Issue December 2015 | presented by JAXenter www.jaxenter.com #48

jaxmagazine

The digital magazine for enterprise developers

Try new things!

But what things?

Data decisions
Apache Apex, Cassandra 3.0, datacentre resiliency

Cloud changes
Cultural adjustment is a major factor

DevOps, microservices, testing
... and other areas to experiment

Smart thinking for next-gen datacentre resiliency

The changing datacentre landscape

The data centre is getting faster, denser and more complex. Opengear's Nadir Yilmaz examines how new smart technologies can help meet the demands of the transition while building new levels of resiliency

by Nadir Yilmaz

The cloud revolution and other trends such as Software Defined Networking (SDN) and the Internet of Everything (IoE) have had a dramatic impact on the data centre landscape. The demand for centrally managed IT capacity has led to worldwide data centre space expected to grow from 1.58 billion square feet in 2013 to 1.94 billion square feet by 2018 according to IDC [1]. Yet the total number of data centres is actually expected to decline moving past 2017 as internal sites consolidate towards cloud and managed data centre environments. This consolidation poses a challenge. In the data centre of the next few years, the sheer density and complexity combined with growing volumes of IoE sensor data will force management strategies to evolve.

Diversity and complexity

Although many data centres aim to standardise around a single vendor environment, the reality is that many are still undergoing transition, particularly as SDN evolves with no clear defacto standard yet to emerge. To this end, the ability to provide both resiliency and management capability within a still largely heterogeneous data centre is vital.

Across the diversity of network elements including switches, routers, firewalls and traffic management appliances; the commonality of the console port provides known and standardised management interfaces for data centre administrators. Unlike vendor differences between SDN and management software, access through a console port, a technology roughly thirty years old, provides a uniform method for direct control. It also meets requirements for flexibility within the future data centre irrespective of device type or supplier.

Another crucial benefit of this approach is the provision for out-of-band management to enhance resiliency. In many cases, like the recent outages at the New York Stock Exchange, Wall Street Journal and United Airlines, the problems are attributed to vague "technical errors". Yet, a deeper dive into the issues often reveal root causes that stem back to the data centre.

For example, an outage at British Telecom (BT) in 2012 [2] which impacted tens of thousands of internet customers was due to single hardware failure at its Donaldson exchange and data centre in Edinburgh. As BT explained, "The affected router has had stop process restarted and the controlled recovery of the device is being closely monitored. Service should be available within the next thirty minutes. The geographical area of impact is across Scotland, the North of England and Northern Ireland, on traffic that was terminating on this router."

Control without compromise

In these types of instances, devices are often not responsive to commands sent over the normal production IP environment. This type of roadblock is a serious issue for data centre administrators and is the reason for the widespread deployment of Smart out-of-band (Smart OOBTM) data centre management technologies.

Instead of device management running through the production IP network, Smart OOB can also connect via a secure alternative path including Wi-Fi or via cellular mobile 3G/4G connections to provide admins with a direct link to the device and the associated power distribution unit (PDU). This is of particular benefit in remote "Lights out" data centres.

In the router failure example, this would allow a hard reset of the device either through the console or via power discon-

nect and reconnect. This is especially critical within the larger consolidated data centres with square footage in excess of a million square-feet where physical access to racks is a time consuming hike. Smart OOB also provides more granular troubleshooting such as rolling back of firmware, configuration changes and corrupted routing tables which are often a root cause of failures.

More power, less people

However, as density and complexity have grown, staffing levels have dropped. For example, Facebook's new 300,000 sq. ft. data centre [3] is run 24/7 by just 35 permanent staff or roughly 1 worker per 8,500 sq. ft. /790 m². In new "lights out" data centres, staffing levels are even lower. The result is that data centres are becoming more automated with designs that constantly check the health of critical elements along with automated fault resolution. It's not just regular polling of devices through methods like SMTP, but more sophisticated policy driven automation that carries out remediation or even preventive failover based on indicators. For example, if a device started to exhibit a higher number of errors of performance logs or latency, automation may well promote an alert and call for administrator intervention well before an anticipated failure.

Yet as data centres become denser and more highly automated, administrators need to pay more attention to the factors behind outages and look at technologies to improve underlying resiliency. Over the last two decades, the reliability of IT devices has dramatically improved with Mean-Time-Before-Failure (MTBF) rates for the popular Cisco Catalyst 6503-E offering over 860,000 hours MTBF [4] as just one example.

Yet, the improved reliability is subject to a number of factors of which operating environments is one of the most crucial. Alongside well understood variables such as operating temperature and airflow, data centres are increasingly charged with monitoring other environmental issues such as humidity and physical security. Issues such as liquid coolant leakage from fractured piping or blocked venting can cause environmental factors that make failures more likely.

This has led to more Smart OOB solutions equipped with sensors that can alert operations teams to issues based on single events and longer term trending such as humidly, airflow and even movement. Sensors also provide validation around whether a rack has been opened and if physical tampering, either authorised or not, has taken place. In combination, this level of intelligence can detect and in some cases auto remediate so that minor issues can be fixed before they become service disrupting outages.

Single pane reduces pain

In much the same way that data centres are built with device and data path resiliency, Smart OOB effectively provides a resilient management and control framework that sits outside of the production environment. Yet, a key best practice recommendation is to ensure that the alternative control path can integrate alongside existing management platforms such as SolarWinds, Nagios and others. So although the network admin can be assured unrestricted and independent access, control and audit of critical data centre infrastructure; the resilient Smart OOB platform is still tied into the already familiar network and data centre management tools.

These benefits also play well with the final factor that underpins data centre resiliency, people. According to a study conducted by Quorum for its 2013 Disaster Recovery Report [5], the top two causes of unplanned downtime were hardware failure with a massive 55% followed by 22% due to human errors such as incorrect implementation, failed upgrades and misconfiguration. One of the fundamental benefits of Smart OOB is its ability to maintain continuous and verified audit of changes to devices made via the console. In addition, these changes are indexed by operator, time, data and actual change to allow for both understanding of root causes and for the rapid rolling back changes.

The additional benefit is that the technology provides a uniform audit across multiple types of devices and enables vendors to create a single source of authority that is also resilient against outages by means of separate out-of-band connectivity.

As data centres head into 2020, the pressures of increased density, fewer staff and more complexity will require operators to become smarter and more pro-active. The advances in Smart OOB are responding to the challenge and helping to build the next generation of true resiliency.

Nadir Yilmaz joins Opengear as Sales Manager for Central and Eastern Europe, Nadir brings a wealth of channel experience having previously worked for Moxa Europe as Channel Sales Manager Eastern Europe and previous to that as Channel Manager for Central and Eastern Europe and Baltics for Axis Communications. Founded in 2004, Opengear delivers next generation intelligent solutions for managing critical IT and communications infrastructure.

References

[1] https://www.idc.com/getdoc.jsp?containerId=prUS25237514

[2] http://www.theregister.co.uk/2012/12/13/bt_outage_edinburgh_newcastle_preston_glasgow/

[3] http://www.greenbiz.com/blog/2012/06/06/turning-good-data-centers-better-neighbors

[4] http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/data_sheet_c78-708665.html

[5] http://oneclick.quorum.net/disaster-recovery-report-quarter-1-2013-step1.html