Network Monitoring

Syslog Overview

- חלק מתפקידו של מנהל הרשת הוא להיות בבקרה מתמדת על הרשת, מכמה בחינות כמו לדוגמה תקינות הרכיבים, פתרון תקלות, ניטור עומסים ותקלות צפויות. משימה אשר בטופולוגיות רשת גדולות יכולה להיות קצת "קוץ בישבן". בכל הקשור לניטור ומעקב אחר האירועים המתרחשים בסביבת הרשת או יותר נכון על רכיבי הרשת השונים, קיים פתרון פשוט ושמו Syslog
- Syslog היא השיטה הנפוצה ביותר להצגת ואחסון הודעות מערכת מכל סוג, מהסוג שאינן קריטיות ועד התראות קריטיות שדורשות התייחסות מיידית. Syslog קיים במערכות מחשוב רבות ולא רק ברכיבי רשת, משום שהוא מזמן הפך לסטנדרט בתחום הניטור ע"י חברינו הוותיקים IETF.
- סטנדרט ה-Syslog מתואר ב- RFC 3164

Syslog Operation

- שירות ה-Syslog מתעד את הודעות המערכת לרוב בצורה מקומית. לתהליך ה-Logging. מאחסון בשני מקומיים עיקריים, על גבי הרכיב מקומית או על גבי שרת Syslog ברשת, תלוי בהגדרות מנהל הרשת. לשני מיקומים אלו קיימים חסרונות ויתרונות כמובן. לדוגמה בשרת היתרון הוא ניהול מרוכז ונוח של הודעות מכל רכיבי הרשת, לעומת החיסרון של גישה לכל רכיב רשת בצורה מרחוקת או מקומית במטרה לצפות בהודעות המערכת האישיות שלו.
- שירות ה-Syslog פועל בפורט UDP 514.
- היעדים המקובלים עליהם ישמרו הודעות ה-Syslog:

1. Logging Buffer-שטח אחסון בזיכרון ה-RAM המוקצה להודעות המערכת.
2. Console Line-צפייה בהודעות בצורה מקומית בחלון ה-Console.
3. Terminal Line-צפייה בהודעות דרך חלון ה-Terminal לדוג' בהשתלטות מרחוק עם Putty.
4. Syslog Server-שרת בעל תוכנה ייעודית, אליו נשלחות הודעות המערכת מרכיבי הרשת.

Syslog Massage Format

- רכיבי הרשת מייצרים הודעות syslog בעקבות אירועים שונים ברשת. לדוג' ממשק שעבר למצב down (כבוי). הודעות מערכת מכילות מספר פרטים, בינהם רמת הדחיפות (Severity) והחומרה (facility) או תוכנה עליו ההודעה מדווחת.
- הדחיפות(Severity) של הודעה מוצגת ע"י מספר או יותר נכון Syslog Security Level. לדוג' Level 3. ככל שערך המספרי של השלב נמוך יותר ככה הודעה דחופה יותר, בעקבות כך ניתן להבין שהודעות Level 0 הם מהדחופות ביותר.
- טבלת השלבים (Syslog Security Level) ומשמעותן:

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant
Information	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Syslog Massage Format

- דוגמה לפורמט הודעת מערכת (Syslog) על רכיבי Cisco והסבר על החלקים השונים של ההודעה:

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

Timestamp

Facility

Severity Level

MNEMONIC

Description

- Timestamp-חומת זמן (שעה ותאריך) בו ההודעה נוצרה.
- Facility-הרכיב/חומרה עליו ההודעה מציגה מידע.
- Severity Level-רמת הדחיפות.
- MNEMONIC-מזהה ייחודי של סוג ההודעה.
- Description-תוכן ההודעה.

