

Business white paper

Top ten reasons to automate your IT processes



Table of contents

- 4 Data center management trends and tools
- 4 Today's challenge
- 4 What is next?
- 5 Automating the remediation of incidents and alerts
- 5 Empower frontline IT operators to resolve more incidents
- 5 Decrease alert floods
- 6 Establish a consistent, repeatable process for orchestrating change
- 6 Create linkages between your ITIL incident management and problem management process
- 6 Capture incident resolution audit trails and create process documentation
- 7 Integrate role-based access control into your incident resolution process
- 7 Capture organizational knowledge in a usable and maintainable way
- 7 Automate repetitive maintenance procedures
- 8 Integrate disparate systems management tools and process
- 8 Summary

Organizations of all sizes are adopting IT process automation. While their critical business initiatives may vary, a standard set of objectives driving the need for automation has emerged.



This white paper explains the top ten reasons why CIOs, managers, and production support teams are adopting IT process automation.

Data center management trends and tools

Today's IT infrastructure is more complex than ever. There are more applications, more servers both physical and virtual, larger global networks, and more data; all of which needs to be managed. Businesses can't afford to solve this problem by continually adding to headcount. They have to find a way to manage it all more efficiently.

Adding to the problem is the inability to retain knowledge. Companies of all sizes struggle to maintain consistent data center processes in the face of attrition. A lack of standardized processes can have a negative impact on overall service quality. There's no indication that either of these trends is subsiding. Industry analysts predict that this growth trend will continue as businesses look to differentiate themselves through innovative new offerings powered by business-specific algorithms and customized applications.

As data centers grow and become more complex, IT organizations are increasingly relying on systems management software and automation to manage their IT infrastructure more efficiently, leverage existing headcount, and improve knowledge retention when faced with staff attrition. The most common systems management products fall into three categories—monitoring, ticketing, and change and configuration management. These products help you manage your infrastructure and determine whether it is performing well and meeting your business objectives.

Today's challenge

As systems management software matures and you become more adept at using monitoring and ticketing, you need new methods to increase organizational efficiency and retain knowledge. Although monitoring products can detect failures in your infrastructure and help desk products can allow you to track tickets as incidents are routed and escalated, they do not help you resolve these incidents. Incidents are often resolved through error prone manual processes. Making matters worse, it's often impossible to determine which incidents require action and that can lead to unnecessary escalations. When the escalations do occur, the insufficient knowledge transfer between level 3 experts and frontline IT operators leads to longer time to incident resolution. Existing solutions have not adequately alleviated these IT pain points. You need a new category of software to take you beyond monitoring and ticketing.

What is next?

IT process automation technology can help you automate the remediation of alerts and incidents, increase your infrastructure uptime, and reduce your operational costs.

You can increase value from using IT process automation by focusing on these ten areas:

- Automating the remediation of incidents and alerts
- Empowering your frontline IT operators to resolve more incidents
- Decreasing the number of alert floods
- Establishing a consistent, repeatable process for orchestrating change
- Creating linkages between your Information Technology Infrastructure Library (ITIL) incident management and problem management process
- Capturing incident resolution audit trails and creating process documentation
- Integrating role-based access control into your incident resolution process
- Capturing organizational knowledge in a usable and maintainable way for reduced training costs
- Automating repetitive maintenance procedures
- Integrating disparate systems management tools and process



1. Automating the remediation of incidents and alerts

Many organizations have adopted advanced monitoring solutions to track the performance of their growing IT infrastructures. With these capabilities in place, you are alerted quickly when an incident occurs with your infrastructure. However, resolving these incidents is largely a manual process that relies on informal, organizational knowledge, escalations, conference calls, and multiple hand-offs resulting in slow resolution and customer dissatisfaction.

With IT process automation, you can automate the remediation of many incidents through:

- Self-healing, automated workflows that can be initiated automatically from monitoring tools or manually by operators
- Rapid diagnostic workflows that can be executed across your data center infrastructure faster than manual processes, providing rapid troubleshooting and the critical information your frontline operators and level 2 and 3 IT staff need to resolve the issue when human intervention is required
- Automatic remediation, including server and service restarts, even for complex, clustered infrastructures with network load balancers
- Automatic ticket creation, updates, and closure in addition to alert updates and closure upon incident resolution

With these features, IT process automation products provide fast, automated responses to alerts, and incidents with the documentation and information you need for diagnostics, remediation, and root-cause correction.

