Essential IT Monitoring

Fundamental to achieving effective enterprise IT management is enabling comprehensive visibility into all essential technology configurations, performance, and status. To enable a consolidated view, these monitoring practices must cross multiple management disciplines, and each organization will have unique sets of requirements that will define which disciplines align most appropriately with their business. Therefore, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts recommend the adoption of management solutions that are modular and fully integrated, allowing each organization to select the most appropriate combination of administrative resources to establish a complete view of their distinctive support stack from a “single pane of glass.”

EMA’s series of Essential IT Monitoring white papers identify key elements enterprises must target in particular management disciplines in order to rapidly identify and resolve issues and to optimize performance across IT infrastructures. Readers are advised to adopt integrated automated monitoring solutions that bring visibility to all the identified elements in the topic areas most applicable to their IT implementation.

Monitoring Priorities for Cross-Domain Management

While rigor is necessary in any specific area of IT management, whether it be networks, systems, applications, storage, security, or endpoint management, in the end all of these technologies must work together in harmony for the ultimate goal of enabling business process to be successful. This higher-level calling is driving IT operations teams, in particular, to try and embrace and understand the systemic whole of IT, so that the full picture can be understood and the true role and value of IT adequately assured.

EMA has heard countless stories of what happens when individual pieces of the whole are managed in isolation. Difficult problems get kicked around because no one has a complete picture. Teams become defensive rather than constructive. End users or customers are left out in the cold. And the source of the issue could be anywhere. Sometimes it is in the network, but just as often, the source is the server tier, or the storage, or the application design, or a firewall rule change, or misconfigured antivirus on the user’s laptop, or something else. The list of possibilities goes on and on. There is a better way, and that way is to integrate IT operations using cross-domain techniques.

EMA maintains regular dialogue with practitioners across each of the individual technology areas within IT, as well as those who seek to understand and solve challenges that are cross-domain in nature. Through those dialogues, and through direct research into the changing nature of IT operations, EMA has identified a significant shift towards integrating IT operations teams and functions, to embrace all contributing technologies, and in the process achieving increasing levels of service orientation. Nearly without exception, teams that are seeking to converge and connect operational monitoring across technology domains find that the path to success lies in aligning their management tools, technologies, and practices around the ultimate deliverables of IT – applications and services that are the lifeblood of IT-enabled business tasks, processes, and transactions.

Teams that are seeking to converge and connect operational monitoring across technology domains find that the path to success lies in aligning their management tools, technologies and practices.
causing another wave of organizations to embrace these strategies. And with this latter wave has come more and more evidence of bottoms–up transformations, led by IT professionals who seek to break down barriers and keep up with stunning rates of change that are not matched by equally advancing availability of human expertise and resources.

In the end, IT teams simply want to make sure that they’re doing everything they can to make the applications and services, which they are depended upon to deliver, available and operating at levels that help their organizations be successful. Regardless of which approach is behind the shift, EMA has identified five priority focus areas for organizations that wish to establish successful cross-domain operations monitoring and management. The first priority is essential for the following four; however, those latter four do not have to be undertaken in the sequence shown here.

**Priority 1: Achieve Coverage Across All Domains**

The driving goal behind cross-domain management is to gather together and establish a collective picture of how all the pieces and parts of IT are coming together in the service of the ultimate mission – to deliver applications and services to IT end users. The first step in this process is to find a means by which to bring together management data that can reveal the health, activity, and status of each piece of the interconnected IT infrastructure, together with the applications themselves. Only by including all of the pieces and parts – network, servers, storage, applications, security, and endpoints – can converged IT operations team be sure that they have the full picture.

But achieving true coverage across all the technology domains may not be as simple as it seems. Historically, tools are purchased, deployed, and used on a technology-by-technology basis. Network management tools are used for the network, systems management tools are used for the systems, storage management tools are used for the storage elements, and so on. And while you may still need to continue using these tools for specific tasks, there must also be a means found for bringing essential data together, either by extracting data from those domain-specific tools or by establishing a new management architecture that collects appropriate data itself.

