PROJEKT

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

V12 Technologická architektúra

KPB4 – Architektúra riešenia

typ – dokumentácia

mesiac odovzdania – M19

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1. Úvod 3
1.1. Prevádzkové prostredia 3
2. technologická architektúra 3
1.1. Technology Viewpoint CTI 4
1.2. Technology Viewpoint EDR/XDR 11
1.3. Technology Viewpoint INNOSOC Common 17
1.4. Technology Viewpoint Inventarizacia aktiv 19
1.5. Technology Viewpoint Kubernetes 23
1.6. Technology Viewpoint OpenStack 48
1.7. Technology Viewpoint Reportovanie 52
1.8. Technology Viewpoint SIEM 56
1.9. Technology Viewpoint Skener zraniteľností 60
1.10. Technology Viewpoint SOAR 63
1.11. Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov 69
1.12. Technology Viewpoint Znalostný portál pre SOC tím 74
3. Záver 78

1. ÚVOD

Zámerom projektu je vyvinúť technologicky moderné, otvorené a škálovateľné riešenie, ktoré bude schopné podporiť organizácie v efektívnom zvládaní kybernetických hrozieb a zabezpečení prevádzkovej odolnosti. Architektúra riešenia je navrhnutá tak, aby spĺňala princípy vysokej dostupnosti, bezpečnosti a flexibility, pričom zohľadňuje aktuálne štandardy a best practice v oblasti informačných technológií a kybernetickej bezpečnosti.

Technologická architektúra predstavuje štruktúrovaný návrh technologických komponentov, ich vzájomných väzieb a spôsobu integrácie do celkového ekosystému organizácie. Zahŕňa definovanie softvérových vrstiev, komunikačných protokolov, bezpečnostných mechanizmov a prevádzkových procesov. Jej cieľom je zabezpečiť optimálne fungovanie systému, jeho škálovateľnosť, interoperabilitu a schopnosť reagovať na meniace sa požiadavky biznisu a regulačného prostredia.

Projekt reaguje na potreby najmä malých a stredných organizácií, ktoré často nedisponujú dostatočnými odbornými kapacitami ani rozpočtom na vybudovanie vlastného bezpečnostného centra. Navrhované riešenie poskytuje centralizovanú správu, automatizovanú detekciu a reakciu na incidenty, monitoring a reporting, čím znižuje riziko kybernetických útokov a zvyšuje úroveň compliance.

1.1. Prevádzkové prostredia

Navrhovaná prevádzka je plánovaná na dvoch identických prostrediach, ktoré sa líšia len množstvom a typom zdrojov:

PROD prostredie – produkčné prostredie s reálnymi dátami a prevádzkou verejného portálu.

TEST prostredie – testovacie, školiace a predprodukčné prostredie. Celé TEST prostredie je dostupné prostredníctvom VPN pre privilegovaných používateľov.

2. TECHNOLOGICKÁ ARCHITEKTÚRA

Technologická architektúra predstavuje jednu z kľúčových vrstiev architektonického rámca organizácie, zameranú na návrh, výber, integráciu a správu infraštruktúrnych a platformových komponentov, ktoré podporujú chod aplikácií, služieb a procesov. Slúži ako spojovací článok medzi biznis potrebami a technickým riešením, pričom definuje, akým spôsobom budú technologické zdroje a nástroje používané na dosiahnutie požadovaných funkčných a nefunkčných cieľov systému**.** Zahŕňa hardvérové prostredie, virtualizáciu, sieťové vrstvy, kontajnerizačné platformy, riadenie CI/CD pipeline, bezpečnostné mechanizmy a spôsob nasadzovania, prevádzky a monitorovania systémových aj aplikačných komponentov.

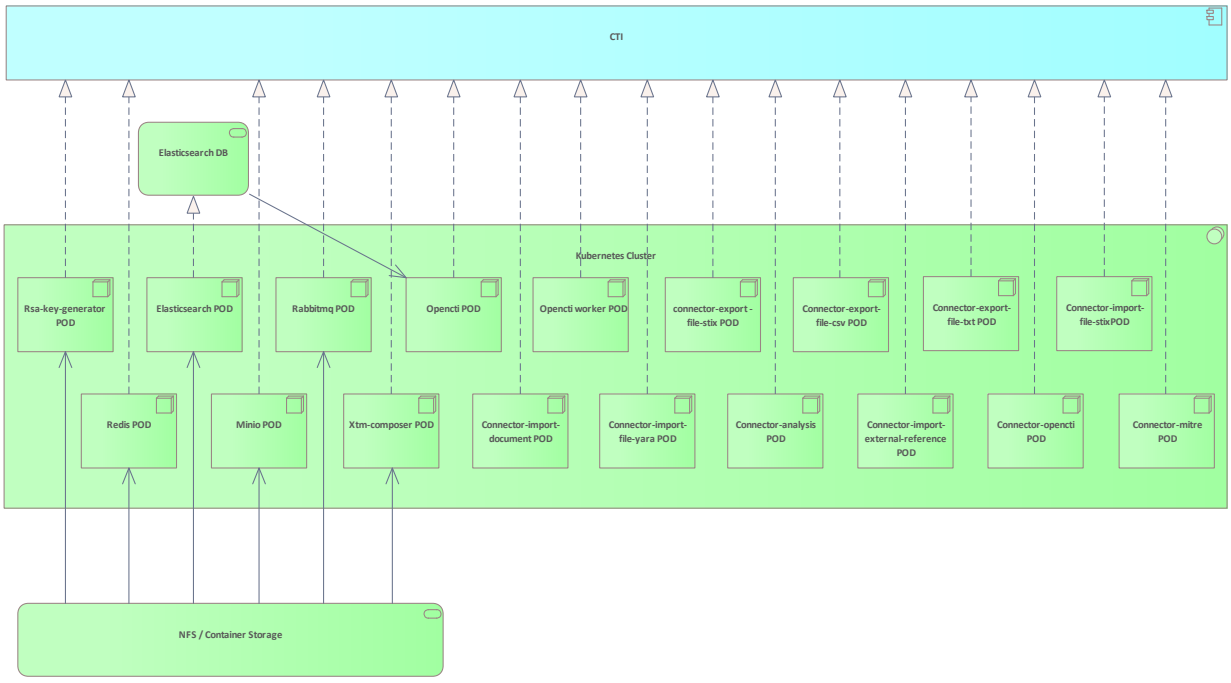
V kontexte moderných informačných systémov – najmä tých, ktoré sú prevádzkované ako cloudové multitenantné služby – je technologická architektúra nevyhnutná pre zabezpečenie škálovateľnosti, vysokej dostupnosti, bezpečnosti a efektívnej prevádzky. Jej návrh musí reflektovať nielen aktuálne požiadavky, ale aj schopnosť systému reagovať na budúce zmeny, podporiť kontinuálny vývoj (DevOps/DevSecOps), integrovať automatizáciu a umožniť flexibilné rozširovanie bez zásadných zásahov do existujúcej prevádzky.

Súčasťou technologickej architektúry sú aj princípy návrhu nasadzovacích jednotiek (napr. PODy pre frontend, backend a podporné služby), využitie kontajnerových technológií a

orchestrace pomocou Kubernetes, nasadzovanie cez GitLab CI/CD Workery, ukladanie artefaktov do Docker Registry, či zabezpečenie komunikácie pomocou validných SSL certifikátov a reverzných proxy vrstiev (napr. HAProxy). Rovnako sú v nej zakomponované mechanizmy na správu sieťových podsietí, zabezpečený prístup k systémovým službám a integrácia monitorovacích a logovacích nástrojov.

Technologická architektúra tak vytvára technický základ celého riešenia – zaručuje konzistentné, automatizované a bezpečné nasadzovanie služieb, efektívne riadenie prevádzky a schopnosť dynamicky reagovať na meniace sa podmienky prostredia aj požiadavky používateľov.

