PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

V14 funkčná infraštruktúra

KPB5 – Realizácia riešenia

typ – dokumentácia

mesiac odovzdania – M19

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1. ELK Stack 5
supOpis systému 5
Dokumentácia systému 5
Inštalácia - variant Docker 5
Inštalácia - variant Openstack 5
Inštalácia - variant ...x... 5
Základná konfigurácia 5
Integrácie 5
2. Shuffle 6
Opis systému 6
Dokumentácia systému 6
Inštalácia - variant Docker 6
Inštalácia - variant Openstack 6
Inštalácia - variant ...x... 6
Základná konfigurácia 6
Integrácie 6
3. Wazuh 7
Opis systému 7
Dokumentácia systému 7
Inštalácia - variant Quickstart 7
Inštalácia - variant Docker 7
Inštalácia - variant Openstack 8
Inštalácia - variant ...x... 8
Základná konfigurácia 8
Integrácie 8
4. Greenbone Community edition 8
Opis systému 8
Dokumentácia systému 8
Inštalácia - variant Docker 9
Inštalácia - variant Openstack 9
Inštalácia - variant ...x... 9
Základná konfigurácia 9
Integrácie 9
5. OpenCTI 9
Opis systému 9

Dokumentácia systému 9
Inštalácia - variant Docker 10
Inštalácia - variant Openstack 10
Inštalácia - variant ...x... 10
Základná konfigurácia 10
Integrácie 10
6. MISP 10
Opis systému 10
Dokumentácia systému 10
Inštalácia - variant Docker 11
Inštalácia - variant Openstack 11
Inštalácia - variant ...x... 11
Základná konfigurácia 11
Integrácie 11
7. GLPI 11
Opis systému 11
Dokumentácia systému 11
Inštalácia - variant Docker (Compose) 12
Inštalácia - variant Openstack 14
Inštalácia - variant ...x... 14
Základná konfigurácia 14
Integrácie 15
8. NetBox 16
1.1. Opis systému 16
Dokumentácia systému 16
Inštalácia - variant Docker 16
Inštalácia - variant Openstack 16
Inštalácia - variant ...x... 16
Základná konfigurácia 16
Integrácie 16
9. DFIR IRIS – Ticketing 16
Opis systému 17
Dokumentácia systému 17
Inštalácia - variant Docker 17
Inštalácia - variant Openstack 17
Inštalácia - variant ...x... 17
Základná konfigurácia 17

Integrácie 17
10. DFIR IRIS – Evidencia, správa incidentov 17
Opis systému 17
Dokumentácia systému 18
Inštalácia - variant Docker 18
Inštalácia - variant Openstack 18
Inštalácia - variant ...x... 18
Základná konfigurácia 18
Integrácie 18
11. Kibana (ELK) 18
Opis nástroja 18
Dokumentácia systému 18
Inštalacia - variant Docker 19
Inštalácia - variant Openstack 21
Inštalácia - variant ...x... 21
Základná konfigurácia 21
Integrácie 21
12. Wiki.js 21
Opis systému 22
Dokumentácia systému 22
Inštalácia - variant Docker 22
Inštalácia - variant Openstack 24
Inštalácia - variant ...x... 24
Základná konfigurácia 24
Integrácie 24

1. ELK STACK

Typ nástroja: SIEM

Názov nástroja: ELK Stack (Elasticsearch + Logstash/Beats + Kibana)

Verzia:

supOpis systému

Centrálna agregácia, indexácia a korelácia logov + vyhľadávanie a analýza

ELK Stack poskytuje rozsiahlu podporu pre zber logov pomocou nástrojov ako Filebeat, Winlogbeat, či Auditbeat. Tieto komponenty umožňujú zber logov z rôznych typov systémov vrátane Windows, Linux, sieťových zariadení a aplikačných služieb. Na úrovni analýzy dát Logstash umožňuje normalizáciu a parsovanie údajov, pričom Elasticsearch poskytuje výkonný indexačný a dotazovací engine. Hoci samotná bezplatná verzia neposkytuje pokročilé ML nástroje, základné alerting mechanizmy je možné nastaviť cez Watcher (alebo Alerting plugin pri OpenSearch variante). Bezpečnostné funkcionality ako TLS medzi komponentmi a RBAC sú k dispozícii až v platených edíciách, čo predstavuje obmedzenie v open-source prostredí. Kibana však poskytuje intuitívne a rozšíriteľné dashboardy s množstvom vizualizačných možností a filtrami.

ToDo popis a účel.

