Business white paper

# Intelligent IT operations

## Making IT smarter with advanced event correlation and management

# Work smarter not harder

It's an old story for IT: Do more with less and faster. Businesses focus investments on business innovation, new markets, mergers, and acquisitions while IT budgets barely creep up. IT operations managers are asked to tighten their belts to support new services with the same resources, sometimes less, but many feel like they have squeezed everything they can out of operations staff and facilities.

IT Operations lacks a single pane of view into business service health, fault, and topology. This results in setting up labor intensive war rooms to triage and determine the root causes. Finger pointing ensues and ill will is harbored across the silos. HP can help with our Business Service Management solution. The heart and soul of our solution is a dynamic run time service model that provides the foundation to view interdependencies. This model is constantly updated with our monitoring data collectors. Our innovative topology based event correlation engine leverages the topology in the run time service model. With performance and fault KPIs being fed into our topology based event correlation engine we can determine the root cause and suppress the "noise". HP has continued to innovate, providing a set of rich integrations to leverage your existing IT operations tools, including BMC, IBM, CA, Microsoft, and many more. Now you can consolidate operations.

Many IT teams have turned to virtualization and consolidation to deploy new business services in fewer and smaller data centers. That's an effort to reduce duplication of effort, lower service costs, increase efficiency and improve business agility. But such projects often produce a sprawl of IT systems and remote services that is hard to manage and change, and that translates to increased operational expenditures (OPEX). For IT operations, achieving a corresponding reduction in ongoing operations costs—while meeting the business's demands for new innovative services—requires consolidating operations itself. And that requires a new set of more intelligent, efficient IT operations processes and tools.

## Table of contents



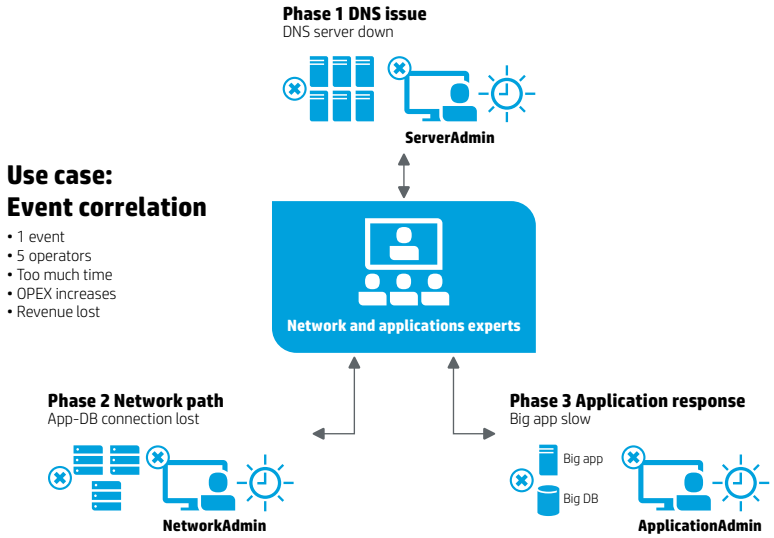
## The cost of silos: a trio of inefficiencies

Over time, as IT has become essential to the business and as technology has become more complex, specialization has increased, and organizational silos have grown up around each domain: applications, networks, databases, servers, and services. In some cases mergers and acquisitions and unplanned use of cloud services pile on the complexity, resulting in silos within silos. But silos reduce efficiency and increase costs.

*What exactly are these costs?*
The first is the cost of duplicated effort. When responsibilities for managing IT operations are spread across isolated silos, multiple teams may chase the same problem. Referring to figure 1, a problem such as a failed domain name system (DNS) server, for example, will be often reported via separate monitoring systems to separate teams. The network operations center will see it as a network problem, server support as a system problem, and application support as an application problem. If the three tier 1 operators don't immediately resolve the problem, each may escalate to their own tier 2 support, and the final resolution may involve as many as five or six specialists. Our research suggests the cost of chasing down a single event is approximately $70 to $80. Multiply that across several domain teams, and it's easy to see how operations costs skyrocket.

Next are the costs of inefficiencies caused by loss of visibility. That can be caused by exploiting virtualization and consuming cloud services. Gaining dynamics through virtualization and mashups of already available services must not result in reduced clarity on what impacts the company's business, yet IT systems supporting business revenues are often a sprawl of IT resources from many sources at any point in time. How can this be managed without sending operations costs through the roof?