1.1. Technology Viewpoint CTI



Obrázok 1 : Technology Usage Viewpoint CTI alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1 predstavuje využitie Elasticsearch databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databáz pre Elasticsearch.

Popis používaných prvkov:

CTI

CTI (Cyber Threat Intelligence) predstavuje kľúčový stavebný prvok SOCaaS architektúry, pretože poskytuje schopnosť obohacovať detekčné pravidlá, korelačné mechanizmy a playbooky o externé informácie o hrozbách – vrátane IOC, TTP, profilovania útočníkov, kampaní a súvisiacich zraniteľností. V prostredí viaczákaznícke služby SOCaaS zohráva úlohu pri:

- Distribúcii a správe threat feedov naprieč tenantmi,
- Automatickom obohacovaní SIEM a EDR dát o známe hrozby,
- Vytváraní časových línií útokov a priraďovaní k MITRE ATT&CK technikám,
- Podpore procesov threat huntingu a forenznej analýzy,
- Prioritizácii incidentov podľa kontextu hrozieb.

Pre návrh riešenia boli zvolené open-source platformy, ktoré pokrývajú rôzne aspekty CTI – od zberu IOC cez vizualizáciu, až po STIX/TAXII kompatibilitu.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

Connector-analysis POD

Predstavuje POD connector-analysis.

Connector-export- file-csv POD

Predstavuje POD connector-export-file-csv.

connector-export -file-stix POD

Predstavuje POD connector-export-file-stix.

Connector-export- file-txt POD

Predstavuje POD connector-export-file-txt.

Connector-import- document POD

Predstavuje POD connector-import-document.

Connector-import- external-reference POD

Predstavuje POD connector-import-external-reference.

Connector-import- file-stixPOD

Predstavuje POD connector-import-file-stix.

Connector-import- file-yara POD

Predstavuje POD connector-import-file-yara.

Connector-mitre POD

Predstavuje POD connector-mitre.

Connector-opencti POD

Predstavuje POD connector-opencti.

Minio POD

Predstavuje POD minio.

Opencti POD

Predstavuje POD minio.

Opencti worker POD

Predstavuje POD Opencti worker.

Rabbitmq POD

Predstavuje POD rabbitmq.

Redis POD

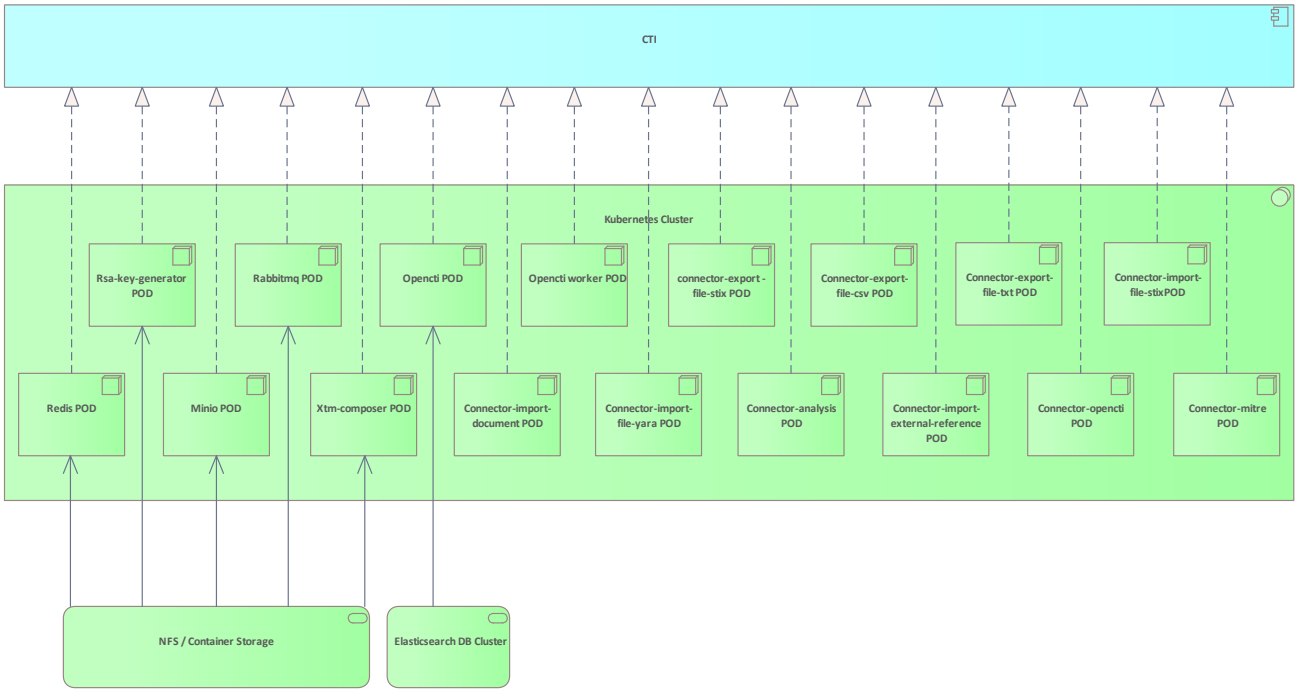
Predstavuje POD redis.

Rsa-key-generator POD

Predstavuje POD rsa-key-generator.

Xtm-composer POD

Predstavuje POD xtm-composer.



Obrázok 2 : Technology Usage Viewpoint CTI alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 2 predstavuje využitie Elasticsearch Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

CTI

CTI (Cyber Threat Intelligence) predstavuje kľúčový stavebný prvok SOCaaS architektúry, pretože poskytuje schopnosť obohacovať detekčné pravidlá, korelačné mechanizmy a playbooky o externé informácie o hrozbách – vrátane IOC, TTP, profilovania útočníkov, kampaní a súvisiacich zraniteľností. V prostredí viaczákaznícke služby SOCaaS zohráva úlohu pri:

- Distribúcii a správe threat feedov naprieč tenantmi,
- Automatickom obohacovaní SIEM a EDR dát o známe hrozby,

• Vytváraní časových línií útokov a priraďovaní k MITRE ATT&CK technikám,

• Podpore procesov threat huntingu a forenznej analýzy,

• Prioritizácii incidentov podľa kontextu hrozieb.

Pre návrh riešenia boli zvolené open-source platformy, ktoré pokrývajú rôzne aspekty CTI – od zberu IOC cez vizualizáciu, až po STIX/TAXII kompatibilitu.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

Connector-analysis POD

Predstavuje POD connector-analysis.

Connector-export- file-csv POD

Predstavuje POD connector-export-file-csv.

connector-export -file-stix POD

Predstavuje POD connector-export-file-stix.

Connector-export- file-txt POD

Predstavuje POD connector-export-file-txt.

Connector-import- document POD

Predstavuje POD connector-import-document.

Connector-import- external-reference POD

Predstavuje POD connector-import-external-reference.

Connector-import- file-stixPOD

Predstavuje POD connector-import-file-stix.

Connector-import- file-yara POD

Predstavuje POD connector-import-file-yara.

Connector-mitre POD

Predstavuje POD connector-mitre.

Connector-opencti POD

Predstavuje POD connector-opencti.

Minio POD

Predstavuje POD minio.

Opencti POD

Predstavuje POD minio.

Opencti worker POD

Predstavuje POD Opencti worker.

Rabbitmq POD

Predstavuje POD rabbitmq.

Redis POD

Predstavuje POD redis.