Dokumentácia systému

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker

Docker compose file + popísané zmeny

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

2. SHUFFLE

Typ nástroja: SOAR

Názov nástroja: Shuffle

Verzia: Release 2.1.0

Opis systému

Orchestrácia a automatizácia reakcií (playbooky)

Shuffle je ľahký open-source SOAR nástroj s moderným webovým rozhraním, ktorý umožňuje vizuálnu tvorbu workflowov. Je možné prepojenie na API rôznych nástrojov (Elastic, Graylog, VirusTotal, Slack, Jira, atď.). Výhodou je jednoduchosť nasadenia (Docker) a flexibilita pri budovaní vlastných akcií. Nepodporuje však taký rozsah IR funkcionality ako TheHive a nemá nativne pripravený incident manažment model.

Shuffle SOAR vyniká jednoduchosťou tvorby a správy playbookov. Umožňuje flexibilnú integráciu pomocou REST API a konektorov. Na druhej strane mu chýba hlbší incident manažment, ale je výborný ako doplnkový orchestrátor pre rýchle workflowy.

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

- https://shuffler.io/docs/about
- https://github.com/shuffle/shuffle

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker

Docker compose file + popísané zmeny

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

3. WAZUH

Typ nástroja: EDR

Názov nástroja: Wazuh

Verzia: Version 4.14

Opis systému

Endpoint monitoring/detekcie a základná reakcia + posielanie udalostí do SIEM

Wazuh integruje komponenty pre SIEM, EDR a FIM (File Integrity Monitoring). Zber dát je možný prostredníctvom agentov, ktorí podporujú logy z operačných systémov, súborov, auditných mechanizmov a aplikačných serverov. Okrem toho dokáže prijímať logy zo Syslog, čo umožňuje centralizovaný zber údajov aj z pasívnych zariadení bez agenta. Wazuh poskytuje vlastný korelačný engine, s množstvom pravidiel založených na MITRE ATT&CK. Tieto pravidlá sú pravidelne aktualizované komunitou. Webové UI podporuje RBAC, správu úloh a prepojenie s Kibana dashboardmi. Jeho hlavnou silou je kombinácia EDR vlastností s prehľadným SIEM, čo ho robí výhodným riešením pre menšie tímy.

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

- https://documentation.wazuh.com/current/installation-guide/index.html
- https://hub.docker.com/u/wazuh

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Quickstart

Nainštalovaný na rocky linux 9 VM podľa oficiálnej quickstart dokumentácie https://documentation.wazuh.com/current/quickstart.html

Inštalácia - variant Docker

Docker compose file + popísané zmeny

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

4. GREENBONE COMMUNITY EDITION

Typ nástroja: Skener zraniteľností

Názov nástroja: Greenbone Community Edition (GVM) / OpenVAS

Verzia: Version 24.10

Opis systému

Pravidelné skenovanie infra/servisov a reporting zraniteľností

GCE je bezplatná open-source verzia riešenia od Greenbone Networks, založená na nástroji OpenVAS. Poskytuje vysokokapacitné skenovanie, rozsiahle databázy zraniteľností cez komunitný GVMD feed, moderné webové rozhranie GSA a podporu pre plánovanie, alerty aj automatizáciu. Podporuje štandardy ako CVE, CPE, a umožňuje generovanie reportov vo formátoch CSV, XML, PDF. Možnosti integrácie zahŕňajú GMP protokol, SSH, LDAP, RADIUS a iné. GCE umožňuje aj master-senzor architektúru, čo je výhodné pre rozsiahle distribuované prostredia.

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

- https://greenbone.github.io/docs/latest/
- https://hub.docker.com/u/greenbone

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker

Docker compose file + popísané zmeny

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

5. OPENCTI

Typ nástroja: CTI

Názov nástroja: OpenCTI

Verzia: Version 6.9.0

Opis systému

Správa a korelácia threat intelligence, obohacovanie alertov/incidentov

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

- https://docs.opencti.io/latest/
- https://github.com/OpenCTI-Platform/opencti
- https://hub.docker.com/u/opencti

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

6. MISP

Typ nástroja: CTI

Názov nástroja: MISP

Verzia:

Opis systému

Evidencia, zdieľanie a distribúcia IOCs/events, feedy pre detekcie

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

- https://www.misp-project.org/documentation/
- https://misp.github.io/MISP/

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

7. GLPI

Typ nástroja: Asset management

Názov nástroja: GLPI

Verzia:

