NOV 2018

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the November 2018 edition of In the Boxing Ring

Back in the September 2018 edition of *In the Boxing Ring*, we talked about logging options available for the upcoming NBSIEM+ services. Moving on, this month, we talk about **Event Logging at Big Data Scale**. The issue of log storage and retention is deceptively simple. The general perception is that it is trivial to just store the events 'on a disk somewhere'. However, there are several key issues that must be addressed for event logging at Big Data scale. On pages 2 to 4, we discuss this in greater detail.

On page 5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

In other news, due to the recent Cathay Pacific Airways data breach, Network Box was interviewed by numerous media outlets including: **Cable TV**, **ViuTV**, **RTHK Radio 3**, and the **SCMP.** In addition, Network Box Hong Kong was at the **Cybersecurity Consortium 2018**, and the **AustCham Cybersecurity Forum**. Furthermore, Network Box USA's Pierluigi Stella was a guest speaker at the **HIMSS 2018** conference. And finally, Network Box Germany, and Network Box Singapore, were at **IT-SA 2018**, and **Cloud Expo Asia 2018**, respectively.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
November 2018

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://plus.google.com/u/0/107446804085109324633

In this month's issue:

NETWORK BOX

NBSIEM+

Event Logging at Big Data Scale

In the September 2018 edition of *In the Boxing Ring*, we talked about the client-side logging options available in the upcoming **NBSIEM+** service. This month, we expand on the server-side (cloud) storage of these events, and options available for log retention. This article is highly technical in nature, and describes the implementation of the data storage sub-systems in NBSIEM+.

The issue of log storage and retention is deceptively simple. The general perception is that it is trivial to just store the events 'on a disk somewhere'. However, there are several key issues that must be addressed for event logging at Big Data scale:

1. **Scalability**
2. **Reliability**
3. **Integrity**
4. **Affordability**
5. **Searching**

Let's talk in detail about how NBSIEM+ addresses each of these key issues.

NETWORK BOX

1. Scalability

The storage system must be scalable. In particular for a multi-tenanted cloud system such as NBSIEM+, that means the storage must be horizontally (not just vertically) scalable. We address this issue by firstly offloading the processing of data to a cluster of machines. We do as much pre-processing as possible on the thousands of Network Box devices doing the actual submission of data (including geo-ip mapping, meta data annotation, formatting ready for NBSIEM+, etc). Then, we receive the event logs on a load balanced cluster of servers which add authentication and integrity meta-data, prior to submission to event log storage.

At storage stage we use the big data technique of '***sharding***'. One day's worth of data, may (for example) be split into 100 shards by a cryptographic hash algorithm, with the algorithm being applied to each incoming event record, to direct it to a particular shard. Each shard can then reside on a different physical server, or each server can be configured to handle multiple shards. We can configure from one server handling 100 shards, to 100 servers each handling one shard. And if we need more horizontal scalability, we simply increase the number of shards. This technique works well both for storing (including indexing) data, as well as searching; a query can be split, distributed, and run concurrently on the entire cluster; increasing the speed by a factor of 100 or more.

NBSIEM+ also supports the concept of geographic clusters. We configure each device to send it's logs to one particularly regional NBSIEM+ cluster, but provide global search-ability.

2. Reliability

The event logs must be reliably stored. That means high-availability storage not reliant on a single individual component, as well as backup. The sharding system helps here as well in that we can configure replica shards to be stored on different servers. As we distribute our servers across different racks (with different power and networking environments), the sharding system automatically ensures that redundant replica shards are stored on servers in different racks. In this way, should one power or network system fail (taking down one rack), the overall system should still remain operational as the replica shards can take over.

NBSIEM+ also utilises snapshot storage, to take regular snapshots of the shard storage, and keep them available as disaster recovery backups.

3. Integrity

One advantage of event log storage, compared to a traditional data storage requirement, is that the event log records should never change. In fact, we want to ensure that they never change (or are maliciously or accidentally tampered with). To do this, we cryptographically sign each event log record as it is written to storage. When we retrieve these events, we can then verify the cryptographic signature to ensure that the record is unchanged. We can also periodically pass over the entire historical storage, verifying each record, to provide pro-active alerts to tampering activity. This system is designed to meet regulatory requirements for data integrity compliance.