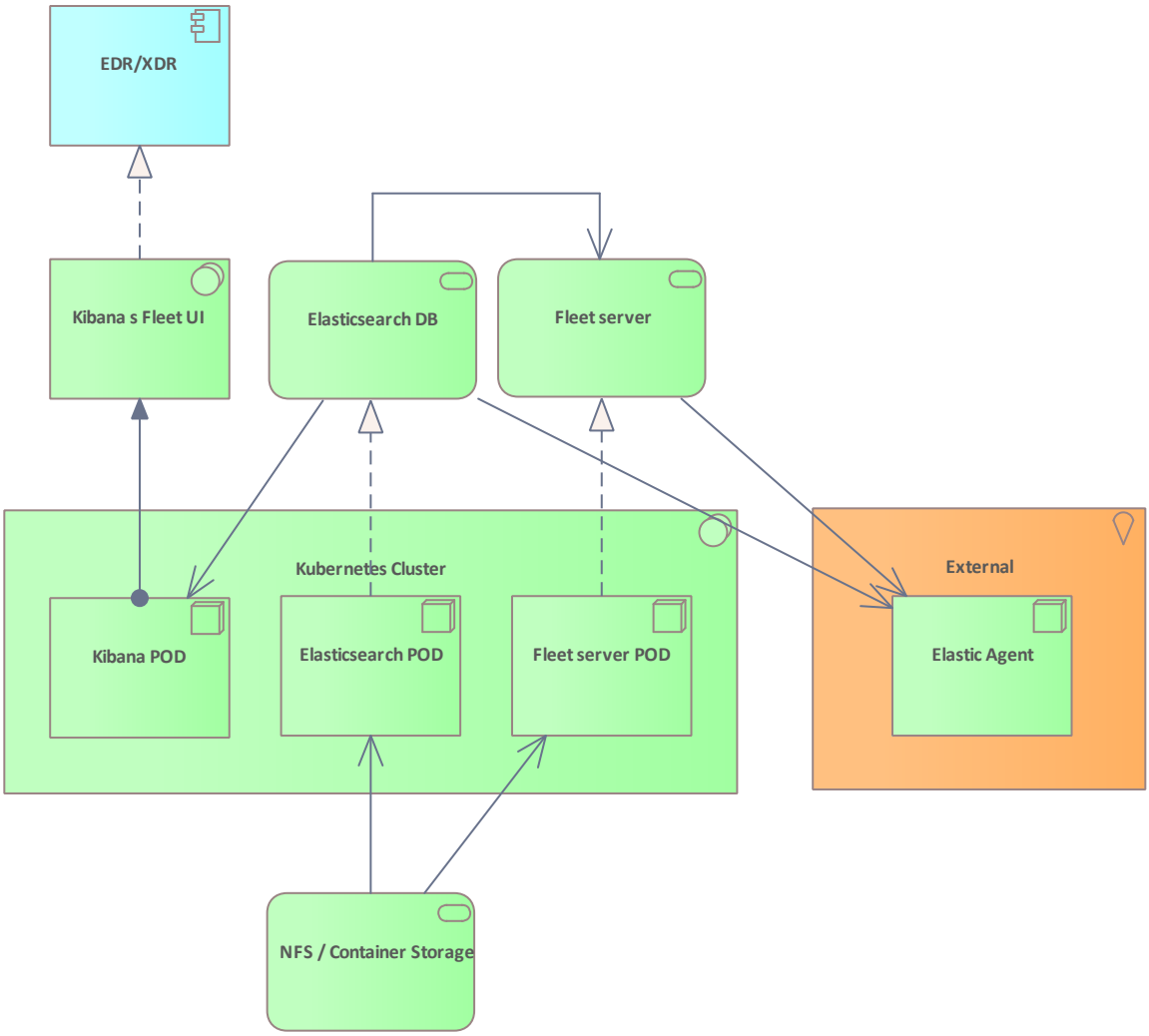
Rsa-key-generator POD

Predstavuje POD rsa-key-generator.

Xtm-composer POD

Predstavuje POD xtm-composer.

1.2. Technology Viewpoint EDR/XDR



Obrázok 3 : Technology Usage Viewpoint EDR/XDR alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1 predstavuje využitie Elasticsearch databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databáz pre Elasticsearch.

Popis používaných prvkov:

EDR/XDR

EDR (Endpoint Detection and Response) a XDR (Extended Detection and Response) predstavujú základné technologické piliere pre detekciu hrozieb na úrovni koncových zariadení. V prostredí SOCaaS slúžia na zber, koreláciu a reakciu na udalosti, ktoré by inak unikli tradičným perimeterovým detekciám. XDR rozširuje koncept EDR o schopnosť integrovať dáta zo sietí, cloudov, e-mailových systémov a iných vrstiev.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

Predstavuje POD Kibana pre SIEM.

Fleet server

Predstavuje technologickú službu Fleet server pre správu Elastic agents.

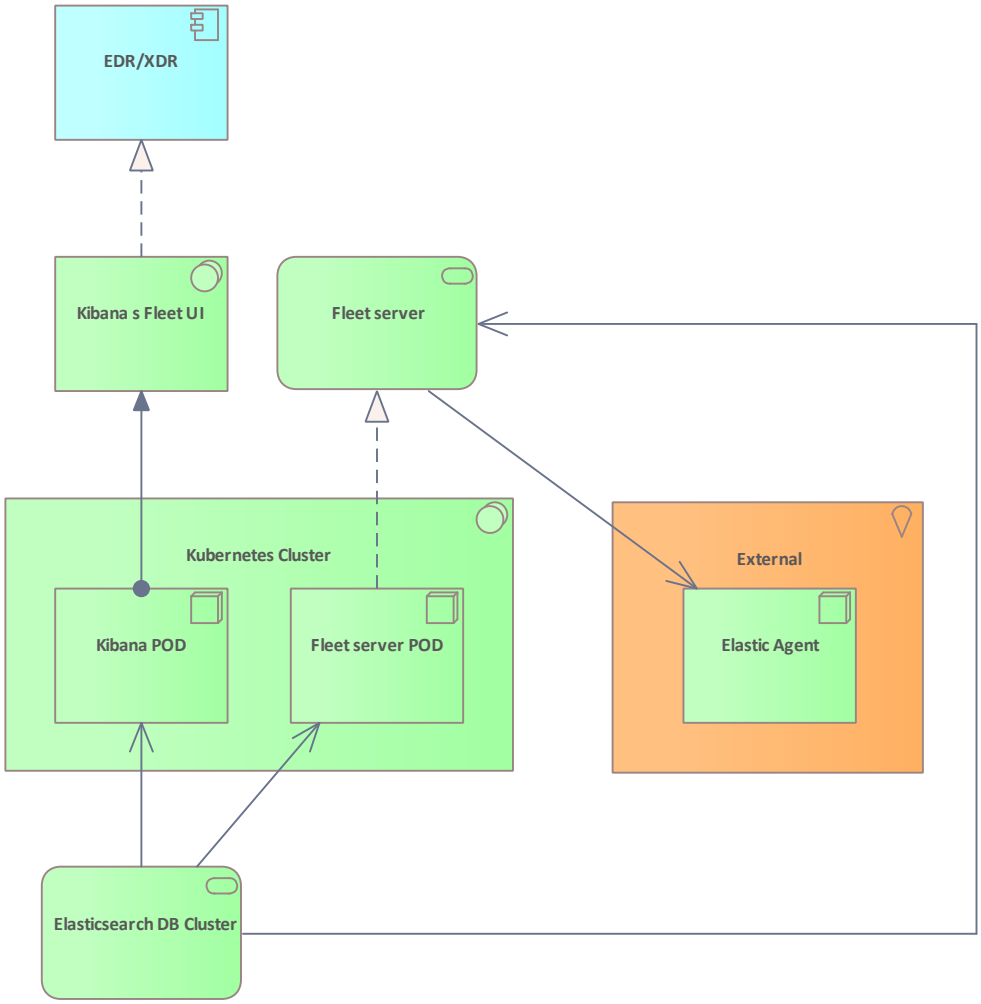
Elastic Agent

Predstavuje inštanciu Elastic Agent pre monitoring a spracovanie logov a ich zapísanie do Elasticsearch a ochranu hosta pred bezpečnostnými hrozbami.

