2018-04-24 - Summary by Ran

Wednesday, May 2, 2018 19:35

1. Most of wireless devices are in constant 'not authenticated' state. Manual revalidate release it, tried to add registry key that maybe will improve that.
    - **Pending update from customer and then analyze logs to understand root cause**
2. One server that is being used for IIS only is not stable - seems DB connection issue. Not that important, will try different server with better latency.
    - ☑ Server is removed. Remote servers will not exist and be managed locally in San Jose.
3. Windows devices moved to phase not getting new ip address in phase vlan. Probably related to wait time but not sure. Customer update the timeout to 7 seconds and check.
    - Need to setup Palo Alto as IP Helper to get ARP for the phase vlan
4. Devices that passed authentication in the past failed (probably due to domain user lockout, which lets say ok for now) but not change to limited but to rogue - need to be limited.
    - Recommend to set Never Lock and reduce back authentication limited from 45 days to 1 day
5. Very often receive message of - system currently experience DB issues - please try later. And cannot execute actions. Need to collect logs and investigate.
    - **Need to investigate logs**
6. There's request to use DHCP FP as part of the signature mechanism. They said Ofer mentioned we should have that soon. Need to check with product management.
    - **Send an email to Omer - Bug 26283:Add DHCP fingerprinting to Portnox FP mechanism**
7. When try to move port back to the LAN from the phase, on converged mode, the process is not clear - what happen with the ip phone, POE vs. shutdown on HP switches.
    - **Need to test (Blum to check with Omer/Vadim/Lab)**
8. Takes a lot of time to identify devices on port. Might be related to traps configuration but probably not, need to check if display / refresh or service issue.
    - **Need an example with the following:**
        - Details of Device, switch and port
        - Exact time device was physically connected to the port
        - Logs to check:
            - Time we received the trap
            - Time search thread started and ended
            - Time Authenticator opened
            - Time authenticator ended
        - Time updated in UI
        - Is NG Experience behaving the same?

2018-05-01 - Summary by Gordon

Wednesday, May 2, 2018 21:28

Maxim – May 1 -2018

Maxim – May 1 -2018

Status: Rolling out enforcement to remote locations. India, Korea,

False positives on some devices in India. Authenticated limited.

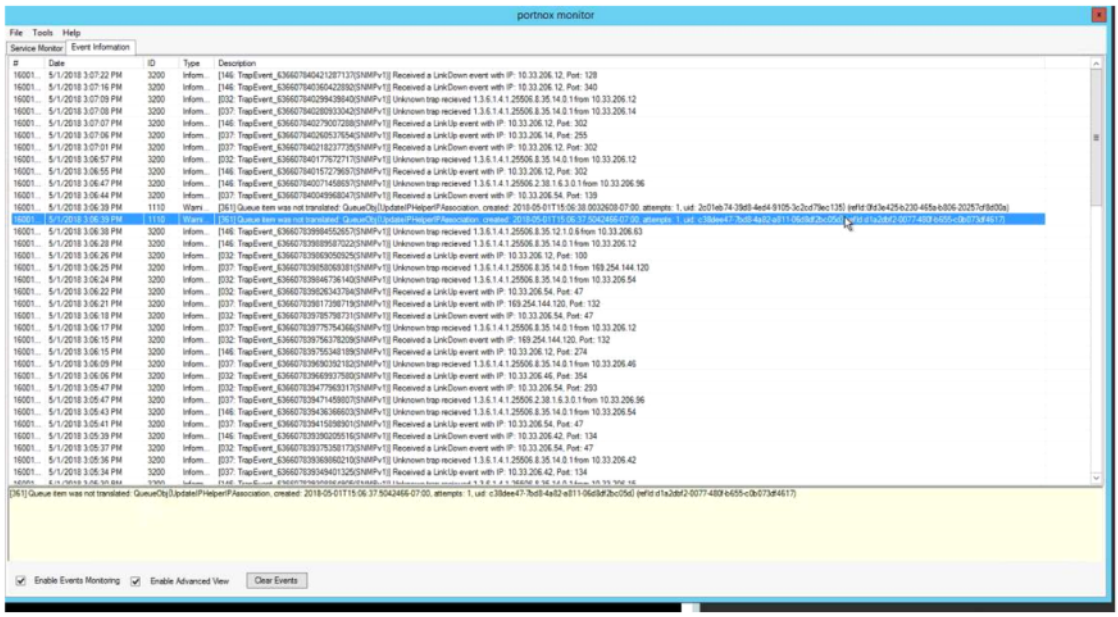
Portnox removed vlan association for large resident group while updating Resident group (problem is not re-creatable)

Internally Documented issues (by Danny):

a) Not Available
b) Authenticated windows WMI-Registry→ Wrong credentials
c) Authentication windows WMI -WMI Failed – wrong credentials not authenticated
    a. Could not use WMI to authenticate, ports are closed: 135 → did not use Windows WMI auth
d) Could not use registry to authenticate, ports closed: 139, 445 did not use windows registry to authenticate
e) Registry authentication windows WMI failed → could not get registry subkeys (x2)
    a. Authentications windows WMI-WMI → WMI authentication windows WMI failed: connection error in com windows error code 800706BA (x2)
f) Failed to verify the IP address 10.92.0.201 of the device for 90 seconds. Device is not responding. Can not proceed with authentication process, monitor action is executed.

