Realtime
publishers

"Leading the Conversation"

The Shortcut Guide™ *To*

Run Book Automation

sponsored by

hp ®
invent

Ed Tittel

Copyright Statement

Chapter 4: RBA Benefits and Best Practices

In the preceding chapters, we have made the argument that process automation is instrumental to sustaining complex and constantly growing enterprise IT environments. At the same time, RBA is also an important key to maintaining priority handling for escalated events as well as for timely delivery of quality services. Automating routine management, maintenance, and monitoring tasks greatly leverages the time and energy that IT professionals bring to their jobs— as opposed to forcing them to remain mired in the nuts and bolts of routine daily tasks that so often make up the vast majority of everyday IT workflow.

Now, let's recap some key concepts from the first chapter: IT process automation (ITPA) and run book automation (RBA) are simply two ways of identifying the same thing. These two terminologies convey similar meanings and seek to achieve the same goals—namely, the orchestration, integration, and automation of rule-based workflows. Each workflow consists of building-block tasks that progress through a series of procedures and events or outcomes, and seek to address and resolve all sorts of IT issues and activities.

The three primary components in any RBA system may be identified as follows:

- Integration: To collect, analyze, and transfer information between products and platforms to enable making input-based decisions and to execute dynamically configured task-related procedures using run-time data, status, and information.

- Orchestration: To coordinate, initiate, and organize actions within and among third-party systems and software to determine the next logical step or activity among a series of workflow tasks.

- Automation: To create self-maintaining processes that can initiate themselves upon receipt of alerts, events, or incident flags, as well as to notify handlers when failures occur, and when hand-off procedures are required to achieve a successful outcome.

It's also highly desirable for modern enterprises to adhere to the best practices and operations processes described as part of services delivery in the Information Technology Infrastructure Library, or ITIL, standards. The most important benefits in an ITIL-compliant RBA solution would include:

- Incident management: achieve higher service levels at lower support cost.

- Problem management: gain proactive resolution and service interruption prevention.

- Configuration management: create infrastructure agility and maintain up-to-date systems.

- Change management: improve service delivery at lower operational cost.

- Release management: reduce operational risk and ensure best practice adherence.

Figure 4.1 provides an illustrated example of RBA's integration into the IT environment and along with a visual representation of workflow orchestration across platforms and processes. There, a flow utilization graph charts a timeline of progress throughout a 7 day reporting period along with alerts, flow executions, and severity ratings for various elements throughout that same time frame. RBA delivers cohesive control over multidisciplinary objects throughout an enterprise combined with a comprehensive perspective on all related workflows, as evidenced by the appearance of Red Hat and Windows health checks alongside application alerts and repairs depicted in Figures 4.1 and 4.2.
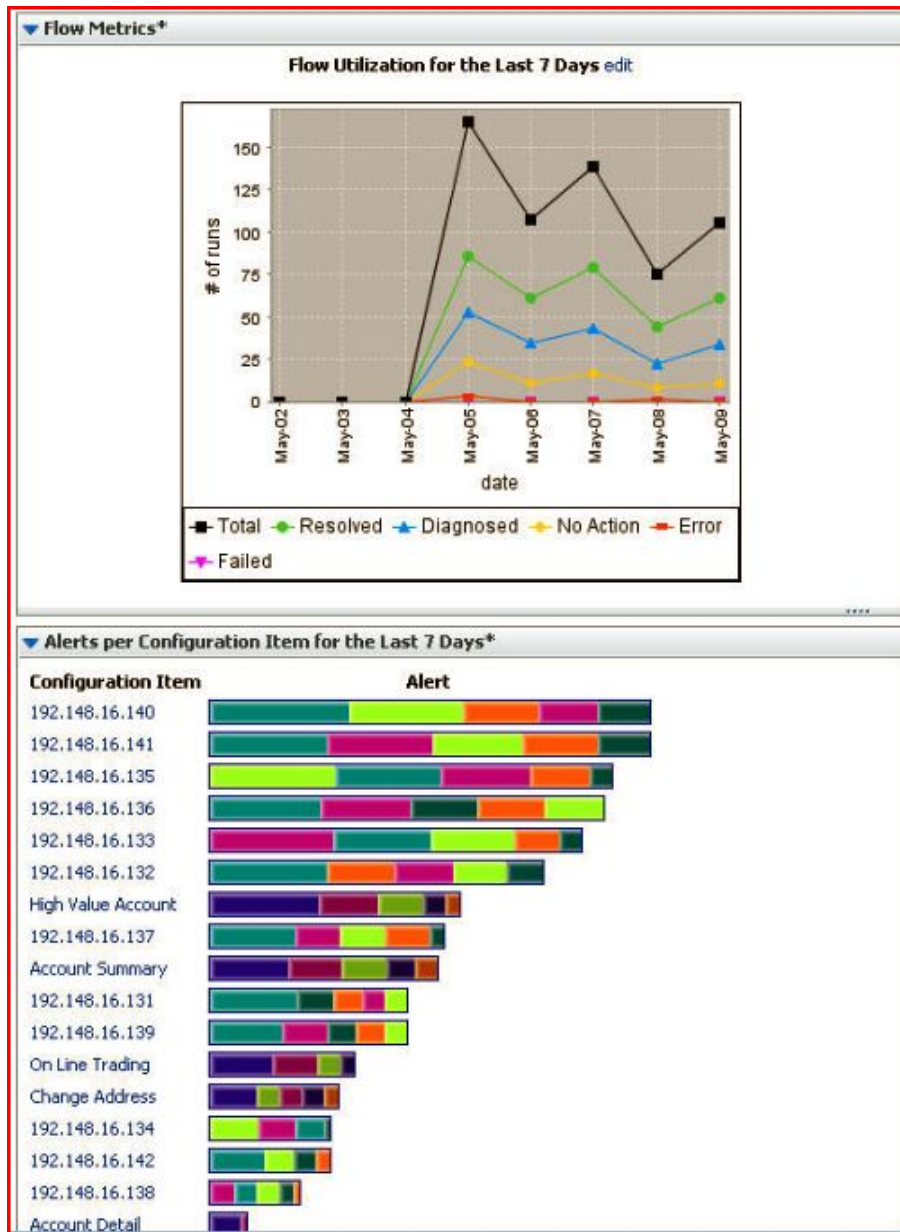
Figure 4.1: RBA provides cohesive control and comprehensive watch over enterprise workflows. This pair of items shows how workflows are distributed over time and by IP address or account ID.

