מסמך אפיון
גרסה 1.5

ע"י אופק אלנבוגן
נחפף

תוכן עניינים

רקע על הסוכן

CD LOG הינו סוכן לאיסוף וניהול לוגים.

בעזרת שימוש ב- CD LOG תוכלו להיות בבקרה על כלל מחשבי הארגון שלכם, כך שתוכלו לעלות על תקלות בזמן, למנוע פרצות אבטחה ולהרוויח הרבה יותר כסף !

לסוכן יש את היכולת לבצע את הפעולות הבאות -

- איסוף מידע מכל סוגי הלוגים השונים במחשב.
- שליחת הלוגים לכתובת יעד בכל פורט/פרוטוקול (TCP/UDP).
- יכולת פרסור של המידע.
- שליחת מוצפנת של המידע בכל פורט.
- יצירת לוגים אפליקטיביים ותפעוליים של הסוכן.

<u>פעולותיו העיקריות של CD LOG</u>

- איסוף כלל הלוגים מהמחשבים השונים.
- פרסור המידע שנאסף.
- הזרמת לוגים אל כתובות יעד שונות.

<u>האפליקצייה מיועד לרוץ בסביבות:</u>

- מערכת הפעלה windows.
- מערכת הפעלה linux.

למה CDLOG הומצא? אילו בעיות הוא בא לפתור ?

בעולם הטכנולוגי העתידי של שנת 2024, הכל מבוסס על טכנולוגיה, על מחשבים וכלל העבודה בכל תחומי החיים מתבססת על זה. ועם כמה שזה נוח, מגיעות עם זה בעיות וסכנות רבות.
לכל חברה כיום יש רשת של העסק שלה, הרשת מורכבת ממחשבים, שרתים ועוד.
בשביל שהחברות יוכלו לעבוד, הi צריכות שתהיה זמינות כמה שיותר גבוהה ברשתות שלהן, שהכל יעבוד חלק, בין אם זה לצרכים הפנימיים שלהן, ובין אם זה לשירותים שחברות מנגישות ללקוחות שלהן.
בעיות שונות יכולות לצוץ בעולמות ה-

- אחסון
- רשתות
- תשתית
- סייבר

ובעצם בכל שירות המונגש דרך המחשבים, שזה בעצם **הכל**.

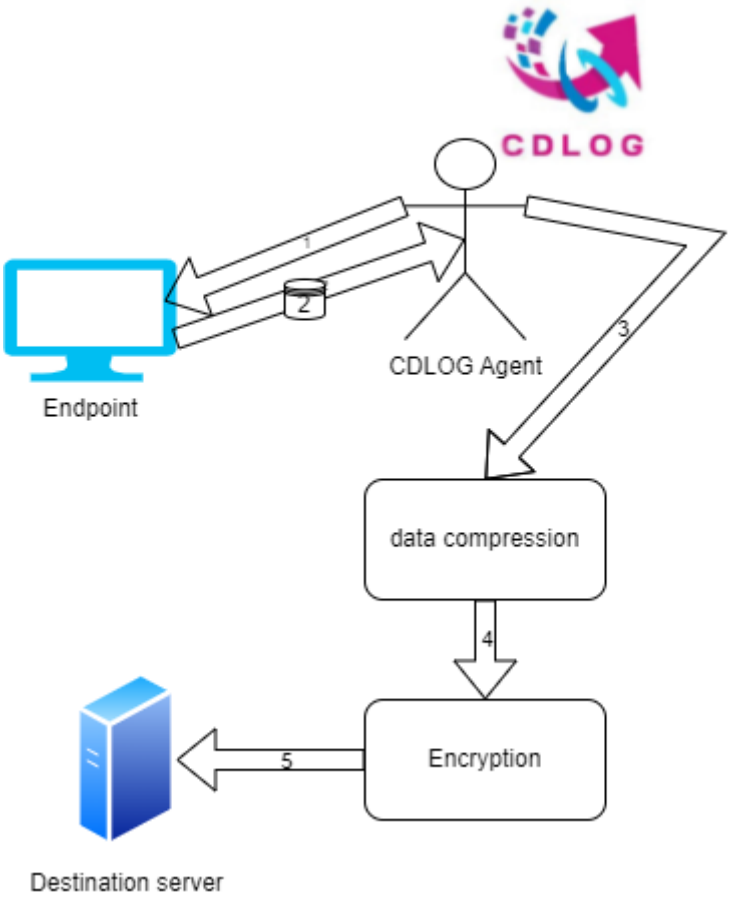
כאן **CDLOG** נכנס לתמונה, הסוכן החדשני שאוסף מידע מכל קבצי הלוגים השונים שנמצאים במחשב.
מה זה אומר?

