks and more

An automated collection, analysis, and reporting tool on over 1000 system and security related risks, information, statistics and demographics. All in one location and easy to use!

- Enables compliance officer to demonstrate adherence to pre-defined or customer-defined security policies.
- System and Security reporting made easy!
Questions?

To Learn More

• DB2 Web Query for i Website
  – Ibm.biz/db2webqueryi

• DB2 Web Query for i Wiki
  – Ibm.co/db2wqwiki

• DB2 Web Query Getting Started Enablement:
  – https://ibm.biz/db2wqconsulting

• Demonstrations:
  – Wizard Analytics: https://ibm.biz/DB2WQWizards
  – End User Demos: https://ibm.biz/db2wqreportingdemos
  – Version 2.2.1 Videos: https://ibm.biz/db2wq-221-videos

• Follow DB2 Web Query guy Doug Mack on twitter at @mckdrmoly or check out his blog at http://db2webqueryi.blogspot.com/ for all the latest

© 2018 IBM Corporation