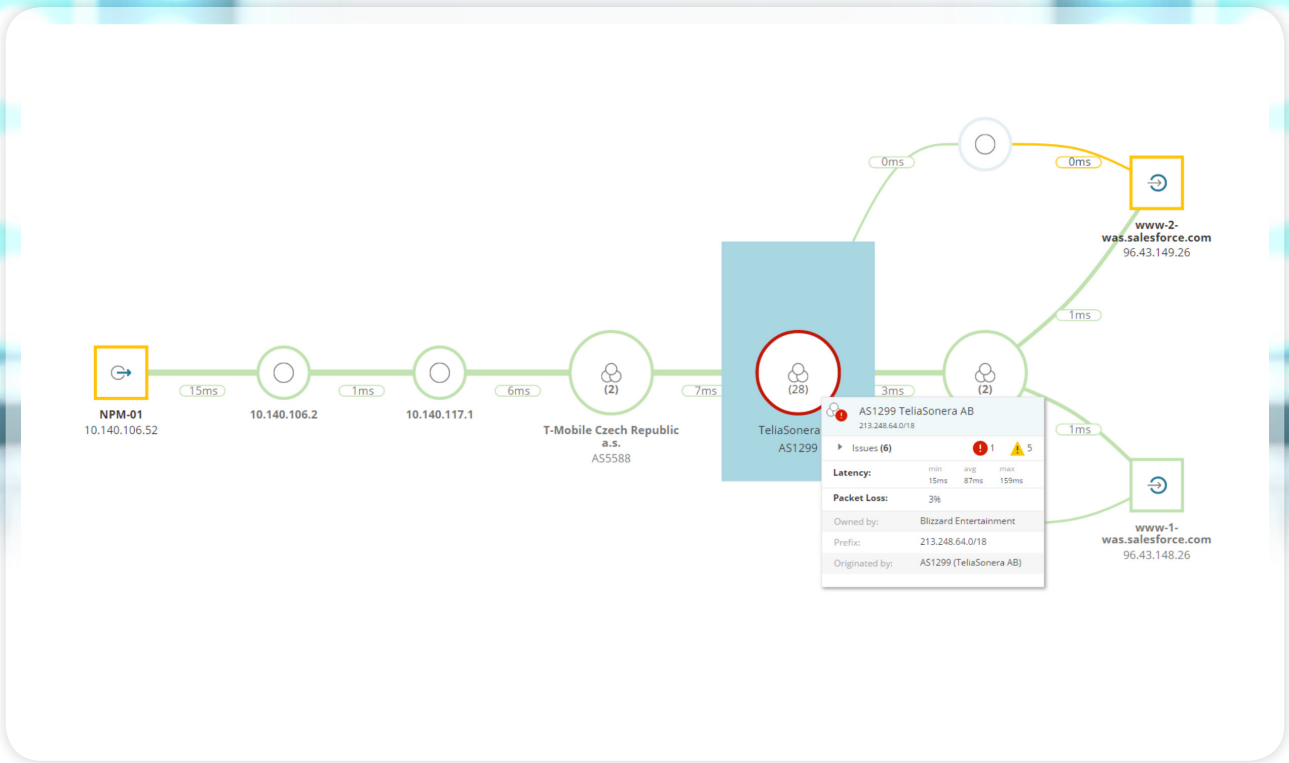
solarwinds

VISIBILITY FROM YOUR NETWORK INTO THE CLOUD:

Today's New Essentials



When cloud services falter, network managers need to know why.

The cloud is supposed to make everything simpler and more cost effective for businesses and their users, but for network managers it adds complexity. Cloud services are made available to users on demand via the Internet. The services depend on extreme network reliability, and that reliability must extend beyond traditional corporate boundaries.

