Traverse:
Root Cause Analysis
in Complex and Hybrid Networks
The job of an IT administrator is packed with daily challenges. As IT pros, they are professional problem solvers. Unfortunately, their problems never seem to end so work days are filled with troubleshooting, which often comes down to network Root Cause Analysis (RCA).

RCA has never been exactly easy, but when networks and IT infrastructure had a simpler architecture, finding a root cause was not overly complex. It was usually either the LAN or the WAN, and if an application were to blame, it was installed on a non-virtualized on-premises server so hunting it down was pretty straightforward.

However, those days are long gone, replaced by complex infrastructure and networks that can contain several cloud services and applications (including hybrid implementations), and virtualization—all spread over several offices and geo-locations.

This paper will outline the major network challenges faced by today’s IT admins, how this leads to the dreaded ‘Swivel Chair’ syndrome, caused by out-of-date network monitoring tools, and how they can break free of this syndrome—and conduct fast, efficient RCA and remediation.

**Network Complexity and the Life of an IT Admin**

Today, the relative simplicity of a simple LAN or WAN is a distant memory—and has been replaced with ever increasing complexity. How complicated have networks become? Let us count the ways.

There are still LANs, but today they often connect ‘these’ servers to ‘those’ servers, and then feed wireless access points through which end users get to the network.

At the same time, computing is more distributed. Applications reside both in-house and in the cloud, and some applications are even hybrid where processing is shared between the two. Even more rare today is the on-premises server that is not virtualized. Virtualization turns one server into many and makes it more difficult to find which virtual machine is actually causing the server problem. This complexity is only magnified when IT has to manage different server virtualization technologies such as VMware, Microsoft Hyper-V, Zen or others.

On the cloud side, most company infrastructures contain a multitude of cloud services, covering everything from public cloud services such as Amazon Web Services (AWS), to business applications such as Microsoft Office 365, to scores of other services. Each cloud service has its own dedicated form of management.

On the other side of the divide, today’s critical applications serve users in multiple departments, spanning various geographic locations. Frequently, these applications either are revenue-producing or revenue-impacting, and the business’ health is directly tied to their performance and availability.

**What IT Admins Need: Superhero Vision**

The problems admins attempt to define are almost infinitely varied. Some are deal breakers where the network or an application is brought down entirely. Others involve slow performance—issues that can actually be harder to trace.

IT has to be adept at managing and troubleshooting this complex infrastructure so that business services stay up and running—with a goal of zero or near-zero downtime. That means holistically managing servers, applications and network devices. And not just managing, but preemptively addressing problems before they turn into downtime.
**What IT Admins Get: “Swivel Chair” Syndrome**

Traditional monitoring tools tend to operate in silos. They often focus on on-premises networks, specific applications—including cloud apps, OSes, virtual servers—or bits of network gear such as routers and switches. This makes it tough to pinpoint the root cause of any single networking problem.

This tangle of tools leaves IT admins staring at a bank of screens, with each displaying a different console. As IT staff search for problems, or try to find a solution, they shift from console to console—an approach that leads to “Swivel Chair” syndrome. They turn this way and that, in a swiveling process that is neither efficient nor holistic. In fact, it can take hours, and even days, to identify the true cause of the problem, never mind fix it.

These challenges have only been deepened as IT groups adopt more and more cloud services.

**The Great Cloud Management Admin Challenge**

Moving applications to the cloud has been an exciting endeavor, filled with promises of flexibility, cost efficiency, and easier end-user access. Admins are happy because leveraging the cloud relieves them of many on-premises IT admin chores. However, they soon find that the cloud raises a host of other admin issues that impact uptime—issues that can be vexing to repair.

Ironically, the section of cloud infrastructure that is most vulnerable to downtime and performance issues is not the public cloud services. AWS, for example, only had two and a half hours of downtime in all of 2015.

In fact, the most vulnerable element in any cloud set up is the company’s own network. Managing that network is still the responsibility of a company’s IT group. Monitoring for problems, both current and pending, requires visibility across both internal networks, as well as any WAN or internet connections. Problems that bring a business service to a halt can come from a number of sources—from a router or NIC issue to another network infrastructure component causing the issue.

As we’ve mentioned, since traditional monitoring tools are often focused on on-premises networks, these tools do little to monitor the public cloud. This makes it tough to pinpoint the root cause of cloud networking problems.

**Hybrid Cloud Impact on Monitoring, Management and RCA**

To make matters worse, the talk today isn’t just about public clouds but also includes hybrid clouds, which combine private and public clouds into one unified system.