Figure 4.2: RBA dashboard elements also report on most heavily used workflows (above) and shows the frequency of workflows in terms of error resolution status (below; note 500 refers to the generic HTTP status code for "internal server error").

The demand for enhanced organization, orchestration, and operations management within the enterprise IT environment expands dramatically as an organization's IT holdings expand to encompass thousands of applications, and as IT seeks to deliver an ever-increasing number of services. The diversity of platforms involved, each with its own unique platform-specific needs, can spawn serious challenges to those IT professionals who are tasked with addressing issues and resolving problems in such complex environments. In a nutshell, RBA seeks to unify and overcome this diversity by creating a flexible, far-reaching, and all-encompassing framework that enables companies and organizations to bridge the technological gaps that might otherwise foil a consistent and coherent approach to managing, maintaining, and monitoring such environments.

RBA's Top Value Creation Methods

Throughout the various chapters in this guide we've expounded upon various top value creation methods that RBA platforms can provide in their various configurations and capabilities. No single RBA solution manages to achieve that magical quality sometimes known as "one-size-fits-all." Instead, you will typically find carefully chosen combinations of components and elements that are governed by some top-level RBA framework in real-world solutions and implementations. This combination of individual connectors (to accommodate specific applications and services) and a general console and framework (to provide a single, coherent point of view and control) is what interconnects and unifies multidisciplinary platforms. Nevertheless, RBA remains capable of addressing platform-specific processes, while enabling the constructing of workflows that can involve any and all elements of the IT environment as task requirements dictate.

Conceptually speaking, there are two types of RBA products: *generic* and *specific* process providers. Generic process providers address all kinds of tasks or techniques to address the IT environment, and farm out workflow procedures to cover the whole enterprise landscape. Specific process providers are like field specialists in that they focus narrowly only on certain types of automation tasks. The best solutions for your particular situation will depend largely on what your particular IT environment already has in place, as well as the kinds of tasks, workflows, and activities it needs and wants to implement.

We review numerous specific value creation methods that RBA offers more fully in the passages that follow, including reduced time to resolution for alerts and incidents, empowering frontline support or help desk personnel to handle and resolve same, reduce escalations and upper-tier staff involvement, and more.

Drastically Reduce Time-to-Resolution for Alerts and Incidents

Basic IT firefighting tasks include many mundane or recurring patterns of processes and procedures that may be repeated *ad infinitum* on a schedule or on demand using an automated run book system. Time-to-resolution hinges almost entirely upon operator availability and rests primarily on root cause diagnostics. Overwhelmed and overworked IT support staff is less responsive to events of any criticality and less efficient at resolving issues of all kinds when they occur in rapid succession, or when demands on time and energy outstrip available human resources. RBA is subject to none of these constraints, and behaves the same way the first time it recognizes an incident or alert, or executes upon some predetermined schedule, and does likewise every time thereafter as well.

