מדריך פעילות NOC הונאות
ניטור שרתים

מנהל מחלקת NOC הונאות- דוד מסיקה

מערכת ה- ZABBIX

ZABBIX

מערכת ה- ZABBIX

מערכת Zabbix הינה מערכת מוניטור שניתן באמצעותה לתכנת כך שתנטר את שרתי החברה והתהליכים בהם.
המערכת יכולה לשמש לזיהוי תקלות והתראה עליהן, להראות אם שירות פעיל, ולהציג נתונים על השרתים עצמם (Ram, Cpu וכו').
המטרה העיקרית: למצוא בעיות ברשת הארגונית הפנימית.

המערכת מציגה תקלות לפי חשיבות שהוגדרה מראש ובסדר חומרה עולה.

לפי חומרת התקלה, נדע לאיזה גורם עלינו לפנות על מנת לטפל בה,
או לחלופין לטפל בעצמנו בתקלות ברמת TIER 1.

מידי פעם אנו נתקל בתהליכים חדשים ולא מוכרים אותם ניתן לחפש מידע על התקלות- מדובר במערכת נפוצה והמידע זמין.

מערכת ה- ZABBIX

דוגמא לשימוש במערכת

התראות הבילינג המעידות על חריגה במנויי WECOM מסייעות לנו לעקוב אחרי פעילויות חשודות של לקוחות החברה.

המערכת לוקחת CDRים מהשרת שמחשב עלות שיחות כדי לחייב לקוחות, מכניסה אותם לחיפוש (Elastic Search) ומאפשרת מעקב וגישה אליהן.

במידה ואחד מהתהליכים באמצע קורס או נתקע, ההתראות יפסיקו לעבוד, ומערכת הZabbix תוכל להתריע היכן התקלה.

Zabbix – מסך ראשי

ZABBIX
Zabbix docker

Monitoring
- Dashboard
- Problems
- Hosts
- Overview
- Latest data
- Maps
- Services

Inventory

Reports

Support
Share
Help
User settings
Sign out

Global view

Edit dashboard

All dashboards / Global view

Zoom out | Last 1 hour

שרתים מנוטרים על ידי המערכת

System information

Parameter	Value	Details
Zabbix server is running	Yes	
Number of hosts (enabled/disabled)	7	6 / 1
Number of templates	234	
Number of items (enabled/disabled/not supported)	564	443 / 95 / 26
Number of triggers (enabled/disabled [problem/ok])	304	233 / 71 [7 / 226]
Number of users (online)	4	1

4 Available	1 Not available	0 Unknown	5 Total

כמות תקלות כוללת, לפי חומרה מהקל לכבד

0 Disaster	0 High	3 Average	1 Warning	2 Information	0 Not classified

תקלות ופירוט שלהן

Problems

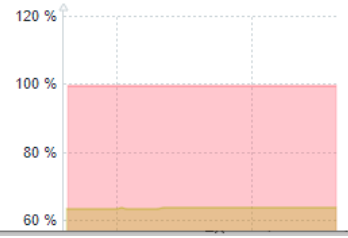
Time	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
12:30:43		CD	"TrustedInstaller" (Windows Modules Installer) is not running (startup type automatic)	14m 30s	No		Application: Services
12:00							
11:39:35		CD	The Memory Pages/sec is too high (over 1000 for 5m)	1h 5m 38s	No		Application: Memory
Today							
2022-02-20 13:42:48		CD	System time is out of sync 3m (diff with Zabbix server > 60s)	10d 23h 2m	No		Application: General
2022-02-20 13:40:54		RATING	System time is out of sync 3m(diff with Zabbix server > 60s)	10d 23h 4m	No		Application: General
2022-02-10 14:39:55		skynet.xfn	Zabbix agent is not available (for 3m)	20d 22h 5m	No		Application: Status
2022-02-10 01:26:26		CD	"nxlog" (nxlog) is not running (startup type automatic)	21d 11h 18m	No		Application: Services

מפת השרתים הארגונית

Xfone map

שטח דיסק באחוזים

rating disk space



במסך latest data נוכל לחפש תהליכים ספציפיים עם מידע מקיף יותר.