Fleet server POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

Kibana s Fleet UI



Obrázok 4 : Technology Usage Viewpoint EDR/XDR alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 2 predstavuje využitie Elasticsearch Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

EDR/XDR

EDR (Endpoint Detection and Response) a XDR (Extended Detection and Response) predstavujú základné technologické piliere pre detekciu hrozieb na úrovni koncových zariadení. V prostredí SOCaaS slúžia na zber, koreláciu a reakciu na udalosti, ktoré by inak unikli tradičným perimeterovým detekciám. XDR rozširuje koncept EDR o schopnosť integrovať dáta zo sietí, cloudov, e-mailových systémov a iných vrstiev.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

Predstavuje POD Kibana pre SIEM.

Fleet server

Predstavuje technologickú službu Fleet server pre správu Elastic agents.

Elastic Agent

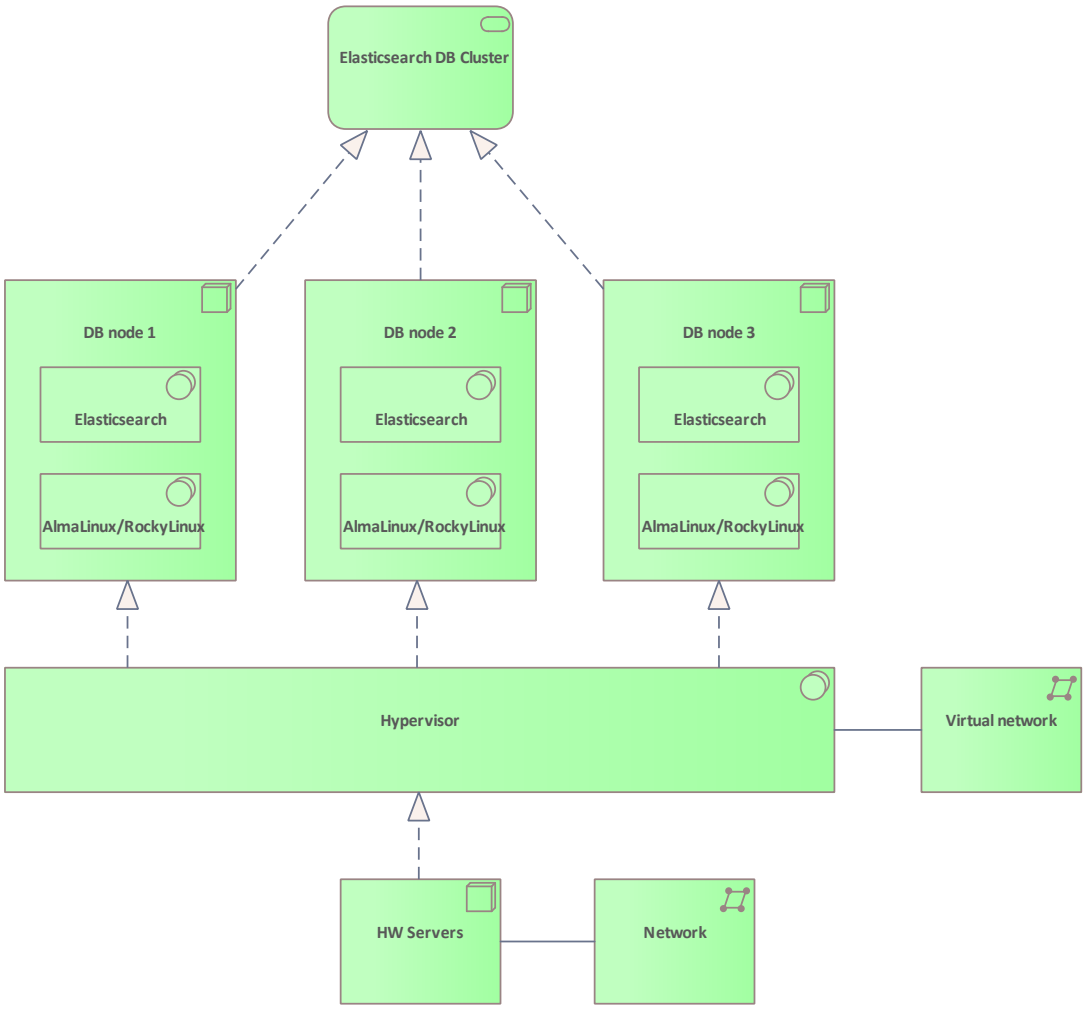
Predstavuje inštanciu Elastic Agent pre monitoring a spracovanie logov a ich zapísanie do Elasticsearch a ochranu hosta pred bezpečnostnými hrozbami.

Fleet server POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

Kibana s Fleet UI

1.3. Technology Viewpoint INNOSOC Common



Obrázok 5 : Technology Viewpoint DB Cluster

Diagram znázorňuje technologickú architektúru PostgreSQL Clustra.

Popis používaných prvkov:

DB node 1

Predstavuje Node 1 Elasticsearch Clustra.

DB node 2

Predstavuje Node 2 Elasticsearch Clustra.

DB node 3

Predstavuje Node 3 Elasticsearch Clustra.

HW Servers

Predstavuje HW serverovú infraštruktúru. HW serverová infraštruktúra predstavuje fyzické výpočtové a sieťové vybavenie, ktoré tvorí základ pre prevádzku IT systémov, vrátane serverov, úložísk, prepínačov, smerovačov a záložných zdrojov napájania. Táto infraštruktúra je nasadzovaná buď on-premise alebo ako súčasť cloudovej platformy, a poskytuje výpočtový výkon, dostupnosť a konektivitu pre virtualizované aj nevirtualizované prostredia.

Hypervisor

Predstavuje Hypervisor 1. alebo 2. typu. Hypervisor 1. typu, známy aj ako "bare-metal" hypervisor, beží priamo na fyzickom hardvéri bez operačného systému, čím poskytuje vysoký výkon a efektivitu virtualizácie; príkladmi sú VMware ESXi, Microsoft Hyper-V (core) alebo Xen. Tento typ hypervisora je určený najmä pre dátové centrá a enterprise prostredia, kde sa kladie dôraz na výkon, stabilitu a bezpečnosť.

Hypervisor 2. typu, nazývaný aj "hostovaný" hypervisor, beží nad existujúcim operačným systémom ako aplikácia, a tým zdieľa systémové zdroje s hostiteľom; príklady zahŕňajú VMware Workstation alebo Oracle VirtualBox. Hoci je jednoduchší na inštaláciu a vhodný na vývoj alebo testovanie, jeho výkon a izolácia sú nižšie v porovnaní s typom 1.

Network

Predstavuje sieť/subsieť HW infraštruktúry. Sieť alebo podsieť HW infraštruktúry je fyzická a logická vrstva prepojenia serverov, úložísk a sieťových zariadení, ktorá zabezpečuje prenos dát, komunikáciu a prístup k službám v rámci dátového centra.

Virtual network

Predstavuje virtuálnu sieť/subsieť Hypervisora. Virtuálna sieť alebo podsieť Hypervisora je logická sieťová infraštruktúra, ktorú hypervisor vytvára na účely prepojenia

virtuálnych strojov (VM) medzi sebou, s hostiteľským systémom alebo s vonkajšou sieťou. Umožňuje definovanie virtuálnych switchov, NAT, bridged alebo internal networking režimov, čím poskytuje flexibilitu v izolácii, komunikácii a routovaní dát medzi VM a fyzickým sieťovým prostredím.

AlmaLinux/RockyLinux

Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

Elasticsearch

Predstavuje Elasticsearch NoSQL databázu.

AlmaLinux/RockyLinux

Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

Elasticsearch

Predstavuje Elasticsearch NoSQL databázu.