Before talking about why hybrid clouds are so popular, let’s touch on why private clouds are so compelling. With the help of server virtualization, any company can take its own infrastructure and make it cloud-like—basically turn it into a utility.

The problem is that as user demand grows, IT Ops has to scale up the private cloud by adding more resources—even if those resources are only needed every now and again. At the same time, there are services that a company may want to provide via a public cloud but still have these applications and data linked to on-premises applications.

Thus the hybrid cloud was born. If more capacity is required than the private cloud can muster, business services can ‘burst’ over to the public cloud. In other cases, applications may need to be distributed between private-cloud and third-party public-cloud resources. For example, a company may use in-house storage as the primary backup location, but use another tier of backup in the cloud. Microsoft Office 365 is another prime example—documents can be accessed and stored on site in laptops and PCs, but also shareable and accessible via the cloud.

These benefits have made hybrid clouds very popular. According to the “Hybrid Cloud Market” report, the market for hybrid clouds will leap from $33.28 billion in 2016 all the way to $91.74 billion by 2021. That represents a Compound Annual Growth Rate (CAGR) of 22.5% for those years.
But while clouds, whether public or private, make things appear simple to the end user, they are complex to undertake and to manage. Add in more than one hybrid architecture and monitoring worries more than double.

**Fixing Hybrid Cloud Performance Problems**

With a private cloud, it is relatively easy to predict performance. The speed of the servers, disks and LAN connections are known. This is a baseline measure of performance. IT also understands the maximum capacity of these resources and has direct control in terms of which IT services are consuming which of these resources.

The integration of the public cloud adds another wrinkle—now the cloud service itself plus WAN connections can impact actual performance. It’s these connections that can make the performance of a business application distributed via a hybrid cloud far slower than when run solely on a private cloud.

Finding the cause of problems, though, is suddenly more complex. Which portion of this complex architecture actually holds the problem? Part of this is requiring cloud service providers to have their house in order and spot problems from within their complex multi-tenant system.

On the other hand, companies, as we’ve mentioned, are responsible for controlling their own network that supports private cloud connections to the service provider. As with all elements of a complex, modern infrastructure, monitoring the connections for performance, doing root-cause analysis and fixing problems is critical so the hybrid cloud works to satisfaction.

**How to Stop ‘Swivel Chair’ Syndrome, Increase MTTR, and Prevent Downtime**

In today’s complicated network world, IT admins need 360° visibility into performance and availability across public, private and hybrid infrastructure. This includes their own network, internal servers, virtual machines, and applications that need to be monitored to keep track of all the cloud services.

This visibility isn’t delivered using traditional siloed monitoring tools (network monitoring, application monitoring, device monitoring, etc.). Swiveling from one control panel to another, over-taxed IT admins try to thoroughly understand current performance, and then valiantly attempt to pinpoint the true root cause of any individual performance issue within this byzantine network environment. This usually means long mean-time-to-recovery (MTTR) stats and unhappy users and executives.

What IT staff first need is a single holistic solution that provides an overview of the entire network infrastructure, armed with a comprehensive database of all network and system elements, as well as applications and the services they deliver. Within this holistic view of the complete network, problems can quickly be surfaced, root cause identified and fixed rapidly—stopping ‘Swivel Chair’ syndrome in its tracks.

**Next Step: Taking a Business-Service View of the Network**

However, IT groups still require one more thing beyond this single console to truly ‘rule’ all their infrastructure and datacenters.

We’ve discussed how traditional network monitoring and remediation tools create siloed views into separate network components. However, this very focus on network components highlights another shortfall of this current approach.

At the end of the day, it’s not IT’s job just to keep servers running. With organizations laser focused on business uptime, IT’s job is now to keep services running and operating with proper performance.

Instead of just asking if the routing table needs work or if a server is down, IT needs to be able to see if business services such as Payroll, e-commerce, or ERP are working properly, and if not, why.

How does a business-service monitoring approach enable faster RCA? One way to explain this is by referencing the traditional seven-layer OSI network model.
Mapping, Monitoring and Managing All Business-Service Layers

To support this business-services focus, this holistic monitoring and management solution should provide high-level insight by intelligently discovering all networks and network components that support any particular business service. This starts with completely mapping all Layer 2 and 3 devices and defining the relationships that exist between all these devices, as well as network connectivity, disks, controllers, VLANs, file systems, fiber channel switches, printers, SAN, NAS devices, including redundant paths in the network to prevent false suppressions. Additionally, this process should discover the capabilities, size, capacity, and other key attributes of each element, and go on to discover applications running on various devices, such as databases, Active Directory, DNS, mail, and application servers.