Opis systému

Evidencia aktív, CMDB/ITSM evidencia, väzba na vlastníkov a služby

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

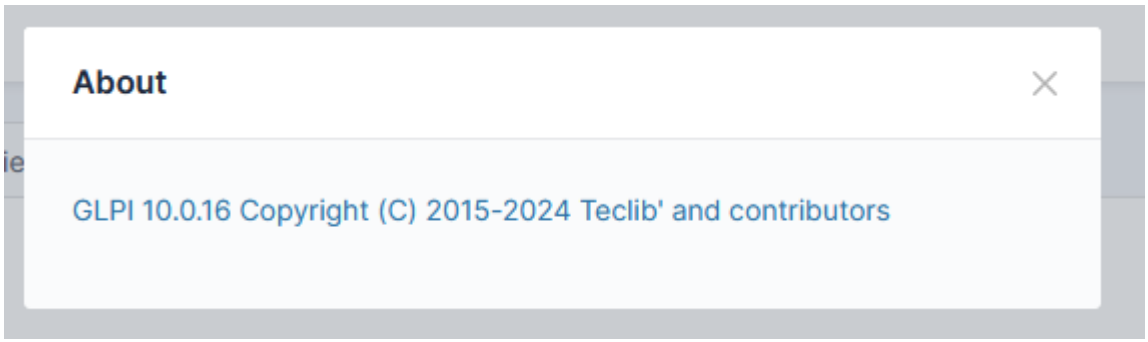
- https://glpi-plugins.readthedocs.io/en/latest/
- https://hub.docker.com/r/glpi/glpi

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker (Compose)



Verzia: GLPI 10.0.16

Docker-compose.yml (zhodný s oficiálnou dokumentáciou, pridaný NGINX ako HTTPS reverse proxy pre SSL/TLS)

```
services:
  glpi:
    image: "glpi/glpi:latest"
    restart: "unless-stopped"
    volumes:
      - "./storage/glpi:/var/glpi:rw"
    env_file: .env # Pass environment variables from .env file to
the container
    depends_on:
      db:
        condition: service_healthy
    ports:
      - "80:80"
  db:
    image: "mysql"
    restart: "unless-stopped"
    volumes:
       - "./storage/mysql:/var/lib/mysql"
    environment:
      MYSQL_RANDOM_ROOT_PASSWORD: "yes"
      MYSQL_DATABASE: ${GLPI_DB_NAME}
      MYSQL_USER: ${GLPI_DB_USER}
      MYSQL_PASSWORD: ${GLPI_DB_PASSWORD}
    healthcheck:
```

```
      test: mysqladmin ping -h 127.0.0.1 -u $$MYSQL_USER --
password=$$MYSQL_PASSWORD
      start_period: 5s
      interval: 5s
      timeout: 5s
      retries: 10
    expose:
      - "3306"
  nginx-https-proxy:
    image: nginx:latest
    restart: always
    ports:
      - "443:443"
    volumes:
      - ./storage/nginx/conf.d/:/etc/nginx/conf.d/:ro
      - ./storage/nginx/certs/:/etc/nginx/certs/:ro
    environment:
      - TIMEZONE=Europe/Bratislava
      - NGINX_HOST=glpi.brainit.tech
      - NGINX_PORT=443
```

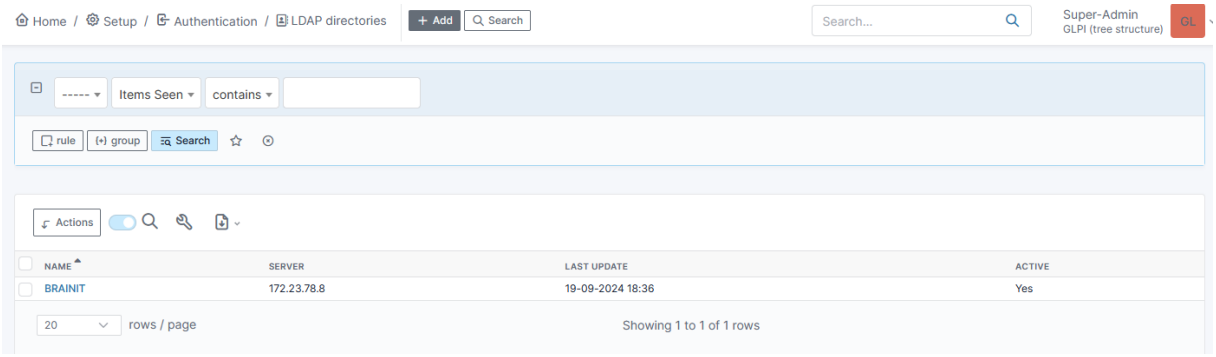
Súbor .env

```
GLPI_DB_HOST=db
GLPI_DB_PORT=3306
GLPI_DB_NAME=glpi
GLPI_DB_USER=glpi
GLPI_DB_PASSWORD=glpi
```

