

# Service crash and backup failover

Thursday, October 20, 2016 10:39

- Ran is the technical lead
- Meeting with Taldor

# 2016-10-25 - Taldor meeting

Tuesday, October 25, 2016 13:54

**issues with crashing service on 1 server and failover to backup server not succesfull in some cases**

שלום רב ,

בהמשך לדיון שהתקיים בחצרות הבנק בעניין מערכת NAC של חברת פורטנוקס :

השתפו בדיון :

פורטנוקס – עידן קופרמן, עידן בלום, רן פריברג.  
 טלדור – רפי הירש, איתן חן, רינת מרקוס, אנה בול.  
 בנק דיסקונט – סמורי צח, איציק מאור, רפאל ששון, סימחוב ולרי .

בפגישה תוארו תקלות ואירועים שאנו חווים במערכת NAC של חברת פורטנוקס באופן רציף בתקופה האחרונה .

**להלן עיקרי הדברים שעלו בדיון :**

1. לקיחת פיקוד של שרתי גיבוי ( באתר גיבוי מדד 1 ) ללא הבנה מושכלת למה זה קורה וללא יכולת תיחוקור כיוון שאין תיעוד ( בפגישה הועלתה השערה על ידי עידן קופרמן מפורטנוקס על כך שיש עומס Thresholds על המערכת . מכיוון שזו השערה יש לבדוק את הנושא לעומק )
2. קריסת שרות – Winpcap הדבר המייצר חסימת פורטים של מערכות עם FP ובנוסף גורם למצב של חוסר איכפה של מתגים על ידי השרת שבה הוא קרס .
3. הכנסת מתגים By Default ל Default Enforcer מייצר מצב של חוסר איזון במערכת . יש לבדוק אפשרות האם ניתן לייצר מצב בו נוכל לבחור את השרת שינהל את המתג
4. מתגים יוצאים ממצב איכפה – לוקח זמן רב ופעולות תחזוקה רבות כדי להחזיר אותם למצב איכפה .
5. הפסקות חשמל – במקרים של הפסקות חשמל מתגים לא מגיבים לאירוע בצורה שקופה , ישנן אירועים של חסימות פורטים רבות.
6. ביצועי מערכת איטית , כל פעולה לוקחת זמן והמערכת מגיבה לאט.
7. סטטוס פורטים – מערכת מדווחת על פורט שהוא ב Down , מבדיקה על המתג הפורט מראה UP .
8. מקרים בהם Device כבוי או מנותק , המערכת לא מצליחה למצוא את הפורט האחרון אליו היה מחובר .
9. מקרים בהם חסימת פורטים יותר מהזמן המוגדר במערכת ( 2 דקות ) .
10. שדרוג גרסה – יש לבחון את שדרוג הגרסה הקיימת אצלנו ( 2.4 ) ל update 1 2.5 . ( עידן אמור לתת תשובות לגביי בדיקותו בעניין והאם נכון לבצע את השדרוג לגרסה זו )

**: Action Item**

1. יש לקבוע ל"ז ותוכנית עבודה ליישור קו ולייצוב המערכת בנקודות שעלו בדיון . העבודה תיעשה בשיתוף פורטנוקס, טלדור , מדור תקשורת בנק דיסקונט . מבקש לקבל תאריכים אופציונליים לשבוע הקרוב מכל הגורמים הרלוונטיים
2. שדרוג גרסה – במידה ותתקבל המלצה של שדרוג גרסה היצרן יספק:
  - 2.1 – תהליך מפורט של השדרוג במסמך המציין - צעדי הפחתה , חזרה לאחור , לקיחת גיבויים והתאוששות במידה ושדרוג הגרסה תיכשל .
  - 2.2 – שדרוג הגרסה ילווה באופן צמוד עם היצרן ( פורטנוקס ) בשיתוף טלדור ( אינטגרטור ) .

