2021-08-23 Spectrum data meeting with Doris Paquin

# Summary

* Spectrum is a monitoring tool using SNMP data
* Doris has provided us some sample export data in CSV format
* Doris thinks its unlikely that this data will help us infer device health / predict failure time.
* Spectrum data is linked to ECD incidents when applicable, referencing ECD ticket numbers
* Some LAN topology is available, but sometimes is scattered between Spectrum servers.
  + “TADDM” is another topology discovery tool; Talk to Martin Pichette (NS branch)
* The Spectrum data is current only, not historical.
  + Unique rows: counts of X event per Y device.
* Once a device is removed/decommissioned, it is removed from Spectrum
  + Some data kept in “Report manager server” for 1.5 years
* Action items:
  + Look at sample data; optionally follow up with Doris for questions (Thursdays best)
  + Contact Martin Pichette re: TADDM topology tool
  + Contact ECC – Jack Chin (onboarding for alerts)

# Notes

Doris:

* Spectrum: monitoring tool
* Log SNMP get/trap from the devices
* Integrated DBs on the spectrum servers (MySQL tables; NODB)
* Switches, firewalls, etc. in certain data centers: Gatineau, Barrie, Montreal..
* Currently onboarding SMnet
* CE: Customer Edge router. Sites are being migrated to a new network “GCnet”.
* Some alerts can be cleared manually, while others require the issue to be resolved before being automatically cleared

Olesia:

* We’d like to predict when a device is likely to fail.

Doris:

* Not much in Spectrum re: device health.
* There is SNMP data for example “interface flapping”
  + Rare, and doesn’t necessarily indicate interface is about to fail
* Unable to determine why a device was decommissioned other than look at ITSM data (ECD)

Olesia:

* Can we get a sample ?

Doris:

* We can do an export. We have device serial numbers.
* Sample data going back until 2014.
* (Doris begins demo of Spectrum console / data)

Olesia:

* Is “criticality” manually entered? What does that represent?
* (note: not sure of what the answer was)

Peggy:

* Linking with ECD?

Doris:

* Tickets get created in ECD automatically through “ECC”. (Enterprise Command Center)
  + based on Critical and major alerts
* There is a field for the ECD ticket number in Spectrum, *Trouble Ticket ID*
* We have topology discovery for some LANs. (graph of devices and connections)
  + (Olesia note: Seems more complete than that of “Legacy” Spectrum.)
* “TADDM” is another discovery tool for topology; its under NS branch. Talk to Martin Pichette.
* SMnet has no topology. The firewalls are all connected to switches somewhere, but on a different server. (Different Spectrum server?)
* GCnet also has no evident topology; we cant “reach behind” that single router.

Doris, explaining columns:

* Number of Switches: stack of 8 switches configured with 1 IP is considered one device in Spectrum. So this device would have number of switches = 8
* Creation time: date added in Spectrum
* Condition: If critical, it doesn’t necessarily mean it is down.
  + This could be a configuration issue, or another related device is down, or an alert about e.g. device running out of disk space.
* Occurrences: Shows how many times the event occurred. “trap based”. It’s an integration with Vsphere.
* Type: System Edge Host = server
* Trouble Ticket ID: should correlate with ECD incident number

Olesia:

* How can you tell when a device was decommissioned?

Doris:

* That would be in ECD. We would act on a ticket from ECD that said to remove a device.

Peggy:

* Does that data get deleted, once the device is removed?

Doris:

* Yes, but it is still in another server. “Report manager server” – for 1.5 years
* Data is not historical; it is current as of the date and there is no record going back in time.
* Name + Alarm Title is distinct**.** There can be more than one Alarm Title per device (“name”). All occurences of that alarm title for that device are aggregated (occurrences count).

Jules:

* Is there anything that you think would help us infer device health in here?

Doris:

* There really isn’t anything that would help determine device health from this data in Spectrum. Maybe in ECD.
* Device errors are not necessarily indicative of device failure
  + neither is failure to obtain device status during polling.
  + ECC is not always made aware of changes. As such, it is not uncommon for alerts/alarms to go off due to a scheduled change.
* There were recently some switches replaced but you would never know that anything was wrong from the Spectrum data.
* I keep the same IP and hostname when we change servers. But Spectrum won’t pick up on a new MAC address, so I don’t always know when things have changed. Asset profiling will pick up on new serial number.

(Doris exports several CSVs to send to us)

* Doris availability is typically best on Thursdays
* Plan to deploy spectrum on the SSC's CMN. No timeline given.
* Try contacting ECC – Jack Chin (onboarding for alerts)