RBA manages alerts and incidents consistently whenever and wherever they occur, whether such occurrences are inconsistent or unexpected or otherwise, and is entirely able to make hand-offs to support personnel where critical thinking or further manual intervention is deemed necessary. Increasing Mean Time to Recovery (MTTR) for common events and incidents requires an agile, responsive IT workforce facilitated by automated recovery and repair workflows. That is precisely what RBA provides.

Figure 4.3 depicts average workflow execution times for repairs (MTTR, or "mean time to repair") over a yearly period graphing the progress of failed, erroneous, diagnosed and resolved procedures.
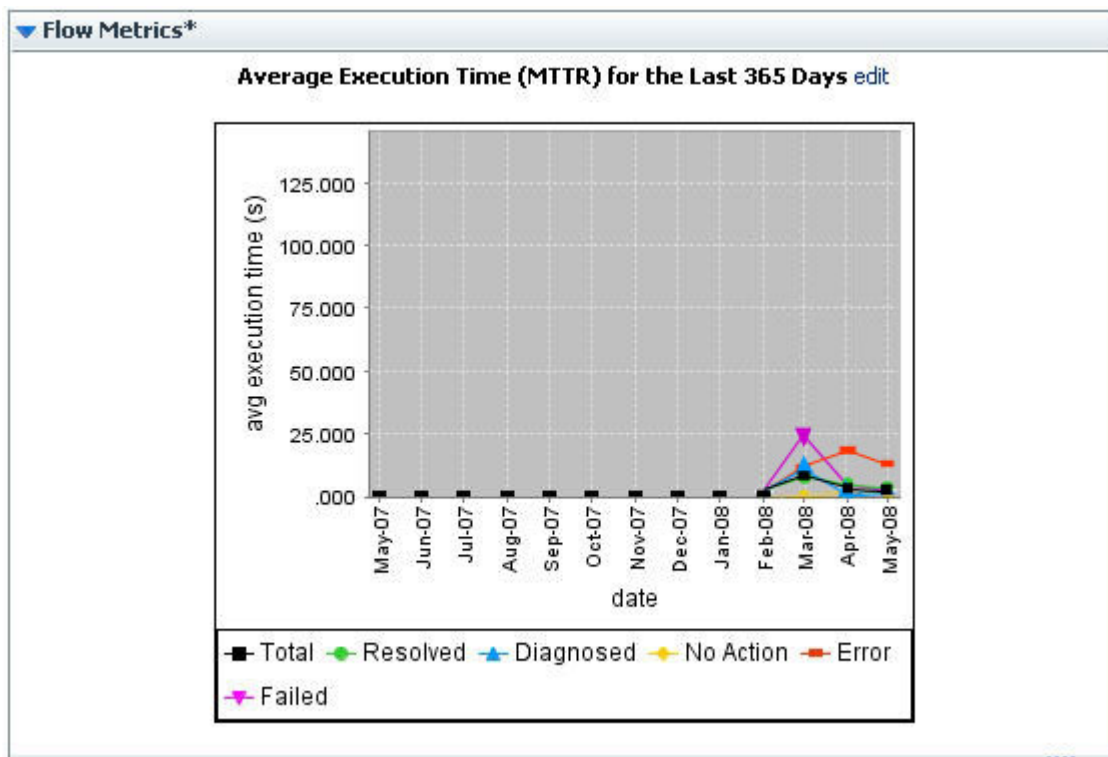

Figure 4.3: Average workflow execution times reporting MTTR in graph format.

RBA enables IT operators to achieve better incident response times and make timely delivery of priority services within an enterprise environment. It uses monitoring agents that detect trouble-ticket issues, prepare supporting documentation for executing visually-guided workflows as needed, and makes uncomplicated hand-offs at the start of a resolution phase wherever and whenever possible. This frees-up critical personnel and other resources to implement new IT tasks or to work toward mapping out and achieving new IT objectives. Perhaps more important, RBA helps to improve the quality of user experiences within the IT environment, thanks to quicker problem solving and fewer (and more time-consuming) escalations.

Empower Frontline IT to Resolve More Incidents

By empowering frontline IT operators to resolve more incidents and produce more results, organizations can come closer to achieving hands-free, self-maintaining management, maintenance, and troubleshooting processes and procedures. RBA helps to lay out and pave the road to IT self-sufficiency, as well as a parallel path to IT operational efficiency. When low-level help desk or support staff become capable of performing more tasks, and resolving more outstanding issues—particularly those otherwise relegated to more experienced handlers—high-level Tier 2 and Tier 3 staff need invest far less time performing the same actions or solving the same kinds of problems over and over again. While this may not necessary lead to reduced needs for senior-level headcount, it certainly does free these valuable people up to spend more time investigating and resolving serious problems (and creating RBA workflows to automate their subsequent resolution thereafter).

