IDC
Analyze the Future

I D C A N A L Y S T C O N N E C T I O N

Ashish Nadkarni
Program Director, Computing Platforms

Considerations for Adoption of AI-Driven, Cloud-Based Systems Management Platforms

July 2017

The worldwide cloud systems management software market continues to expand as more and more enterprise and service provider customers embrace cloud-based architectures for a wide range of production and DevOps workloads. IDC forecasts growth from $2.105 billion in 2016 to $4.236 billion in 2020 — a 19.1% compound annual growth rate (CAGR). IDC also expects a growing portion of this revenue to come from cloud-based systems management platforms (CSMPs) given the success that some vendors have had by introducing such functionality as key differentiators of their solutions. Customers are gaining confidence with their ability to optimize multicloud environments that match workloads to a mix of on-premises and/or public cloud infrastructure, development platforms, and software-as-a-service options. IDC expects that by 2018, more than 85% of enterprise IT organizations will commit to hybrid cloud architectures, driving up the rate and pace of change in IT organizations.

The following questions were posed by Cisco to Ashish Nadkarni, program director for Computing Platforms within IDC's worldwide infrastructure practice, on behalf of Cisco's customers.

Q. How will CSMPs improve customer experience, specifically in terms of productivity, risk, and service delivery quality?

A. We live in an era where digital infrastructure forms the backbone for business-to-business and business-to-customer interactions. As the size of the digital infrastructure increases, so does the size of the systems management infrastructure, which is used to ensure its normal functioning. Any disruption to this systems management tier has an immediate and profound impact on customer experience. Organizations that move to CSMPs will find that service delivery quality is significantly improved, the overall risk to the business goes down, and IT staff productivity is increased. Ultimately, making this move results in an improved customer experience that follows from:

- **Improving service delivery quality.** As the infrastructure in a firm becomes bigger, more complex, and distributed, it puts a proportionate strain on systems management functions and capabilities, which also need to scale and be highly available. Balancing these various needs is no easy task, and it is one that can quickly get expensive. Unless the provisioning and operations tasks, including pattern detection, analysis, and remediation, can be carried out seamlessly and in an automated fashion, this systems management layer is nothing but a white elephant in any organization — an essential tier that is expensive to maintain and offers little value. Fortunately, IT can make systems management functions resilient, highly available, scalable, and cost effective by adopting infrastructure that features or supports a CSMP approach.

- **Reducing risk to the business.** The size and complexity of the systems management infrastructure in most environments are directly proportional to the size of the infrastructure itself. The systems management infrastructure requires the same maintenance as the business-critical systems in the environment. This means maintaining the currency of software patches, ensuring the availability of hardware, and making certain that these systems comply from a security and data governance perspective. The lack of upkeep of the systems management infrastructure exposes the entire organization to security vulnerabilities. Furthermore, when such systems are compromised or unavailable, they halt or severely cripple all provisioning and operations activities. The ability for a CSMP to scan thousands of customers, "fingerprint" component quality or other issues as they emerge, and then proactively alert customers who may be impacted enables proactive risk mitigation on the part of the infrastructure vendor in support of IT.

- **Increasing IT staff productivity:** CSMPs free IT staff from managing and maintaining "an infrastructure to manage the infrastructure." The ongoing management of these systems is not easy, whether patching the operating systems and applications; auditing these systems for compliance, security vulnerabilities, or breaches; or maintaining the hardware. It is an overhead on precious resources. By shifting the systems management tools to the cloud, IT staff are free to dedicate their productive time to big-picture initiatives.

CSMPs enable organizations to scale capacity without additional capex investment in infrastructure to manage infrastructure. Furthermore, artificial intelligence (AI)–infused cloud-based management tools provide deep insights into the state of the infrastructure, identify troubles before they become major issues, and enable quicker "root cause" identification and analysis of issues.

Q. What functionality needs to be incorporated into CSMPs to make them far more effective in managing distributed computing at scale?

A. CSMPs need to gain feature parity with equivalent on-premises variants to be considered viable long-term alternatives. Gaining feature parity means that such tools need to:

- **Be secure.** CSMPs need to capture, store, analyze, and dispose of operational data in a secure fashion. Access to the portal should be granular and tiered. Features such as role-based and multistage access mechanisms enable IT to permit selective access to development and operations personnel.

- **Support consolidation of multiple point tools and functions.** CSMPs must function as a "must-have," which means that they serve as a singular portal that can perform all infrastructure provisioning and management functions, making on-premises point tools redundant. Additionally, they must integrate with corporatewide technical support, help desk, and ticketing applications that are essential for tracking change requests and events. Finally, they must support advanced machine learning–based operations analytics functions that track the history of the environment, making it easier for IT staff to identify and act on recurring problems and events.