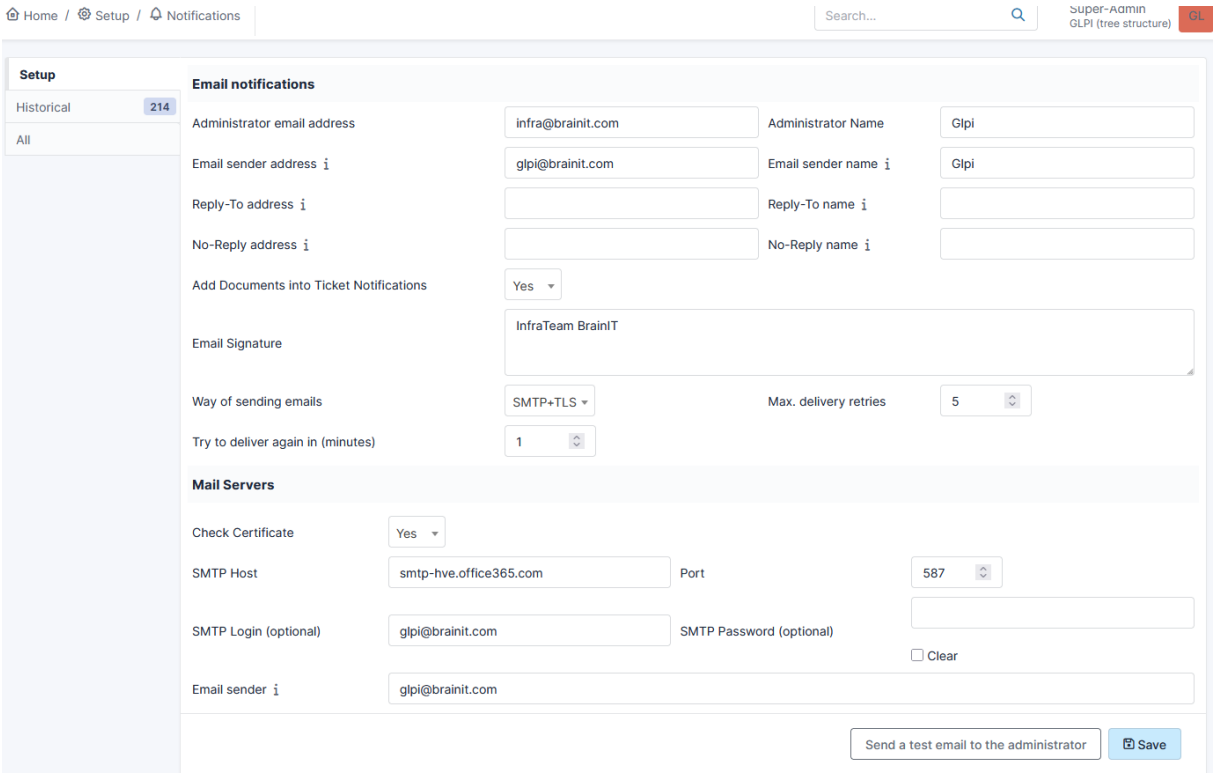
Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia



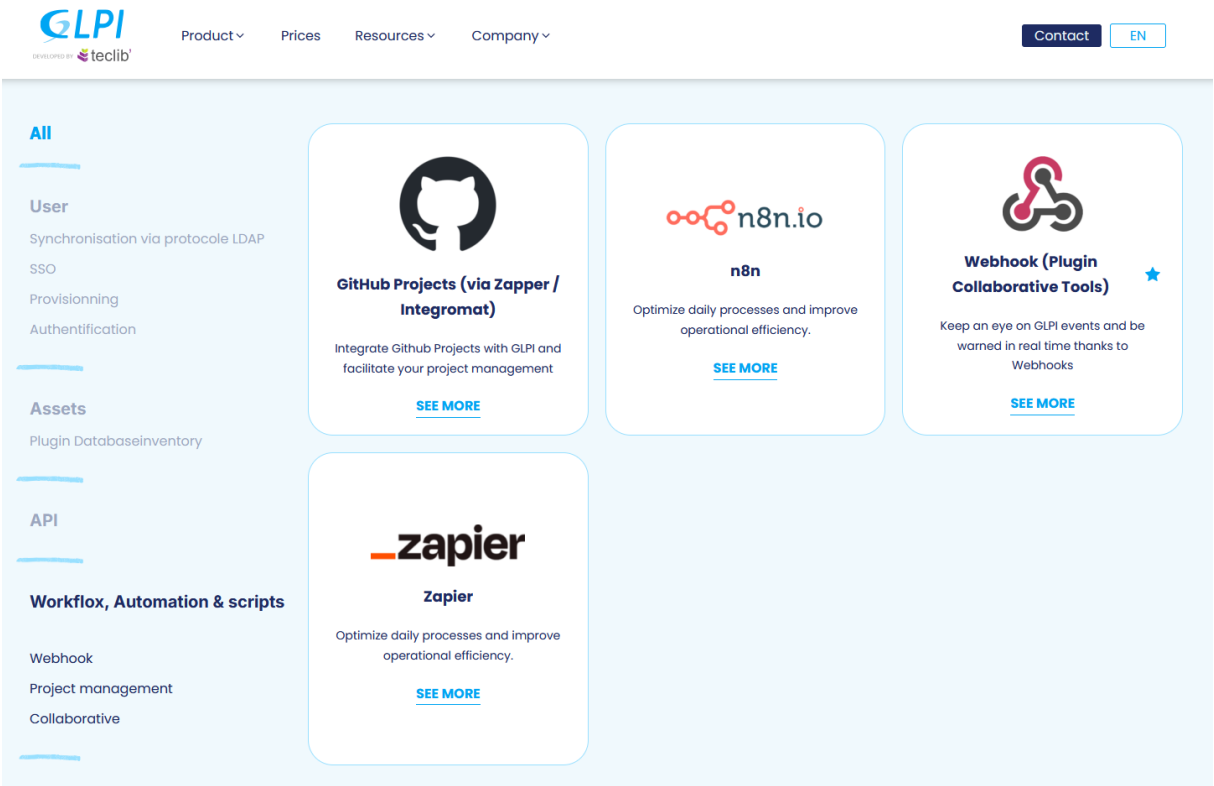
Autentifikácia cez AD/LDAP pre doménu brainit.tech