Those IT operators who may lack sufficient batch scripting, workflow creation, or job execution experience can obtain valuable assistance from RBA. This occurs automatically, thanks to the visually-guided scripting facilities normally used in RBA systems. Such work no longer requires users to become fully-versed in platform-specific tasks or scripting procedures—there are adapters and examples for all kinds of existing applications and issues that IT professionals can use as templates or "go-bys" to implement workflows for all kinds of tasks. Even junior IT administrators can create visual step-by-step workflows that can be reviewed, tested, and debugged, then deployed across the entire production IT landscape.

Reduce Escalations and Minimize Alert Floods

A reduction in alert call volumes and incident response handling procedures is probably the most significant benefit that RBA systems deliver. Such systems seek to eliminate the often unnecessary escalation of routine alerts, events, and incidents to better empower frontline IT operators to perform more tasks and attain IT self-sufficiency. With lower-level IT personnel performing more heavy lifting, higher-level network and system administrators become empowered to provide better oversight, assess and optimize IT infrastructures, and to dig into those occasional "Black Swan" events that can threaten the bottom line and demand immediate, full-on engagement to tackle and solve.

📖 The Black Swan Theory stems from the ancient Western conception that "All swans are white" and a black swan represents a metaphor for some improbable or perhaps even inconceivable occurrence. In short, "Black Swan" events are highly unlikely events rare beyond normal expectation that are difficult to predict though they will often come bearing significant impact and associated cost. This makes planning for such events challenging, to say the least! Nicholas Taleb's excellent book *The Black Swan: The Impact of the Highly Improbable* (Random House, April, 2007, ISBN-13: 978-1400063512) still offers the best exploration and discussion of this concept around.

Common, repeatable IT tasks follow a trend that is recognizable and reproducible through an automated platform. High alert volumes and subsequent incident handling activities consume an overwhelming majority of IT "processing cycles" in terms of systems and system administrators. A single alert can potentially cascade into thousands of software notifications, and directly impacts support staff—particularly first responders. Alleviating such management burdens and empowering management personnel is a significant advantage—indeed some might argue it is the primary reason for—using RBA systems in the modern IT workplace.

Enable Consistent, Repeatable Process for Automating Change

Even a simple change request can cascade into a complicated collage of system alerts and unhandled exceptions, and bog down responsible or related IT resources. Fortunately, most change requests satisfy the RBA requirements for consistent, repeatable processing to automate change request response and resolution procedures.

Consider your most basic IT tasks: these are the primary building blocks for enterprise IT operations. For each task-based unit, there is a definable and discernible pattern that can be copied and reproduced via automation. Tasks such as provisioning a new virtual or physical server—and all the integrated logic or configuration settings that go along with it—and decommissioning archaic platforms or programs for transition into new products. Automate these, and you can alleviate all the hard work typically associated with IT chores, to speed handling times and make better use of IT staff resources.

Establish Linkages Between ITIL Incident and Problem Management Processes

The IT Infrastructure Library (ITIL) integrates IT best practice recommendations, incorporates mission-critical resources, and implements enterprise security requirements. ITIL gives an almost complete perspective on the enterprise IT landscape in its entirety to include all the processes, platforms, and products that make up its underlying elements. ITIL is the documentation that describes best practices in IT service areas including change and configuration management, software control and distribution, and help desk dispatch and notification.

ITIL is a customizable framework that supports IT initiatives and facilitates IT service providers in planning consistent, documented, and repeatable processes to improve service delivery. Establishing a linkage between ITIL incident and supporting problem management processes is crucial to building a self-healing, self-sustaining IT infrastructure. Because workflows are essentially self-documenting and provide the glue that ties best practices into every day routine tasks and events, RBA can help to demonstrate the value of ITIL, while also enabling IT organizations to move toward ITIL compliance.

Capture Incomplete Incident Resolution Audit Trails and Create Process Documentation

As part of the ongoing RBA process, tasks and technologies are documented as they are introduced, utilized, and eventually removed from the IT landscape. Documentation supports personnel and process. Without documentation, IT operators may be left to cope with possibly unknown and potentially unclear procedures and processes for handling hardware or software, responding to particular incidents or issues, resolving problems, and so forth.

RBA captures and documents incomplete incident resolution audit trails and automatically generates process documentation for executed procedures. IT operators are thereby unburdened of the clerical work involved in documenting such procedures while an automatically generated audit trail facilitates later administrative review, and may even help to drive modifications to existing RBA workflows, or creation of new workflows as problems and failures for new or existing workflows reveal themselves over time. Under RBA, both maintenance engineers and frontline operators can benefit from the experiences of their predecessors thanks to documented procedures and audit trails that persist after incidents are handled, alerts fielded, routine tasks undertaken, and so forth.