AlmaLinux/RockyLinux

Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

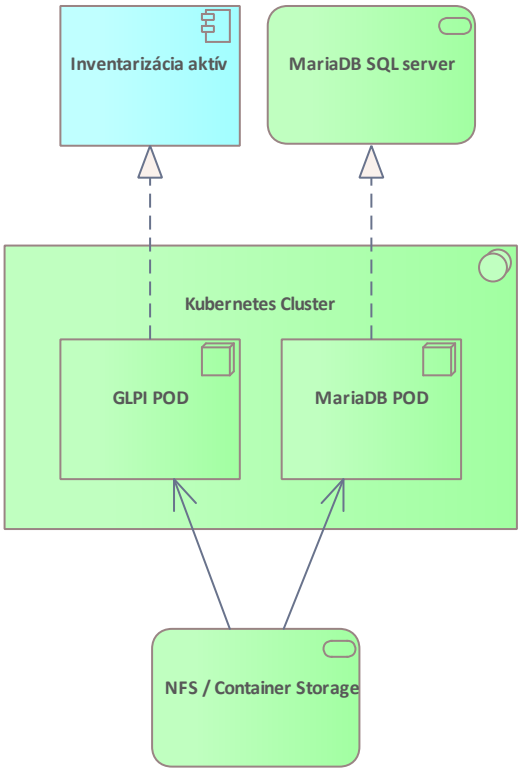
Elasticsearch

Predstavuje Elasticsearch NoSQL databázu.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

1.4. Technology Viewpoint Inventarizacia aktiv



Obrázok 6 : Technology Usage Viewpoint Inventarizacia aktiv alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1 predstavuje využitie Databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou SQL servera.

Popis používaných prvkov:

Inventarizácia aktív

Inventarizácia aktív je základným pilierom každého bezpečnostného riešenia. Umožňuje SOC tímu získať prehľad o všetkých zariadeniach, systémových entitách, aplikáciách a virtuálnych či cloudových zdrojoch, ktoré tvoria infraštruktúru organizácie. V prostredí SOCaaS zohráva ešte významnejšiu úlohu, pretože umožňuje centralizovanú správu, kategorizáciu, monitorovanie a sledovanie bezpečnostného stavu infraštruktúry naprieč rôznymi zákazníkmi.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

MariaDB SQL server

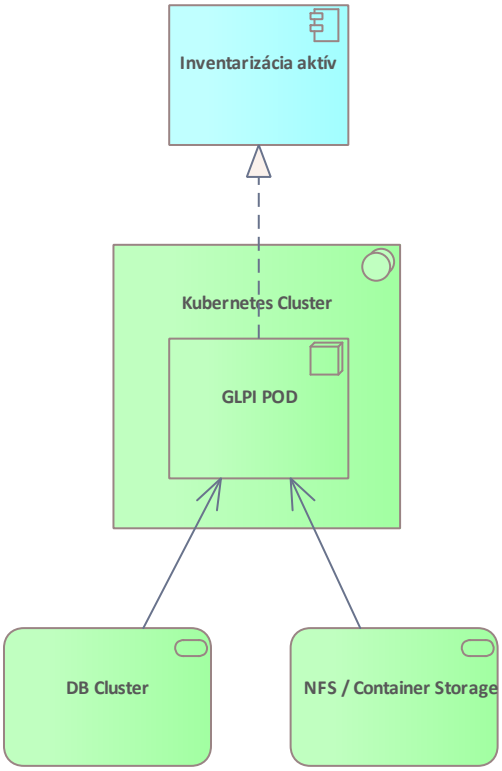
Predstavuje technologickú službu relačnej MariaDB SLQ databázy. Technologická služba v oblasti databázových systémov označuje softvérový komponent alebo platformu, ktorá poskytuje konzistentné, riadené a škálovateľné prostredie pre ukladanie, manipuláciu a správu štruktúrovaných údajov. V prípade relačnej databázy MariaDB, ide o platformovo nezávislú databázovú službu, ktorá sprístupňuje relačný model pomocou SQL (Structured Query Language) prostredníctvom konzistentného a transakčne bezpečného aplikačného rozhrania.

GLPI POD

Predstavuje POD GLPI pre invertarizáckiu aktív. GLPI (Gestionnaire Libre de Parc Informatique) je open-source systém pre správu IT služieb (ITSM), ktorý ponúka funkcionality ako správa IT aktív (hardware, software), incident management, service request management, správa zásob a používateľov a CMDB (Configuration Management Database). POD (Point Of Deployment) v kontexte GLPI predstavuje modulárne a distribuované nasadenie GLPI komponentov na viacerých miestach alebo lokalitách, pričom každé POD pôsobí ako lokálny uzol pre zber, aktualizáciu a správu IT aktív.

MariaDB POD

Predstavuje POD MariaDB pre relačnú SQL DB. MariaDB je pokročilý open-source relačný databázový systém (RDBMS), ktorý vznikol ako fork MySQL. Dodržiava štandard SQL (Structured Query Language) a poskytuje výkonné nástroje na správu a manipuláciu s relačnými údajmi. MariaDB podporuje klasickú ACID architektúru (Atomicita, Konzistencia, Izolácia, Trvácnosť) a MVCC (Multiversion Concurrency Control) pre bezpečné a konzistentné databázové transakcie.



Obrázok 7 : Technology Usage Viewpoint Inventarizacia aktiv alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 2 predstavuje využitie Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

Inventarizácia aktív

Inventarizácia aktív je základným pilierom každého bezpečnostného riešenia. Umožňuje SOC tímu získať prehľad o všetkých zariadeniach, systémových entitách, aplikáciách a virtuálnych či cloudových zdrojoch, ktoré tvoria infraštruktúru organizácie. V prostredí SOCaaS zohráva ešte významnejšiu úlohu, pretože umožňuje centralizovanú

správu, kategorizáciu, monitorovanie a sledovanie bezpečnostného stavu infraštruktúry naprieč rôznymi zákazníkmi.

DB Cluster

Predstavuje službu clustrovanej relačnej databázy. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

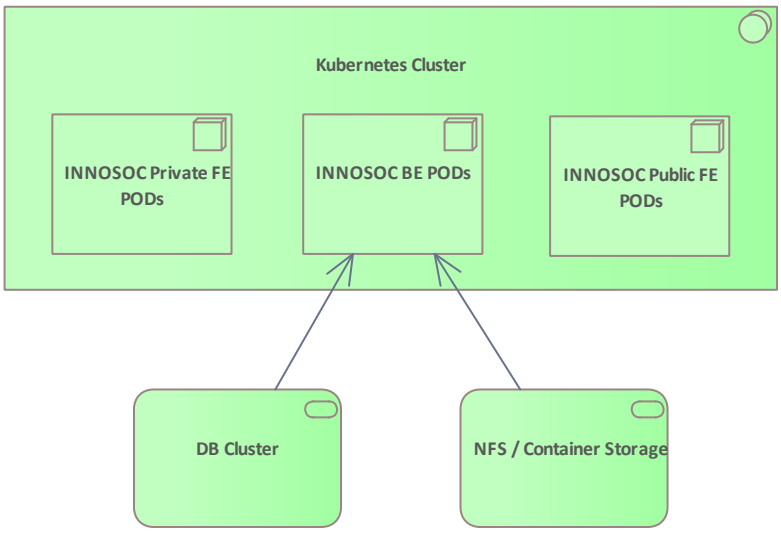
Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

GLPI POD

Predstavuje POD GLPI pre invertarizáckiu aktív. GLPI (Gestionnaire Libre de Parc Informatique) je open-source systém pre správu IT služieb (ITSM), ktorý ponúka funkcionality ako správa IT aktív (hardware, software), incident management, service request management, správa zásob a používateľov a CMDB (Configuration Management Database). POD (Point Of Deployment) v kontexte GLPI predstavuje modulárne a distribuované nasadenie GLPI komponentov na viacerých miestach alebo lokalitách, pričom každé POD pôsobí ako lokálny uzol pre zber, aktualizáciu a správu IT aktív.