**Figure 1.** One failure results in multiple events handled by several silos.




Finally costs are multiplied when siloed IT operations result in inefficient use of IT domain experts. Highly trained and expensive experts should spend their time working on innovation and ways to serve customers more cost effectively, not firefighting. When tier 1 support staff members lack the insight needed to adequately analyze and efficiently resolve issues, they involve domain experts unnecessarily.

## A better way: intelligent operations using a centralized operations bridge

The primary problem in the scenario illustrated here is a lack of visibility into the end-to-end IT infrastructure and the health of its components. Although IT infrastructure is an interdependent collection of applications, systems, and technologies, a domain-focused approach to IT operations means no single person ever sees it as such. Each domain owns its part, but no one sees the whole.

On the other hand, intelligent IT operations funnels all events to a single location—the operations bridge. Building on the ITIL® definitions, an operations bridge is manned exclusively by staff in the IT operations domain, which frees up resources in other domains to focus on higher-value activities. By consolidating events and enabling IT operators to view them from a single location, an operations bridge makes it easier to understand the context of related events—which is the cause and which are only symptoms.

To be effective, the operations bridge must determine the relationships and dependencies among individual infrastructure elements. The bridge should exploit varying monitoring and discovery tools to automatically discover and map these relationships and dynamically update the model that is created. This lets operators on the service and operations bridge find the root cause of an event cluster and then route issues to the correct domain team. Problem resolution time goes down and efficiency goes up.

### Value in numbers

According to IDC, IT organizations that consolidate operations can benefit significantly.

- Reduction in downtime incidents: 33%
- Increase in IT productivity: 17%
- Improvement in users managed per engineer: 60%

IDC, "Determining the return on investment from deploying consolidated event and performance management," July 2006.

Some customers have measured 66% reduction in time to determine root cause, reducing service call volumes by 33%, and $100,000s savings per year in operations costs following HP BSM solution implementations.

Building on the framework of event correlation in the operations bridge and a dynamic real-time service model (RTSM), we add service health capabilities to extend the solution and provide reporting and analytics of the health, availability, and performance of the managed objects and their dependencies as apparent in the RTSM. That not only makes operations more efficient, it also enables optimization and forecasting—key functions needed for capacity planning. The result is a service and operations bridge that becomes the heart of an intelligent operations solution for IT.

In the case of our failed DNS server, having event correlation would enable a single operator to understand the underlying relationship among the network, server, and application events. With better understanding of the hierarchy of these events (how one causes the other and which is the root cause), he has a much better chance of fixing the problem independently or assigning it to the appropriate domain group on the first attempt. Further, intelligent operations reporting can help detect reoccurring problems, and that lets domain specialists make changes to prevent future failures as well as plan evolution for new business services.

A consolidated service and operations bridge for advanced event correlation provides a single, intelligent version of the truth.

Event correlation drives down IT costs and reduces downtime. Because of that, the IT Infrastructure Library version 3 (ITIL v3) identifies an operations bridge as one of the first steps any organization should take for improving IT efficiency and increasing value to the business—a low-risk, easily attainable business win for IT. Adding automated intelligence for reporting, analytics, and optimization further improves the ability of IT to visualize and measure what needs to be managed for both reactive and proactive IT staff.

## Boosting event correlation with intelligent operations

**Three goals:**

- Reduce distractions for highly paid domain experts by increasing the effectiveness of tier 1 support operators.
- Resolve events and incidents before the quality of business services degrades.
- Exploit events and performance information in improvements and to assist in planning for change.

This enables IT to improve service levels to the business while reducing cost.

Implementing advanced event correlation requires standardizing IT processes for managing all events and incidents that occur within the IT infrastructure. In many cases, events and incidents are resolved on the service and operations bridge with automated tools or guided procedures. Where an event or incident must be escalated to a domain expert, clear incident and problem management processes kick in to resolve the underlying issue and prevent reoccurrences downstream.

Here's what is required to make it happen.

**Comprehensive infrastructure monitoring supported by a centralized management console**

Intelligent operations starts with monitoring and event management. We have been doing that for years, yet research shows that many IT organizations still lack visibility into what's happening in their infrastructure—especially when incorporating virtual resources, physical resources, and cloud services in an IT service. Monitoring and event handling of all components within the distributed IT infrastructure to measure utilization, response times, usage, and resource availability is the first function of an effective event management operations bridge.