Integrate Role-Based Access Controls into Incident Resolution Processes

Any complex system that comprehensively manages business IT infrastructure must also capably and carefully implement security processes and procedures as well. The biggest challenge in dealing with sensitive data comes from properly securing it from unauthorized access. Confidential business processes and sensitive client data are specific and important elements over which RBA should apply proper control, and against which RBA should also review relevant security policy requirements and conditions.

Integrating role-based access controls (RBACs) into the RBA platform is necessary and warranted. As certain systems retain certain types of personally identifiable and privately-held information they are often subject to prevailing notions and policy (and even sometimes legislation) that governs how sensitive data be stored and processed. In such situations, RBA platforms must comply with guidelines, policies, best practices, and relevant rules or legislation, even as it implements its own integration, orchestration, and automation procedures.

Capture Tribal (Informal) Knowledge in a Reusable, Maintainable Form

A big problem with tribal knowledge is that it instantly disappears when the person who possesses it leaves the tribe. Isolating information in this manner is counterproductive to proper function of the IT environment, which demands that all things operational about and within itself be known. It's a great disservice to those maintainers and managers who remain behind, when tribal knowledge is not made explicit as individual leave to go elsewhere. Companies and IT organizations may be left only with the idea that a specific, possibly arcane process, program or procedure exists to handle certain systems or situations, but be unable to put that idea to work for want of specific details and information.

This is a phenomenon that RBA eliminates. By automatically generating documentation for workflows, RBA eliminates the potential for new pockets of tribal knowledge to emerge, while flushing out all the relevant and important details from such pockets as may already exist. Furthermore, a complete RBA system can also provide the means necessary for administrative personnel to author content on how to conduct procedures, execute workflows, or carry-out tasks related to infrastructure management and maintenance routines.

Automate Repetitive Maintenance Procedures

The third key benefit of RBA is automation of repetitive maintenance procedures, such as running the gamut of discovery and dialog commands involved in server uptime identification. For example, a simple procedure might involve the invocation of ping and the inquiry of remote server uptime followed closely by platform identification and eventual log-in discovery tasks. This process, when followed consistently, may be reproduced easily within the facilities of RBA.

Part of that frontline operator empowerment we've already mentioned is based directly upon this automation aspect. It depends on reduced manual, hands-on interventions on behalf of support personnel, while also training platforms to take care of themselves through RBA. As a result, workers at all levels—including priority high-level system or network administrators and managers—are able to tackle new tasks and create new goals instead of servicing the same old requirements for some archaic process or procedure that has eluded automation or codification.

Integrate Disparate Systems, Management Tools, and Platform-Specific Processes

Acquisitions, inheritance, and mergers often introduce diversity among disparate systems, related management tools, and platform-specific processes within the existing enterprise space. Though often welcomed as a sign of growth and ultimate convergence, such introductions also carry with them the complications inherent to a difficult and demanding integration process. AIX, BSD, and UNIX are all different within themselves despite belonging to a similar breed—yet each one requires different plans, procedures, and processes to manage and maintain.

Then factor in the additional cost and complexity of unifying management and maintenance tasks across these platforms in combination with Linux, Mac OS, and Windows platforms. Each has its own particulars and peculiarities that make jobs increasingly difficult for IT support staff. In many cases, they're already stretched thin handling and operating an increasing array of systems and platform-specific duties. RBA's demonstrated ability to tie all these puzzle pieces together continues to drive its adoption in many enterprise environments.

Provide a Basis to Orchestrate and Coordinate Complex Change Requests

Imagine a collection of tribal peoples each set in their own ways, speaking their own languages and governed by their own laws, coming together under a common umbrella. Envision yourself as the ultimate coordinator over all these tribes, tasked with orchestrating their activities and movements. You'd have to be a pretty capable linguist and careful strategist to pull this off.

That analogy aptly describes most modern IT environments. Two apparently alike platforms may nevertheless be completely unalike in their processes and procedures, leaving IT professionals to determine discernible differences and definable distinctions about how those elements operate individually. That's one way to sketch out a visual depiction of how to coordinate and orchestrate a commonly-applied change request across several systems simultaneously (instead of individually). RBA deftly handles this heavyweight duty with relative ease.

Apply Change Management Across Multiple Systems and Services in Concert

In addition to applying a single common change request across multiple systems, RBA can also handle situations that potentially involve a diversity of multidisciplinary platforms. BSD, Linux, Mac OS, UNIX and Windows platforms commonly converge in the same enterprise IT space to achieve independent platform tasks in parallel with business objectives. RBA eliminates the administrative headache involved in individually implementing changes across system, service, and platform boundaries to better orchestrate, automate, and manage change across the board in a cohesive fashion.

Change management across systems and services through the automated and self-documenting component of an RBA system yield two principal benefits:

- Provides automatic documentation of changes applied, and change processes followed.

