מסמך אפיון
גרסה 1.1

ע"י אופק אלנבוגן
נחפף

- **תתעלם**

https://docs.fluentd.org/installation/install-from-source

תיאור כללי של 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 כל הלוגים מכל קבצי הלוגים השונים במחשב
- שליחת הלוגים לכתובת יעד בכל הפורטים דרך TCP/UDP
- יכולת פרסור
- שליחת מוצפנת של המידע בכל הפורטים
- יצירת לוגים על עצמו

<u>מטרותיה העיקריות של CD LOG:</u>

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

<u>האפליקצייה תפותח ותיבדק בסביבות הבאות:</u>

- מערכת הפעלה windows
- מערכת הפעלה linux

אז למה CDLOG הומצא, ואילו בעיות הוא בא לפתור ?

בעולם הטכנולוגי העתידי של שנת 2024, הכל מבוסס על טכנולוגיה, על מחשבים וכלל העבודה בכל תחומי החיים מתבסס 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, הם 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 האחסון, הרשתות, התשתית, הסייבר 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?
זה אומר שהוא מאפשר למנהלי הרשתות לדעת בכל רגע נתון מה קורה ברשת המחשבים שלהם, ולפתור בזמן אמת בעיות שקורות, לפני שהן עושות השפעה דרמטית, ויותר מזה, אפילו למנוע בעיות עתידיות.

ארכיטקטורה ודרישות טכנולוגיות

1. **תשתית**
   a. <u>צד המחשב עליו מותקן הסוכן</u>
      i. שירות ששמו CDLOG שהוא הסוכן עצמו
      ii. תיקייה המכילה את כלל התלויות הנדרשות לשירות
      iii. קובץ קונפיגורציה של הסוכן
   b. <u>שפת התכנות של הסוכן</u>
      i. פייתון

CDLOG

ארכיטקטורה של קוד הסוכן

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 בכל הקוד, לטיפול בבעיות כגון שגיאות גישה לקבצים או כשל בתקשורת.
- כל השגיאות שנתקלו מתועדות או מודפסות למסך לצורך ניתוח ותיקון.

קונפיגורציה:

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

לוגים וניטור עצמי:

- הקוד יכלול יכולות לוגינג עצמיות בעבור כל פעולה שהוא מבצע או מנסה לבצע
- הקוד ישלב יכולות ניטור כדי לעקוב אחר ביצועי הסוכן, כגון כמות הלוגים שנאספו, שיעור הצלחת השליחה, וכל חריגות המזוהות.

פונקציונליות הסוכן

- קריאת לוגים

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

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

- יכולת שליפה כנגד DB אל מול שאילתת SQL
- יכולת האזנה

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

- יכולת פרסור מינימלית

על הסוכן להיות מסוגל לבצע את הפעולות הבאות על הלוגים-

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

- הצפנה ואבטחת מידע

לסוכן תהיה יכולת לשלוח באופן מוצפן את כל סוגי המידע בכל הפורטים השונים

- קובץ קונפיגורציה

לסוכן יוגדר קובץ קונפיגורציה שמשתמש קצה יוכל להגדיר הגדרות.

הקובץ יוגדר בפורמט yaml

- log rotation

יכולת התמודדות עם קריאה מקבצי לוגים שמבצעים log rotation

- בקרה עצמית

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

- התאמה למערכות הפעלה

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

windows - ?

בקובץ הקונפיגורציה המשתמש יוכל להגדיר -

- כתובת יעד ופורט אליה ישלחו הלוגים
- פורמט קבצי הלוגים אותם הסוכן יחפש
- נתיב התיקייה שבה נמצאים קבצי הלוגים

```yaml
# 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
```