TIME TO GET TOGETHER

DR.PARTHA BHATTACHARYA OF ACCELOPS EXPLAINS WHY INTEGRATING SECURITY, NETWORK AND DATA CENTRE MONITORING IS BECOMING SO IMPORTANT

Virtualisation, unified computing systems, cloud computing and mobile devices have changed the dynamics of the modern data centre. The drive towards optimised computing has blurred the boundaries between network, server and storage. A data centre is now any collection of CPU, memory, network and storage resource pools, on-premise or in the cloud, where applications are deployed by choosing from existing sharable resource pools. This enormous flexibility comes at a price as the increasing interdependencies can cause simultaneous multi-point failure. For example, a security vulnerability in the virtualisation layer could render all VMs on a physical machine vulnerable, or a server rack hotspot could lead to multiple simultaneous machine failure. There is an urgent need for holistic, service availability focused data-centre monitoring.

While IT infrastructure is rapidly converging, system management tools remain anchored to individual functions with separate tools for network, server, storage, and applications. In the application space, there are distinct tools for monitoring metrics, end users, real users and transactions. There are separate tools for different overlay functions - availability, performance, security (SIEM), log management, change monitoring as well as separate tools for monitoring virtualisation and cloud services. While there are attempts to integrate point tools by combining them under a common user interface, the lack of a unified data model, common analytics, and the inability of the tools to communicate at a low level and exchange information, makes actionable intelligence rare. Each tool requires its own expert to perform true root-cause analysis, making it impossible to be proactive in this new data centre world.

With a different view, one can consider infrastructure as an engine that generates data, so a system could learn that infrastructure, understand its data and the domain from which it comes, correlate automatically across multiple domains, and create alerts that traverse issues across those domains. This enables a business service approach to IT infrastructure management that connects the dots and accelerates understanding.

The same result cannot be achieved by superficially stitching multiple tools together via APIs because it avoids the real challenges. The first is the diversity of devices and applications. While many complex Change Management Database (CMDB) models exist, a simpler framework is needed for rapid implementation and extension. Another challenge is data quality. The information is highly unstructured, ad hoc, and with gaps that can only be filled by combining data from other domains in real time. The final challenge is the need for a scale out architecture. VM server sprawl and growth of mobile devices attest to the need for scale. At best, single-function tools scale only within their domain. A unified tool looks at all domains and scales incrementally in a limitless fashion, as required.

A unified monitoring tool could handle the challenges of a virtualised, converged IT infrastructure but what exactly is required? Firstly, it should be based on a flexible event operating system, offering efficient mechanisms for collecting, parsing, indexing, storing, searching, trending and correlating events, in real time and historically. It should make no assumptions about structure and content of an event, work across multiple domains, storing events in a no-schema database for rapid, unlimited integration of new devices and applications.

It should also be able to enrich events in real time with dynamic context collected from various domains. The context should include user identity, location and network entry point information and ideally be able to handle infrastructure both on-premise and in the cloud. The system must scale (both in search and real time correlation) by simply adding compute nodes and storage with minimal downtime. Finally the system must be easy to use, automatically discover the infrastructure and remain up to date by learning any changes.

Rapidly converging IT infrastructures have created an imperative for converged systems management; converged through a single tool to unify cross-domain issues and quickly provide accurate, actionable intelligence to the organisation. NC

accelops

AccelOps, Inc.
2901 Tasman Drive, Suite 100
Santa Clara, CA 95054
USA
Web: www.accelops.com
Tel: 1 (408) 409-0903
Email: sales@accelops.com