As events are consolidated into the central management console, the event stream is refined by functions like storm detection, suppression, substitution, de-duplication, and correlation. That helps filter out event noise, allowing operators to focus on what's most important to the business and its customers. They can address fluctuations in demand and deal more effectively with infrastructure complexity. The centralized management console must be highly scalable and flexible enough to integrate with a wide range of heterogeneous, multi-vendor technologies: servers, operating systems, network elements, applications, and application components.

Intelligent operations means having the choice of how measurements are collected. Agent based monitoring relies on software installed on each monitored machine. That's the most powerful and customizable approach. It collects the most data. And it performs filtering and executes intelligence locally, whether the agent is connected to the central console or not. Agent-less monitoring uses standard protocols to probe activity on remote systems and allows IT to cast a wider monitoring net. This dual agent approach enables maximum coverage at lower cost.

### End-user monitoring

Even with comprehensive monitoring, some events may escape detection. IT should supplement infrastructure monitoring by deploying non-intrusive probes to monitor the end-user experience. Such probes can detect problems with customer-facing applications, provide critical diagnostic information, and alert IT to take action before users ever feel the impact.

End-user monitoring can help operations prioritize corrective actions. For example, if an operator receives three alerts at the same time, she might see that two events come from web servers connected to an online ordering application that customers use to purchase goods from the company and the other alert comes from a database server connected to an internal inventory system. The operator knows that the online ordering application is load balanced across eight servers to effectively manage peaks and troughs in demand. Even with two servers down, the application is still operational. The database for the inventory system runs in a two node cluster, and the alert indicates that one node has failed. She might conclude that the database for the inventory system should have the higher priority.

Let's now assume that IT has implemented monitors to track the end-user experience. Now the operator also receives an alert indicating that the online ordering application is extremely slow. Even though the application has access to six web servers, an unanticipated peak in demand requires the other two downed servers to maintain acceptable service levels. Because it is a critical revenue-generating application, she makes their restoration a top priority. Without end-user monitoring and alerts coming into a centralized operations bridge, IT would not have the whole story, and that could have negatively impacted customer satisfaction and retention. Ideally an Intelligent operations solution would incorporate an immediate indication of the business impact of such events, to facilitate prioritization.

### Key triggers for consolidating IT operations

- Data center consolidation—Consolidate management tools at the same time to save money.
- Virtualization initiative—Monitor virtual applications, too.
- Cost-cutting mandate—Consolidate to reduce costs.
- Merger or acquisition—Streamline the process by standardizing on a common management console.
- Cloud service adoption—Measure service delivery.
- Embarrassing service outage—Meet SLAs with comprehensive monitoring.

### Smart event handling and correlation

Detecting all the infrastructure and end-user experience problems is necessary, but it leads to a follow-on problem—the "sea of red." Hundreds or even thousands of events can overwhelm operators. Some of our customers handle as many as 350,000 events per month. To address this problem, we need a smarter approach to handling and processing events.

Smart event handling starts with consolidating events, eliminating obvious duplicates, and refining the event stream. This simple step can reduce the number of IT staff members required to chase events and rectify critical issues. And that can dramatically reduce the organization's mean time to repair (MTTR).

The operations bridge needs to provide time- and stream-based correlation across multiple events as a rapid step toward performing efficient event management. For example, combining multiple events into a single event; waiting for additional events before showing earlier events; or even creating a new event when an expected event doesn't arrive.

The next step is to understand how events relate to one another using a model-based approach. For complex infrastructures, a single event can lead to a cascade of follow-on events obscuring the actual root cause of the problem. Imagine a faulty network table that blocks a network path causing an application server that supports a corporate email system to time out. This could trigger multiple events for each of the domains affected. Event correlation based upon a dynamically updated model of dependencies can help operators find the root cause thus saving time and effort.

Smart event handling and correlation help IT filter out event noise and focus on the issues that they must address to solve the problem at hand. Unfortunately, most organizations approach event correlation manually. They spend staff time defining event relationships, or they manually build complex rules that must be constantly updated as the infrastructure changes. Both approaches are expensive and error prone. From traditional to hybrid cloud IT landscapes, organizations need event correlation technology that adapts to automatically discovered changes in the infrastructure.