- Captures important organizational skills and knowledge, problem-resolution methods.

Automatically-generated documentation means no procedure is a repeat cycle of rediscovery when procedural knowledge is lost, and no more wasted effort seeking out supportive field manuals for operating programs and invoking processes. Applied and followed change processes are documented in real-time so that support staff needn't waste any time creating and preparing such material themselves.

Furthermore, a repeatedly touted feature of RBA is its ability to capture organizational skills, knowledge and wisdom encompassing all silos of enterprise IT and comprehensively organize such information. In context, this provides greater manpower and mobility in IT support staff to achieve new goals and resolve new problems.

RBA Suggested Usage

Resistance to change—perhaps the one thing RBA cannot automate—can appear a seemingly insurmountable force and impassible object in the path to implementing RBA, which is why you've got to play hard and work hard. RBA alone "looks good on paper" but it's up to you how RBA is presented and impressed upon your superiors and stakeholders, so you must prepare accordingly.

RBA implements many universal IT best practices and imparts its own implementation and utilization best practices. Each configuration individual circumstance brings its own unique challenge to the development and implementation process for establishing RBA in the enterprise. The following passage generically briefly examines and explains a few best practices for RBA to serve as a jump-off point for your own experiences.

Best Practices

Implementing best practices is primarily achieved through defined and automated IT operations management processes that orchestrate activities between applications, departments and silos. The ITIL framework outlines best practices for all IT-related activities within the enterprise environment and can be applied accordingly to RBA's implementation and operation.

Report generation is part of RBA's automatically-generated documentation. Generated reports provide historical and statistical data representing everything from alert handling to incident testing and even application repair workflows. Observing these reports and fine-tuning your workflows or implementation procedures accordingly is instrumental to maintaining a consistent level of service performance. Figure 4.4 depicts a summary of workflows over a period of 24 hours with a number of runs, individual steps and average repair time reporting—among many other useful values.

Figure 4.4: Automated reporting summarized over a 24-hour period.

Visualization tools (see Figure 4.5) leverage enormous competitive advantage in the IT management space. RBA promotes a greater sense of administrative empowerment by eliminating the mental visualization and diagrammatic sketching used to describe scenarios, situations and solutions that likely encompass multiple platforms, programs and practices. Figure 4.5 depicts the visualization of a workflow that removes a failed node from a cluster, including all necessary shutdown procedures.

Figure 4.5: Visualization lends great insight to individual tasks and entire workflows.

Below, we enumerate five best practices for establishing and maintaining RBA. Apply these practices when presenting the case for RBA to higher-level management and stakeholders and keeping them informed with every captured goal of the implementation process.

- Start small: Begin with a high-profile project that utilizes a small number of workflows to snag and automate "low-hanging fruit". Capture low-level tasks in a compartmental manner (i.e., online backup and data replication tasks) according to related functionality or purpose, and introduce several workflows over a 90-day probationary period.

- Stay informative: Involve as many stakeholders in the RBA pilot and implementation process as possible. The better informed the stakeholders are, the better prepared they'll be to enact upon the appropriate decisions that support the RBA solution.

- Sell strengths: Market activities and capabilities to internal constituencies vigorously and repeatedly. Adoption may be slow and met with unexamined resistance, so focus on key advantages and specific strengths when exploring and explaining the RBA solution.

- Train specifically: Use "train the trainer" techniques to develop product champions and subject matter experts within key internal organizational units. These minted gurus of their private technology spaces are then able to establish a chain of command and central information resource for departmental RBA workflows.

- Play hard: Concentrate on exposing and exercising RBA in the enterprise IT environment. There is no need for grandiose, formal or splashy releases over a long, drawn-out period—a strategy of starvation that promises little immediate return for hungry investors. Show stakeholders what RBA is capable of achieving and experts will be flooded with implementation requests instantly.

RBA provides the solution to define and automate end-to-end IT processes across a diversity of infrastructure elements in a consistent and dependable fashion. IT best practices can be standardized and compliance enforced with up-to-date tracking and reporting of all system activities. Most data center tools provide narrow task-level automation within select domains of operation but none achieve the broader workflow-level automation provided in RBA solutions.

Perhaps the biggest win of all that inheres to RBA implementation, deployment, and regular use is the global perspective it provides across the entire IT infrastructure. Though many enterprises and organizations start with measurable gains that derive from automation of routine and scheduled maintenance tasks, or from user and system provisioning, over time most RBA users appreciate the coherent and consolidated viewpoint on the IT infrastructure that RBA delivers. Though the vantage point is broad and the perspective deep, RBA remains able to address platform specifics and details at the lowest levels. The combination of an Olympian view and atomic-level capability offers IT levels of command and control that are otherwise quite difficult to attain.