There are three key challenges that EMA has uncovered in the initial foundational phase of achieving cross-domain operations monitoring and management:

1. **Reconciling multiple sources and data types:** Management data types and formats typically vary between managed entities and management tools. When collecting together data across multiple technology types and domains, this can be a nontrivial challenge to overcome, particularly if one attempts to do so by merging information from management tools sourced from multiple technology vendors. In parallel, there are often multiple viewpoints that will provide information on the same managed target, and these viewpoints will need to be aligned and reconciled. For instance, application performance can be measured from the end-user perspective, as part of network transit, within the hosting servers, or from inside the application code itself. In the end, there needs to be an aggregate or an overriding choice made as to which measurements will be considered primary and which will be considered secondary/complementary.

2. **Understanding relationships:** Bringing all of this data together gives you, well, a big pile of data. In order to make sense of this data and understand relevant patterns, it is essential to identify key relationships and dependencies between the data sets. There are a number of means of doing this, but most will start with designating critical systems and simply mapping all known infrastructure and management/measurement sources relevant to those systems or applications.
3. **Accommodating cloud**: A confusing and confounding factor that aggravates the objectives of cross-domain management is the entry of external cloud services. While on its surface cloud services represent simply one more part of the extended infrastructure, it does introduce significant barriers to visibility, because the infrastructure aspects of cloud services are typically not exposed to the IT operations team. It is still essential to gather as much direct availability and performance data as possible from the cloud provider, either from providers’ platform APIs or from supplemental agents and instrumentation deployed along with cloud-based workloads. In this way, even though the visibility is not as complete, at least there is a reasonable hope of understanding the health and activity of cloud-hosted resources.

**Priority 2: Integrated Availability Monitoring**

Once all IT infrastructure and application components have been accounted for, the first priority for IT operations is to establish and maintain an active knowledge of current operational efficacy. Since so many pieces must work together in order to deliver applications and services to the IT end-user community, an initial push to bring together fault and availability information across all supporting technologies is extremely helpful for assuring basic IT viability. The goal here is to establish and maintain true end-to-end visibility and awareness, including every contributing piece of IT equipment as well as the applications executing upon and carried by that infrastructure. EMA has identified three key areas of focus for establishing cross-domain integrated availability monitoring:

1. **Common dashboard**: The IT operations team must start by bringing together multi-domain information together into a common dashboard or console view. The common dashboard is what helps IT operations teams understand the “what” aspect of incident management. This may be accomplished by purchasing and deploying a management aggregation platform product, and then plugging all of the various monitoring sources into that platform. Alternatively, more and more management tools are able to provide common dashboards as part of their core architecture. Important for this latter case is ensuring that the dashboard can collect and present data across all of the technology domains – network, systems, storage, applications, and even end devices and security systems. The common dashboard must include an alert/alarm view, so that the IT operations team can see where problems have been identified, and ideally will also provide quick context – sensitive navigation to deeper details within any technology element or area, to assist and accelerate incident diagnosis.

2. **Grouping and organizing data**: To help IT operations focus on the most critical services and assets, grouping functions should be used that can organize monitored data. Groups will commonly be defined according to technology type or device type, geographical or site location, and organizational or line of business constructs. Topological maps can also be helpful, as are geographic depictions of the IT infrastructure and user community. Grouping helps to answer the “where” and “who” of incident management, and lays the groundwork for impact analysis.

3. **Prioritizing critical assets**: Finally, while the integrated IT operations team will be responsible for all aspects of IT infrastructure, applications, and services, every organization has systems and applications that are relatively more important than others. Attaching elevated attention to mission-critical systems and applications via alert/alarm prioritization and escalation policies ensures that IT operations is and remains aligned with the served business or organization.
Priority 3: Cross-Domain Performance

With the basic needs of availability monitoring established, organizations should seek to move to understand performance of the integrated, cross-domain IT infrastructure and the applications and services that it hosts and delivers. This allows teams to move beyond “is it up/available?” and onto “is it meeting responsiveness and performance expectations?” Availability monitoring is primarily built around harvesting automated events and notifications of any problems that have arisen, sometimes combined with very basic proactive “heartbeat” checks to ensure that devices and systems are indeed up and running. Moving towards performance assessment fundamentally changes the methods of monitoring data collection and the volume of monitoring data collected. Performance monitoring requires regular harvesting of Key Performance Indicators (KPIs) as well as a range of other health and activity measures from each of the technology domains. EMA recommends the following three data sets for making the transition to a performance orientation across domains:

1. **Device/component-level performance data**: Gathering performance metrics from devices and components within the IT infrastructure involves the use of technologies such as SNMP, log files, and APIs for repetitive, periodic polling or harvesting. The data is then consolidated and stored, so that it can be viewed and browsed via dashboards and reports. The greatest challenge here is to identify, among thousands upon thousands of potential metrics, the select KPIs that will be focused upon most heavily for real-time monitoring. Further, those KPIs will be the ones that should be used for defining thresholds and related performance alerts, so that problematic situations such as resource exhaustion can be flagged for operator attention. For example, memory capacity within network devices and compute systems should be watched closely, as memory exhaustion will most always lead to functional degradation. Similarly, capacity utilization such as network throughput, storage volume, and server CPU should also be closely watched to understand when individual components have reached or are nearing hard functional limits.