2. Empower frontline IT operators to resolve more incidents

Research has shown that in many organizations up to half of all incidents are escalated beyond the frontline IT operators to level 3 system and network administrators and management. These escalations result in less productivity and also cut into personal time as days, nights, and weekends are spent on exchanging information and on conference calls trying to resolve the issue.

IT process automation can help transform this manual ad hoc effort into streamlined and standardized workflows. When an incident occurs, a workflow is automatically launched to execute diagnostics to better understand the root cause of the problem. With an easy-to-follow, wizard-based user interface, frontline operators can run these automation flows, eliminating the need for level 3 experts and management to intervene. After identifying the source of an incident, frontline IT staff can remediate or escalate as needed. IT process automation helps frontline operators respond more quickly to incidents by enabling them to perform more diagnostics, triage, and remediate using knowledge that previously resided solely with the level 3 administrators.

3. Decrease alert floods

Alert floods can happen when IT staff is barraged with alerts. They often lack the data to know which alerts require action and which are just noise. Even a small reduction in alert volume can help IT staff become more productive and focus on high-priority critical issues.

IT process automation integrates with your monitoring and ticketing product to help identify actionable alerts from noise and helps the frontline operators quickly prioritize their response to real issues.

The following is an example of an automated alert management process:

- Proactive monitoring tools detect an incident and trigger alerts.
- An IT process automation workflow initiates in automatic mode to identify actionable alerts from noise alerts and creates incident tickets only for actionable alerts with appropriate priority using impact relationship from configuration management database (CMDB). Using IT process automation, the frontline operator is presented with actionable and prioritized incidents.

In summary, IT process automation helps the frontline operators to concentrate their efforts on actionable incidents and avoid false incidents. IT process automation helps you operate efficiently and reduce alert flood.

4. Establish a consistent, repeatable process for orchestrating change

Organizations often face problems with undocumented or outdated processes for implementing change. As a result, frontline operators can find themselves responding reactively when rogue changes result in production issues.

IT process automation provides significant advantages when automating the change and configuration management process:

They consistently run automated change management procedures. With change and configuration management procedures captured in IT process automation, IT system administrators can initiate an automated set of procedures to check applications and servers for compliance status and trigger server, network and storage automation products to perform necessary updates. These change management workflows can run across hundreds of servers and devices with complete audit trail, creating documentation you need for compliance requirements.

They improve overall cost efficiency. With IT process automation tools for orchestrating change and configuration management, previously siloed IT specialist teams can eliminate manual and error prone procedures by automating the end-to-end change and configuration management process.

They drive increased agility and responsiveness. Capturing provisioning actions in automated IT process can help you react more quickly to changing business needs and also reduce the time to deploy new infrastructure. Organizations can see a 50 percent to 70 percent reduction in the time needed to provision new systems and infrastructure.

5. Create linkages between your ITIL incident management and problem management process

Responding to hundreds or thousands of alerts each day puts most IT operations groups into “fire-fighting” mode. They need to respond to incidents as quickly as possible to maintain critical application and infrastructure uptime. However, tickets are usually not updated with relevant troubleshooting information after clearing an alert. Industry studies show that on average only 2 percent of incidents are tracked to closure with a ticket. Unfortunately, many IT operations groups manage symptoms, or incidents, instead of addressing root causes to fix problems.

When you implement IT process automation, you can begin to link incident management to more effective problem management. IT process automation flows let you quickly respond to alerts through automated diagnostic, triage, and repair and also capture the inputs and outputs for each automation activity. For example, an automation flow for a slow-responding J2EE application checks the application and server status, network status, load-balancer status,

and database status and records the inputs and outputs as part of the diagnostic and repair process. If necessary, the automation flow can restart specific servers and then recheck application performance. Over time, if the application is consistently slow and the automation flow runs routinely, data in the IT process automation is aggregated, allowing for detailed analysis of specific devices, such as insufficient memory in a server, or potential application issues, such as memory leaks. Leading IT process automation products can capture and record all inputs and outputs as part of incident response and support aggregation and parsing of the data to analyze performance and root causes of incidents by domain, applications, and configuration items (CIs).

6. Capture incident resolution audit trails and create process documentation

IT process automation creates value by automating alerts and incident resolution, typically performed manually, thus increasing application uptime and letting you focus on strategic IT issues. IT process automation also captures information automatically for each automation step and flow. The flow information is stored in a database for the IT process automation product.

