IBM Security

BigFix Best Practices Webinar

TOP 5 ~~ACTIONS~~ THINGS TO IMPROVE YOUR PERFORMANCE!

Stephen Hull, Senior Software Architect, BigFix Development

John Golembiewski, WW Technical Leader BigFix

6/30/2017

IBM

Your Webinar Hosts

I <3 Best Practices!

I'm not even supposed to be here today.

Where is Mike? What is AVP?

I am on a mission to civilize.

Stephen Hull

Senior Software Architect, BigFix Development

IBM Security

http://ibm.biz/hull_bigfix

John Golembiewski

WW Technical Leader BigFix

IBM Security

http://ibm.biz/jgo_bigfix

If you are looking for Mike Pashion?

IBM BigFix - Best Practices Webinar

BigFix Best Practices Webinar: Top 5 actions to improve Bigfix performance!

July 7th 2017 - 2:00 PM EST

Registration (Mandatory): https://ibm.biz/BigFixWebinar

Michael Paishon who has over a decade of BigFix experience, will be sharing his Top 5 actions to improve an environment. Mike works on the IBM BigFix Accelerated Value Program (AVP) and daily delivers on the business value of BigFix by making wise technical decisions.

https://ibm.biz/BigFixWebinar

What is AVP?

Accelerated Value Program

- IBM offering that goes beyond standard support with a focus on proactive assistance and problem prevention
- Includes the following components:
  - Percentage of Accelerated Value Leader (AVL) and/or Accelerated Value Specialist (AVS) supporting specific IBM software products
  - Onsite days used for critical issues, upgrades, and/or planning sessions
  - AVP-only knowledge sharing sessions
  - Specific number of named callers that can utilize priority PMR handling

Benefits of AVP for BigFix

- **Product Expertise** – Work with the most skilled BigFix resources having architecture and support experience with the largest BigFix deployments (up to 750,000 endpoints)
- **Trusted Advisor** – Works with you regularly to understand the details of your environment, achieve product goals, keep you informed of issues/changes and represent your needs to development
- **Proactive Support** – Periodic health checks and reviews of deployment/project status to help avoid problems, coverage of off-hours scheduled activities (Upgrade, DR, etc)
- **Custom Content Support** – Resolve issues with or help create custom content, reports, dashboard not covered by standard support

Starting point→ Best Practice – a Definition

A Best Practice is a technique or methodology that has been proven, through experience and research, to reliably lead to a desired result.

Observations → Applications of Best Practices

- Situations addressed by the application of Best Practices are dynamic
- Complex business situations require the consistent application of multiple Best Practices *over time* in order to achieve a desired result
- Best Practices need to dialogue with the environment in which they operate in order to maximize their effectiveness and to continually produce a predictable result

BigFix Best Practices →Desired Result

- An optimized BigFix deployment that, on a ongoing basis, maximizes the achievement of predictable results delivered through BigFix while efficiently utilizing human, monetary, and computing resources

Approach → BigFix Best Practices

- Level Set
  - Review BigFix Platform Architecture
  - Examine BigFix Platform Communications Protocols

- Discuss Focus Areas that yield a high ratio of result to effort:
  - BigFix Server Best Practices
  - BigFix Administration Best Practices
  - BigFix Baseline Best Practices

BigFix Server

- The BigFix Server performs key communications activities:
  - Takes reports from Relays/Clients
  - Frequently Inserts/Updates database rows
  - Propagates actions
- Heavy use of TCP/IP (HTTP)
- BigFix Server Best Practices focus on maximizing communications efficiencies without diminishing functionality

BigFix Server Best Practices

- Manage the interaction of Virus Scanners with the BigFix Server Folder Structure
- At a minimum, exclude these structures from real-time scanning in favor of a scheduled scan :
  - [BigFix Server]\FillDBData\BufferDir
  - [BigFix Server]\wwwrootbes\bfmirror\bfsites
  - [BigFix Server]\wwwrootbes\bfsites
- Disable the Windows Indexing Service and compression on the BES Server file structure

BigFix Server Best Practices

- Database I/O management has a positive effect on BigFix's overall performance
- Set SQL Server transaction logging to 'simple'
- Mount the database log and the transaction log on two separate arrays (both RAID 10 OR SSD), each using a different controller.
- We have seen massive increases in large environments with IBM Flash Systems over SSD. 7.x
- https://forum.bigfix.com/t/new-white-paper-bigfix-capacity-planning-performance-and-management-guide/15868

BigFix Administration Best Practices

- When a Master Operator does anything that requires signing an action (types in password), an new actionsite is created. All Master Operators share a single actionsite
- By definition, the new actionsite MUST be gathered by ALL computers in the deployment
- Many Master Operators signing many actionsites can cause each Client to gather large amounts of data
- Use Master Operator Roles to:
  - Assign management rights to Non-master Operators
  - Create Retrieved Properties
  - Manage site subscriptions
  - Deploy certain policy actions
  - Create Custom Content that can be seen by all Operators and will likely be used on most machines

BigFix Administration Best Practices

- Retrieved Properties vs Analysis Properties
  - Is it applicable globally or to a subset of systems?
  - How intensive is the evaluation?
  - Use analyses when possible

- Use evaluation intervals other than “Every Report”
  - How often does this data change?
  - How quickly do I need to know about a change?
  - How intensive is the evaluation?
  - Ties to minimum report interval, and impacts speed of reporting
  - Even “5 minute” intervals are better than “Every Report”

BigFix Baseline Best Practices

- Baselines create copies of included content to be evaluated in addition to the source fixlets
- Keep Baselines at 250 components or less
- Use applicability relevance in the Baseline
  - name of operating system starts with ”Win2012”
- Avoid duplicate deployments of a baseline to the same endpoints
  - 2 or more NMOs manage the same computers/overlapping computer groups
- Sunset older baselines or migrate them to separate site for build/provisioning process

Summary

- We established a working definition of Best Practices
- We discussed application areas for BigFix Server, Administration and Baseline Best Practices
- Let’s put these into action!

- Thank you!

IBM Security

THANK YOU

FOLLOW US ON:

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

IBM