Application Availability Monitoring

How application availability can be distilled from existing network data
## Table of Contents

3 Executive summary
3 The problem with application monitoring today
5 Tuning the network
7 Conclusion
Executive summary

This business white paper discusses the considerations you need to be aware of before you decide to deploy applications in a virtualized environment. Topics that will be addressed in this paper are:

• Problems governing application performance and monitoring
• The impact of a unified policy in application assurance
• The HP offering as a complete application management solution

The problem with application monitoring today

Application performance monitoring and management is not new, but its adoption remains fairly low because full-blown application monitoring tools that deliver deep-packet inspection are expensive. This does not imply application monitoring is not performed. It is performed using a piecemeal approach with several tools performing different aspects of application monitoring. Unfortunately this leaves gaps in application monitoring.

Today’s tools still do not provide enough visibility to troubleshoot application performance. In recent findings by Enterprise Management Associates, it is reported that IT is notified of application-related problems nearly 50 percent of the time by the user, instead of monitoring or application management tools, which accounts for only 34 percent of notifications.

The challenges that IT professionals reported while managing applications include poor performance, intermittent problems that are difficult to troubleshoot, and high fixed costs related to application support. The similarities in response illustrate the complexity with application management. An application relies on performance of several systems—network, servers, storage, and the application itself, irrespective of where the application is hosted.

1, 2 Source: “Application performance management in the age of cloud,” Enterprise Management Associates, December 2013
Providing application assurance for cloud and on-premise applications

There are two aspects to consider for application assurance. You need to ensure that the applications are deployed with the right policies. Once the application is setup, you need the right monitoring tools that provide feedback through policy, as well as auto tune the ecosystem.

Steps to achieve application assurance

Figure 1. Application assurance

Deploying application and provision network requirements

A key factor in application performance when applications are deployed is the infrastructure policy enforcement for the workload and network. Applications need the network to be provisioned with the right Quality of Service (QoS). The policy of best effort no longer works. Also, increasing bandwidth as a solution to the problem is not cost effective as we move to a cloud-based application model, because the number of applications running on the network also increases.

To meet user expectations, applications need to be characterized and the right network policies need to be developed based on application requirements. Policies need to be enforced from the point of entry up to the end user’s quality of experience. For instance, from the point of entry port 80 for cloud applications, or the on-premise virtual machine hosting the application, through the path, and the supporting resources, right up to the end user.

Network policies need to contain the appropriate security, QoS, and bandwidth for each application type. Traditional network management, Software-defined Networking (SDN), or a cloud environment can apply this policy to influence physical or virtual fabric behavior. These discrete network policies can be subsumed by an overarching cloud orchestration policy when deploying specific application types.

As well, multi-tiered applications require often host their web front-end, application, and database components on separate physical or virtual hosts requiring network administrators to understand not just the application path between the user and the application, but also the various components and network paths that make up the service the user is consuming.

Figure 2. IMC managing multi-tiered applications
Application monitoring requirements

A complete application management solution should provide visibility by rationalizing application performance and network telemetry across the various layers of infrastructure, throughout the network. Application management solutions become even more powerful if the functions are unified in a single tool, allowing administrators to quickly correlate and troubleshoot issues.

The primary requirements to provide sufficient visibility are the following:

- **Monitoring** various layers including networks, storage, virtualization, and servers using one tool to allow for better correlation
- **Visibility into the application stack availability** such as servers, operating system, database, and application
- **Relational mapping** of components and architectural layers, usually covered with dynamic creation of network topology
- **Proactive notification** mechanism based on threshold monitoring
- **Synthetic transactions** to determine service availability and measure Quality of Experience
- **User monitoring** to determine the end-user experience of the application performance
- **Log analysis** as one of the proven ways of gathering network data, and events for troubleshooting.
- **Executive dashboard** that displays meaningful actionable information from abstracted data

As many of these functions primarily reside as separate functions, administrators have difficulty being proactive when it comes to application-performance management. Administrators only learn of issues as they reach the help desk. The lack of integrated functions when it comes to application management prevents administrators from predicting issues with performance. The state of application health should be governed by performance thresholds, allowing administrators to uncover underlying issues with network performance before they blow up.

