451 Research | Business Impact Brief

Distributed Network Monitoring in a Hybrid World

The 451 Take

Distributed applications are the future, and this means network and performance monitoring must be distributed as well. As applications become more distributed and dynamic, the need for reliable and consistent network monitoring is more important than ever so that DevOps and SecOps teams can effectively manage monitoring throughout the application lifecycle. In a recent 451 Research study of IT professionals, tools for monitoring – including network monitoring, logging and alerting – were some of the most sought-after technologies.

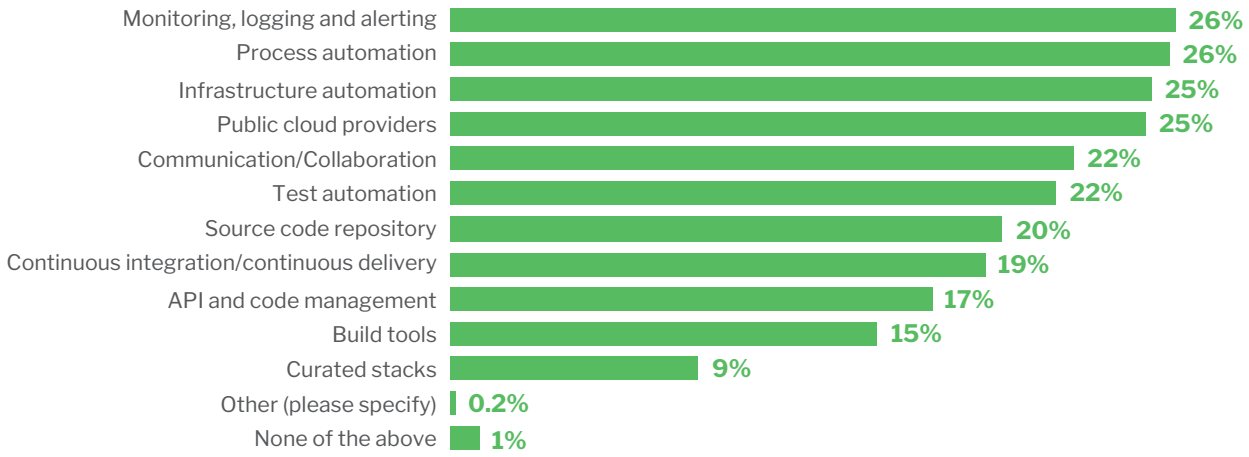
Supporting distributed functions can be complex – from addressing technical requirements in multiple environments and determining where and how processing will take place, to effectively collecting and analyzing network data. A consistent network monitoring strategy applied to all application environments, both on-premises and cloud, will reduce the complexity and streamline operations to ensure reliable monitoring.

Most Important Tools for DevOps Efforts

Source: 451 Research's Voice of the Enterprise: DevOps, 2H 2019

What tools are most important to your organization's DevOps implementation? (Choose up to three.)

Base: All respondents (n=474)



Business Impact

INCONSISTENCY WILL DISTORT DATA USABILITY. Workloads are being deployed in a variety of application environments from different cloud services, colocation datacenters and on-premises datacenters. Each location will have its own set of capabilities and operating environment for performance monitoring and data collection. Enterprise IT can use the native capabilities in cloud services for CloudOps, but that involves making compromises in functionality that will lead to complex and costly operations, as well as inconsistent data collection. This will result in inconsistent performance and security analysis, and will also impact data retention and any other use case for collected data.

451 Research | Business Impact Brief

Business Impact (continued)

PROCESS IN PLACE. Most cloud services charge for exporting data out of a cloud instance, and these costs can add up. Processing or pre-processing network packet data where it is collected reduces the amount of data transferred out of the cloud and can provide immediate insights. However, some data may have to be transferred out for storage or processing, requiring intelligent packet capture that can identify which application flows must be sent outside the cloud environment, slice packet data, apply time-stamps, and perform other functions before sending it to its destination.

LACK OF VISIBILITY HINDERS OPERATIONS. With IT managing applications in multiple locations and environments, having network visibility instrumented by NetOps is critical to ensure performance requirements are being met and to quickly resolve performance issues as they arise. Programmability becomes an important feature of monitoring because DevOps-mediated application deployments treat network functions, including packet data capture, as programmable resources to be automated throughout the entire application lifecycle.

VISIBILITY GAPS COMPROMISE SECURITY OPERATIONS. Similar to performance monitoring, security teams need visibility into network traffic for intrusion detection and prevention, anti-malware inspection, reputation scanning, and other forms of active and passive analysis. SecOps will need to have reliable network monitoring where applications reside, along with methods to ensure that monitoring systems move with applications. Ensuring consistent, reliable network monitoring in all application environments is far more difficult when IT uses multiple products and services with varying capabilities in different environments.

Looking Ahead

A consistent, network-aware application monitoring framework is a foundational element in proactive performance management. Taming operations and management in diverse and dynamic application environments means that consistent, distributed data collection and reporting is critical to build an accurate understanding of application performance end-to-end. Blind spots with no network monitoring or gaps in capabilities across locations hinder IT's ability to properly manage service-level agreements, perform root-cause analysis and predict when failures are likely to occur. With consistent network monitoring tools, IT can gain an accurate picture of application performance and respond more quickly to issues because it has a set of tools that are well understood and integrated into a set of performance management workflows.

Enterprises can take advantage of distributed network-aware performance monitoring for multiple use cases, increasing the value of system purchase, IT skills and integration capabilities. Distributed network monitoring systems can replicate and filter traffic to multiple destinations, which significantly reduces the purchase and management of redundant capture systems. Distributed network monitoring can also quickly change destinations for traffic flows should the need arise.

Making effective use of distributed network monitoring takes planning from the start of an application project, or as early as possible with existing applications. In enterprises with DevOps IT strategies, network monitoring needs to be part of the application deployment process, including the development of filters and processing required for application traffic and the selection of the appropriate virtual or physical capture system. Equally important is preparing the destination tool. Planning for distributed network monitoring works best as part of planning for application networking since it's related, but developers should be thinking about network monitoring requirements and collaborating with colleagues on performance management, security and governance.