Courtesy Of:

Dyn

Internet Visibility & Control is Critical to Your Cloud Success

Gartner Research: Internet Performance Monitoring Helps Fill the Cloud Monitoring Gap

Gartner

Welcome: Minding the Internet Performance Gap

Cloud. Hybrid IT. Agile. Digital Transformation. The pace of innovation in IT has never been faster, but, as the following Gartner brief makes clear, tools to manage ever-increasing variety and complexity in IT environments largely haven't kept apace. This leaves many organizations with a critical gap in network visibility and control: the internet.

Dyn is proud to be pioneering a new category of technologies to fill this gap called Internet Performance Management (IPM). This research by Gartner identifies a component of IPM, internet performance monitoring. The ability to unlock the black box imposed by internet transit to gain visibility and alerting of critical internet paths and their impact on your applications and users. But visibility without control will only get you so far, like having headlights to see the road ahead, but no steering wheel to avoid obstacles. Monitoring needs to be combined with control for organizations to fully achieve the potential of the internet.

Source: Dyn

Research from Gartner

Network Performance Monitoring Tools Leave Gaps in Cloud Monitoring

by Sanjit Ganguli

Migration to the cloud, in its various forms, creates a fundamental shift in network traffic that traditional network performance monitoring tools fail to cover. I&O leaders must consider cloud-centric monitoring technologies to fill visibility gaps.

Key Challenges

- Migration to the cloud fundamentally changes the flow of network traffic in the enterprise, but most I&O leaders do not have a network monitoring strategy to deal with these new patterns of traffic.
- I&O leaders are still ultimately responsible for the uptime and performance of cloud-hosted applications, even though performance degradations or outages may be beyond their control.
- A majority of network performance monitoring and diagnostics (NPMD) tools have been unable to provide holistic monitoring in a cloud, or hybrid IT, environment.

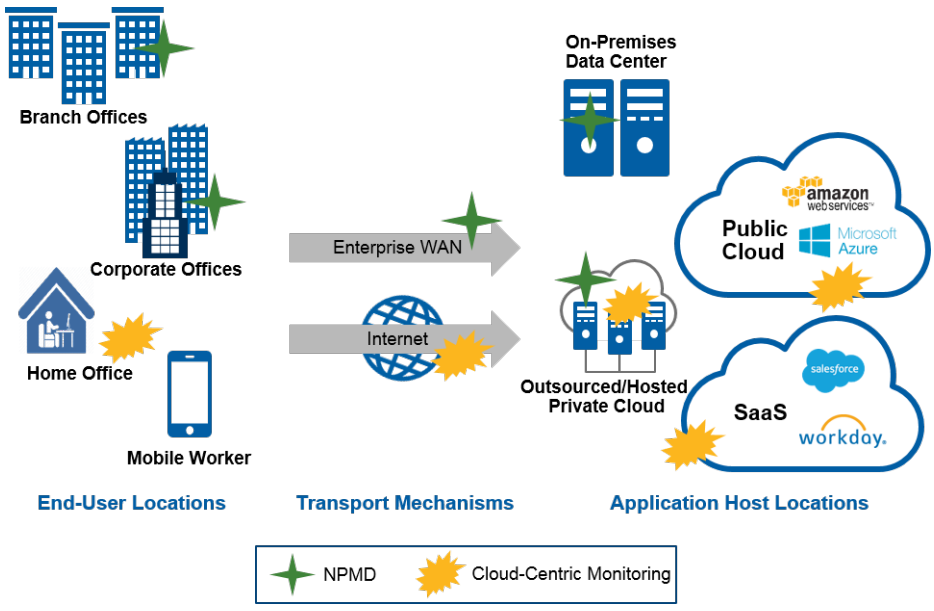
Recommendations

- Uncover dangerous blind spots with an understanding of how present and future cloud deployments impact the flow of traffic in the network.
- Deploy cloud-centric monitoring technologies alongside traditional NPMD technologies to fill the visibility gaps and shed light on the blind spots.