Data Center Automation: A Holy Grail for RBA

If there's one area where automation pays really big dividends, it's in the large data centers that beat at the hearts of so many enterprise IT operations. As the places where large collections of networking and computing equipment congregate, along with the staff to manage and maintain such gear, data centers are also where automation of manual activities can deliver the biggest savings simply because of the scale of activity involved. Small gains in productivity and staff availability from a handful of servers quickly compound into significant savings on costs or billable hours when large server farms begin to benefit from rapid, reliable automated processes and procedures.

In addition, RBA provides the means for enforcing compliance and acquiring audit data as processes and procedures are enacted. It doesn't matter if this is viewed from a security perspective, where security policy enforcement, compliance and audit are paramount, or from regulatory compliance perspectives, where responses to privacy and data integrity requirements (HIPAA), audit and reporting requirements (Sarbanes-Oxley and similar regulatory frameworks), and so forth may be addressed via the out-of-the box compliance reports that RBA systems routinely provide. Automatic reporting, audit and activity logging, and document generation reduce time and expense involved in achieving compliance, while also making it easier for enterprises and organizations to demonstrate that they are indeed in compliance.

Furthermore, RBA's global perspective on the IT infrastructure makes it an ideal source for up-to-date views of the entire IT edifice, along with visibility into individual systems and software components. This not only serves to speed problem diagnosis and resolution, it also creates a real-time model of the IT infrastructure that can serve to drive disaster recovery if and when it should be needed. Indeed, RBA offers the ability to capture and store the information necessary to drive disaster recovery as only one of the many categories of routine tasks it can schedule and execute—including backups, replication of configuration management databases (CMDBs), global directories and databases, and all the other infrastructure elements that must be reconstructed as part of any disaster recovery implementation.

Finally, because RBA makes it simple, straightforward, and routine to implement best practices for change and configuration management, RBA also helps to minimize and even to handle the impact of change on complex, multi-platform IT infrastructures. The cookie-cutter approach that RBA uses to create standard builds and configurations across the enterprise also helps to eliminate human error, and can increase the availability of the networks, servers, and applications that deliver information technology to its users, be they inside or outside organizational boundaries.

The ultimate goal for RBA is what is sometimes called business technology optimization. This approach is designed to ensure that the money and resources invested in IT, and the applications under development or in use as part of the IT infrastructure, meet business goals. A lifecycle approach to managing and operating IT lets organizations and enterprises align IT with business priorities, while also delivering increased value and efficiency in the data center, across the networks, and all the way out to the clients and customers who depend on IT to access information, conduct business, and get on with their lives.

RBA on Rails: Automation at a Railway Company

At a Texas-based railway company, a subsidiary of a major national railway system, RBA rode to a different kind of rescue. Here, its job was to help consolidate and coordinate assets distributed at a multitude of locations in 28 states in the continental US, as well as in two Canadian provinces. To improve communications between railway operators all over the place and headquarters, this company recently initiated a wireless networking project that resulted in the deployment of over 2,000 new wireless networking devices in all 28 states. Adding so many devices was sure to strain the railway's IT staff, already more than busy with managing an existing 5,000 networking devices to support inventory and train management applications, as well as Voice over IP (VoIP) applications.

Prior to the introduction of RBA, regular maintenance tasks were labor-intensive and often involved lots of travel. In addition, though changes may have been implemented on hundreds to thousands of network devices, no records were kept about which devices were updated, who performed those updates, and what those updates actually entailed. Wholesale updates, patches, and fixes required individual access to each network device, one at a time. Mistakes and misconfigurations could involve extensive troubleshooting efforts, and often posed difficulties in restoring systems to known, good, working configurations. Worse yet, such difficulties might mean that cargo operations and inventory reporting could be in limbo, delayed until problems were fixed.

The railway operator determined that RBA was its best solution for managing network operations, and deploying mass changes (such as SNMP community string or password updates) to thousands of devices. Automation offered the promise of consistency across the entire operation, and the opportunity to finally enforce compliance to IT change management and security policy requirements.

In particular, the railway operator was able to make good use of RBA in the deployment of its 2,000 new wireless networking devices. Whereas before RBA, network engineers had to log into devices individually to make configuration changes, automation let IT staff set up workflows to automate password and SNMP community string management, deployment of access control lists, and configuration updates and tracking. Provisioning workflows for new devices enabled complete, consistent set up for each and every one identified as a target for those workflows.

The RBA environment lets the railway company manage hardware from numerous vendors, as well as its various VoIP and wireless networking systems. Using RBA, this company was able to double its wireless usage with a near-zero increase in labor costs and IT resources. Even better, its switch to standardized network device configurations and automated management of those configurations helped accelerate delivery of new products, reduce delays caused by IT glitches, and drastically lower the amount (and impact) of downtime on mission critical applications including train scheduling and inventory control.

