פסח – זמן טוב לעשות סדר גם ב-ArcSight

ה-ArcSight צובר עם הזמן יותר ויותר מידע, ויחד עם המידע מצטברים עוד ועוד תכנים (קונקטורים, חוקים דו"חות וכו') למערכת אשר יכולים להשפיע על כמות המשאבים שהמערכת צורכת ועל תפקודה.

הכנו עבורכם סט כלים, בואו נתחיל את הסדר:

1. רכיבים מדווחים - קונקטורים

- ✓ נמחוק קונקטורים לא פעילים. (לעצור את ה-Service, Uninstall את הקונקטור משרת הקונקטורים, למחוק את הקונקטור מרשימת ה-Resources בקונסול).
- ✓ נבדוק תקינות דיווחים של קונקטורים פעילים:
  - » האם רכיב שאמור לדווח, אכן מדווח?
  - » האם הלוגים מגיעים תקינים (מפורסרים)
  - » האם ניתן לבצע אגריגציה ופילטור ללוגים?
- ✓ נגיע למצב שבו כל הקונקטורים נמצאים במצב תקין (ירוק).
- ✓ נפעיל התראות על נפילת קונקטורים.

2. חוקים

- ✓ נבצע סימלוץ לחוקים חשובים אחת לתקופה על מנת לוודא שכל שרשרת הדיווחים תקינה.
- ✓ נבדוק חוקים אשר מעמיסים על משאבי המערכת.
- ✓ נבחון את כמות החוקים שקופצים אל מול הזמן המצריך טיפול בהם:
  סך הזמן (כמות החוקים שקופצים X הזמן הממוצע לטיפול בחוק) צריך להיות פחות או יותר שווה לזמן של כמות הזמן שיש לעובדים לטפל בחוקים שקפצו.

3. דו"חות

- ✓ נבדוק עם מקבלי הדו"חות שהם אכן רואים ומנתחים את כל הדו"חות שנשלחים אליהם באופן אוטומטי. (מניסיוננו, לאחר מספר דו"חות שהם מקבלים, הם יוצרים Role ב-Outlook שמעביר את הדו"ח לתיוק ולא רואים מה יש בדו"חות).
- ✓ האם כל המידע שאמור להיות בדו"חות אכן מופיע. האם הדו"חות שיוצאים ריקים, אכן צריכים להיות ריקים.

4. לוחות תצוגה (Dashboard)

- ✓ נעבור על לוחות התצוגה ונעצור (להעביר למצב Disable את ה-Data Monitoring) את מה שלא פעיל. דבר היכול לחסוך משאבים רבים מהמערכת.
- ✓ נכוון את חלונות הזמן של ה-Dashboard על פי הצרכים.

5. רשימות (Active Lists)

- ✓ נוודא שה-Active Lists לא הגיעו ל-100% תפוסה.
- ✓ מהצד שני, Active Lists עם 0 רשומות – לוודא תקינות החוקים שמכניסים ל-List.

6. מערכת

- ✓ נבדוק את ה-Retention Time אל מול ייתרת מקום לאחסון.
- ✓ גיבויים:
  - » נשמור את הגיבויים באחסון חיצוני!
  - » נוודא שיש ייתרת מקום באחסון החיצוני לגיבויים על פי המדיניות שלכם.
  - » נוודא תקינות הגיבויים ע"י ביצוע שחזור מערכת (מומלץ פעמים בשנה לפחות).

להתייעצות עם המהנדסים שלנו לביצוע פעולות אלו (ולא רק לפני פסח)

ניתן ליצור קשר במייל Sec-Support@we-ankor.co.il

סדר פסח שמח!