Most organizations today are evolving toward a hybrid IT enterprise architecture, meaning their operations are split between the cloud and a traditional on-premises infrastructure. A 2016 survey by the market research firm IDC found 58 percent of organizations are embracing cloud computing, and 70 percent of heavy cloud users are pursuing a hybrid strategy. Over the next 24 months, survey participants said they expected to increase their use of public cloud resources by 48 percent.[i]

70%

of heavy cloud users are pursuing a hybrid strategy

58%

of organizations are embracing cloud computing

The SolarWinds IT Trends Index, based on a December 2015 survey of 257 IT practitioners, managers, and directors in the U.S. and Canada, found that nearly all (92 percent) say adopting cloud technologies is important to their organizations' long-term business success. More than a quarter (27 percent) of survey respondents call it extremely important. At the same time, only 43 percent estimate that half or more of their organizations' total IT infrastructure will be in the cloud within the next 3-5 years, and 60 percent say it's unlikely all of their infrastructure will ever be migrated to the cloud. In other words, hybrid IT is here to stay. Yet only 27 percent of survey participants said they were confident their organizations were equipped to manage the hybrid environment.[ii]

Hybrid IT is here to stay.

60%

say it's unlikely all of their infrastructure will ever be migrated to the cloud

43%

half or more of their organizations' total IT infrastructure will be in the cloud within the next 3-5 years

27%

said they were confident their organizations were equipped to manage the hybrid environment

Meanwhile, many important enterprise applications are moving to the cloud, along with more basic infrastructure, such as storage and application development platforms. In categories such as customer relationship management (CRM) and marketing automation, cloud-based services are the norm. Most new software in all categories is delivered to the market in the cloud first. If it is delivered secondarily, it comes as a product that you can install on your own network. By 2020, IDC predicts packaged software will account for just 10 percent of new enterprise implementations.[iii]

BY THE YEAR **2020**

IDC predicts packaged software will account for just 10 percent of new enterprise implementations

Rather than fighting to retain control of computing services, IT leaders have pivoted to a role of vetting cloud services for security and reliability, negotiating contracts, and facilitating the migration of services to the cloud. IT organizations increasingly will be judged by their ability to manage cloud services, which brings with it the inherent challenge of managing resources they do not directly control.

Consider what this means for network management. By definition, adopting a public cloud service means relying on an application or other cloud resource (such as storage) that resides outside the traditional on-premises network. Yet when a cloud service is defined as part of the enterprise architecture, it becomes an extension of the enterprise network. The trouble is, that extended network is beyond the reach of traditional network management tools designed for traditional corporate networks.

On a good day, cloud services may seem to make everyone's life easier. But what about on a bad day?

A day in the life of a hybrid IT network manager

Nathan is sitting in his own cubicle, minding his own business, monitoring and optimizing the corporate network, when he hears a commotion in his manager's office. Whoever is on the other end of the phone is very loud and indignant. Nathan hears his boss say, in soothing and deferential tones, "Yes, of course. We'll get right on it."

The call ends. Moments later, Nathan is not surprised to get a tap on the shoulder. "That was the VP of Sales," the boss tells him. "It's the end of the quarter, and the whole sales team is complaining they can't get on Salesforce.com® to look up customers or enter orders. Everything is slow, and half the time connections are timing out. His Salesforce® rep assures him everything is fine on their end, and I told him we're not aware of any problems with our network, which is true, right?"

Nathan pulls up his enterprise network monitoring dashboard to be sure but sees mostly green lights, representing the health of the network nodes under his control. "Everything looks good," Nathan says. "I definitely don't see any issues with Internet access from the sales department. Trying to puzzle out what's happening to that traffic after it leaves our network would take a lot more work, though – if we even can."