4. Affordability

The price of data storage depends primarily on access speed; the faster the access, the higher the cost. For a system like NBSIEM+, with log retention requirements (including scalability, reliability, integrity, and search-ability), this is critical. We address that, and keep costs affordable, by utilising tiered storage.

When the event logs are first received, they are tagged as *'hot'*, and directed to storage of that 'hot' class. Typically, this means a large number of servers, each storing a small number of shards, and using the fastest (and most expensive) storage such as directly attached SSDs. This storage cluster stores the latest, and most often accessed, data and allows for the fastest retrieval times (measured in milliseconds).

After a few weeks, when the data is not required to be accessed so frequently, it is re-tagged as *'warm'* and automatically migrated to slower storage (typically using hard disk technology). A smaller number of servers exist in this cluster, each storing more shards and more data, to keep costs down. This data is still online, readily available, and still accessible at sub-second speeds.

Those first two tiers comprise the standard offering, and are able to store event logs for several months (depending on service commitment). For customers who require longer-term log retention, a third layer is optionally available. Here, specific log entries are migrated to *'frozen'* storage. This still maintains indexing information online (for quick searching), but the event log records themselves are moved offline to the most affordable storage available. While searches are online and quick, should the actual detailed event log data be required, it must be brought back online (a process that typically takes several minutes).

Using these three tiers of storage, NBSIEM+ balances affordability against availability.

5. Searching

Data indexing and search capabilities are at the core of NBSIEM+. We require fast rich searching across a variety of data types. The core indexing engines support not just full text searching, but understand basic data types such as numbers, as well as more complex types such as geo location points, and IP addresses. This means searching not just for simple individual items (such as a country, or a host name) but rich searching such as all IPs within **202.52.42.0/24.** These searches are, of course, available across all devices submitting their logs to the NBSIEM+ clusters.

Conclusion

The issue of log storage and retention is deceptively simple; but meeting the requirements of scalability, reliability, integrity, affordability, and search-ability, is not. By using the latest big data technology, and cloud infrastructure, NBSIEM+ meets these requirements. We've designed NBSIEM+ to meet the most stringent log retention specifications for ISO, PCI, and SAS certifications, as well as international data privacy regulations.

So far, in beta testing, we've pushed approaching a billion live event log records through NBSIEM+, as we continue to prepare for the upcoming launch.

NETWORK BOX

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th November 2018, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
November 2018

This month, for Network Box 5, these include:

- Improvements in license status control and display
- Enhanced gateway failover, to choose highest weight backup gateway on primary link failure
- Improved performance and reliability of push signature downloads
- Enhanced support for mail server header checks, including removal/sanitising unwanted headers (for PCI compliance and others)
- Decrease the minimum update interval for host ACLs from 1200 to 60 seconds
- Improved display of IPSEC tunnel status
- Enhanced support for host name destination NAT (as an alternative to host IP) in proxy configurations
- Enhanced support for configurable transaction bypass rule support in mail and web protocols
- Improved support for STARTTLS ssl interception in IMAP4 protocol
- Improved handling of HTTP error code 100 in web protocols
- Support for uncategorised websites in nb-productivity ACL
- Enhanced support for LDAP, Radius, and other such authentication protocols, in Admin portal
- Introduction of experimental support for pure NTLM v2 in directed web proxy
- Support extraction of envelope recipient in IMAP4/POP3 protocol used by Exim and other similar mail agents

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

NETWORK BOX

Network Box HIGHLIGHTS

BizIT Excellence Awards 2018
Unified Threat Management Managed Security Services

Network Box is extremely pleased to be able to announce, that the company won **BizIT Excellence Awards**, for outstanding performance, in both the, 'Unified Threat Management,' and 'Managed Security Services,' categories.

Network Box Hong Kong
VTC Visit

Network Box was visited by Professor Simpson Poon, and Ir Dr Joseph Leung; accompanied by Terence Yap, GuardForce's CEO, to discuss possible cooperation on cyber-security, as well as the protection of smart devices, and the Internet of Things (IoT).