IT process automation can also automatically create documentation from automation flows. After a flow is created, you can automatically create documentation that describes each step of a flow. As a result, you can quickly document the process automations instead of spending time on manual documentation.

IT process automation documents the diagnostic, triage, and remediation process from initial alerts through resolution, including automatic ticket and alert updates and closure. Automating this end-to-end process can help you to fully document your process and its outcomes—two critical requirements for Sarbanes-Oxley Act compliance audits.

7. Integrate role-based access control into your incident resolution process

Many IT organizations struggle with information sharing and efficient escalation among levels 1, 2, and 3 of support. These information exchanges can occur in the middle of the night without capabilities for capturing the current state of systems or problem solving.

When properly implemented, IT process automation can help through two features:

- Role-based access control
- Capture of input and output data, as previously discussed

Role-based access control complements the capturing of input and output data, so that you only perform the automation actions for which you have authorization. IT process automation requires credentials that are appropriate for each automation step. You can also map these requirements to your Active Directory—directory service for proper credentials.

When used together, these two features result in fewer and more efficient escalations. Automation flows escalate only when frontline operators do not have proper permissions or when an automation flow requires expert operator intervention. Also, escalations are more efficient, because level 2 and 3 staff can easily determine which diagnostic and repair steps have been executed, what the output of each step is and what the likely set of next steps should be.

8. Capture organizational knowledge in a usable and maintainable way

Turnover in IT organizations continues to challenge IT management in its efforts to serve the business in a repeatable and consistent manner. Many procedures are undocumented, unused, or outdated, so IT groups often rely on organizational knowledge when responding to incidents. When these professionals leave, they take this core knowledge with them, leaving the organization struggling to address critical alerts.

With the help of IT process automation, IT process and procedures are represented as automation flows. These flows are maintained and current as they constantly execute diagnostic and repair actions. Two-way communication with the CMDB, can help you initiate, record, and discover changes in your infrastructure. As a result, IT process automation flows are automatically kept current as changes occur. This knowledge remains during turnover because it is captured in a usable and easily maintained system.

You can execute IT process automation flows manually, using visual guidance. Visual guidance makes it easy for new frontline operators to learn step-by-step diagnostic and repair process as they respond to alerts.

9. Automate repetitive maintenance procedures

In addition to automating key ITIL processes, IT process automation applies to common, repetitive maintenance procedures.

Periodic maintenance procedures are repetitive and time-consuming when performed manually. Tasks are usually scheduled and predictable with standard, well-understood process and predictable outcomes. These types of tasks are also appropriate for automation.

Examples include:

- Stopping, starting, and restarting services at timed intervals
- Rebooting and reconfiguring file, and print servers
- Changing passwords and creating users
- Rotating, reviewing, and monitoring log files
- Periodically defragmenting your database

Because of their predictability, you can document and automate these process and procedures using IT process automation. They can execute as needed by a IT process scheduler or an operator, or be triggered by a specific event. With IT process automation, you can perform these tasks using visual guidance or through automation. You can also capture the output of completed tasks for audits and reporting. IT process automation of maintenance and repetitive tasks helps you focus on more critical business issues.

Through visual guidance, IT process automation can help you cut new-hire ramp-up time by half.

10. Integrate disparate systems management tools and process

Systems management products have resulted in mixed success. Many are partially deployed, and most are not well integrated with other systems management products. Most organizations run heterogeneous products from multiple vendors. Not only does IT process automation need to support the variety of process in today's data centers and network operations centers, it also needs to support the heterogeneous products used in today's enterprise IT organizations.

Leading IT process automation products provide out-of-the-box integration with common monitoring products, event console products, configuration management databases, and ticketing products. Out-of-the-box integrations help large enterprise businesses automate IT processes, integrate disparate process and integrate the products that support these processes. Product and process integration, combined with automation, leads to an effective, efficient, and proactive IT operations organization.

Summary

You can begin automating your data center operations by implementing IT process automation. Getting started is easy. Through a focused approach in a few key areas, an experienced IT organization can quickly achieve a return on investment and reduce IT complexity, and support costs.

To understand how IT process automation can help you meet your business needs, please visit: hp.com/go/processautomation

Get connected

hp.com/go/getconnected

Get the insider view on tech trends, alerts, and HP solutions for better business outcomes



Share with colleagues

© Copyright 2007-2008, 2010, 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

