2019-03-24 OpenU on site visit

Sunday, 24 March 2019 12:42

- A lot of traps received. Customer asked for a report to show problematic ports.
- Devices are constantly revalidated. With assistance and recommendation by Vadim we disabled "Enable under authentication ports patrol".
- Compliance failures: **TFS 49904**
  - Classroom computers are restored to image every restart and thus fail compliance until anti-virus is updated again (every few months the image is updated)
  - Compliance failure due to timeout seems to trigger "not updated" / "not running" / "not installed" and thus executes reaction.
- QFX5100 mapping is incorrect - mapped as switch instead of IAF (Yoram claims to have mapped it in the past as model 62)
- Add Switch takes very long time - 1.149.225.112 (~15 minutes), reprobes take few seconds to ~ 150 seconds at times.
  - Need to understand if probes are failing
  - Recommended setting for switches:
    - Timeout: 30
    - Retries: 2
  - Recommended setting:
    - Reprobe interval: 300
- Authenticator stuck for more than 2 days. Logs collected which indicate thread failed to kill wmi. **TFS 49905** updated with info and logs

NG Experience feedback:

- Newnox does not allow export/save of port history
- Newnox graphics:
  - Switch logo looks horrible - not placed correctly (indents ports)
  - Important details (port and device details) are displayed in small windows where switch is not important and displayed on almost entire screen.
    Windows/frames cannot be resized or "unpinned"
  - In switch stack, unit numbers are not shown in unit section (only in port desc.)
  - Error message on UI timeout (connection with Portnox server could not be established) is horrible.
    - Should indicate timeout (as warning)
    - This error is displayed sometimes with no reason (no action taken)

2019-04-18

Monday, 25 March 2019 17:46

- Customer updated that during upgrade, process got stuck, attempted to roll back failed and eventually was able to complete.

- No backup executed prior upgrade
- Upgrade logs not checked or collected
- 2019-04-16 11:06:34 service started after upgrade
- 2019-04-16 11:07:49 service failed to start
- 14 additional attempts to start service
- 12:07 start succeeded (no logs written)
- Current version: 3.37

- 2019-04-18 10:00
  - Set enforcement off
  - Restart service
  - Logs started to be written
  - Repeating snmp exception at service start process
- 2019-04-18 10:14:06 Services successfully started

- Matias:
  - Open TFS for Juniper port order reset to 0
  - Open TFS for service does not start

- Blum
  - Send internally summary of issue

- Snmp (only v3?) are now run in linear instead of parallel
- Logs are sometimes written not in time order
- Juniper switch attempt to set (enforce?) using snmp at start after upgrade - need investigation - 1.3.6.1.2.1.1.4.0

2019-04-29 On site visit

Monday, 29 April 2019 10:24

- Complaint of ports displaying as Red or Green with no mac while device is connected.
  - In a call with Yoram, he was not sure a device is connected behind the port
  - We followed ports on switches according to Yoram's instructions and found all ports with issue show a display issue (state up + Red/Green) instead of WOL but NO device exists behind the port
  - Issue known and fix will be provided at **TBD**
- Customer explained compliance checks are urgent for him.
  - Classes where compliance limited is needed can wait (less urgent)
  - **Compliance false positive is urgent for the rest of the networks**
  - Current compliance status shows only 3 devices not complied outside classes. All statuses shown were confirmed to be correct.
  - **Need to define plan to set enforcement for compliance check**
- Collected logs to verify fixes planned are aligned with issues specified above
- Enforcement was set for the system as requested by customer

- Switch communication recovered does not update the red indication until page is refreshed

2019-05-08

Wednesday, 8 May 2019 9:12

- Logs stopper writing after 1 day. Need to validate fix.
- Yellow ports under auth instead of WOL
    - Hub fixed but still 4 ports in yellow
    - Matias to open child TFS
- Linkup/down threads
    - Increased amount of threads from 15 to 20
    - ID in monitor all have ID 9 instead of unique index
    - After restart, all threads busy for a long time even though there are no "real" link up/down
    - Logs show link up load every 1 minute with increase in number of events per 1 minute
    - Observed link up ignored due link down at later time - seems there is a blinking phenomenon (internal)
    - **Found a port with 804 traps sent within 1 hour. Customer disabled port.**
- Port state down instead of up with device
    - Believe lack of Linkup resource (thread) due to high load of events (blinking ports?)
- Long probes
    - Increased reprobe interval from 180 to 300
    - Probes seem to complete within consistent time after change
    - Collected logs in trace
- Compliance failures found 7. Need to coordinate with customer to locate those that are false positive if any.