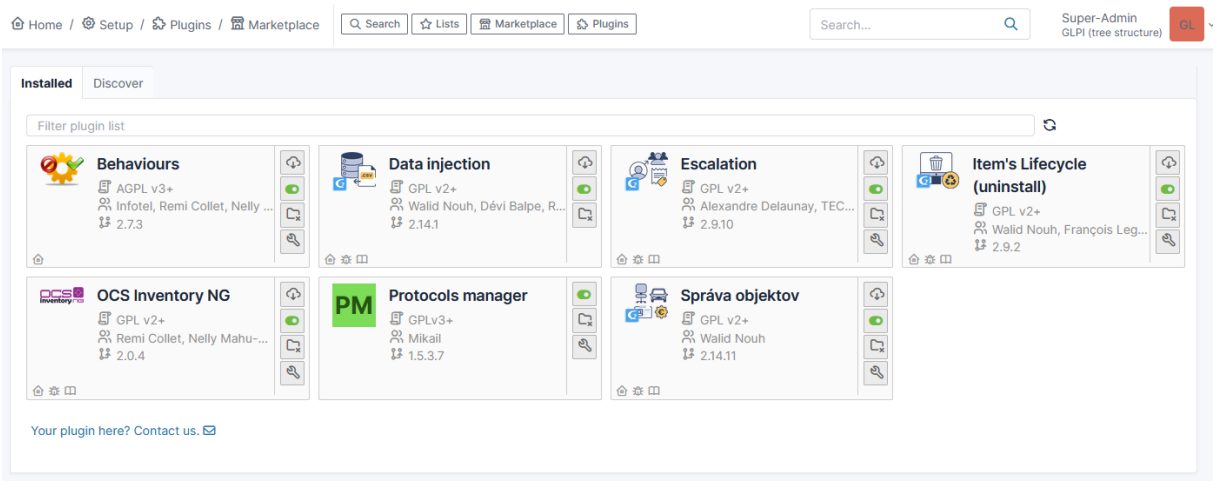
Nastavenie emailových notifikácií ako glpi@brainit.com

Vystupy/Výstupy ???

Integrácie



Viac o možnostiach integrácií na: https://www.glpi-project.org/en/integrations/



Zoznam pluginov v našej inštancii:

https://github.com/InfotelGLPI/behaviors - pridanie povinných polí, vynucovanie formátovania údajov, ...

https://plugins.glpi-project.org/#/plugin/datainjection – import dát vo formáte CSV

https://github.com/pluginsGLPI/escalade – ticket management a eskalácia

https://github.com/pluginsglpi/uninstall – pridanie inventárnych stavov pre vyradzovanie

https://github.com/pluginsGLPI/genericobject – pridávanie vlastných typov objektov

https://github.com/pluginsGLPI/ocsinventoryng – pre synchronizáciu s „OCS Inventory NG“

8. NETBOX

Typ nástroja: Asset management / IPAM/DCIM

Názov nástroja: NetBOX

Verzia:

1.1. Opis systému

Zdroj pravdy pre IP rozsahy, zariadenia, lokality, topológiu (podklad pre skeny a monitoring)