Of course, to ensure that IT admins don’t spend all their waking hours defining these maps, this comprehensive monitoring system needs to automatically discover and map these connections and components, across the entire network—including cloud and virtualized environments. And keep updating these maps dynamically and automatically.

With these connections properly mapped, IT admins can focus on spotting service problems—not just infrastructure problems—then quickly diagnose and ultimately repair the issue, even within the most complex infrastructure.

Fast RCA – Layer by Layer

The right solution systematically troubleshoots all the layers that support any particular service, such as an ERP service. In many cases, a problem will initially present at a high layer such as Application. In this case, IT can now drill down deeper and deeper to discover and isolate the true root of the problem—all the way down to the details of Network Flows.

With this approach, IT narrows down the problem as it moves through the layers. Since all the IT components that support any business service have already been identified, finding which
router supports which service, for example, can take minutes instead of the hours or even days traditional methods take.

On the other hand, this business-service approach doesn’t preclude a more layer-specific approach to monitoring and troubleshooting.

**A Layered Approach to RCA – the Device Layer**

One of the lower levels is devices which largely operate at the lower three levels of the OSI model. These are mainly physical items such as routers, switches, servers, storage and other devices such as load balancers and traffic shapers. While most of these are actual hardware devices, with network virtualization such Software Defined Network (SDN) one can have software that mimics the function of hardware.

When troubleshooting these devices, IT can ping them to see if they are reachable, and use a monitoring solution to check whether the ports, disks, CPUs and other components are operating within the thresholds you established.

**Dealing with Network Faults**

Up from the Device Layer are Network Faults which are really OSI Layer 3 concerns. Here the monitoring and remediation solution should carefully map how network devices are related. When a network fault is identified, all devices closely related to the failed device can be shown. This helps isolate the problem device or devices rather than chasing a bevy of alerts that don’t point to a specific isolated problem.

**Mastering the Application Layer**

The Application Layer is where many problems are spotted. After all, if the CEO calls IT to complain that Microsoft Exchange or Salesforce is down, IT has a problem. Network Flow analysis can help by showing what applications are on the network, and how they are operating such as detailing their bandwidth use. The latter can point to performance problems which could slow or derail application usability.

**Keep the Hybrid Cloud Network Running Fast and Smooth**

Hybrid cloud infrastructure is complex. Private clouds are based on virtualization, and to properly monitor, any comprehensive solution needs to support virtual technologies such as VMware, Microsoft Hyper-V, Xen and KVM.

To have a holistic view, the same monitoring tool must support key cloud infrastructure offers such as Amazon AWS, Microsoft Azure, as well as CloudStack and OpenStack-based services.

**Kaseya Traverse: Next-generation Monitoring and Management for Fast RCA**

Kaseya Traverse, a next-generation monitoring solution from Kaseya, provides the unified network monitoring and management capabilities required by today’s complex, hybrid networks and infrastructure. Traverse allows enterprises to monitor, manage and optimize their entire IT infrastructure and distributed data centers—including hybrid and virtualized infrastructure—in a single unified console.

Traverse enables IT groups to create virtual views of discrete business services—again, including all OSI layers. Then, Traverse finds all associated connections and network components automatically and dynamically. IT no longer has to spend hours, days or weeks creating maps of their infrastructure.

With Traverse, IT can quickly spot all relevant components to quickly drill down and discover the underlying issue for any performance issue. Its deep, unified monitoring lets IT pros see where performance problems lie, and through fast RCA, supports rapid remediation.

Because IT can now see the entire landscape for any application or business service, they can be more proactive and identify ways to prevent problems before they occur. Even better, the same understanding of network performance allows IT to predict future needs and plan network upgrades accordingly.

Organizations worldwide are leveraging Traverse’s technology for to radically improve MTTR
as well as key performance KPIs. Customers using Traverse include Fortune 100 enterprises as well as small- and medium-sized businesses. Traverse’s fast expanding customer base includes Sony, Cisco, Paypal, Yale University, US Postal Service, and US Army. So put a stop to ‘Swivel Chair’ syndrome, enable fast, efficient RCA, and increase network performance with Kaseya Traverse.

Learn more and sign up for a free trial today!