אראה לציון – בעניינים טכניים וקביעת תאריכים לביצוע הנ"ל אין צורך בהחזרה מייל לכל המנותבים

תודה ובהצלחה.

איציק מאור  
 אבטחת תשתיות וערוצי קישור  
 מחלקת תמיכת תשתיות

**דיסקונט**

הרצל 160 תל אביב, 6810122  
 טל': 03-5158038 | פקס: 03-5153500 | נייד: 052-2461170

## 2016-11-15 (event from 2016-11-14)

Tuesday, November 15, 2016 14:58

### ★ Internal: Current version seems more robust and stable

- Reviewed logs for hotswap with no findings
- Logs were not found for the incident investigated
- >400 devices with duplicate MACs
- Requested to turn off enforcement and set system to monitor before configuration changes
- Started investigation to reduce load of the system
- Uplinks were not marked and thus started marking uplinks manually (technician added the switches without correct configurations)
  - No proper procedure for addign and configuring new switches
- Compliance fine-tuned to match bank requirements. Reduced noncompliance from 5500 to 700 (Revalidated)
- Added 2 configurations:
  - Recover to server 5 from backup server 3 (miscommunicated and customer perceived it after the action taken) ~15:30
  - Dynamic port configuration did not exist at all. Added new dynamic port configuration rule to over 3 vlans and over 20 devices (most uplinks do not have more than 2 vlans)
    - During change the update was communicated to the customer but looking back it seems communication was not clear.
    - Popup with impacted ports is displayed. Marked ports will not be changed (message is not clear). Ports were not marked and popup confirmed. (noticed about 15 ports in the popup table).
  - Activity ended and on the way to the car customer called Jehuda back.
    - Enforcement was disabled by customer.
    - About 100 switches were blocked. (It may be due to a backbone)
    - Disable by policy changed to 6 minutes which opened several switches.
    - Customer sent relevant personnel to enable the switches in management by enabling the port/reset the switch
    - Customer sent people to reset switches at customer branches.
  - Dynamic port configuration rule updated to over 2 vlans only
    - Specific places had issues and were scheduled to be handled in the morning.

### Conclusions:

- ★ Internal: We did not realize the wide system impact as in general from past experience removing uplink (alerting duplicate MACs) does not block the port.
- ★ Internal: Lack of technical understanding
  - Public: Change to Monitor had to be insisted or recommend and not make the change

# 2018-01-31 plan

Wednesday, January 31, 2018 12:19

- שלב 1
  - פיזור עומסים בין שרתים (פורטנוקס)
    - הורדת שרתי אפליקציה
    - הרצת שאילתות DB למציאת רכיבים שניתן להעביר + העברתם + העברת devices לשרת אפליקציה של המתג הרלוונטי
  - הגדרת snmp traps בכל המתגים (בנק דיסקונט)
- שלב 2 - שדרוג המערכת מ 2.4 ל 3.1
  - הורדת שרתי אפליקציה
  - הרצת סקריפטים DB בצורה ידנית
  - התקנת גרסה 3.1 ללא הרצת סקריפט DB
  - התקנת HF אחרון כולל הרצת סקריפט DB
- שלב 3 - טיוב הגדרות
  - מעבר על הגדרות מתגים ולוודא קיום והגדרות מתגים אשר מופיעים ב offline
  - מעבר על הגדרות אימות וחוקים על מנת לאשרר תוקפם והגדרתם ברשת
  - מעבר על בדיקות compliance וטיוב ההגדרות
  - מעבר על פורטים המוגדרים ב location : not\_enforced
  - בדיקת זמן חסימה לתחנה לא חוקית וטיפול בהתאם לממצאים

# 2018-03-01 Upgrade plan

Thursday, March 1, 2018 11:53

## Upgrade:

- Backup DB
- Take snapshots of all enforcers
- Take statistics of current state (amount of rogues, authenticated, compliance fails...)
- Run tests to verify current state of system
  - Execute an action (e.g. disable/enable port) on switch under each enforcer
- Set system to Monitor
  