**Automated service discovery and mapping**
Smart event correlation requires automated service dependency mapping so IT can understand the relationships among events. Service dependency maps infrastructure into a model to clearly define how elements relate to one another. Until recently, whenever a change occurred in the IT infrastructure, highly paid engineers would have to spend time modifying the models and correlation rules. The maintenance overhead required to keep the maps up to date made them unpractical and cost-prohibitive.

Today, however, inclusion of discovery information in key monitoring tools as well as specific probes to perform dynamic automated discovery detects the changes within your infrastructure and maps the relationships among elements as changes occur. Dynamic automated discovery mated with the monitoring agents and probes saves time and reduces overhead while providing a near real-time picture of IT infrastructure. Intelligent operations provides automatic rule definitions for newly discovered objects and as new instances are included in the model, they will inherit the rules associated with the objects they depend on, greatly reducing the otherwise manual overhead this defines, and providing a dynamic update to the model. The service dependency map provides the foundation for event correlation. Since IT infrastructures evolve at a dizzying pace—with hundreds or thousands of changes made daily—automated discovery makes service dependency mapping feasible and effective.

**Automatic task and incident management**
Automation can be employed across a wide range of common IT activities to speed response times and enable consistency. For example, alerts can trigger automatic fixes. Where this is not feasible, automation can populate alerts with guided procedures that lead operators through the fix process to increase efficiency and shorten MTTR.

Organizations can develop automated procedures over time by applying learning from problem management processes where engineers determine the best approach for resolving incidents. Run books—documents that contain operational procedures for performing specialized tasks—are ripe for automation. Organizations can automate problem and incident resolution workflows and even IT processes that speed audits and enable compliance with IT governance standards. In an initiative to implement an operations bridge and consolidate event management, automation plays a critical role in helping organizations improve staff efficiencies and enhance IT service quality. Where automation cannot be applied to fix issues or provide a simple run book automation to the operator, then intelligent operations should include a mechanism to automate trouble ticket creation and management. Eventually this should include execution of remedial actions, and enhance knowledge for full closed loop management of the event lifecycle using bidirectional integration between the help desk and operations management.

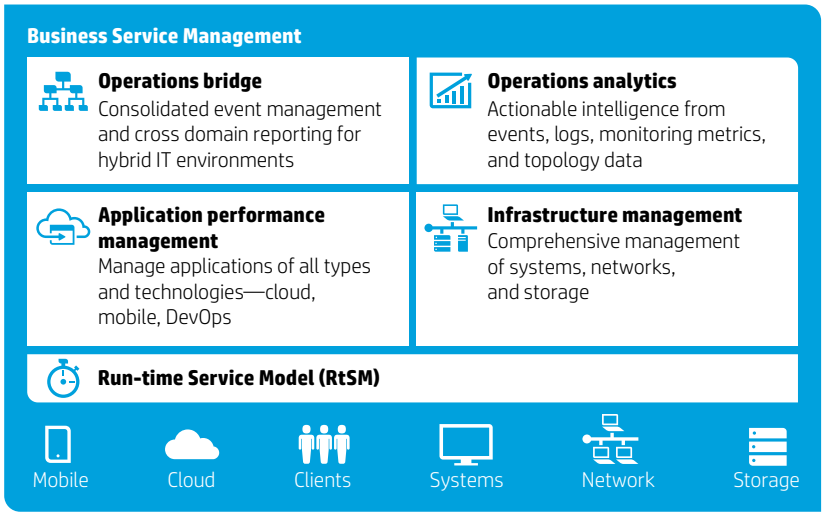
**Operations analytics—visualize, analyze, optimize, forecast**
Keeping systems alive and services running is IT's most pressing task, but you must also manage IT resources to get the most from your investment. Virtualization provides flexibility in deploying new business services, and it helps IT organizations do more with less. Businesses are increasingly exploiting cloud services to innovate and cut costs. But these recent technology paradigms both introduce new risks. Once again, improved visibility and analytics can come to the rescue. Centralizing events and correlating them against service dependency maps enables more incidents to be resolved at tier 1. That liberates skilled specialists to innovate and discover how to deliver more value to the business.