Introduction

While conventional wisdom says that moving to the cloud is a way for I&O leaders to get out of the self-monitoring mindset, in most cases, the exact opposite is true. Outages and performance degradations still occur, and I&O leaders are still looked at to resolve these problems, whether

FIGURE 1 Monitoring Strategy for Hybrid IT



Source: Gartner (May 2016)

they are cloud-based or not. Given the diversity of ownership of these infrastructures, problem resolution becomes that much more complicated.

While the network itself remains an on-premises issue, no matter where the application is hosted, the network architecture and network monitoring strategy is very different when the IT stack is hosted in the cloud. Unfortunately, the vast majority of NPMD technologies deployed today leave significant visibility gaps. As such, I&O leaders need to formulate a new network performance monitoring plan as part of their hybrid IT strategy incorporating both NPMD and cloud-centric monitoring to fill the gaps (see Figure 1).

Analysis

Uncover Dangerous Blind Spots Left by Migration to the Cloud

An important first step in coming up with a network monitoring strategy for hybrid IT is to understand the impact that cloud migration has had, or will have, on the flow of network traffic. The destination of application data and where end users are located are major factors in terms of cloud-based network architectures and the monitoring of them.

Network traffic, which traditionally was generated by an end user accessing a centralized data center, is now generated by an extremely diverse set of traffic-generating devices going to and from a diverse set of locations where data is accessed. Network connections, which were traditionally dedicated WAN circuits, now also include broadband or wireless network access over the public internet — this fundamentally changes the flow of traffic around the enterprise network. Traditional data aggregation points like the core switch at the data center can no longer function as a central point for monitoring, which makes defining a holistic monitoring strategy difficult, if not impossible. Network traffic will often bypass the data center completely.

To help understand this impact, determine the following for both current and future plans:

- Where the mission-critical application tiers are hosted, to understand the extent of the hybrid IT environment
- Whether end-user traffic flows through the data center or goes directly to the cloud, to understand where network instrumentation needs to occur to monitor all application traffic
- The distribution of end users and whether they are constrained to corporate and branch offices, to understand the scope of endpoints that may need to be monitored
- Where the network traffic aggregation points are, to determine if there are easily accessible points to get a consolidated view of end-user traffic

Answering these questions should begin with discussions with the desktop, system, network infrastructure and application teams, to understand current and future application deployments that may involve the cloud. If an enterprise architecture group exists, it should be brought into this discussion as well. Business units should also be queried to ascertain if they have any cloud application requirements that may affect the network and the ability to monitor. The information garnered should then be coupled with whatever network monitoring data is currently being captured to ultimately create a map of end-user traffic flow and infrastructure ownership, both current and planned. Completing this exercise will inform the proper network monitoring strategy and allow I&O leaders to best choose technologies that can monitor the traffic patterns created.

Recommendations:

- Assess the impact of data flows, affected by cloud migration, on your ability to monitor cloud-destined network traffic, by involving both IT and the business units.
- When making cloud migration or architectural decisions, understand and base decisions on the ability to maintain visibility of cloud-destined network traffic.

Deploy Cloud-Centric Monitoring Technologies Alongside NPMD Tools to Shed Light on the Blind Spots

Network performance monitoring in a hybrid IT environment has various end goals — understanding current and future bandwidth requirements, understanding the end-user vperformance of cloud-hosted apps, calculating chargeback on internet usage for cloud-based apps, diagnosing the root cause of performance problems, and identifying dependency relationships of on-premises and cloud elements.

Achieving these goals in a hybrid IT environment has challenges. Compute latency and communication latency become much harder to distinguish, forcing

network teams to spend more time isolating issues between the cloud and network infrastructure. In addition, different cloud deployment options (including internal private cloud, outsourced private cloud, hosted private cloud, public cloud and SaaS) offer a different level of control over the network and infrastructure, which, in most cases, severely limits the ability to monitor.