2. **Application performance data**: While most IT operators will be familiar with infrastructure-oriented performance monitoring, only some are familiar with Application Performance Monitoring (APM). And yet, APM monitors are precisely tracking the end value that IT delivers to the organization – the applications and services that underpin business tasks and processes. APM data is commonly harvested from agents that watch essential application architecture components (such as processes on compute systems) as well as rates of transactions. This may be done passively, and may also be done actively via synthetic session/transaction replication. Identifying KPIs from the application performance monitoring systems are an important additional viewpoint to add to the integrated IT operations dashboard.

3. **End-user experience**: Oftentimes a subset of APM, end-user experience monitoring is perhaps the closest measurement that IT operations can include for approximating the actual experience that IT and users are having with the applications and services they consume. The technologies used for this can either be direct measurement via user/client-side agents or passive approximations generated while watching activity from either the network or server perspective. It is also possible to use synthetic/robotic test agents to run common user interaction scenarios and measure responsiveness. Regardless of the approach, including user experience metrics as a KPI, it is a great indicator of potential productivity and/or customer satisfaction impact of any performance or availability issues, and is perhaps the highest level of sophistication for a cross-domain, integrated IT operations function.
Priority 4: Change Management

Whenever failures or degradations occur within IT services, some change in the elements, applications, or environment has occurred that precipitated the issue. In today’s complex, interconnected, multi-domain IT architectures, the unfortunate truth is that changes within any technology area may have adverse effects. Consequently, the truly effective cross-domain IT operations monitoring strategy must embrace and accommodate changes both expected and unexpected. Environmental changes should be captured and recognized within standard availability and performance monitoring, as described above. But another category of potential stability threats exists when operators make changes to the configurations of infrastructure elements or systems. These configuration changes are sometimes executed incorrectly or have unintended side effects, either on their own function or on other aspects of the infrastructure and the applications being delivered. EMA recommends the following focal points for incorporating configuration change awareness into cross-domain IT operations:

1. Collect change events and information: Availability monitoring is built around collecting and evaluating asynchronous notifications and events coming from IT infrastructure and monitoring systems. The same approach can be taken to collect and incorporate change events. Most IT infrastructure systems and elements have embedded functionality for recording and sending notifications whenever a configuration change takes place. These may come in the form of SNMP traps, API triggers, or log entries.

2. Correlate changes with availability and performance data: Regardless of the technique used, change events should be gathered and added to cross-domain dashboards, so that the time–related impacts of configuration changes can be visually correlated with other event and performance data. The effects of a change may not be immediately recognizable, so the ability to trace change history for contributory or suspect components is also important. This means that historical change records should be kept and, if possible, directly integrated with historical health and activity data.

3. Consider a CMDB: a Configuration Management Database, or CMDB, is a management architecture component that is specifically designed to capture and maintain a record of expected IT infrastructure components, connectivity, relationships, and dependencies. A successfully deployed CMDB can be a tremendous asset to integrated, cross-domain IT operations, as it represents “as-designed” expected state of the infrastructure, to which the “as-is” reality of the production infrastructure can be compared. This reduces surprises during deployment of infrastructure and applications, and speeds troubleshooting when things go wrong. It also significantly limits the number of surprises that occur when configuration (and changes thereof) are not closely managed. Some of these values can be achieved as well by using informal, standard reference configurations on a domain-by-domain basis – an approach known as “domain CMDB.”