Tuning the network

Converting telemetry to policy

Delivering the right user experience requires that application monitoring and policy must work together. Today, network telemetry feeds into a system that administrators do very little with because current management platforms have limited capabilities to provision the network in response to poor application performance. If the network can be provisioned for specific applications beyond quality of service parameters to include bandwidth and security requirements, then the network can be tuned based on the incoming telemetry. Of course, provisioning site-wide policies can be challenging and Software-defined Networking is the answer to dynamic provisioning of the network. For networks that are not yet software-defined, automated provisioning of policies that can be modeled, defined, and replicated throughout the network is requirement to minimize the complexities of tuning applications for the network.
Components

Intelligent Management Center
IMC, a comprehensive network management modular platform, aims to simplify IT operations, deliver greater management control, and increase agility through automated provisioning of services. IMC delivers comprehensive infrastructure monitoring. By integrating modules geared for monitoring application health, administrators are able to correlate application performance data with network events from one interface, and allowing them to troubleshoot application issues proactively before the issue is escalated to a help desk.

IMC monitors the various components including networks, storage networking, virtualization, and servers, from one interface providing administrators a better way to make sense of the network data. It also provides an automated topology so that administrators can see how components are relationally mapped to each other. IMC has full-fledged logging capabilities so that administrators can gather network data and events for troubleshooting application issues.

Figure 3. Application availability lifecycle

Application deployment and tuning

IMC VAN Connection Manager
IMC VAN Connection Manager is designed to accelerate the delivery of applications by providing a consistent, policy-based approach that leverages profiles. With IMC VAN Connection Manager, your IT team can provision network services faster, more consistently, and securely along with the added benefit of reduced downtime and manual errors. Policies can be defined on a per-application basis, which include bandwidth, QoS, and security and are provisioned when the application is deployed.

VAN Resource Automation Manager
VAN Resource Automation Manager orchestrates a virtual network slice or path, tuned for a specific service or application through automated resource provisioning of network devices (multivendor supported). It includes L2 and L3 switches, routers, load balancers, DNS and more. VAN Resource Automation Manager provisions desired network characteristics tuned to the application of interest. The creation of these tuned virtual slices is possible through manual methods, but it would take significant time to plan, test, and deploy. Automating these processes ultimately saves administrators time spent in troubleshooting deployment challenges and enables a good end-user application experience.
Monitoring

**Application Performance Manager**

IMC Application Performance Manager (APM) allows administrators to visualize and measure the health of business applications and the impact to network performance. APM supports monitoring, thresholding, and notifications of key metrics in the components that actual provide an application or service. APM provides the ability to simulate transactions so that the administrators can determine the availability and response time of different applications. APM leverages various protocols such as WMI, SOAP, REST, as well as various others to simulate real transactions, ensuring that the service is not just active, but responding to client request in a predictable manner. Monitoring the individual components can help administrators to quickly identify the cause of application performance issues allow network administrators to quickly return their users to the appropriate level of service.

**Service Health Manager**

IMC Service Health Manager (SHM) delivers end-to-end service monitoring and service assurance, through the visualization of infrastructure or network factors that are in the path which provides the service, in this case a specific application. It aggregates key performance indicators to provide a key quality index for application performance. SHM leverages capabilities in the network infrastructure to create synthetic transactions from individual switches and routers. Protocols such as the HP NQS and Cisco’s IP SLA can be used to help ensure that the application is performed from the devices that your users are directly connected to, providing network administrators the ability to “see” things from their users perspective.

**Network Traffic Analyzer module**

Network Traffic Analyzer is a graphical network-monitoring tool that provides network administrators with real-time information about users and applications consuming network bandwidth. Network Traffic Analyzer also delivers user monitoring to determine the performance and response that the end user is experiencing with their application. NTA leverages industry-standard protocols such as sFlow and IPFIX to monitor the application composition of the traffic as it flows through the network, allowing network administrators to discover unauthorized network applications that may be affecting business critical applications.

**Conclusion**

Application performance management requires a three-step process to deliver the right application user experience—deploy the applications with the right policies, monitor the network and applications to obtain telemetry, convert telemetry to policy and tune the network. By leveraging a network and application management platform, like the HP Intelligent Management Center that enables you to automate network provisioning when you deploy applications and tune the network, provides comprehensive monitoring from application to the network, users can experience the application better and will less likely call the help-desk for application troubles.

**Learn more at**

[hp.com/networking/cloudnetworking](http://hp.com/networking/cloudnetworking)