Major League Baseball makes a run at network visibility

Legacy network-monitoring tools weren't cutting it for MLB with its demanding lineup of video, gaming, and AI workloads across its data centers, ballparks, and the cloud.

BY ANN BEDNARZ, NETWORK WORLD

Major League Baseball is taking network visibility to the next level.

"There were no modern network-management systems in place before I came in. It was all artisanally handcrafted configurations," says Jeremy Schulman, who joined MLB two years ago as principal network automation software engineer.

Legacy systems, including PRTG for SNMP-based monitoring and discrete management tools from network vendors, allowed MLB to collect data from switches and routers, for example, and track metrics such as bandwidth usage. But the patchworked tools were siloed and didn't provide comprehensive visibility.

"At our ballparks, we could see the bandwidth utilization, from a traffic-flow perspective, on our circuits. That gives us a very high-level view of how much data is being transmitted between the ballpark and our data centers. It doesn't give us insight into the users of the traffic—how much bandwidth is being used by, say, the video cameras, versus how much traffic is VoIP phones or other aspects of the ballpark infrastructure," Schulman says.

To gain greater visibility into its networks, MLB rolled out Kentik's network-flow analytics platform, which is designed to unify diverse streams of monitoring data across clouds, data centers, edge, SaaS, and the WAN. It supports a broad range of telemetry formats, which is critical for MLB with its multivendor network environment that includes gear from Cisco, Arista and Extreme Networks.

It's a complex network environment that supports 30 teams across the U.S. and Canada. The league runs its own data centers and maintains traditional campus

environments at MLB offices, including in its replay center at Rockefeller Center in New York, where plays that are subject to instant-replay review are analyzed using feeds from high-frame-rate TV cameras. The ballparks function as mini data centers at the edge, with infrastructure for a slew of applications including VoIP, commerce, and mobile devices in the dugouts and bullpens that deliver in-game video. The parks connect to the internet via MPLS circuits. MLB also provides fan-facing wi-fi services in some ballparks, and it streams video over a multicast network.

"We've got campus networks, we've got WAN, we've got wireless, we've got data-center networks, we've got MPLS," Schulman says. "And then we use a multicast network to transit our video feeds to all the ballparks. So on top of all of the infrastructure itself, we have a very sophisticated set of network services that we deploy."

MLB also runs workloads in the cloud, such as gaming platforms for fans and its big-data, stat-tracking system, Statcast.

To get a handle on all that, the Kentik platform collects traffic data and telemetry —including device metrics, performance data, configuration details, routing, and orchestration processes—from MLB's network devices such as routers, switches, and wireless access points. On the analysis front, the platform provides insights that help MLB's network teams streamline

root-cause analysis and capacity planning.

The platform, called the Kentik Network Observability Cloud, is delivered as a service and licensed by device, and it collects, stores and analyzes network data on its own infrastructure, which the company built and operates in leased data-center space. A setup of that scale enables users to access larger data sets, kept for longer periods of time, than typical on-prem capacity would afford. Having that depth of collected data, in turn, boosts the analytic capabilities of the platform. Kentik offers prebuilt visualizations, often organized around IT job roles, that are geared for optimizing how network traffic is routed or for detecting DDoS attacks, for example.

That setup is critical for MLB. "What attracted us to Kentik was that it is a SaaS-based solution. Meaning, we wouldn't have to manage and deploy on-prem infrastructure to scale out a flow collection," Schulman says. "I didn't want to buy a product that would require me to stand up servers and load balance them."

Tim Gouw / Manuchi (CCO)

Insight into cloud providers' networks was another must-have. The Kentik technology can ingest flow data from within Amazon AWS, Google Cloud, IBM Cloud and Microsoft Azure. Users can drill into traffic to, from, in, and between cloud providers, regions, availability zones, VPCs, subnets, and instances, and the system can present traffic breakdowns by application, IP address, and business attributes.

"So it isn't just showing how much traffic is going in and out of these various projects in the cloud. It's actually showing you a visual representation of how your physical equipment connects via those virtual private connections in the cloud," Schulman says. "It also gives us information like latency, throughput, and jitter, across on-prem, through the cloud, and back on-prem."