In terms of raw numbers, the railway company was able to avoid $600K in extra labor costs it would have otherwise had to absorb to extend its wireless networks, and to keep IT headcount flat as well. The value of automated change and audit tracking is harder to quantify, but certainly gives the company a much better sense of the condition of its IT infrastructure elements as well.

RBA Today

In its initial phase of development and deployment, RBA was simplistic and limiting. Early designs merely focused on harnessing existing tasks and tools rather than prototyping and piloting entirely new workflows. Originally, RBA proved satisfactory for addressing mostly mundane lower-level IT procedures such as help desk (or Tier 1) work patterns—trouble ticket issuance and tracking, basic alert-flow triage and response, etc. RBA was also initially static in nature, making hardcoded assumptions about the platforms, versions and the state of the environment it encountered and any underlying tools. Much of this cumbersome and awkward functionality only complicated efforts higher up the administrative chain (i.e., Tiers 2 and 3).

RBA's initial efforts primarily serviced junior IT operators and administrative staff whom were presumably less capable of coding and scripting in heterogeneous environments or when working with unfamiliar hardware and software. Generic, out-of-box exercises range from basic automations (i.e., opening and closing tickets), rebooting stalled servers and job scheduling. Any tasks that weren't directly addressed might be addressable through integration packs allowing interactions with particular tool sets already utilized within the IT environment.

We mention this historical footnote because you may encounter some resistance in the field when adopting RBA where others have experienced the initial setbacks and shortcomings of early designs. RBA has evolved beyond that original sticking point to include a broader range of capability and features. Any remaining negative impressions may prohibit the adoption of RBA and merely represent opportunities for you to emphasize advances and underscore the importance of new RBA solutions.

In its latest revolution, RBA is developed with a keener sense of insight and intelligence with regard to handling dynamic workflows. Now practically any authorized personnel are capable of producing new workflows to handle new tasks including the ability to "pop the hood" and examine the mechanical aspects of each procedure. RBA is fully capable of addressing virtually any IT-related issue in the enterprise—an enterprising ambition, indeed—to better orchestrate and automate upper-tier areas: ongoing database administration, multidisciplinary systems administration and diverse application support. That's not to say that overcoming most operational deficiencies is easy—producing model workflows and mapping exact procedures and tasks is still subject to review and approval.

Dynamic workflows evolve as the environment undergoes change. RBA maintains a metadata repository between workflow automatons and the target environment that captures current state for inclusion with and comparison against historical data. This information is then taken into account prior to or during run-time—a process referred to as metadata injection. RBA keeps record of its own native metadata information and integrates with Change Management DBs (CMDBs) where applicable.

The latest in RBA is also much more flexible to better accommodate higher complexity. By exposing the source code beneath each workflow, operators even with minimal experience may explore and examine the underpinnings and add new steps as necessary. Managing a multidisciplinary enterprise IT environment has never been more comprehensive or complete.

It's All About Achieving Efficiency

Various studies indicate that enterprises seeking to achieve compliance manually spend up to five times as much on attaining that goal as do organizations that use automated systems like RBA instead. Over 40% of the compliance costs involved can be attributed to labor itself, where much of that investment goes to tasks and activities that are repeated time and time again during the compliance process. Other cost components include time- and labor-intensive compliance checks, plus generating the audit trails and reporting necessary to assess and document compliance levels and details. RBA helps enterprises and organizations to achieve these cost efficiencies by automating routine tasks and incident handling, enabling easy implementation of change management and compliance disciplines, and generating audit trails and documentation as part of the automation process.

Future visions of the data center call for increased use of automation technology as well. Not only does the volume and need for automation of repetitive tasks, scheduled maintenance and lifecycle management, and other regular activities continue unabated, many future projections call for self-configuring data centers to respond to current and project application and service demand. Increased use of virtualization lends itself particularly well to RBA, because the process of launching and managing virtual servers and the services they provide is easy to automate and manage once initial workflows involved are worked out, implemented, and tested. Because users ultimately decide what content and services they need to use at any given moment, RBA can help to support a more dynamic and fluid enterprise IT environment by making it easy to bring up and manage virtualized systems as they're needed, and to "put them away" when demand abates, and other needs arise.

Ultimately, the case for RBA rests on the return on investment that this technology delivers. With its ability to speed incident handling, reduce support and help desk costs, implement IT efficiencies, and help the relentless drive toward regulatory and best practices compliance, making the case for RBA depends more on your situation and your needs than on the vast range of savings and efficiencies that RBA can deliver. Choose those most relevant to your situation, run the numbers, and the case for RBA will largely make itself.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.