Given that access to centralized points of data capture are fewer and the ownership of the infrastructure is diversifying, traditional NPMD methods of data ingestion become unusable in some cases. End users accessing cloud-based applications over internet connections will not be easily monitored. Packet analysis through physical or virtual appliances do not have a place to instrument in many public cloud environments. Flow monitoring solutions are vendor-derived and fail to provide critical response time metrics for cloud applications. SNMP-/WMI-based infrastructure metrics, if even available for the cloud, fail to provide enough information for performance analytics.

This is a new reality that has yet to be addressed by most NPMD vendors. Even those vendors that claim to provide hybrid IT monitoring have yet to truly offer solutions that provide end-to-end visibility into all varieties of cloud environments. Today's typical NPMD vendors have their solutions geared toward traditional data center and branch office architecture, with the centralized hosting of applications.

NPMD Technologies

Given these deficiencies, NPMD solutions still do play a part, and some network architectures do still allow NPMD tools to provide monitoring of data center and cloud-hosted infrastructure and applications. Traditional NPMD technologies like packet and flow monitoring can suffice to handle the new patterns of traffic, if the following holds true:

- Packet capture appliances can cost-effectively be placed in remote offices to monitor cloud-destined traffic not hitting the data center. All remote users can be monitored.
- Virtual probes or agents can be installed in the private or public cloud, or in branch offices.
- Traffic spans for packet data can be set up on the private or public cloud.
- Flow-based technologies are enabled at the branch routers, to report on cloud-destined traffic.

Packet monitoring is a traditional NPMD technology that is applicable for environments where virtual or hardware appliances can be deployed and spans/taps can be created to feed the solution with cloud-destined packet traffic. Packet monitoring provides the deepest network-based visibility of cloud application traffic, with the ability to report on network metrics along with end-user experience and business analytics data pulled from the packet. It is useful for private cloud environments, where there is the ability to install packet monitoring tools.

It can also be useful when cloud-destined traffic is backhauled through the data center or distinct aggregation points for easy capture. This technology may be possible to deploy, using virtual instances, in public cloud environments.

However, packet monitoring is not applicable in situations where the number of monitoring points becomes too numerous to be able to place probes in each of those locations. Packet monitoring close to the edge is often not economically or operationally feasible. It may not be feasible for public cloud environments that don't allow virtual instrumentation, and rarely for SaaS applications, unless there are aggregation points where this traffic can be easily captured and analyzed. Sample packet monitoring vendors that do cater to hybrid IT environments include ExtraHop and Viavi.

Flow monitoring is a traditional NPMD technology that can be useful for highly distributed networks, by understanding the bandwidth consumption of cloud-hosted applications from the branch offices that goes directly from the branch to the cloud. Flow monitoring provides a relatively nonintrusive way to get enterprisewide network visibility and metrics, and to identify SaaS applications in use and their bandwidth consumption. It can be applicable in all cloud-based deployments, including public cloud and SaaS applications.

However, unlike packet monitoring, flow data is vendor-derived and summarized data, and offers no ability to monitor end-user response time or to harvest business intelligence metrics. Additionally, it is not able to provide data on end users accessing cloud-based applications that are not situated in a branch office. Sample flow monitoring vendors that cater to hybrid IT environments include SevOne and Flowmon Networks.

Cloud-Centric Monitoring Technologies

Given the limitations of packet and flow monitoring, there still remain many areas in a hybrid IT world where there are blind spots. This includes situations where hardware appliances cannot be cost-effectively deployed to monitor cloud-destined traffic not hitting the data center; when the distribution of remote users makes network monitoring infeasible; when virtual probes or traffic spans in private/public cloud environments cannot be deployed; or when flow-based technology is not available. These cloud-centric monitoring solutions are especially applicable for public cloud or SaaS environments, and the monitoring of non-office-based user traffic. I&O leaders must strongly consider a number of cloud-centric monitoring technologies in place today that can fill the gaps that hybrid IT creates and NPMD tools ignore, including:

- Synthetic and availability monitoring
- IT infrastructure monitoring
- Endpoint monitoring
- Internet performance monitoring

Synthetic and availability monitoring solutions provide the ability to measure the response time and uptime of applications, with the ability to identify network bottlenecks based on preconfigured tests that are run from agents. These are most applicable to SaaS applications, because often there is no way to monitor real user transactions because instrumentation cannot be placed within the SaaS provider hosting, and it is difficult to provide monitoring close to the end user.