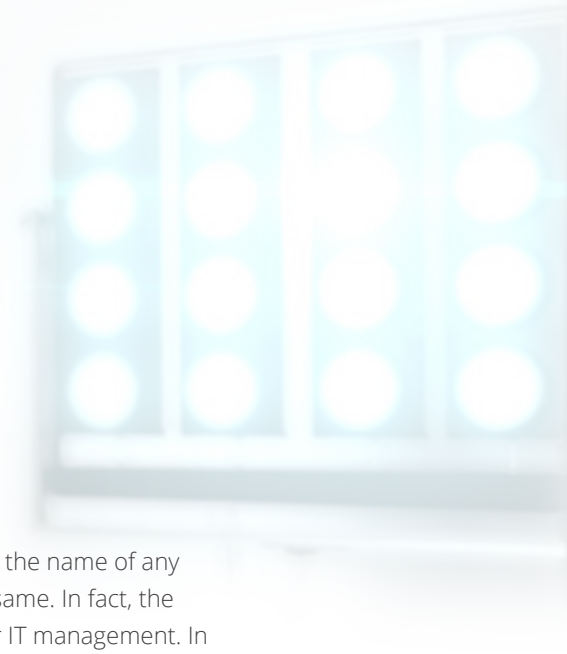
"Run a traceroute or something, but get me some answers," says the boss, who is about a decade removed from hands-on network management. "You can't leave me twisting in the wind. We can't be to blame for sales missing its numbers."

For the rest of the day, Nathan does his best. He enlists colleagues to visit members of the sales team and try accessing the cloud application from their desks, confirming that the issue does not seem to be the choice of one browser over another or some quirk related to JavaScript® or content caching. They try to piece together a picture of the path network traffic is traversing from the sales desk to the cloud service using basic utilities like ping and traceroute. Yet it turns out their own firewall blocks outbound traceroute connections for security reasons, and even a probe initiated from outside the firewall runs into many roadblocks where network nodes do not respond to that protocol.

The result is a partial and confusing picture of the connection between the enterprise network and the cloud service.

Near the end of the day, Nathan is relieved to hear that the problem has cleared up and the sales staff is getting caught up on work. His boss tells him to make sure it never happens again. The trouble is, he still has very little idea what went wrong or how to fix it next time. He's mainly concerned that a problem that seemed to "fix itself" will not be back tomorrow.

How network management must change



For the sake of our story, we used Salesforce.com as an example, but you could substitute the name of any cloud application, or any important service like cloud storage, and the issue would be the same. In fact, the underlying issue of pinpointing the cause of outages and malfunctions is a very old one for IT management. In the absence of good evidence of where the fault lies – is it the application, the database, or the network? – we tend to get finger-pointing instead of solutions.

Cloud service providers can take some complexity out of IT management, but they also have a limited span of control. When customers complain about access to their services, the fault really may be with the customer's network, the customer's Internet service provider, or some intermediary network node failing to route traffic appropriately. On the other hand, cloud provider networks have their own complexities and vulnerabilities. Many offer service status dashboards where major outages are announced, but a green light there doesn't preclude the possibility of problems the cloud operator may be unaware of.

Within a well-run enterprise network, network monitoring systems like SolarWinds® Network Performance Monitor (NPM) can be used to watch for problems and prevent them from arising on an ongoing basis. In the event of an application failure or severe slowdown, network managers can diagnose exactly what went wrong and take steps to prevent a recurrence. Cloud computing needs a dose of that same discipline. The trick is to extend it beyond the firewall, into remote systems beyond your direct control.

One of the ways we have made enterprise networks more manageable is with visual tools, such as interactive network maps that show green / yellow / red indicators for the health of network nodes. The network map can be supplemented with probes for monitoring databases, application servers, and other key elements of the network architecture.

Historically, tools have been designed to monitor the performance of the corporate network (inside the firewall) or to monitor application and service performance in the cloud (outside the firewall) but there have not been any that can monitor the entire service delivery path, from source to destination. When trying to follow paths through the Internet, network managers have had to rely on multiple tools that do not work together.