<u>בתחום מנהלי הרשת -</u>
הוא מאפשר למנהלי הרשתות לדעת בכל רגע נתון מה קורה ברשת המחשבים שלהם, ולפתור בזמן אמת תקלות שמתרחשות, לפני שהן עושות השפעה דרמטית, ויותר מזה, אפילו למנוע תקלות עתידיות.

<u>בתחום ההגנה בסייבר -</u>
הוא מאפשר למגני הסייבר לזהות בעיות אבטחתיות שקורות במחשבים ולחקור ולעצור אותן בזמן אמת, לפני שהנזק הגדול ייגרם.

ארכיטקטורה ודרישות טכנולוגיות

1. **תשתית**
   a. <u>עבור מחשב הקצה</u>
      i. קובץ קונפיגורציה של הסוכן בפורמט yaml.
      ii. קובץ הרצה שמתקין שירות של הסוכן CDLOG.
      iii. תיקיית קבצים המכילה את כלל התלויות הנדרשות שתותקן עם הרצת קובץ ההרצה.
   b. <u>שפת הפיתוח של הסוכן</u>
      i. פייתון



מבנה הקוד

מודול איסוף הלוגים:

- מודול זה אחראי לאיסוף הלוגים מקבצי הלוגים במערכת המקומית.
- הוא עובר דרך ספריית הלוגים המצויה בנתיב שמתקבל וקורא קבצי לוג.
- כדי לייעל את הביצועים, הוא שומר על מיקום הקריאה האחרון בכל קובץ לוג באמצעות מילון `log_positions`.
- הלוגים מתוך כל קובץ נאספים מהמיקום שנקרא לאחרונה ועד סופו של הקובץ כך שרק לוגים חדשים נאספים.

מודול תקשורת רשת:

- מודול זה מטפל בתקשורת עם השרת המרוחק שאליו ישלחו הלוגים.
- הוא מקים חיבור לשרת באמצעות socket ושולח את הלוגים שנאספו.
- מנגנוני טיפול בשגיאות קיימים לטיפול בבעיות רשת או אי זמינות של השרת.

מודול ראשי:

- מודול ראשי של הקוד רץ באופן רציף (בלולאה אינסופית), ובכך מבטיח כי הסוכן תמיד יאסוף וישלח לוגים.

בכל ריצה של הלולאה:

- הלוגים החדשים נאספים באמצעות מודול איסוף הלוגים.
- הלוגים שנאספו נשלחים לשרת המרוחק באמצעות מודול תקשורת הרשת.

אתחול:

- בעת האתחול, הקוד מאתחל את מילון `log_positions`, המאחסן את מיקום הקריאה האחרון בכל קובץ לוג.
- אתחול זה מבטיח כי הסוכן יתחיל לאסוף לוגים מההתחלה של כל קובץ במהלך ההרצה הראשונה.

טיפול בשגיאות:

- מנגנוני טיפול בשגיאות נמצאים לאורך כל הקוד, לטיפול בבעיות כגון שגיאות גישה לקבצים או כשל בתקשורת.
- כל השגיאות שנתקלו מתועדות לקובץ לוגים ייעודי.

