HOW TO USE AUTOMATION IN EVENT REMEDIATION

With the ever-evolving demands on IT operations, it has become increasingly difficult to deliver technical services in a timely manner. The chief reason being that IT staff are overwhelmed by labour intensive, day-to-day operations due to the complexity of multitier, hybrid application stacks, constantly changing industry regulations, and increased security threats. The burden of repetitive, manual tasks affects productivity and innovation for IT staff and business users alike.

While technology itself continues to develop at an incredible pace, IT as a business function has become slow to evolve because many organizations struggle to use automation effectively enough to free up time and budget for value enhancing, innovation initiatives. However, there is hope. By automating workflows across applications, platforms, and tools to orchestrate critical activities for compliance and security, IT resources can spend more time focusing on adding innovative technologies that enable competitive advantage for the company. To ease this dynamic, IT organizations need to implement automation into event remediation. The purpose of this blog is to describe the opportunity automation can deliver into event remediation, describe a best practice for achieving it, and share an example of how it helped a large US financial services company.

The Scope of the Opportunity

(Source: Smartsheet report)

Based on the Smartsheet report, you can see from the statistics above

the average IT professional is bogged down in repetitive tasks that preclude them from spending as much time on innovation as the business and they as individuals desire. This is true in any company across all industries. At BMC, we are being asked to help customers navigate and implement automation technology as well as reconfigure the people, processes, and data flows to help reduce this burden and better benefit from it. Through our work with clients, we have found that the automation benefits are higher when large repeatable activities of operational tasks, such as patch management, release and change execution, application deployment, and

service fulfilment, are identified and automated thereby saving quality time of the workforce to work on more strategic projects by streamlining complex operations.

Best Practice for Automating Remediation

There are three key factors to ensure an effective implementation of automating event remediation:

- Defining the Scope of Automation
- Selecting the Tool to Perform the Automation
- Key Steps to Ensure Success

Defining the Scope of Automation: Automating remediation is most effective when the scope of automation tasks has been broadly classified and then subdivided into smaller tasks based on certain factors such as time and level of re-occurrence so that some business value can be derived from this implementation.

Selecting the Tool to Perform the Automation: The selection of the tools automating remediation should be done based on:

- Their ability to support multiple integrations with other tools;
- Whether the tools can provide role-based permissions;
- Scheduling mechanism;
- Allows code reusability; and
- If they can be used in multi-tier deployments.

Key Steps to Ensure Success: First, a thorough study of the types of events that occur in IT environment needs to be conducted. Know which systems log events and where, and what the events mean. This makes it much easier to understand and define which types of events require additional care, whether it's human intervention or automated workflows for handling changes or raising incidents. The end goal is to create a simple, streamlined set of workflows to automate and alert your team when more significant events that impact services (or that require human assistance of any type) occur.

For implementing any automation, the common tasks need to be targeted first, for example in case of Database events, it could be Blocked Transactions, Listener issues (Oracle), DB Backup issues, TempDB Space issues or Filesystem issues etc. Then, gather the requirements and subdivide the tasks as independent User stories. Document the process flow requirements for the user stories, this would involve documenting all the commands, scripts, etc. which will be utilized in the automation task. The next step is to decide on the timelines for developing and testing the automation tasks. Along with this, once the automation is in the production environment and based on the feedback

provided by the business users, the automation can be further enhanced to keep up with the dynamic business needs. Regular meetings can help track progress on user stories and backlogs.

Finally, the automation should capture the appropriate level of detail like what happened, when it happened, how it was handled (diagnosed/remediated), who it was escalated to, and any details of communication with other people or systems to support any actions taken. It may also be required to capture the data whether events are breaching any of the defined SLAs or OLAs, thus ensuring that compliance is maintained and accurate reporting is provided.

An Example from a Large US Financial Services company

For one customer in the banking industry, they were grappling with a large number of manual tasks, particularly the events pertaining to database which were overloading database support teams. Consequently, highly skilled support people had to spend a lot of time on mundane manual tasks instead of focussing on higher value complex technical tasks. A large number of tickets were generated, approximately 30,000 per week, by both the monitoring tools and users which added to the burden. The bank decided that automation of these tasks would help free up their staff to work on more critical projects. By implementing TrueSight Orchestration, the bank is able to create a seamless, centralized automation platform that orchestrates end-to-end processes across the entire ITSM environment. With TrueSight Orchestration all authorization and authentication challenges are more easily addressed. Even further, complex challenges related to information security are handled by leveraging TrueSight Orchestration which uses agentless methods to connect endpoints thereby incorporating existing policies into the processes. TrueSight Orchestration also incorporates custom data sources which often have operational data critical for automation steps to carry out.

As a result of these changes, the bank achieves faster service and reduced risk via a reduction in human errors. They are able to automate response to approximately 35% of tickets generated. The technology automates manual checks and composes full characterizations of issueswhich reduces administrator time spent per event analysis and thus, contributes to a significant effort savings. This means that support teams now have more time to focus on other higher value, complex user generated incidents which are related to product enhancements, problem investigation, and so on.

Utilizing automation for remediation is the innovation that can start alleviating the burden of menial tasks for your IT team. It reduces the chance for human error and even further enhances the opportunity for your IT team to focus on new, innovative programs that help them grow their skill and careers. IT wants to deliver innovation as much as the business demands. Adding automation where it makes sense and can reduce risk creates a win-win-win for IT, the IT professional, and the enterprise.

To learn more about how TrueSight Orchestration can be used in Event Triage and remediation automation, refer the whitepaper Event Triage and Remediation Management.

Some last words

Automation is a key factor in IT event remediation, because without it unnecessary duplication of tasks and human intervention is required, hampering IT support and operations teams worldwide. The more advanced the monitoring tool, the more automation capabilities it can provide without any undesirable results on the environment. Moreover, adoption of the automated approach helps in standardizing the way events are handled across the team thereby reducing the probability of errors in resolution. Without automation, all operations are reactive in nature. However, by adopting the

automated approach you perform a review of system health and proactively address the problems based on the alerts that can be generated from base operating platforms, middleware, applications, databases, etc. These alerts often unnecessarily force organizations to increase the resource costs by having more system admins, middleware admins, and database administrators as they move up the stack. Adopting automation approaches in these areas provides the biggest bang for the buck. Lastly, once the links among technology, process, and organization are established, it is then possible to begin viewing the services being delivered to the business on a more holistic level.

If you can use assistance with using automation in event remediation, contact BMC Customer Success and speak to one of our experts.