Statseeker
every port. every minute. everywhere.

Monitoring a Growing Network

In the IIoT Realm - Auditing and Compliance is a Vital Concern

Whether it is a mandatory industry compliance regulation or a company wide rule, knowing what you have on the system and ensuring it is working is a must in these days of growing networks.

On top of that, effective management of your network, cost-effective visibility in near real-time, and keeping your network availability high, will be key aspects to network value within your business.

In 2016, 5.5 million new devices will connect to the Internet of Things (IoT) every day, according to Gartner. “Gartner, Inc. forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020.”

These days and in the future, you will have to be able to operate your network at the highest level of efficiency and capability. Doing this will require doing some things differently, and with discipline. It is unlikely any network consists of devices installed at the same time, from a single vendor. You are much more likely to have an “archaeological dig” of a network, with devices and connectors ranging from very old, to middle aged, to relatively new. Chances are your switches, routers, other devices and appliances will all be of different vendors, models and ages.

Changes in network architectures, operations, and usage, demand that you do things differently. After all, uptime is key.

In addition to technology another important area to consider is regulations. Many established regulations must undergo review. This will ensure they still serve their intended purpose even as the impact of disruptive technologies such as IIoT/IoT, BYOD, Wireless, and Big Data Analytics are deployed. Whether it is a mandatory industry compliance regulation or a company wide rule, knowing what you have on the system and ensuring it is working is a must in these days of growing networks.

Audit and compliance rules dictate that data must be true to ensure processes and systems are running to the height of their performance capabilities. After all, manufacturers have an obligation to ensure they remain in compliance with the law and the data stored is accurate, secure and managed correctly.

Auditing and network monitoring also provide historical information that can help diagnose problems and track malicious activity. Furthermore, it can help predict future trends by being able to look at historic data.

The following example provides a good perspective on the location of equipment and its operating status. Through the use of network monitoring tools, a manufacturer can collect data from all the connected equipment, extracting vital information in near real-time. This information may include serial numbers, operating system versions, product model, build version of the model, and the vendor of the devices. All of this helps with change-control management and auditing certification.

Saving on Costs

This information at auditing time is critical to make sure from a cost perspective, that if you spend money on 20 of the devices, you know where they are and if they are online and in use.

In addition, it allows a manufacturer to track serial numbers throughout the organization. For example, you would know that the serial number you bought in June is in use in your Oakland office and that another serial number purchased in the same shipment is working in your Australian office.

A network monitoring system can assist in the auditing of devices to ensure they are online and in use. This is important because tracking hardware from a network administrator’s perspective is burdensome, as every six months a report needs to be created to advise the finance team.

It is possible to automate the process completely, so with ten minutes of work you can set up a report that can go up to accounting or the C-Suite every six months showing the location and details of every piece of equipment.

In addition to that data, it is also possible to collect network statistics like data usage, latency, errors, discards, CPU, memory, disk and temperature values. Statistics are collected via non-intrusive Simple Network Management Protocol (SNMP) polling, and Internet Control Message Protocol (ICMP) polling.

The issue is all about having an awareness and knowing the network, and a logging capability of events occurring at all times. That all can happen once the user develops a solid understanding of what the network should look like. Over time the network monitoring tool collects and stores data points that demonstrate how the network is operating.

Audit Trail

The goal is to keep the history as long as the user wants. By knowing the history of that baseline that could go back for years, it can also help to show that everything is staying within normal parameters.

By logging network traffic and keeping it forever, it is possible to view an audit trail in an effort to reconstruct a sequence of events. So if the user finds something negative occurred, history available through the tool's logging component can be analyzed to determine exactly what occurred, and then put some mitigation measures in place.

On the PC or operating system level, a user can record who logs in to which machine at any particular time of day and what applications they run. You are not going to catch someone who has social engineered a password from an authorized user, but you can record what that person did and that provides an audit trail so you can come back to do a forensic analysis. That is the value of a logging system where you can rebuild the sequence of events and figure out where the gaps are and then address them.

Logging also works in the event of an intrusion, where the user can use data collected from the monitoring tool to understand when and where the event occurred.