Q. Why are machine learning–based operations analytics capabilities essential to achieving greater security and efficiency?

A. Managing enterprise infrastructure today is a complex job fraught with perils. IT administrators have their hands full already. They now find it increasingly challenging to take on the role of developers and data scientists in order to scan and analyze large amounts of (constantly changing) infrastructure-related telemetry and operations data for current or potential issues and events. Even with well-written scripts and log analyzing software, there

is always the possibility that operational lapses, security violations, and other potentially catastrophic events can pass through filters undetected. In a recent IDC survey, participants were asked, "What are the most important drivers and requirements shaping your organization's overall IT operations analytics (ITOA) strategy from today through 2020?" The number 1 response was to increase security and compliance.

The task of gaining deep insight into the state of the infrastructure by analyzing operational data, event logs, security audit logs, and other time-sensitive data is best left to CSMPs, especially those powered by operational analytics and machine-learning algorithms. These algorithms add a level of intelligence and automation to operations processes (i.e., preventive maintenance, troubleshooting, and post-event root cause analysis) that humans cannot match. These platforms are better at detecting threats and potential vulnerabilities — akin to searching for a needle in a haystack — than their on-premises equivalents. By using "crowdsourcing" concepts, IT can benefit from patterns detected in other environments.

Q. How do predictive analytics improve infrastructure optimization and problem resolution?

A. CSMPs make use of crowdsourcing concepts to securely and anonymously collect and pool operational data, event logs, and technical support interactions across a vendor's installed base of hundreds or thousands of customers. They then apply predictive analytics algorithms on this data to examine familiar patterns, identify new recurring patterns, correlate the patterns with historical trends, and perform "what-if" and "if-then-there-that" simulations " on these trends. Such systems are designed to self-learn and to become highly trained to identify patterns and potential issues more quickly than humans can. By relying on CSMPs, IT staff can:

- Establish baseline performance and workload patterns that are typical of their profiled infrastructure.
- Cut through the noise and false positives to detect real event patterns and anomalies and respond in a timely fashion.

Q. What will accelerate or slow the customer adoption of this new generation of AI-driven CSMPs?

A. Much rests upon the robustness and functional capabilities of CSMPs. IDC believes that adoption of these tools depends on:

- **The security of the platform from an access and data sharing perspective.** This attribute is crucial because no buyer will want to invest in a platform that is less secure than other off-premises platforms. In fact, given that CSMPs have the keys to critical on-premises infrastructure, these platforms must be built with extreme security in mind.
- **The importance of application programming interfaces (APIs) that enable CSMPs to integrate into developer and application life-cycle toolsets.** IT administrators need to enable deep integration with orchestration and automation tools that enable infrastructure as code (i.e., the deployment and management of infrastructure via frameworks such as OpenStack and methodologies such as DevOps).

Ultimately, IT staff must gain a level of comfort and confidence with the concept of "machines managing the machines" and "autonomic management" for them to embrace CSMPs in their environment. Gaining this comfort and confidence will occur incrementally as CSMPs prove their value and reliability.

Q. What should the key attributes of a new CSMP be?

A. In conclusion, the key value pillars of a new CSMP offering should be:

- **Pervasive simplicity:** The platform should be simple to operate and manage.
- **Security:** The platform should be secure and offer the flexibility for customers to run private instances on-premises — in complete isolation — if required.
- **Continuous optimization:** The platform should continuously learn from usage patterns.
- **Agile delivery:** New features and functions should be made available continuously.

ABOUT THIS ANALYST

Ashish Nadkarni is a program director within IDC's worldwide infrastructure practice, which includes research on computing platforms, operating environments, storage systems and software, and networking infrastructure for enterprise and cloud datacenters. Ashish oversees IDC's Computing Platforms research, which spans x86 and non-x86 servers and integrated systems, Unix systems, mainframe-class servers, and edge computing devices. This research also examines the impact of server architecture on systems software such as operating environments, server and client virtualization, and cloud system software. It also includes areas such as workloads and deployments, segmentation of server hardware based on current and next-generation workloads, emerging computing paradigms such as composable/disaggregated systems, rackscale architectures, cloud frameworks such as OpenStack and datacenter initiatives such as Open Compute. Additionally, Ashish participates in IDC's research on enterprise and cloud storage systems and software, software-defined infrastructure, infrastructure for and in the cloud, and infrastructure for the Internet of Things. Ashish also co-leads IDC's Global Overview program on Big Data and Analytics, one of the four pillar programs of IDC's 3rd Platform research agenda.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.