Dokumentácia systému

Officialna dokumentácia:

https://github.com/netbox-community/netbox

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

9. DFIR IRIS – TICKETING

Typ nástroja: Ticketing

Názov nástroja: DFIR IRIS

Verzia:

Opis systému

Správa ticketov a úloh SOC (triage, eskalácie, SLA)

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

- https://docs.dfir-iris.org/latest/

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

10. DFIR IRIS – EVIDENCIA, SPRÁVA INCIDENTOV

Typ nástroja: Evidencia, správa incidentov

Názov nástroja: DFIR IRIS

Verzia:

Opis systému

Správa ticketov a úloh SOC (triage, eskalácie, SLA)

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

- https://docs.dfir-iris.org/latest/

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalácia - variant Docker

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

11. KIBANA (ELK)

Typ nástroja: Reportovanie

Názov nástroja: Kibana (ELK)

Verzia:

Opis nástroja

Vizualizácie, dashboardy a reporty pre SOC a management

ToDo popis a účel.

Dokumentácia systému

Officialna dokumentácia:

- https://github.com/kibana-community/kibana3

Neoficiálna docker compose dokumentácia:

https://github.com/deviantony/docker-elk

Odkazy na officiláne weby + docker hub

Požiadavky na HW

Schémy

Inštalacia - variant Docker

```
services:
  elasticsearch:
    build:
      context: elasticsearch/
      args:
        ELASTIC_VERSION: ${ELASTIC_VERSION}
    volumes:
      -
./elasticsearch/config/elasticsearch.yml:/usr/share/elasticsearch/co
nfig/elasticsearch.yml:ro,Z
      - elasticsearch:/usr/share/elasticsearch/data:Z
    ports:
      - 9200:9200
      - 9300:9300
    environment:
      node.name: elasticsearch
      ES_JAVA_OPTS: -Xms512m -Xmx512m
      # Bootstrap password.
      # Used to initialize the keystore during the initial startup
of
      # Elasticsearch. Ignored on subsequent runs.
      ELASTIC_PASSWORD: ${ELASTIC_PASSWORD:-}
      # Use single node discovery in order to disable production
mode and avoid bootstrap checks.
      # see:
https://www.elastic.co/guide/en/elasticsearch/reference/current/boot
strap-checks.html
      discovery.type: single-node
```

```
    networks:
      - elk
    restart: unless-stopped
  logstash:
    build:
      context: logstash/
      args:
        ELASTIC_VERSION: ${ELASTIC_VERSION}
    volumes:
      -
./logstash/config/logstash.yml:/usr/share/logstash/config/logstash.y
ml:ro,Z
      - ./logstash/pipeline:/usr/share/logstash/pipeline:ro,Z
    ports:
      - 5044:5044
#       - 50000:50000/tcp
      - 514:50000/tcp
#       - 50000:50000/udp
      - 514:50000/udp
      - 9600:9600
    environment:
      LS_JAVA_OPTS: -Xms256m -Xmx256m
      LOGSTASH_INTERNAL_PASSWORD: ${LOGSTASH_INTERNAL_PASSWORD:-}
    networks:
      - elk
    depends_on:
      - elasticsearch
    restart: unless-stopped
  kibana:
    build:
      context: kibana/
      args:
        ELASTIC_VERSION: ${ELASTIC_VERSION}
    volumes:
      -
./kibana/config/kibana.yml:/usr/share/kibana/config/kibana.yml:ro,Z
```

```
    ports:
      # - 5601:5601
      - 80:5601
    environment:
      KIBANA_SYSTEM_PASSWORD: ${KIBANA_SYSTEM_PASSWORD:-}
      SERVER_PUBLICBASEURL: http://elk.innosoc.brainit.tech
    networks:
      - elk
    depends_on:
      - elasticsearch
    restart: unless-stopped
networks:
  elk:
    driver: bridge
volumes:
  elasticsearch:
```

Zmeny v docker compose: Zmenené niektoré sieťové porty – viď zakomentované riadky vyššie.

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia

Konfigurácia nástroja

Vystupy/Výstupy

Integrácie

API, BRAC...

12. WIKI.JS

Typ nástroja: Znalostná databáza

Názov nástroja: Wiki.js

Verzia: 2.5

Opis systému

Znalostná báza (runbooky, postupy, playbooky, onboarding)

ToDo popis a účel.

Slúži pre dokumentáciu interných systémov a postupov.