This technology includes testing of path conditions or availability testing of cloud-based applications using regular health checks. These vendors can also use an understanding of routing to perform path analysis across multiple providers. These solutions provide valuable response time statistics for SaaS applications, or a view into network path-related issues. However, this data is not based on real user traffic, and local agents may have to be deployed and configured at user locations to run these tests, or predeployed cloud agents from the vendor can be utilized. Sample synthetic and availability monitoring vendors include ThousandEyes and Dynatrace.

IT infrastructure monitoring solutions leverage APIs, among other technologies, primarily in public cloud environments like Amazon Web Services and Microsoft Azure, to capture compute metrics. They can be used alongside NPMD tools to assist in the disentanglement between network and compute metrics to isolate causes of performance degradation. Some SaaS vendors provide limited API access to performance metrics as well.

However, most of the data reported through these means is limited and do not provide much insight into the performance of the application or network to do a true root-cause analysis. In many cases, the API data is provided mostly to determine whether additional compute resources should be purchased

from the cloud provider, as opposed to determining performance issues.

At its worst, vendor-supplied API data can provide misleading information when it may not match industry practices. As an example, Microsoft Skype for Business APIs report voice quality scores differently than industry standards. I&O leaders should strive to corroborate with additional sources whenever possible, and should push their providers for as much visibility as is required to maintain desired performance levels. Sample IT infrastructure monitoring vendors include ScienceLogic and Datadog.

Endpoint monitoring is most applicable to monitoring the performance of web applications that are hosted anywhere in a private or public cloud, through browser-based instrumentation (also known as JavaScript injection). They provide browser-side monitoring that measures page load times and can highlight client issues in performance, along with server-side or network-related delay components. This can be used to track end-user performance for anyone using the web application, even those on mobile devices. However, this is limited to web applications and can only be used when the JavaScript can be injected, or a browser plug-in installed. In most cases, SaaS applications won't support this monitoring technology because there is no practical method to instrument the pages. Sample endpoint monitoring vendors include Soasta and Catchpoint Systems.

Finally, internet performance monitoring technology is applicable to any cloud-hosted application that is accessed via an internet connection or over a content distribution network (CDN). These solutions are able to leverage distributed agents that monitor the health of connections to cloud providers and CDNs from various points around the world, to identify network issues. This can provide insight into the cloud service itself and the optimum paths available. Some of these tools can also help with traffic steering to avoid network bottlenecks. This technology only provides general visibility of overall internet connectivity to CDNs or cloud providers, but there is limited information on specific user transactions unless endpoint monitoring is used. Sample internet performance monitoring vendors include Dyn and Cedexis.

Bottom Line

A successful cloud monitoring strategy involves taking packet and flow monitoring from NPMD vendors and putting them together with the cloud-centric monitoring technologies discussed above to get a cohesive view of the hybrid IT environment. If SaaS application performance is critical, invest in a synthetic monitoring solution. If public cloud environments are in use, invest in an IT infrastructure monitoring solution that has the proper API support. If website performance is critical, but it is not possible to capture the traffic off the network, invest in an endpoint monitoring solution. If heavily reliant on CDNs or internet connections, invest in an internet performance monitoring solution.

Additionally, there is a need to shift the balance between data ingestion and analytics. Traditional NPMD tools are still about capturing data, observing it and, at most, summarizing it. The ideal hybrid IT monitoring strategy involves the collection of data from a greater variety of traditional NPMD and cloud-centric sources, and the use of advanced analytics to gain meaningful insight.