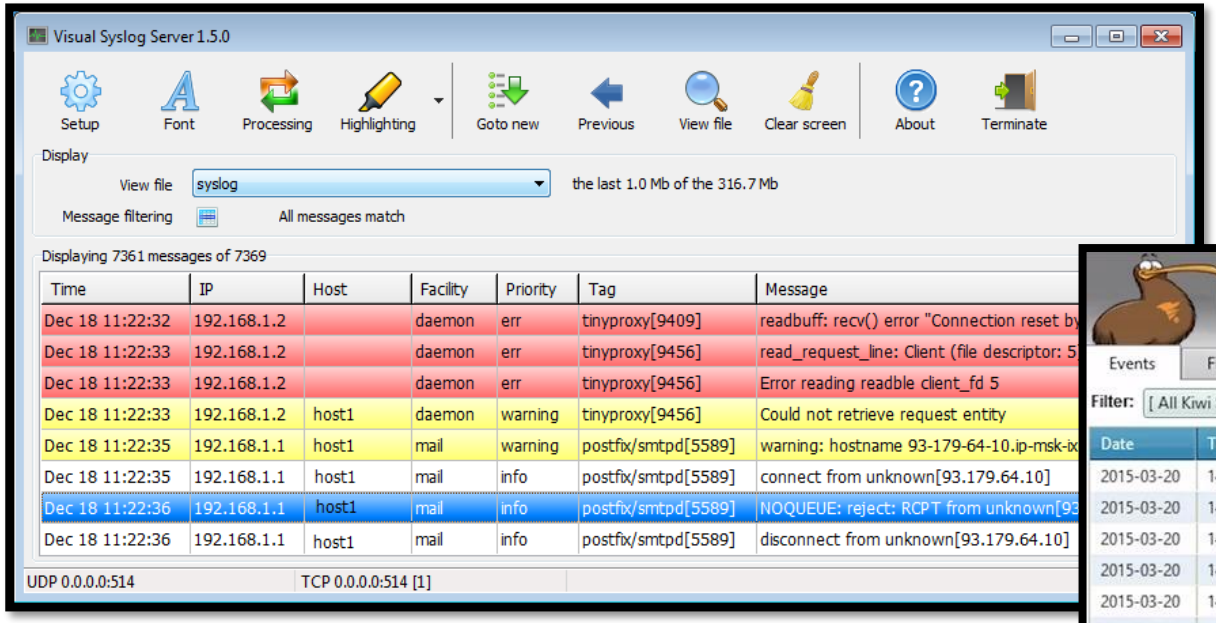
- חומות זמן לא נוספות להודעות מערכת בצורה דיפולטיבי, צריך לאפשר את השירות ה-Timestamp.

Syslog Server

- כפי שהזכרנו מקודם מיקום אחסון מקובל של הודעות Syslog הוא שרת. שרת Syslog היא שיטה נפוצה מכיוון שהיא נוחה מאוד. בשיטה זו כל רכיבי הרשת שולחים את הודעות המערכת שלהם לשרת או שרתים, השרת מספק ממשק נוח וידידותי למנהל הרשת, שם המנהל יכול לעקוב ולצפות בצורה נוחה בכל אירועי הרשת. הודעות המערכת מסודרת בארכיון בצורה כרונולוגית, לפי עמודות פרמטרים: שעה, סוג, תיאור. סינון וחיפוש של הודעות לפי סוג ותאריך הופכות למשימות פשוטות גם הן.
- כמובן שעל גבי השרת חייבת להיות מותקנת תוכנה של Syslog Server.
- מנהל הרשת יכול לבחור אילו סוגי הודעות ישלחו אל השרת, זאת אומרת לא כל הודעות המערכת נשלחות. אלא רק מה שהמנהל מחשיב כרלוונטי, כמו לדוגמה רק הודעות קריטיות רמות 0-4.
  - כברירת מחדל הודעות המערכת נשמרות על רכיבי הרשת בצורה מקומית. יש לבצע מספר הגדרות לפני שרכיבי הרשת יעבירו הודעות אל שרת ייעודי.

Syslog Server Software

- צילומי מסך שונים של תוכנות מסוג Syslog Server



NTP & Syslog

- NTP או בשמו המלא Network Time Protocol הוא פרוטוקול סנכרון שעונים ותאריכים בין רכיבי רשת בצורה אוטומטית.
- שעון התוכנה על רכיב הרשת הוא המאפיין היחיד שיכול לספק זמנים מדויקים בהקשר לאירועים מסויימים על הרכיב. יש לדאוג שכל רכיבי הרשת יכוונו בצורה מדויקת לאותה שעה. בגלל שכל מאפייני הניהול, אבטחה ופתרון תקלות מסתמכים על תיעוד שעתי מדויק (Timestamp). כשהזמן לא מסונכרן בין המכשירים, זה יהיה בלתי אפשרי להחליט את סדר האירועים או סיבת האירוע. לדוג' תקלת ניתוב בנתב ה-Gateway.
- שתי שיטות להגדרת השעון:

1. ידנית.
2. דינמית Network Time Protocol (NTP).

- השיטה הידנית היא פחות מומלצת או מציאותית, השיטה העדיפה היא שימוש בשרת NTP מדוייק ממנו רכיבי הרשת מסתנכרנים. NTP מבטיח סנכרון שעונים בכל מצב גם לאחר הפעלה מחדש או כשל של אחד הרכיבים.

NTP Operation

- ניתן להגדיר מספר רכיבים כ"שרת שעון" כמו נתב, מתג וכמובן שרת.
- רכיבי הקצה מקבלים את כתובת ה-IP של הרשת ומושכים את בשעה והתאריך האחרונים מהשרת. לכן חשוב מאוד שהשעון והתאריך בשרת יהיו מדויקים תמיד.