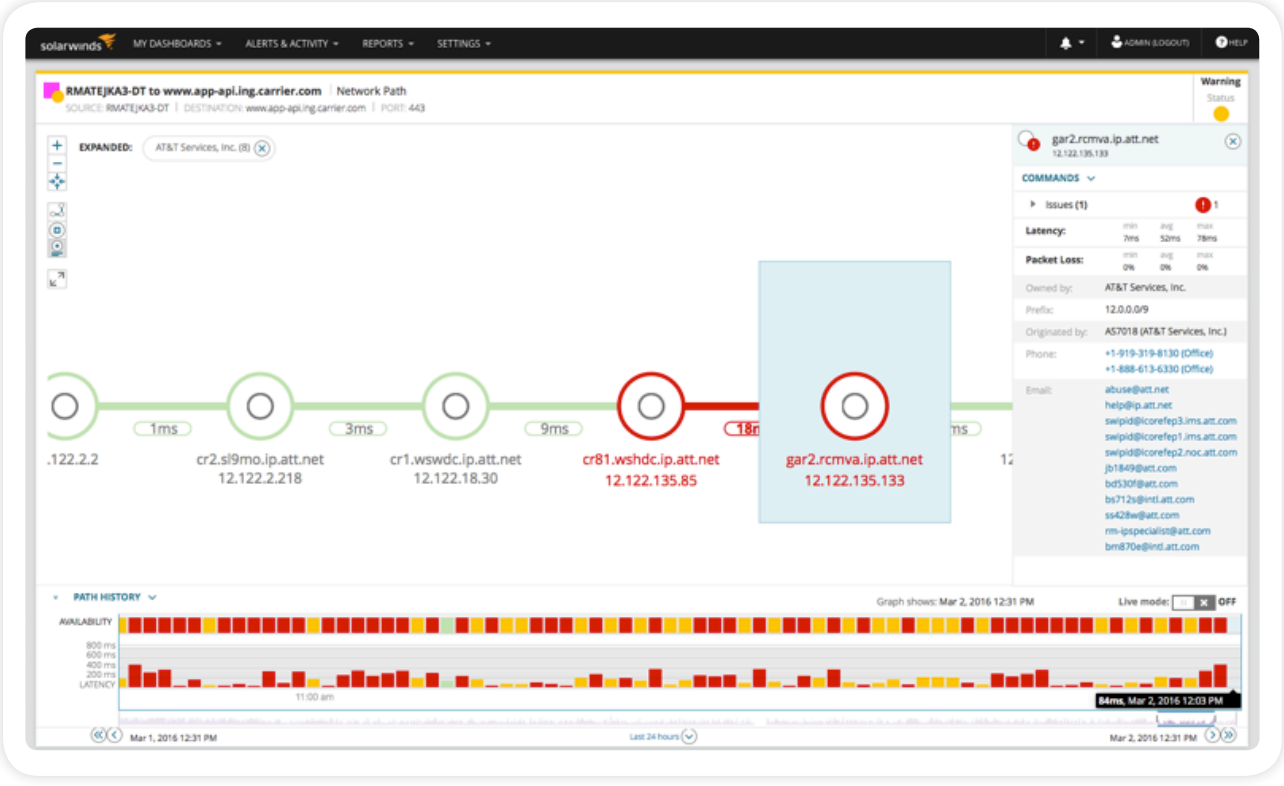
With increased adoption of cloud-based applications and services, our customers have been asking for a tool that can monitor and analyze performance regardless of location: on-premises or in the cloud.

The SolarWinds Answer? NetPath.

NPM 12 introduces a feature called NetPath™, which lets network managers visually monitor the performance of both their own networks and the cloud. NetPath is able to trace the path and nodes that application traffic travels through to reach its destination, including paths within the corporate network, the ISP, and the cloud provider's domain. Without overwhelming you with complexity, NetPath shows the network path required by a specific application, giving you just enough detail to let you see the trouble spots.

To enable NetPath within NPM, you define the service you want to monitor, which is comprised of a destination IP/DNS name and port. The path is comprised of a source machine (or user) trying to reach the service.

NetPath discovers and displays a path from the source to the destination, a list of the nodes that the traffic passes through, and the performance of each hop within the path.



NetPath lets you see where traffic exits your internal network, how it moves through external ISPs, and how it enters the final service domain, highlighting errors and slowdowns.