- Large hive crashes/stuck UI when opened

- Matias will create a script to extract port with high hits of traps
- Reopen bug of settings not loading mandatory params: Max and Min device connected to hub ports - thus failing to set settings

2019-05-18

Thursday, 16 May 2019 11:52

- Hive doesn't open in IE only - Chrome and Edge work fine
- Compliance failure verified (2 devices other than classes)
    - 1 XP requires configuration update - will be done by customer and integrator
    - 1 device (NOIDER) waiting verification from customer
- Authentication details (of device) opens empty
- Device Details opens NAS Device view instead of device details page
- Device Details (opened from NAS Device view search MAC and open in same tab) - device information disappear and left empty
- Switch down although up - lock issue of get all macs - fixed on site
- Hotswap - system did not start after replaced exe. Rolled back private fix.
- Could not load utilities dll (replaced in previous private fix)

- WOL ports are checked and defined as linkup even when no trap is sent and between probes
    - We have internal processes which check WOL ports continuously for WOL timeout. **WHY????** What is different from converged port with only IP Phone?
    - WOL port blinks for a while until displayed as WOL

2019-06-03 On site visit

Monday, 3 June 2019 16:12

Goals:

- Install build to address compliance fallback to remote registry when wmi fails
- Fix Set VLAN failure

Summary:

- Build was not deployed due to critical bug found by Matias before leaving the office
- Dll to address SSH issue and prompt configuration believed to cause set vlan failure was deployed
- Several issues still exist causing set vlan to fail. All issues are new to the environment following change of Juniper switches to NOT keep alive
- Customer is waiting for following 3 items by priority:
    - Fix for set vlan
    - Build to allow compliance check failback to remote registry (enforcement on compliance is pending this build)
    - Powershell script (created by Matias) fine tuning to show relevant blinking ports only (exclude internal link up events created in Portnox for WOL ports)

2019-06-12 On site visit

Monday, 3 June 2019 16:12

Summary:

- Build was deployed
- Compliance check fallback to remote registry was rolled back and will not be deployed.
    - Roll back due to all compliance checked failed (false positive) after fix deployment
- Fixes deployed:
    - Fix for set vlan
    - Powershell script (created by Matias) fine tuning to show relevant blinking ports only (exclude internal link up events created in Portnox for WOL ports)
- System status is good
    - 0 yellow ports observed
    - ~10 compliance failures in classes (expected due to image restore at reboot)
- 2 minor issues:
    - Correct behavior but slow reflection in Portnox:
      1 specific port disabled and then enabled took a few minutes to display correct status but device was checked, found rogue and port disabled by system (followed by technician setting port as rex)
    - Some switches do respond to SSH connection request until 3rd attempt.
      Portnox overcomes it by retry mechanism but issue should be checked from network aspect (switch/communication)

2019-06-12 סטטוס או"פ

15:23 Wednesday, 12 June 2019

נושאים שטופלו:

- סדר הפורטים - תוקן
- תקלה של מערכת לא עולה לאחר שדרוג - תוקן
- Thread תקוע - תוקן
- בדיקות :compliance
  - כל התקלות הידועות בנושא תוקנו
  - תחנה אחת נמצאה עם WMI לא תקין. המחשב הוחלף.
  - כיתות לא יכנסו לאכיפה בגרסת המערכת הקיימת מכיוון שהמחשב עולה מ IMAGE
- QFX5100 טופל ע"י הגדרות ומיפוי
- FALSE DUPLICATE MAC - תוקן
- סטטוס מתג DOWN\UP בהיראכית HIVES - תוקן
- בעיה בכתיבת לוגים - תוקן
- פורטים ב WOL מוצגים בסטטוס לא נכון - תוקן
- פורטים HUB המוצגים כצהובים - טופל ע"י עדכון הגדרות
- עומס על המערכת הגורם לסטטוס לא מוצג - סופק סקריפט למציאת פורטים מהבהבים אשר טופלו ע"י הלקוח.
- PROBE ארוך בחלק מהמתגים - הותאמו הגדרות מערכת
- 2 שדות חובה ב NG - תוקן
- מתג סיסקו שאיבד קשר לפורטנוקס - תוקן
- Device details נתונים לא נפתחים תקין - תוקן
- מתג ג'וניפר מהבהב עקב כשלון במשיכת נתוני פורטים ע"י פורטנוקס - מתג ענה בצורה חלקית. הסתדר לבד בביקור הבא
- כשלון ביצירת סשן מול מתג עם זמני תגובה איטיים יחסית - תיקון הגדרות על מנת שימתין ל prompt
- פורטנוקס לא מזהה כישלון ומציג סטטוס לא נכון - תוקן

נושאים פתוחים:

- איטיות \ עיכוב בהצגת סטטוס פורט בזמן טיפול בתחנה ע"י תהליך PROBE ו LINKUP במקביל
- חלק מהמתגים לא עונים בבקשת סשן SSH ורק לאחר ניסיון שלישי נוצר הסשן