Auditing IIoT

Understanding network traffic and being able to analyze it becomes all the more important as the industry moves toward a more connected IIoT environment. Realizing just what is on the network becomes mind boggling when you start talking about IIoT.

Currently, the numbers of sensors at typical process plants cluster around 40,000. The IIoT will increase those numbers to over 250,000 sensors per plant. Each of those sensors will produce near real-time data at an update rate of four times a minute, or 250 milliseconds per datum. That means each sensor will produce over 5,000 data points per day. That is a massive amount of data points per plant, per day. Each sensor needs to be monitored and diagnostically checked for proper operation as part of the network.

IIoT will help solve key business issues all plants face in terms of production efficiency, process reliability and safety. In addition, IIoT will allow moving ancient legacy systems into the new age of technology to take advantage of all the things new technology and connectivity bring to the table.

Among the multitude of benefits that IIoT brings, is being able to aggregate data from multi-vendor equipment. Another element of IIoT is being able to leverage data across the entire manufacturing enterprise to ensure maximum productivity.

While all that data is coming in, the network monitoring tool must utilize active and passive scanning to discover and audit configurations.

Users can receive detailed information on the configuration of systems, applications, firewalls, routers and switches. They can also automate continuous configuration and compliance assessment, making it easier to tune and modify custom policies. In addition, reports and data views provide visibility of important network information.

Subsequently, being able to see and show what you have on your network is a must in the industry today - especially as IIoT begins to rev its engines.

Summary

✓ Knowing what you have on the system and ensuring it works is a must.

✓ Data must be true to ensure processes and systems are running at the height of their capabilities.

✓ To remain in compliance manufacturers must ensure stored data is accurate, secure and managed correctly.

✓ Auditing and network monitoring provide historical information that can help diagnose problems and track malicious activity.

✓ Help predict future trends by being able to look at historical data.

✓ Understanding network traffic and being able to analyze it becomes vital as the industry moves toward IIoT.

References

Gartner Press Release, *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*, www.gartner.com/newsroom/id/3165317, 10 November 2015 (Source Viewed 12 November 2016).

Related Reading

Statseeker White Papers

- Statseeker eBook
- Analytics Through Network Monitoring
- Understand and Assess Risk
- The Wireless Edge
- Gaining Visibility on Malware Attacks
- Benefits of Virtualization
- The Internet of Things Part 2: Virtualization & Cloud Technologies
- The Internet of Things Part 1: IoT's Impact
- Networks from the OT Point-of-View
- Wireless Reshaping IT/OT Network Best Practices
- Proactive Network Management
- Virtualizing Your Network
- The IT/OT Convergence
- Three Key Challenges

Statseeker Blog Articles

- Software Defined Network Deployment
- Rapid Changes in Network Technology - Are You Prepared?
- Getting The CFO's Attention to Improve Your Budget Position
- Network Optimization - Meaning and Benefits
- Best Practices for Handling BYOD
- Predicting Network Utilization
- Rightsize Your Network - Improve CAPEX & OPEX Costs
- Sensors and Sensor Networks for Enterprise IT Professionals
- "I've Got Wireless In My Network!"

About Statseeker

Statseeker was founded in 1996 as a privately held company of expert network monitoring software developers. Statseeker then incorporated in 1998, and has enjoyed continuous growth and profitability based on our product strengths, our integrity and our high levels of customer service.

In 2015 Statseeker Pty Ltd announced the formation of Statseeker, Inc. headquartered in San Diego, CA. Statseeker, Inc. provides focus and support to the growing American market. Statseeker is now a global company with staff based around the globe ready to assist our customers.

Statseeker is a global provider of innovative network monitoring solutions for the IT enterprise and OT industrial market space. With active deployments in over 22 countries and many Fortune 100 firms, Statseeker monitors millions of interfaces in real-time. These companies trust Statseeker to deliver big data, make decisions and take action. Statseeker allows them to identify critical issues, isolate what needs work with confidence and fix problems instantly.

Statseeker offers licensing options for a single license fee from 1,000 interfaces to deployments scalable to 1 million interfaces per server with worldwide electronic delivery of technical support and all upgrades.