NetPath also eliminates detective work within an enterprise network, providing a simple map of the network path used by specific applications. Particularly in a global enterprise where different organizations are responsible for different parts of the network, pinning down the source of problems can be almost as

challenging as it is in the cloud. If an issue is identified within your own network and you have NetFlow Traffic Analyzer or Network Configuration Manager installed, you can see additional flow information as well as any configuration changes that may have impacted the performance of a device or interface.

Alternatively, you might discover the problem lies somewhere within the telecommunications infrastructure in between your network and the cloud service. In that case, you can click on the network node to get contact information for the responsible organization. You will not waste your time trying to get a resolution from the cloud service provider if the problem lies elsewhere.

The initial reaction of beta customers has been surprise – NetPath does things they had not thought possible. "How do you get this information?" they ask.

It works because NetPath mimics real application traffic, rather than sending specialized diagnostic protocol traffic like traceroute does with ICMP. That means NetPath can reach any cloud application in the same way it would normally be accessed. As a result, NetPath sees exactly the same problems a user would, but with the ability to track each hop across the network, IP address by IP address.

In one of our demos, we captured the origin of a glitch on amazon.com, the main shopping portal, not Amazon's cloud services business. As opposed to a simulated problem, this was a natural experiment, a problem we happened to catch by monitoring normal traffic to the website. NetPath identified a specific network node within amazon.com that was experiencing 75 percent packet loss, the kind of conditions where an application will time out and form submissions will fail. In this case, the problem was fleeting because Amazon's systems quickly rerouted traffic around the problem node. But not every online service is so resilient. It's when problems like this persist, or persistently recur, that the enterprise cloud applications' users get frustrated.

NetPath is what our customers have been telling us they needed to manage the transition to the cloud more effectively. It allows you to replace guesswork about the causes of cloud service failures with facts. Those facts become ammunition when you need to battle the cloud service provider who says, "We're not seeing a problem on our end," when, in fact, they are just not looking in the right place. Actually, armed with the facts, you probably will not have to fight. Network engineers tend to respect other network engineers who come to them with evidence of a problem, rather than vague complaints.

With that understanding, you can work together toward solutions. Simplifying the management of cloud networks turns out to be a prerequisite for the simplicity cloud computing promised in the first place.

Network Insight

FOR F5 BIG-IP

Going deep

If NetPath is about breadth, the Network Insight feature of NPM 12 is about depth. NetPath lets you see the path any application traverses, even if it leads outside of your network and into the cloud. Network Insight provides deep insight into the behavior of specific devices, including insights that can be gleaned only with access to product specific APIs.

Monitoring the CPU, memory, and network interface utilization was generally sufficient for diagnosing the problems with routers, switches, and other basic components of a corporate network. But suppose you are running a cloud service of your own, or a high traffic website, or a private cloud application for a global company. CPU and memory statistics will not tell you everything you need to know about the performance of the load balancers that keep it all working and highly available. Modern network infrastructure like that is based on pools of resources, where local traffic managers feed global traffic managers and every layer of the infrastructure must interact with the others to deliver the expected level of application availability.

The initial Network Insight offering focuses on exactly this challenge, with support for F5® application delivery controllers including LTM and BIG-IP® DNS.

While NetPath is designed to reach beyond your own network, Network Insight is for infrastructure equipment that is under your control and necessary for delivering applications. These network functions, such as load balancers, could reside in a cloud provider such as Microsoft® Azure™ or in your own data center. Typically, a Software as a Service cloud application provider would not let you monitor their network devices at the level of intimacy Network Insight allows, but NetPath would still provide the outside-in perspective to let you know when a cloud application problem is in their network, not yours.

With its combination of depth and breadth, NPM 12 lets you solve the problems that arise in a hybrid IT network much more quickly.

VISIBILITY FROM YOUR NETWORK INTO THE CLOUD:

Today's New Essentials

[i] IDC CLOUDVIEW 2016, FEBRUARY 2016
[ii] SOLARWINDS IT TRENDS REPORT: THE HYBRID IT EVOLUTION, MARCH 2016
[iii] IDC 50TH ANNIVERSARY STUDY: TRANSFORMATION EVERYWHERE, 2014

solarwinds