כאן נחפש תהליכים מסוימים שרצים או מנוטרים.

ZABBIX
Zabbix docker

Monitoring
- Dashboard
- Problems
- Hosts
- Overview
- Latest data
- Maps
- Services

Inventory

Reports

Support
Share
Help
User settings
Sign out

Latest data

סינון, לדוגמא לפי שרתים

Filter

Host groups: type here to search — Select
Hosts: MultiSite.xfn × CD × RATING × type here to search — Select
Name
Tags: And/Or | Or — tag — Contains — value — Remove — Add
Show details
Show items without data
Apply | Reset

שם שרת

שם תהליך

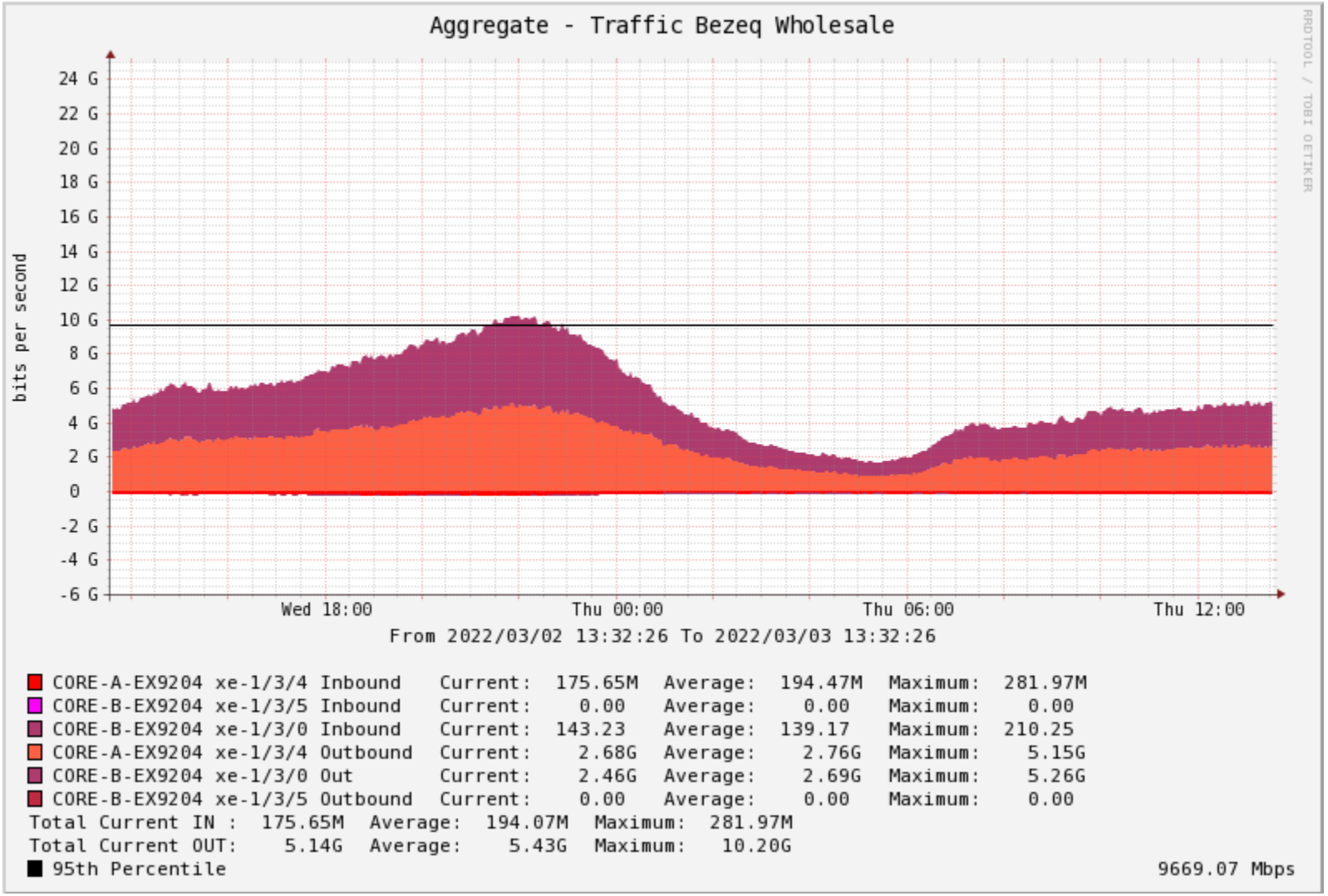
Host	Name ▲	Last check	Last value	Change	Tags	
MultiSite.xfn	Apache: Bytes per second				Application: Apache	Graph
MultiSite.xfn	Apache: Get status				Application: Zabbix ra...	History
MultiSite.xfn	Apache: Requests per second				Application: Apache	Graph
MultiSite.xfn	Apache: Service ping	2022-03-03 12:48:45	Up (1)		Application: Apache	Graph
MultiSite.xfn	Apache: Service response time	2022-03-03 12:55:44	0.43ms	-0.037ms	Application: Apache	Graph
MultiSite.xfn	Apache: Total bytes				Application: Apache	Graph
MultiSite.xfn	Apache: Total requests				Application: Apache	Graph
MultiSite.xfn	Apache: Total workers busy				Application: Apache	Graph
MultiSite.xfn	Apache: Total workers idle				Application: Apache	Graph
MultiSite.xfn	Apache: Uptime				Application: Apache	Graph
MultiSite.xfn	Apache: Version				Application: Apache	History
MultiSite.xfn	Apache: Workers closing connection				Application: Apache	Graph
MultiSite.xfn	Apache: Workers DNS lookup				Application: Apache	Graph
MultiSite.xfn	Apache: Workers finishing				Application: Apache	Graph
MultiSite.xfn	Apache: Workers idle cleanup				Application: Apache	Graph
MultiSite.xfn	Apache: Workers keepalive (read)				Application: Apache	Graph
MultiSite.xfn	Apache: Workers logging				Application: Apache	Graph
MultiSite.xfn	Apache: Workers reading request				Application: Apache	Graph
MultiSite.xfn	Apache: Workers sending reply				Application: Apache	Graph