Dokumentácia systému

Officialna dokumentácia:

- https://docs.requarks.io
- https://github.com/requarks/wiki
- https://hub.docker.com/r/requarks/wiki

Požiadavky na HW:

CPU: 2 jadrá

RAM: 1GB

Storage: 1GB

Schémy

Inštalácia - variant Docker

Docker-compose.yml

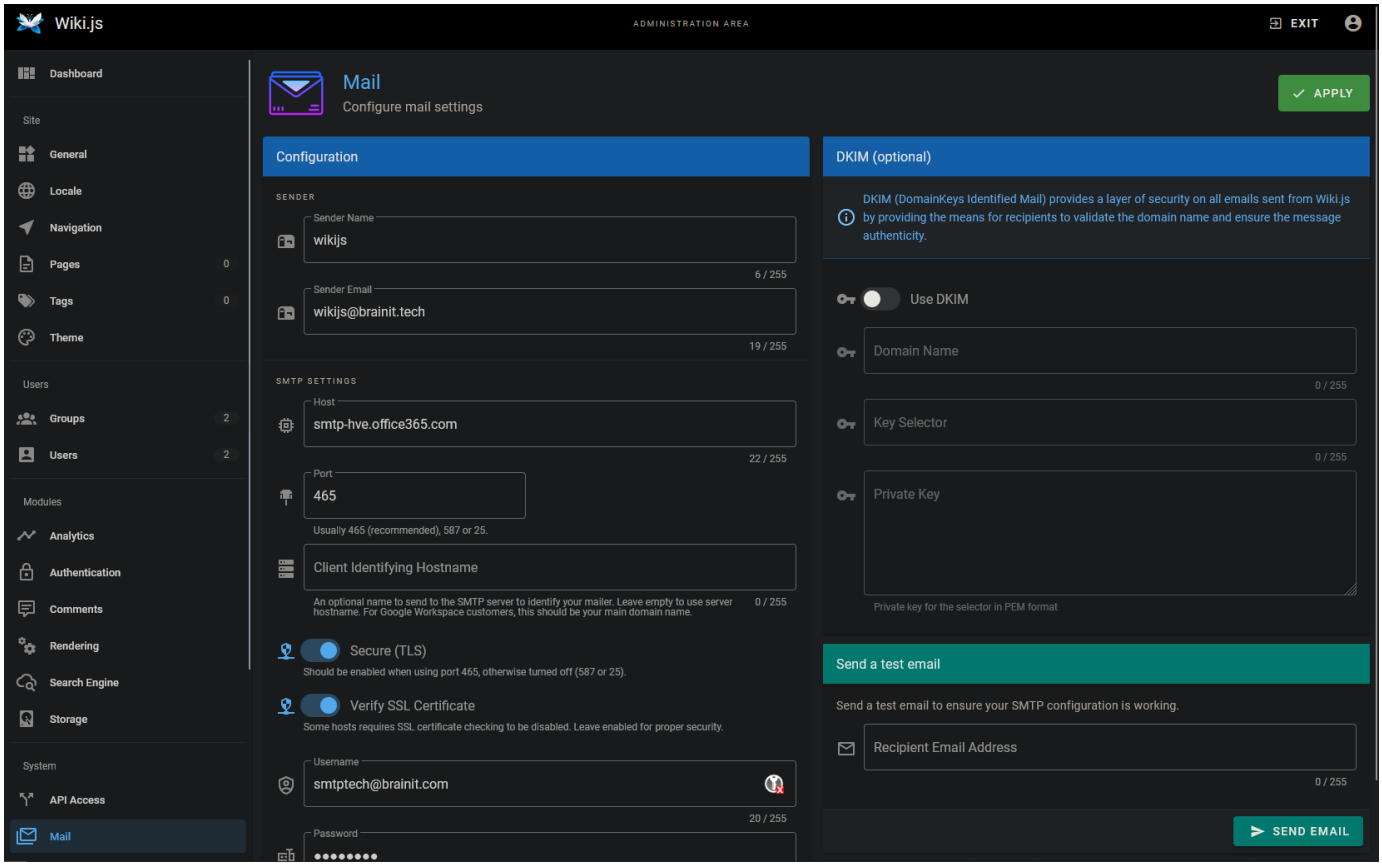
```
services:
  db:
    image: postgres:15-alpine
    environment:
      POSTGRES_DB: wiki
      POSTGRES_PASSWORD: wikijsrocks
      POSTGRES_USER: wikijs
    logging:
      driver: none
    restart: unless-stopped
    volumes:
      - db-data:/var/lib/postgresql/data
  wiki:
    image: ghcr.io/requarks/wiki:2
```

```
    depends_on:
      - db
    environment:
      DB_TYPE: postgres
      DB_HOST: db
      DB_PORT: 5432
      DB_USER: wikijs
      DB_PASS: wikijsrocks
      DB_NAME: wiki
    restart: unless-stopped
    ports:
      - "80:3000"
volumes:
  db-data:
```

Inštalácia - variant Openstack

Inštalácia - variant ...x...