- Shutdown services on all enforcers (Services will be kept down until entire upgrade is complete)
- Upgrade each enforcer according to upgrade instructions in our guide
  - Upgrade to current version latest update (run db script only on first enforcer upgrade)
  - Upgrade to v2.51 (run db script only on first enforcer upgrade)
  - Upgrade to v3.1 (run db script only on first enforcer upgrade)
  - Install latest HF for v3.1
- Start services on default enforcer (verify functionality)
- Start services on all active enforcers (verify functionality)
- Confirm statistics state is valid
- Start services on backup enforcers

## Rollback:

- Stop all enforcers machines
- Restore DB from backup
- Revert all snapshots
- Start services on default enforcer (verify functionality)
- Start services on all active enforcers (verify functionality)
- Confirm statistics state is valid
- Start services on backup enforcers
- Set system to Enforce

# 2018-06-12 Upgrade plan

Thursday, March 1, 2018 11:53

## Upgrade:

- Take statistics of current state (amount of rogues, authenticated, compliance fails...)
- Run tests to verify current state of system
  - Execute an action (e.g. disable/enable port) on switch under each enforcer
  - Restart services
- Shutdown services on all enforcers (Services will be kept down until entire upgrade is complete)
- Backup DB + Take snapshots of all enforcers
- Set system to Monitor
  
- Upgrade each enforcer according to upgrade instructions in our guide
  - Upgrade to current version latest update 2.43(run db script only on first enforcer upgrade)
  - Upgrade to v2.51 (run db script only on first enforcer upgrade)
  - Upgrade to v3.1 (run db script only on first enforcer upgrade)
  - Install latest HF for v3.1
- Start services on default enforcer (verify functionality)
- Start services on all active enforcers (verify functionality)
- Shutdown services on all enforcers
- Migrate DB to new DB 2014
  - Backup + Upgrade
  - Update all enforcer with new DB address using cluster util (verifying non-standard port used)
- Start services on default enforcer (verify functionality)
- Start services on all active enforcers (verify functionality)
- Confirm statistics state is valid
- Start services on backup enforcers
- Backup new DB
- Run failover test
- Failback
- Set enforcement

## Rollback (3:00am rollback decision):

- Stop all enforcers machines
- Restore DB from backup
- Revert all snapshots
- Start services on default enforcer (verify functionality)
- Start services on all active enforcers (verify functionality)
- Confirm statistics state is valid
- Start services on backup enforcers
- Set system to Enforce

# Links

Sunday, June 17, 2018 13:44

2.43 - iso

<https://portnox.box.com/s/b4k93wyb68jst80r45raxdlj8o703i13>

2.51 - iso

<https://portnox.box.com/v/nox25UP1>

3.1 - iso

<https://portnox.box.com/v/3UP1iso>

Hf9

<https://portnox.box.com/v/3UP1HF09>



# 2018-07-16

Monday, July 16, 2018 13:01

- Part of the agreement provides 6 training.
  - When is the next training ?
- Failover / Recover not working
  - TFS
- Device Unreachable:
  - TFS - authenticate OSFP when device does not answer to ping affects Windows devices
  - Need solution for devices in sleep (OSFP and none OSFP)
- Check possibility to provide a report for switches that no trap is received from them.
- TAM + Health check
  - Schedule a bi-weekly visit of 2-3 hours to do health check and provide a list of action items for the Discount Bank team

# 2018-07-25 - Unreachable

Wednesday, July 25, 2018 15:02

- Unreachable incidents:
  - Printers:
    - Do not answer to ping
    - Are not communicating
  - Windows:
    - Do not answer to ping (declared rogue due to bug)
    - Using firewall - should be blocked
- ICMP scan is turned off.
- MAC address stays on port although device is in sleep
  
- Root cause is MAC address not removed from port on switch. Should be addressed by the bank network team.