Network Box Hong Kong
Cyber Security Consortium 2018

Network Box was at the **Cyber Security Consortium 2018**, held at Hong Kong Police Headquarters, where this year's main topic was, *'How to survive in the volatile and ever-changing cyber world.'*

Network Box Hong Kong
AustCham Cybersecurity Forum

Network Box took part in the **AustCham Cybersecurity Forum**, which was held at ICBC Tower, in Hong Kong.

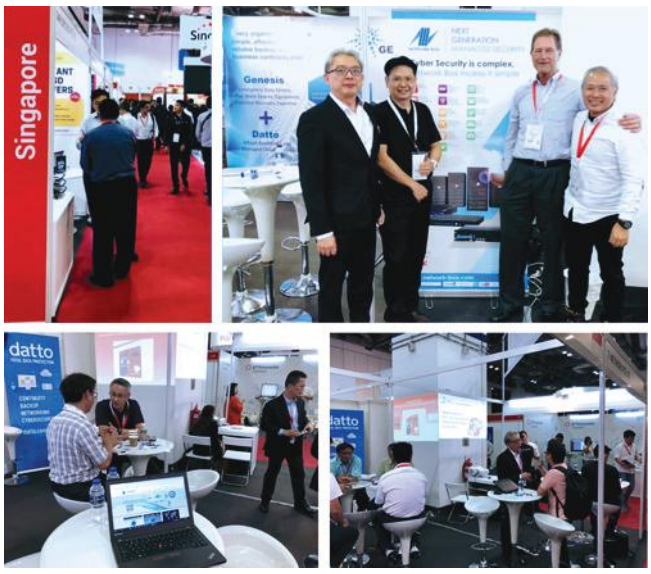
Network Box HIGHLIGHTS

Network Box Germany
IT-SA 2018

Network Box Germany, in association with partners, Digitrace and Sicdata, exhibited at **IT-SA 2018**, held at the Nuremberg Exhibition Centre, in Germany. IT-SA is Europe's largest expo for IT security, and highlights the latest in cloud, mobile, cyber security, data, and network security.

Network Box Singapore
Cloud Expo Asia 2018

Network Box Singapore was at **Cloud Expo Asia 2018**, held at the Marina Bay Sands Convention and Exhibition Centre, with Premium Reseller: 7 Network; and Collaboration Partners: Genesis Networks, Poytech Component, BDT Singapore and Zero1



Network Box USA
HIMSS 2018 - Houston Chapter

Network Box USA's CTO, Pierluigi Stella, was a guest speaker at the **HIMSS Houston Chapter's Lunch & Learn** seminar, held at Mays Clinic, in Houston, Texas. Aptly entitled, "Compliance Strategies to Reduce Cyber Risk", Pierluigi Stella talked about the dangers of Ransomware and Cryptomining.

Network Box
Media Coverage

In light of the recent Cathay Pacific Airways data breach, Network Box was interviewed by numerous media outlets:

CABLE TV

Network Box's Managing Director, Michael Gazeley, was interviewed at **Cable TV**, by their Hong Kong International Business Channel (HKIBC) presenter, Isabel Wong.

Link: https://bit.ly/2zwtgGk

viuTV

Network Box's Managing Director, Michael Gazeley, was interviewed on **ViuTV News**, by their news anchor, Diane To.

South China Morning Post

Cathay Pacific data leak: airline warns customers to guard against phishing attempts

Link: https://bit.ly/2AL3W1g

Cathay Pacific data leak: what can customers affected do to protect personal data and get redress?

Link: https://bit.ly/2ALCHUa

Radio3

RTHK Radio 3

Backchat
with Hugh Chiverton and Danny Gittings

Link: https://bit.ly/2D65UuM

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Kevin Hla** Production Support **Network Box HQ** **Network Box USA** Contributors	Network Box Corporation nbhq@network-box.com or via mail at: **Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong Tel: +852 2736-2083 Fax: +852 2736-2778 www.network-box.com

NETWORK BOX