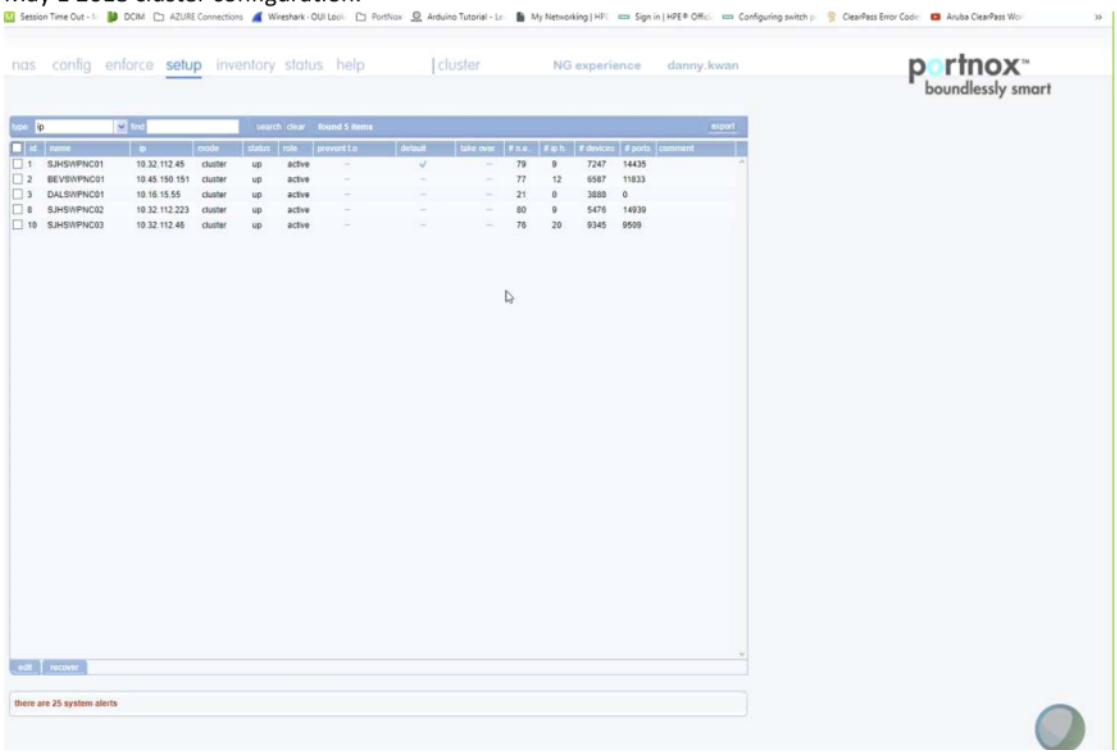
From May 1 session

1) Request for Aruba Wireless controller to support ACL creation/addition to MAC blocking
    a. Wireless issues
2) Large database transfers from remote Cluster servers (Dallas + Beaverton) to Azure DB server
3) Primary KEY error – many times
    a. [007: DBAccess] There was an error with the SQL statement. (refId:f49804eb-ed57-4187-81d4-685e2ce17a32) [Message: Violation of PRIMARY KEY constraint 'PK_pnConfRL_DeviceInvApp'. Cannot insert duplicate key in object 'dbo.pnConfRL_DeviceInvApp'. The duplicate key value is (15800, 274).The statement has been terminated.]
4) Queue item was not translated (below)
5) Asked to collect logs and upload
6) SNMP host trap settings in many switches needs to be updated to send to active/current server



Check Queue depth?

May 1 2018 cluster configuration:




edit
recover
there are 25 system alerts
ENG
3:12 PM
5/1/2018

2018-04-01 Maxim

Monday, 1 April 2019 10:49

- **VLANS deleted from resident group - suspected to occur when 2 users update group at same time**
  - The BUG of removing/blanking " Allowed VLANs" when updating Large resident groups can be reproduced internally using Portnox Classic Gui and large resident groups when two Portnox servers or even two portnox users are active on the same resident group at the same time. This is a behaviour we identified that Maxim was doing quite often and they were to stop accessing the same resident group simultaneously from two user accounts (servers) or use the NG GUI.

    Bug 44530:VLAN information is deleted from resident group in database when group is open and another user updates - HF8

- FP is completely different when ran from different enforcers

Bug 50410:Main service do not start on cluster environment because of N.E miscommunication between servers - New
Bug 50434:Failover to Monitor system to monitor in DB and in current enforcer but does not update other enforcers which continue to enforce - New

Bug 48047:Add HSRP and similar protocols false positive prevention system - HF8

Bug 48154:HP 5500 Switch - Maxim- Version 3.33 on Phase Set vlan removes Default VLAN from Permitted vlan - logic is incorrect.racheli i added reconstruction bug from DF - HF9
Bug 48158:HP 5500 - Maxim - Switch - Phased Port with Phone will not return to default Vlan - Need More Info. pending for 2 months
Bug 48153:HP Switch 5500 - MAXIM - Access ports cannot Enter LAN after Phase - Need More Info. pending for 2 months

2019-04-01 - Management meeting

Monday, 1 April 2019 20:21

- Resident group edit deletes all vlans
    - Maxim seen 2 different scenarios for this issue. Need to verify. Edit by same user in 2 different pages (nas view and group)
- **QA margin - love the product but scared to upgrade as quality is not done very well.**
    - **New code brings new issues**
- FP different between enforcer - take offline for Gordon to check
- Return to lan
- Multiple Phase vlans - expected within this Q
- Email fields are limited in length. Need to check if this is enhanced in newnox
- Failover to monitor - lower priority than vlan but will be attended and planned for 3.38 (hf9)
- Hard coded timeout in UI
- Security module in newnox to deny set rex port is required
    - Raise to PM to see if we can provide this feature in classic or provide newnox

- Enforcement set last Friday but critical systems are not monitored by Portnox