1.5. Technology Viewpoint Kubernetes



Obrázok 8 : Technology Usage Viewpoint CNM and Containers maping

Diagram znázorňuje priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Popis používaných prvkov:

DB Cluster

Predstavuje službu clustrovanej relačnej databázy. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

INNOSOC BE PODs

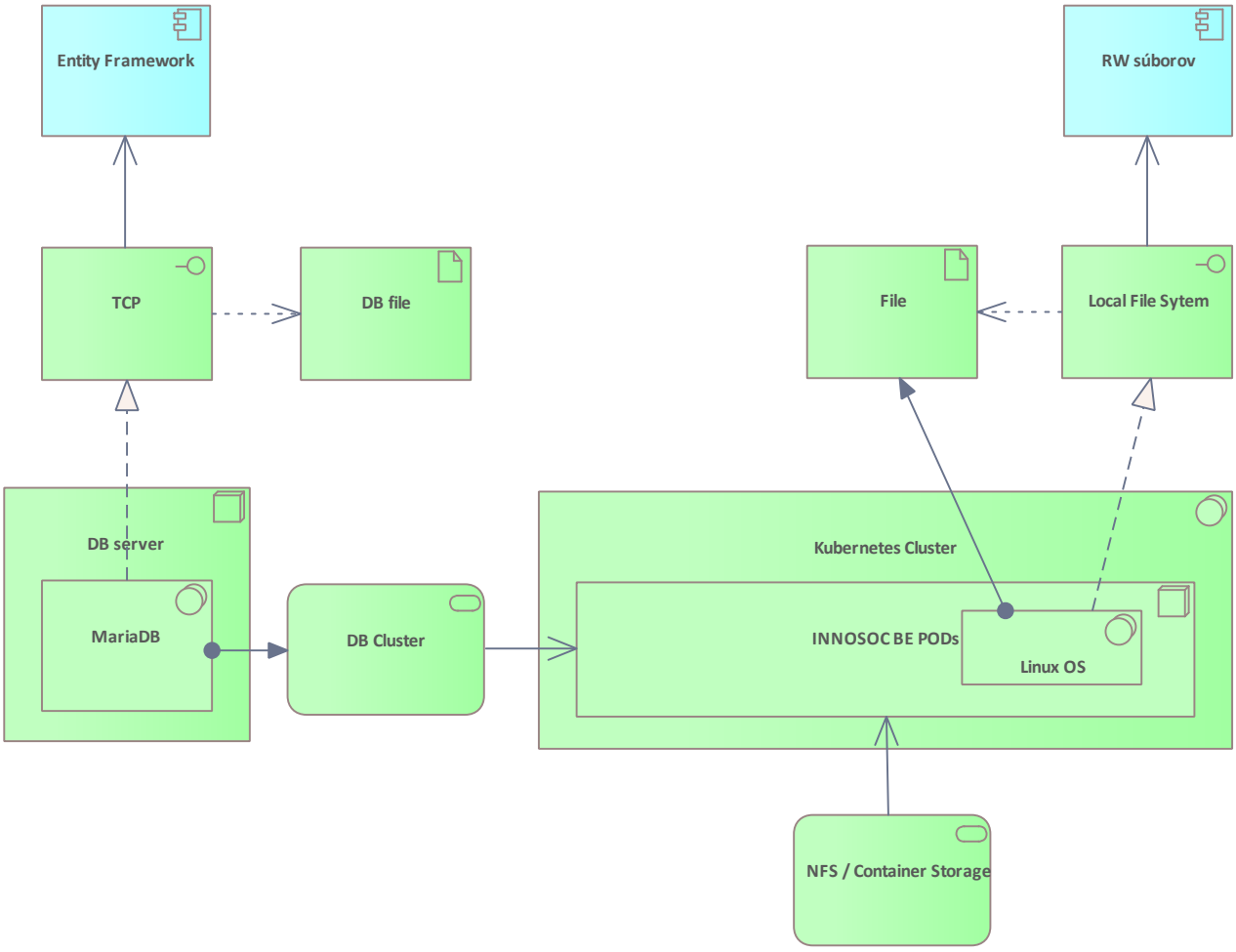
Predstavuje PODy CNM BE. PODy CNM BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému Core Network Management (CNM), ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu CNM architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

INNOSOC Private FE PODs

PODy CNM FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v privátnom prostredí zákazníka. Ide o architektonický prvok vychádzajúci z princípov kontajnerizácie a mikroservisnej architektúry, kde každý POD obsahuje samostatne nasaditeľné prvky prezentačnej vrstvy (FE – frontend), ako sú webové aplikácie, Single Page Applications (SPA), či UI moduly.

INNOSOC Public FE PODs

PODy CNM FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v verejne dostupnom cloudovom alebo hybridnom prostredí, ktoré je spravované poskytovateľom služby alebo centralizovanou infraštruktúrou organizácie. V rámci tejto architektúry sú frontendové komponenty – typicky Single Page Applications (SPA) alebo webové rozhrania – prevádzkované ako súčasť viacnájomného (multi-tenant) systému, dostupného cez verejnú sieť (internet), pričom komunikácia a prístup sú riadené prísnymi bezpečnostnými politikami. Tieto PODy fungujú ako izolované deploymenty v rámci centralizovaného cloudu (napr. Microsoft Azure, AWS, GCP), prípadne v spravovanom Kubernetes clustri. Ich cieľom je zabezpečiť škálovateľné, vysoko dostupné a jednoducho aktualizovateľné rozhranie pre koncových používateľov alebo zákazníkov, ktorí pristupujú k CNM službám bez nutnosti lokálnej inštalácie alebo privátnej infraštruktúry.



Obrázok 9 : Technology Usage Viewpoint CNM BE, DB and File System

Diagram repezentuje a bližšie popisuje využívanie perzistentnej vrstvy pre potreby BIT NC a CNM BE modulu a pomocou jeho komponentu Dátovej vrstvy ktorý zabezpečuje prácu s PostgreSQL a Local File System.

Popis používaných prvkov:

DB Cluster

Predstavuje službu clustrovanej relačnej databázy. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

DB file

DB file - súbor reprezentujúci databázový súbor MariaDB. DB file (database file) v kontexte systému MariaDB predstavuje fyzický súbor na úložisku, ktorý reprezentuje perzistentnú dátovú štruktúru databázy. Tento súbor obsahuje samotné dáta, metadáta, indexy, transakčné logy alebo systémové štruktúry používané databázovým enginom (najčastejšie InnoDB alebo MyISAM) na správu relačných dát.

DB server

Predstavuje MariaDB server. MariaDB Server je relačný databázový serverový systém (RDBMS) typu open-source, určený na správu, uchovávanie a manipuláciu s štruktúrovanými údajmi. Je kompatibilný s MySQL (jeho pôvodný fork), využíva jazyk SQL a je optimalizovaný pre výkon, bezpečnosť, transakčnosť a škálovateľnosť.

File

File - súbor je základná jednotka ukladania dát v súborovom systéme, ktorá reprezentuje štruktúrované alebo neštruktúrované dáta ako prílohy, obrázky, dokumenty, multimédiá a iné digitálne objekty. Súbor obsahuje metadáta (napr. názov, typ, veľkosť, časové značky, prístupové práva) a binárny alebo textový obsah, ktorý je interpretovaný podľa MIME typu alebo prípony.

Entity Framework

Aplikačný modul Entity Framework (EF) predstavuje logickú softvérovú vrstvu v aplikácii, ktorá využíva technológiu Entity Framework na objektovo-relačné mapovanie (ORM) medzi databázou a objektmi programovacieho jazyka (najčastejšie C# v .NET ekosystéme). Tento modul zabezpečuje, že aplikácia môže pracovať s databázovými tabuľkami ako s objektami a kolekciami tried, pričom všetky CRUD operácie (Create, Read, Update, Delete) sú automaticky prekladané na SQL príkazy.