קונפיגורציה:

- הקוד יקבל הגדרות קונפיגורציה מהקובץ הייעודי כמו נתיב התיקייה שבה ממוקמים הלוגים, כתובת ה-IP של השרת, פורט השליחה ועוד.

לוגים וניטור עצמי:

- הקוד יכלול יכולות יצירת לוגים אפליקטיבים ותפעוליים עצמיות בעבור כל פעולה שהוא מבצע או מנסה לבצע.
- הקוד ישלב יכולות ניטור כדי לעקוב אחר ביצועי הסוכן, כגון כמות הלוגים שנאספו, אחוזי הצלחת השליחה, וכל חריגות אחרת.

פונקציונליות הסוכן

- <u>קריאת לוגים</u>

על הסוכן לקרוא לוגים מכל פורמט לוגים הקיים במערכות הפעלה השונות:

  - טקסט - txt, log, json ועוד.
  - מערכתיים - EVTX.

- <u>יכולת שליפה כנגד DB אל מול שאילתת SQL</u>
- <u>יכולת האזנה למידע משרת האיסוף</u>

על הסוכן להיות מסוגל להאזין לכל פורט שייבחר ב UDP או TCP.

- <u>יכולת פרסור</u>

על הסוכן להיות מסוגל לבצע את הפעולות הבאות על הלוגים-

  - לשנות פורמט של לוגים.
  - להוסיף, להסיר ולשנות שדות.
  - לשנות פורמט של timestamp בתוך event כולל UTC.

- <u>שליחת לוגים לשרת יעד</u>

על הסוכן להיות מסוגל לשלוח את הלוגים אל שרת ייעד בכל פורט שנקבע בקובץ הקונפיגורציה.

- <u>הצפנה ואבטחת מידע</u>

לסוכן תהיה יכולת לשלוח באופן מוצפן את כל סוגי המידע .

- <u>קובץ קונפיגורציה</u>

לסוכן יוגדר קובץ קונפיגורציה שמשתמש קצה יוכל להגדיר הגדרות.

הקובץ יוגדר בפורמט yaml.

- <u>log rotation</u>

יכולת התמודדות עם קריאה מקבצי לוגים שמבצעים log rotation.

- <u>בקרה עצמית</u>

הסוכן יצור לוגים אפליקטיבים ותפעוליים על עצמו המסבירים על כל פעולה שהוא מנסה לבצע או מבצע וגם על שגיאות.

לסוכן תהיה אופציה אם לבצע log rotation לקבצי הלוגים של עצמו.

- <u>התאמה למערכות הפעלה</u>

הסוכן יעבוד כשירות במ"ה windows וlinux.

דרישות מעטפת נוספות לסוכן

- חבילת התקנות

לכל מערכת הפעלה תהיה את חבילות ההתקנות שלה (rpm, tar.gz, msi, zip) המכילה קבצי קונפיגורציה והרצה דיפולטים.

- קונטיינרים

יצירת docker image של התקנת הסוכן כדי שהסוכן יוכל לרוץ על containers.

- READ.ME

הוספת קובץ READ.ME שיבוא עם הקבצים בהתקנה, שיכיל הסבר מפורט על הסוכן.

קובץ קונפיגורציה של הסוכן

linux - /etc/cdlog/cdlog.conf

בקובץ הקונפיגורציה המשתמש יוכל להגדיר -

- כתובת יעד ופורט אליה ישלחו הלוגים.
- פורמט קבצי הלוגים אותם הסוכן יחפש.
- נתיב התיקייה שבה נמצאים קבצי הלוגים.
- האם הפרסור יהיה מוצפן או לא.

```
# Configuration for Python Log Agent - CDLOG


# Here put the directory of where the log file are
log_directory:
  - "/var/log"

# Here put the file formats you want the agent to look for
file_formats:
  - "txt"
  - "log"

# Here put the destionation server details
destination_server:
  ip: "192.168.1.100"
  port: 12345

# Here put if it is encrypted or not
encrypted: "no"
```