Základná konfigurácia



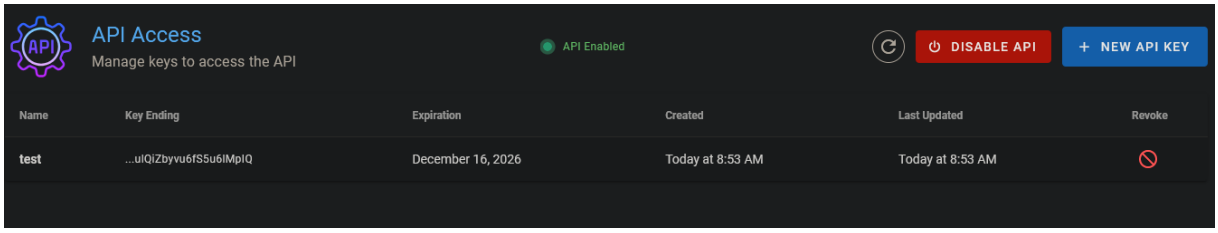
Konfigurácia SMTP

Konfigurácia nástroja

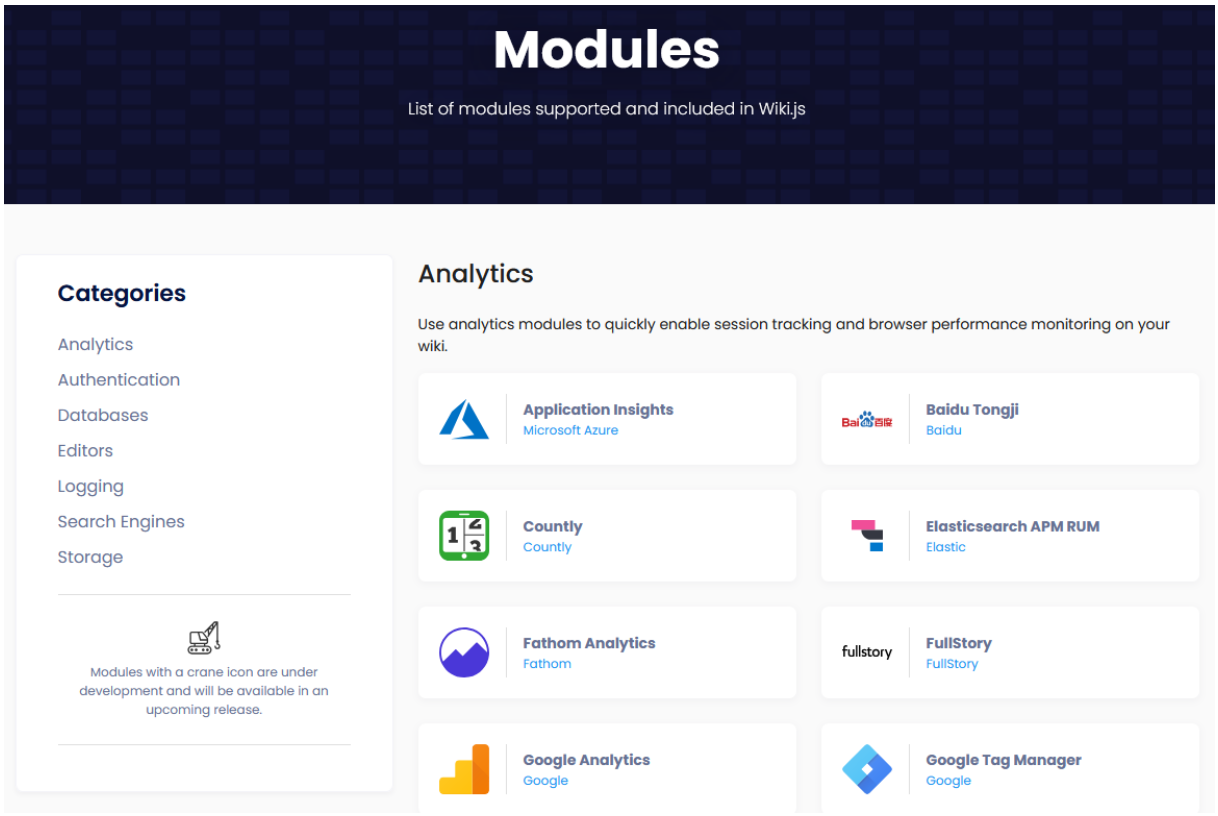
Vystupy/Výstupy

Integrácie

API, BRAC...



Možnosť integrácie cez API kľúče



Iné možnosti integrácií... https://js.wiki/modules

13. OPIS PROSTREDIA NASADENIA