"That was an important factor so that we would have visibility into our traffic, not only from the multivendor network infrastructure that we have, but also as the traffic transits our cloud infrastructure, where much of our baseball applications live."

It's a common need. Enterprise IT teams are struggling to achieve visibility into networks and systems as IT environments become more complex. In particular, hybrid networking is taxing legacy tools that aren't built to monitor and analyze interactions among on-prem and cloud infrastructure. Gartner predicts that, by 2024, 50% of network operations teams will be required to rearchitect their network-monitoring stack, due to the impact of hybrid networking, up from 20% in 2019.

For network teams, achieving greater visibility enables them to increase efficiency and speed problem resolution. In the broader IT sphere, observability at the network layer is often missing from enterprise application monitoring and analytics frameworks. Filling those visibility gaps can enable higher-level capabilities—correlating network data with that of other business intelligence and predictive analytics systems, for example.

Taking network analytics from tactical to strategic

MLB's first projects using Kentik's monitoring and analytics capabilities have centered around traffic distribution, network reliability, and end-user experience.

Last year during the off season, MLB used the Kentik platform as part of a data-center consolidation effort. "What the Kentik software allowed us to do was monitor traffic in the data center that we were looking to decommission, so we could figure out who was still using the data center," Schulman says. The technology can analyze application and usage data to provide a clearer view of data-center traffic; that helped identify application owners who needed to relocate their apps before MLB consolidated its data-center workloads and decommissioned one of its properties.

For in-season use, MLB relies on network monitoring and analysis to spot anomalies and odd behaviors. The Kentik platform lets MLB visualize critical traffic flows during the season, which speeds root-cause analysis of problems.

"For example, we have the ability to see our multicast video streams. Kentik can break down the analysis of traffic flow and show us data for every stream coming out of cameras," Schulman says. If there's a problem with a camera feed, Kentik makes it easier to zero in on whether it's a device glitch or a network performance problem, and that analysis can speed meantime to resolution from hours to minutes.

For now it's a tactical tool, but MLB is also using the platform to be more proactive as it builds out its broader observability capabilities. That's a work in progress, and Schulman is hopeful about what it means for the future.

Seeing network analytics in context

As the network team has expanded its use of the Kentik technology, MLB is looking to reap benefits outside of network operations. The goal is to allow users across IT to correlate network data with other performance management and predictive analytics sources.

To do that, MLB has been building a league-wide platform for monitoring and analytics that crosses multiple IT domains—applications, systems infrastructure, cloud infrastructure, and network infrastructure. That platform was created by the software development team for application performance monitoring. Monitoring and analytics

technology from Circonus underpins it, augmented by commercial products, open-source and custom-developed capabilities. Now the Kentik-collected data and insights will be added to the mix. (Kentik offers an API and a means by which to extract data and pull visualizations into other dashboards.)

"All this very rich information is being put into a common observability platform, and that democratizes the data in a very important way at MLB," Schulman says.

Enabling other IT disciplines to access network data will potentially speed troubleshooting and improve performance, Schulman says.

"It means that when somebody in the systems team is trying to troubleshoot or diagnose something, they don't have to send an email to the network team and say, 'Hey, can you tell me what the bandwidth looks like on this port, on this interface.' They can just pull the data out of our observability platform. We'll have this beautiful, very deep, rich set of metrics, cross-functionally."

"It's amazing to have a seat at that table," Schulman says. "We don't have to make isolated tool decisions. We get to work with a group of very sophisticated engineers across all these other domains in cloud infrastructure, systems infrastructure, and we get to use their tools, along with their technology. We just bring our data to the table, and then everybody has a democratized access to it."

"I don't know how many enterprise companies are doing what we're doing, this way. I think it's very unique."

Getting off the legacy SNMP products and getting involved in a more strategic, cross-team management effort is part of Schulman's charter at MLB. He has a background in software engineering, and he's spent the last decade exploring the potential for network automation.

"The reason why I took a job at MLB was because the executive leadership, from the top down, recognizes that they must have network automation as a core technology going forward," Schulman says. "As a software engineer, that's why I'm in the network infrastructure team—to bring forward that technology and evolve our network infrastructure so that it's as agile as we hear the cloud people are doing, the server people are doing."

kentik®