מערכת Cacti

מערכת Cacti משמשת על מנת לנטר את פעילות קווי הרשת החיצונית של החברה מול ספקים אחרים וחברות תשתית. המערכת מראה את התעבורה ויכולה להראות על תקלות בה, כמו קפיצה בגרף, גרף שנעלם (משמע שהופסקה זרימת הנתונים) ועוד. על תקלות כאלה נצטרך להתריע. עיקר הפעילות הוא מול בזק, שם רוב הלקוחות שלנו, אבל יש לכל חברה גרף עם נתונים (HOT,IBC ועוד).
כדאי להסתכל בטווח של 4 שעות אחורה. לפעמים בקצה הגרף עוד אין נתונים מעודכנים וזה ייראה כמו נפילה, צריך לחכות.

גרף לדוגמא של לקוחות סימפלסייל אקספון

ניתן לראות שהשימוש משתנה לפני שעות.
למטה רואים את הקווים הנדגמים.



GRAFANA

גרפאנה הינה מערכת מובילה להצגת מידע של מדדים metrics בפאנלים מסוגים שונים כגון טבלאות, גרפים, שעונים וכדומה.

את הפאנלים מחברים למקורות מידע שונים כמו למשל: Prometheus, MySQL, MongoDB, Graphite, ElasticSearch ואחרים.

הכל נעשה בממשק נוח לשימוש שאינו דורש כתיבת קוד

מערכת הניידות NPG