IBM Security

Using the REST API in Action Script

PRODUCT PROFESSIONAL SERVICES

Automating the deletion of Stopped/Expired actions using a task

- Why does it matter?

- In many customer environments, Operators are responsible for deleting their own actions. In many cases this is not performed in a timely matter and the number of closed actions grow to a point where it affects console performance.

- The BigFix Console will list every action that has been taken including every result from every BigFix Client. As the number of actions grows large, the BigFix Console will use more memory to load the actions and the cache load/write times increase. You can right click and delete old actions, which will mark them as deleted in the database. Once they are marked as deleted, the BigFix Console will no longer load them saving memory and load time. The actions will continue to be in the database after they are deleted, but they will not be accessible to the BigFix Console or to web reports.

- Why not automate this using BigFix?

Automating the deletion of Stopped/Expired actions using a task

- What is it?
- A BigFix task that runs on the Root Server
- Can be scheduled to run every *n* days so you no longer have to worry about action maintenance on the BigFix console

Automating the deletion of Stopped/Expired actions using a task

- How does it work?
- We call the REST API CLI within an action script
- We use Relevance Substitution to query the database and give us the results of all Stopped actions (whose time stopped is older than *n* days from the current date) and/or Expired actions (whose time issued is older than *n* days from the current date)
- We use Relevance Substitution again to parse these results so we are only left with a list of Action IDs
- Using a bat file, we call the REST API CLI again deleting these actions using a loop.

Automating the deletion of Stopped/Expired actions using a task

- ## How do I use it?
- Import the task, ‘~~Delete Expired and Stopped Actions.bes’ into the BES Console.
- On the ‘Description’ tab, enter the Master Operator User Name, The Master Operator Password, The RunAs User Name (used to run the bat file when no user is logged into the system) and the age in days of the stopped/expired actions to target.
- Schedule the action to run as you would any other action.
- Run it against the Root Server.
- Note: You will be prompted to provide the RunAs User password upon deployment.

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANYSYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM®

The Fixlets!

~~Delete Expired and Stopped Actions.bes

~~Delete Expired and Stopped Actions (2).bes