Priority 5: Collaboration and Communications

One of the pleasant byproducts of adopting a cross-domain IT operations strategy is that it eliminates many of the traditional communications and collaboration barriers between IT teams. By bringing data and personnel together from each technology area, the day-to-day focus changes from assigning blame for incidents to collectively solving and restoring service function. It is hard to understate the value of
this accomplishment, when it is realized, and from this position IT can move ahead and cement its position as a true partner to the organization, aligned with the needs and requirements of the business. EMA recommends focusing upon a few key areas to capture available synergy:

1. **Connecting to help desk/service center**: The first touch point for most IT end users is the help desk or service center. By taking the higher-level and more comprehensive understanding of operational status and health that comes from cross-domain monitoring and sharing that directly with the help desk, tier one support becomes empowered to a degree not previously possible. As a result, tier one is able to better recognize which calls represent known problems and thus their status, improving user/customer satisfaction.

2. **Reporting for managers/executives**: Business executives and line of business owners rely upon IT to make their work efforts, processes, and transactions effective and efficient. Having aligned IT operations monitoring upon applications and services, IT can translate the cross-domain dashboard and console viewpoints into reports to be shared with business leaders, using the grouping outline in Priority 2: Integrated Availability Monitoring. Since the information is aligned around organization and/or application groupings, it is more readily understandable by non-technical employees.

3. **Reporting for the user/customer community**: Having a true systemic understanding of how IT is delivering applications and services to IT end users and customers, IT operations can now elevate essential KPIs, status, and health information about those services to end-user information portals. This can significantly improve end-user awareness and expectations without requiring calls to the help desk. It can also open new degrees of dialogue around end-user expectations.

**The TCO Challenge**

No discussion of cross-domain, integrated IT monitoring and management strategies would be complete without considering the cost of such projects. There are number of ways to go about achieving the capabilities described in this EMA white paper, and a widely ranging scope of cost for getting there. One angle of approach involves acquiring and deploying an independent, cross-domain, integrated operations monitoring platform sometimes referred to as a “service operations bridge,” and integrating data collected from the many individual domain-specific management tools that may already be in place. The costs in this case will be comprised of licensing for the bridge, and integration (whether staffed internally or via professional services), followed by the ongoing administrative burden of keeping such an architecture current as new releases of each of the integrated components are received. An alternative approach is to find a unified platform, or some close variant of tightly aligned/modular tools, that have been pre-integrated and require little or no services to deploy and maintain. The latter approach will always have a significantly lower total cost of ownership than the former.

**EMA Perspective**

The goals of effective cross-domain IT monitoring and management are laudable, and quite frankly are nothing new. IT organizations have for many years recognized the value of such an approach; however, getting there has been prohibitive for a number of reasons. But thankfully, due to the steady progress and evolution of management technology, such approaches are becoming practically achievable on a much broader basis – and the benefits are huge in terms of improved efficiency, improved awareness, improved responsiveness, and a realistic path to proactivity.
Essential IT Monitoring: Five Priorities for Cross-Domain Management

By focusing on collecting together management systems and data across network, systems, storage, applications, security, and end-user client devices, IT organizations can put themselves in the position to truly understand how well they are playing their essential role in supporting the business. Getting devices and elements of all technologies under management together, adding integrated availability monitoring, integrating performance monitoring, and establishing change awareness are the essential steps on the path to success. Sharing the results and using that new level of awareness as a basis for achieving a truly strategic, partnership status with the business then becomes possible.

SolarWinds is a provider of IT management technologies that covers a broad range of the cross-domain IT monitoring needs discussed here. The company has constructed a core management technology architecture that operates as a common platform for integrating multiple domain-oriented modules, including Network Performance Monitor (NPM), Server and Application Monitor (SAM), Virtualization Manager, and Storage Manager. Direct application performance awareness is addressed via SAM as well as NetFlow Traffic Analyzer (NTA). The result provides common dashboards and reporting that address the cross-domain coverage, integrated availability, and integrated performance monitoring needs outlined above. This collection of components can also intrinsically supply much of the change awareness needs for cross-domain monitoring, augmented with greater depth when adding components such as Network Configuration Manager (NCM), IP Address Manager (IPAM), Log & Event Information Manager, and Firewall Security Manager.

About SolarWinds
SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. SolarWinds’ approach is consistent across all market segments – focusing exclusively on IT Pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Additional information on SolarWinds can be found at [http://www.solarwinds.com/](http://www.solarwinds.com/).

Additional Reading…
For information on optimal monitoring practices in other management disciplines, please see EMA’s other white papers in the Essential IT Monitoring series:

* Essential IT Monitoring: Ten Priorities for Systems Management
* Essential IT Monitoring: Seven Priorities for Network Management
* Essential IT Monitoring: Five Priorities for Security Management
About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries. ©2013 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.