RW súborov

Modul RW nad súbormi predstavuje softvérovú komponentu alebo logickú vrstvu, ktorá zabezpečuje čítanie (Read) a zápis (Write) údajov do súborov v rámci súborového systému. Tento modul slúži ako abstrakcia medzi aplikačnou logikou a fyzickým úložiskom, pričom využíva štandardné systémové rozhrania operačného systému na manipuláciu so súbormi (napr. POSIX API alebo abstraktné I/O knižnice).

Local File Sytem

Lokálny súborový systém poskytujúci prácu so súbormi realizovaný operačným systémom pod ktorým je spúšťaný BE modul. Tento súborový systém umožňuje nízkolatenčný prístup k súborom, typicky prostredníctvom štandardných POSIX operácií a je viazaný na konkrétny fyzický alebo virtuálny uzol. V kontajnerizovaných prostrediach (napr. Kubernetes) je tento typ úložiska obvykle reprezentovaný typom hostPath alebo emptyDir, čím sa viaže na konkrétny uzol a stráca perzistenciu pri reštarte alebo presune PODu. Lokálny súborový systém je vhodný pre dočasné, vysokovýkonné operácie (napr. cache, scratch space), ale nie je určený na trvalé alebo zdieľané ukladanie dát, keďže neumožňuje nezávislé zotavenie dát po výpadku alebo škálovanie medzi uzlami.

TCP

Predstavuje client server komunikáciu pomocou TCP protokolu. Client-server komunikácia cez TCP (Transmission Control Protocol) je spôsob výmeny dát medzi dvoma entitami v počítačovej sieti, kde klient iniciuje spojenie a server pasívne čaká na pripojenie. Prenos je realizovaný prostredníctvom TCP protokolu – transportného protokolu vrstvy 4 (transport layer) modelu OSI, ktorý poskytuje spoľahlivý, riadený a orientovaný prenos dát cez sieť.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

INNOSOC BE PODs

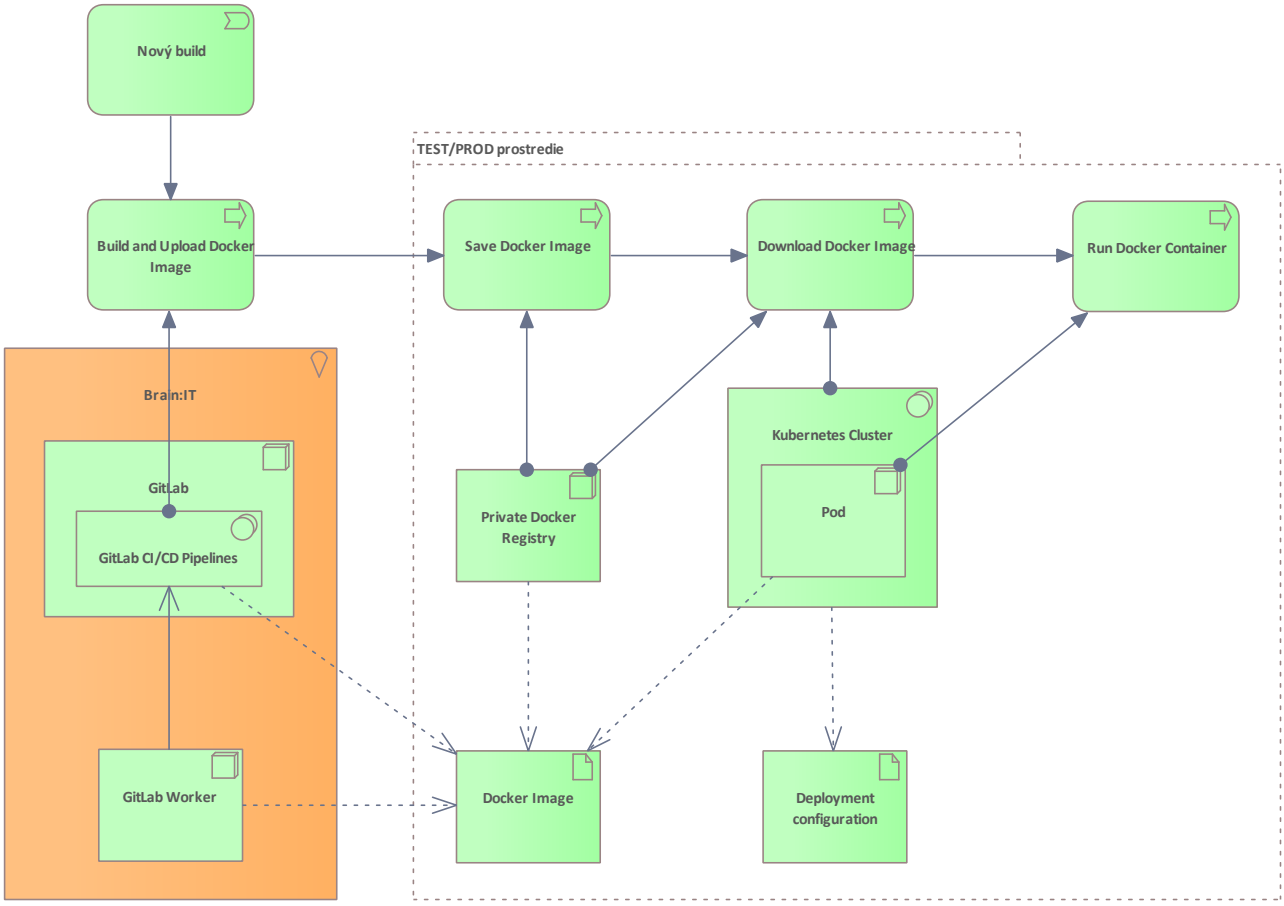
Predstavuje PODy CNM BE. PODy CNM BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému Core Network Management (CNM), ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu CNM architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

Linux OS

Linux je viacúlohový, viacpoužívateľský, unixovo kompatibilný operačný systém (OS) postavený na monolitickom jadre, vyvíjaný ako open-source softvér. Vyznačuje sa modulárnou architektúrou, vysokou prispôsobiteľnosťou a je používaný v serveroch, desktopoch, mobilných zariadeniach, embedded systémoch a superpočítačoch. Linux je technicky softvérová vrstva medzi hardvérom a používateľskými aplikáciami, ktorá zabezpečuje správu procesov, pamäte, súborových systémov, zariadení a sieťovej komunikácie.

MariaDB

Predstavuje MariaDB relačnú databázu. MariaDB predstavuje relačnú databázu (Relational Database Management System – RDBMS). V zmysle formálnej definície je MariaDB databázový systém, ktorý: pracuje s relačným modelom (údaje sú organizované do tabuliek, stĺpcov a riadkov), používa jazyk SQL (Structured Query Language) na manipuláciu a dotazovanie dát, zabezpečuje integritu údajov pomocou primárnych a cudzích kľúčov a implementuje ACID vlastnosti prostredníctvom svojich storage enginov.



Obrázok 10 : Technology Viewpoint Development CI/CD TEST/PROD

Diagram znázorňuje proces buildu a nasadenia novej verzie balíka v podobe Docker image do TEST/PROD prostredia. Diagram je využitelný pre prípad vlastných balíkov, pre ostatné existujúce sa využíva verejný DockerHub zdroj.

Popis používaných prvkov:

Build and Upload Docker Image

Build proces s následným nahratím Docker Image do Docker Registry je štandardný krok, ktorý zabezpečuje automatizované zostavenie aplikačného kontajnera, jeho označenie a publikovanie do centralizovaného repozitára, odkiaľ môže byť nasadený do vývojových, testovacích alebo produkčných prostredí.

