



Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444



תמצות מפגש שולחן-עגול

טכנולוגיות ומתודולוגיות בתחום שליטה
ובקרה ארגונית

מנחה
פיני כהן

לקוחות נכבדים,

תודה על השתתפותכם במפגש שולחן עגול בנושא שליטה ובקרה ארגונית.

היה זה מפגש טוב מאוד מבחינתי. קיבלנו פרספקטיבה עמוקה על סטטוס יישומי שו"ב בארגונים. יש לציין שתחום זה נמצא בעיצומו של תהליך (שו"ב לפי LOGS, ענן, קוד פתוח, דומיננטיות פחותה של big 4) אך בעת הנוכחית אין הבדל גדול בין הנושאים שהועלו במפגש זה לבין נושאים שהועלו במפגשים קודמים (אולי למעט המעבר הגורף יחסית לניטור סביבת windows עם מיקרוסופט וגם תחילת שימוש ב- elasticsearch).

להלן תמצות הנקודות שעלו במפגש:

1. צוות השליטה והבקרה חייב להיות חלק מתהליך ההעברה לייצור. כלומר ללא אישור של צוות השו"ב אין להעביר שינוי לייצור (למי שמעוניין נושא קריטי זה מופיע אצלנו בכתובים וגם במידה ויסייע נשמח להיפגש בארגון עם המנהלים בכדי לתמוך בסוגיה זו).
2. Containers-docker הנה טכנולוגיה אשר תשפיע מהותית על התנהלות גופי ה- IT (פיתוח, תפעול, תשתיות ושליטה ובקרה).
3. רובם של הלקוחות משתמשים במוצרי השו"ב tier 1 בתור קונסול מרכזי (hp, ibm, bmc, ca).
4. ישנו מעבר של שימוש ב- agents מבוססי scom על חשבון שימוש בagents של מוצרי tier 1. גם בגלל האיכות הטכנולוגית של פתרון מיקרוסופט בתחום זה וגם בגלל הורדה של עלויות.
5. לקוחות מטמיעים מוצרים רבים של יצרני ה- tier 1. ובנוסף לכך מוצרים נוספים (כמו SCOM). כולם נתקלים בבעיות אינטגרציה בין המוצרים. לדוגמה בין SCOM לבין הקונסול המרכזי של הספק tier 1.
6. ישנם מספר לקוחות אשר מבצעים ניטור מערכות לינוקס באמצעות SCOM אולם מדובר על משימה שאינה טריוואלית.

7. לקוחות מודעים לאלטרנטיבה של פתרונות קוד פתוח. לדעת רובם המכריע של הלקוחות שימוש בקוד פתוח יחייב מאמץ אינטגרציה יותר כבר מאשר אינטגרציה אשר נדרשת במוצרים מסחריים.
8. לקוחות נמצאים בשלבים ראשונים של יישום טכנולוגית big data בתחום שו"ב. בעיקר elastic search. אחד היישומים שהוזכרו הוא העברת כל ה-events שמתקבלים לתוך קונסול מערכת השו"ב. elastic search בגרסת הקוד הפתוח מאפשרת תחקור מהיר ויעיל מאשר בניית דוחות מתוך כלי השו"ב (דברים כמו – "איזה תקלות הראה המחשב בחודש האחרון"). במידה ורוצים גם לקבל התראה על תקלה – מדובר כבר על גרסת elastic search שאינה קוד פתוח. לקוחות גם שוקלים שימוש ביכולת של predictive analytics אשר תנסה לאתר קורלציות בין התנהגות של רכיבים במערכת.
9. לקוחות שמתחילים ליישם Devops מחפשים פתרון אשר יאפשר לנהל את השינויים בהקשר גרסאות Devops. לדוגמה ירצו לקבל חיווי – "יש כשל במודול X של מערכת אשר עודכן לפני יומיים בגרסה מספר Y".
10. לקוחות עדיין מתקשים למצוא פתרון אשר ידע למדל עסקית את המערכות. מידול כזה יאפשר תובנות רבות כגון – "אם שרת נפגע- איזה תהליכים עסקיים יפגעו". פתרונות מידול ה-CMDB הקיימים אכן מסייעים אך עדיין מחייבים השקעה רבה (לדברי לקוחות הפתרונות מורידים 40-60% ממלאכת המידול הידנית). ישנם דרכים אחרות לסייע במידול – קונבקציית שמות, הגדרה של כתובות IP וכד'.
11. לקוחות רואים תועלת מיישום של CMDB אולם מדובר על השקעה לא מועטה כאשר התועלת בדרך כלל נשארת ברמות הבסיסיות/שתיתיות של התמונה. מידול עסקי מלא לא נראה בר השגה כעת.
12. לקוחות עדיין מתקשים למצוא פתרון אשר שומר היסטוריה חכמה של שינויים במערכות וקונפיגורציה מועדפת. דוגמה לשימוש כזה "טכנאי אמור היה לבצע שינוי ב-10 שרתים. האם השינוי בוצע בכלום באופן זהה או שאולי נשכח אחד השרתים". הערת STKI, ככל שנתקדם ביישום אוטומציה ו-containers בפרט, הסיכוי לטעויות אנוש מסוג זה יקטן. הערה נוספת – evolgen אמור לטפל בנושא זה.
13. לקוחות מדברים על הצורך בניטור חויית משתמש ב-mobile אצל לקוחות אך יישום בתחום זה אינו רחב. רוב הפתרונות מחייבים ביצוע קומפילציה עם ספריות של הספק.
14. מצ"ב לינק לבלוג הארכיטקטורה של martin flower בו התייחסות ל-event sourcing.
- כתיבת כל שינוי במצב באפליקציה ב-LOG.

מתוך ה-LOGS. ישתנה השו"ב האפליקטיבי באופן מהותי כי ניתן יהיה להבין מה הסטטוס של האפליקציה

מתוך ה-LOGS. מעבר למוצרי tier 1 ולמיקרוסופט הוזכרו בדיון מספר מוצרים נוספים שהוזכרו בדיון:

- Aternity – חויית משתמש כעת נרכשו על ידי riverbed.
- Ayehoo – לאוטומציה של צוותי NOC
- ++SNS לשליחת התראות וניהול צוות פעולה
- <http://highnetsystems.com/> SNS++
- Dynatrace – פתרון APM
- New ralic – פתרון APM
- App dynamics פתרון APM
- Solarwinds – ניטור רשת
- SPLUNK – ניתוח לוגים
- [/http://xpolog.com/](http://xpolog.com/) - ניתוח לוגים
- VNT – עבור discovery CMDB
- Nebula – כיום חלק מ- servicenow עבור cmdb discovery . כעת מתרחב ל- asset management
- <http://www.correlsense.com/> - APM ישראלי מתקדם
- Loom systems - סטאטאפ בתחום. אוסף LOGS ונותן תובנות על מצבים בתחום זימינות.
- Big panda. דיי דומה.
- Zabbix – פתרון ניטור תשתיתי קוד פתוח
- <http://www.anodot.com/> זיהוי אנומליות בייצור בהקשר שו"ב.
- Evolgen – לזיהוי שינויים בקונפיגורציה של רכיבים במערכת.
- <http://emcosoftware.com/ping-monitor> - מוצר בסיסי לביצוע PING