Recommendations:

- Evaluate utilizing existing NPMD solution sets (including packet and flow monitoring) to monitor the performance and consumption of cloud-based applications and services, while recognizing the visibility gaps presented by these technologies.
- Shift investment from traditional NPMD monitoring to cloud-centric monitoring vendors to fill visibility gaps, based on specific requirements.
- Aggregate, correlate and analyze data from NPMD and cloud-centric monitoring technologies to garner meaningful insight on the overall health and performance of the hybrid IT environment, while also gaining deeper root-cause analysis capabilities to diagnose performance degradations or outages.

Evidence

Based on over 200 inquiries regarding this topic over the 2015 to 2016 time frame.

Gartner Research Note G00301635, Sanjit Ganguli, 27 May 2016

The Dyn Take: Monitoring + Control = Internet Performance Management (IPM)

As Gartner makes clear, cloud-centric monitoring is quickly becoming a must-have for IT teams moving workloads to the cloud. The ever increasing scale, complexity, and volatility of the internet introduces significant operational risk, as public cloud outages threaten both business continuity and the quality of digital experience you deliver to users. And while monitoring is critical, without control it may leave IT pros frustrated or struggling to resolve issues (or just plain scared).

Full Internet Performance Management (IPM) requires the pairing of monitoring with advanced analytics and internet traffic steering capabilities. First, analytics are critical to making sense of the vast quantities of internet "events" impacting performance, and serving up actionable insights. But while such insights would undoubtedly be useful for long-term planning and cloud vendor management, real-time, proactive control unlocks the full potential of internet visibility.

For example, an advanced, managed DNS service can be deployed by organizations to shift traffic between cloud and on-premise assets based on real-time internet conditions. Additionally, IPM platforms infuse the DNS capability with the data and analytics to increase the reliability and resilience of workloads and to provide policy-based traffic management, automating dynamic traffic steering decisions based on any number of factors (price/performance, user SLAs, etc.).

IPM allows organizations to manage the internet as an asset, under their control. This approach helps de-risk cloud- and CDN-dependent applications that use the internet to connect users with digital assets. As a result, IPM not only has the potential to help fill the gap for existing applications, but also increase the potential of the internet for a broader range of use cases.

Source: Dyn

About Dyn

Dyn is the Internet Performance Management (IPM) company, allowing IT organizations to manage the internet like they own it. The Dyn IPM platform monitors, controls and optimizes applications and infrastructure through Data, Analytics, and Traffic Steering, ensuring traffic gets delivered faster, safer, and more reliably than ever.

Dyn provides IPM capabilities, including Managed DNS, Internet Intelligence, and Dynamic Traffic Steering, to the largest enterprises and most visited web properties in the world, including eight of the top 10 internet services and retail companies, and six of the top 10 entertainment companies in the Fortune 500. Dyn helps everyone from high-growth startups to global leaders like Pfizer, Visa, Netflix and Twitter solve the challenges associated with internet scale, complexity and volatility. For more information, visit www.dyn.com or follow Dyn on Twitter @Dyn

Dyn customers use IPM to:

- **Increase Revenue Growth:** Slow DNS response times were to blame for steep revenue implications for a Fortune 500 e-commerce company, where dollars are measured in milliseconds. Adopting Dyn's DNS services improved latency by 90%, leading to >50% reduction in page load times, directly impacting the bottom line.
- **Optimize Infrastructure Spend:** Searching for a solution that would scale rapidly and satisfy strict security requirements, a Fortune 100 pharmaceutical company used Dyn's Traffic Management solutions to vastly decrease costs related to constantly growing infrastructure.
- **Mitigate Risk:** After an outage that cost an estimated $25 million in revenue, a Fortune 10 manufacturing company turned to Dyn seeking redundancy at the DNS layer to avoid future disruptions in business continuity.

Dyn

Contact us
For more information contact us at:

dyn.com
sales@dyn.com