Server farms that exploit virtualization for servers, storage, and networking can grow quickly, because the increased flexibility means new business services can be deployed quickly. However, "copy and paste" deployments can result in sprawl. Standard configurations add to the agility of IT but may challenge your ability to properly control changes to the IT landscape. Over time, resources can be wasted—over allocated and underutilized.

*What tools does IT need for this?*
These issues are addressed by IT capacity planning and advanced event and performance data analytics. Reports can include event, availability, and performance data for all vital elements, virtual and physical, supporting a business service. Effective intelligent operations can automate the generation of these reports, which, because they are linked to the RTSM, use the latest definitions of target components and their dependencies, using existing information to feed What-if? analyses. IT staff can visualize current event trends, resource usage across servers, storage, and networks, and can analyze workloads to propose optimal allocation alternatives without impacting SLAs. Furthermore, trend data can be analyzed and exploited to forecast problems that might result from current workloads. And it can help IT dynamically establish baselines for thresholds and detect anomalies based on expected versus observed behavior.

**Log file and machine data management with analysis**
As IT organizations adopt new technologies such as cloud and virtualization, physical and virtual machine sprawl grows exponentially, so the amount of data such as logs, events, and machine data collected across the IT environment has also exploded. Throughout the data center and cloud, devices and applications emit large amounts of data that contain information pertinent to the performance of the system and are critical for resolving issues and managing security.

**Figure 2.** HP Business Service Management (BSM)
Ensuring the health of your services and applications




Collecting every item of information results in an unmanageable big data problem. However, if you do not collect everything, you may miss pertinent information that is required to resolve issues. And if you do collect everything, how long should you store it all? Archiving renders data inaccessible that could otherwise be used to determine if similar events have occurred before. Pattern matching and learning from previous information becomes impossible. Finally, if you do collect and store everything, analyzing this overwhelming amount of unstructured as well as structured data can take time, experts, and knowledge.

Specialists in individual silos decide what they want to collect, based on experience and best practice. At best, that approach results in a fragmented view of IT services and infrastructure. At worst, it results in important data not being collected because specialists simply didn't foresee the need. Further, lack of a consistent, systematic approach to data collection and retention can result in the loss of data that could prove to be valuable. Thus a more ideal solution is one which marries both monitoring paradigms, best-practice-based monitoring, and data storage coupled with analytics to detect patterns.

**Resources**

**To learn how we can help you improve IT efficiency so you can survive today's economy and thrive in tomorrow's, contact your HP representative today or visit us online at**
**hp.com/go/perfectstorm**
**hp.com/go/bsm**
**hp.com/go/omi**
**hp.com/go/si**
**hp.com/go/opsanalytics**

Intelligence can allow IT operations to manage structured and unstructured data (such as logs, machine data, or events), and it provides IT the ability to easily analyze complex data from any source over long periods of time. The intelligent operations that result provide a centralized analytical capacity to detect and visualize key patterns and databased events. It helps us understand patterns, gain insight, and make more informed decisions. Furthermore, infrastructure management events may be used to launch analytics that search real-time information and historical events for vital patterns that characterize the behavior of the IT Infrastructure. That can give you insight into recurring issues, so you can respond quickly and resolve issues faster.

## HP can help

Consolidating IT event management in a centralized operations bridge can help you increase efficiency in the short term while setting the stage for greater competitiveness over the long term. Organizations that consolidate IT event management and exploit event correlation against a dynamically updated topology model eliminate costly duplication of effort and focus IT activities on what matters most to the business. Adding operations analytics capabilities to the core platform for event management and correlation extends the operations platform to a service and operations bridge. This provides increased return on investment, and augments the intelligence and efficiency of IT operations. The result is faster advanced event management, problem resolution, higher service quality, and lower overall IT costs.

HP Software and Solutions has helped IT organizations all over the world reduce service downtime and cut duplication of effort by up to 50%. Hawaiian Electric, for example, consolidated 13 different toolsets into a single, centralized console and reduced downtime by 33%. Another customer Kuveyt Turk has measured costs savings of several $100,000s following deployment and production usage of HP Software Business Service Management solutions.

**Learn more at**
**hp.com/go/omi**

**Sign up for updates**
**hp.com/go/getupdated**

Share with colleagues

Rate this document



4AA2-7408ENN, June 2013, Rev. 2