Download Docker Image

Uloženie Docker image do Docker Registry začína vytvorením image z Dockerfile pomocou príkazu docker build. Následne sa image označí podľa názvu a verzie cieľového registry. Po autentifikácii sa image nahrá príkazom docker push a stáva sa dostupným pre ďalšie nasadenie.

Nový build

Spustenie nového build procesu predstavuje inicializáciu a konfiguráciu automatizovaného reťazca úloh, ktorého cieľom je zostavenie, testovanie a príprava softvérového artefaktu na ďalšie spracovanie alebo nasadenie.

Run Docker Container

Spustenie Docker kontajnera začína stiahnutím alebo výberom existujúceho Docker image, z ktorého sa vytvorí inštancia aplikácie. Kontajner sa spúšťa príkazom docker run, kde možno definovať parametre ako porty, volume mounty, premenné prostredia či sieťové nastavenia. Po spustení beží kontajner ako izolovaný proces, pripravený na komunikáciu so službami alebo používateľom.

Save Docker Image

Proces uloženia Docker image do Docker Registry zahŕňa vytvorenie image pomocou príkazu docker build, jeho označenie s cieľovou adresou registry a verziou. Následne prebehne autentifikácia do registry a samotný upload cez príkaz docker push. Výsledkom je, že image je uložený v centrálnom repozitári, odkiaľ ho možno nasadiť do ľubovoľného prostredia.

TEST/PROD prostredie

Predstavuje interné DEV a TEST prostredie

Brain:IT

Lokalita Brain:IT

Private Docker Registry

Predstavuje private Docker Registry, Private Docker Registry je súkromný repozitár, v ktorom organizácia bezpečne ukladá a spravuje vlastné Docker imagy mimo verejných registry ako Docker Hub. Umožňuje plnú kontrolu nad prístupom, verziovaním, retention politikami a bezpečnostným skenovaním kontajnerov.

Deployment configuration

Reprezentácia Kubernetes Deployment artifaktu. Kubernetes Deployment artefakt je konfiguračný súbor, ktorý definuje želaný stav nasadenia aplikácie v Kubernetes klustri – vrátane počtu replík, Docker imagu, portov a stratégií aktualizácie. Tento artefakt slúži ako vstup pre kubectl alebo CI/CD pipeline, ktoré ho aplikujú do klastru na zabezpečenie deklaratívneho a opakovateľného nasadenia.

Docker Image

Reprezentácia Docker Image artifaktu, Docker Image ako artefakt je výsledný balík aplikácie zostavený počas build procesu, ktorý obsahuje všetky potrebné vrstvy, závislosti a konfiguráciu na spustenie v kontajnerovom prostredí. Tento artefakt sa ukladá do Docker Registry, odkiaľ môže byť opakovane použitý na nasadenie v rôznych prostrediach.

GitLab

Predstavuje inštaláciu GitLab. Inštancia GitLab predstavuje samostatné nasadenie platformy GitLab, ktoré môže bežať ako cloudová služba (GitLab.com) alebo ako self-managed verzia na vlastnej infraštruktúre. Obsahuje všetky komponenty potrebné na správu repozitárov, CI/CD pipeline, issue tracking a DevOps workflow v jednom integrovanom prostredí. V rámci organizácie umožňuje úplnú kontrolu nad projektmi, používateľmi, bezpečnosťou a prístupovými právami.

GitLab Worker

Predstavuje insštanciu GitLab Worker, inštancia GitLab Worker (nazývaná aj GitLab Runner) je samostatná služba, ktorá vykonáva úlohy definované v CI/CD pipeline, ako je build, testovanie alebo nasadenie aplikácií. Beží na vyhradenom prostredí (Kubernetes) a komunikuje s centrálnym GitLab serverom, kde prijíma joby na spracovanie.

Kubernetes Cluster

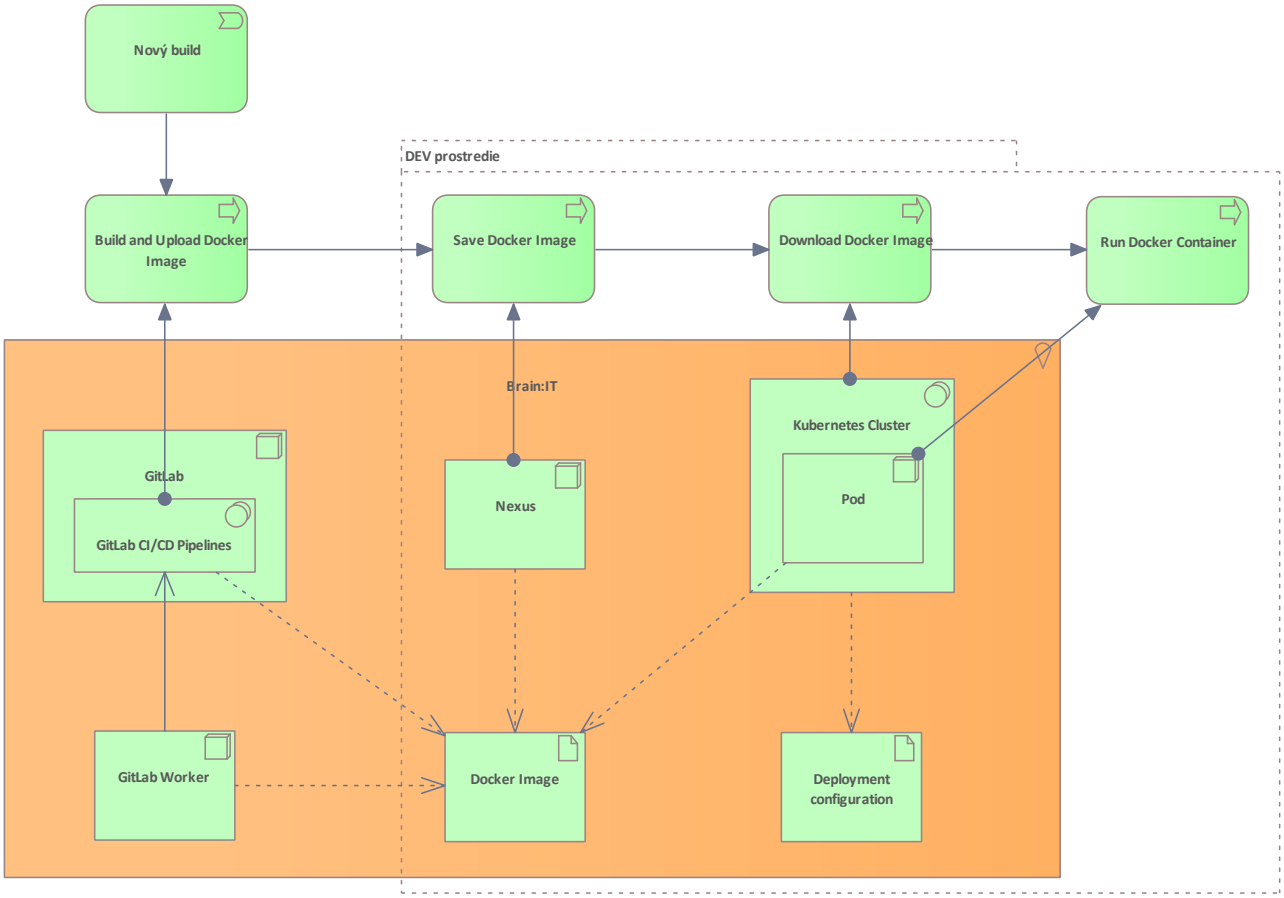
Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

GitLab CI/CD Pipelines

GitLab CI/CD Pipelines je séria úloh zabezpečujúca kompiláciu, testy, konfiguráciu, nasadenie a iné v rámci GitLabu.

Pod

Predstavuje inštanciu Podu, v rámci ktorej je spustený nový Docker Image v podobe Docker Containera



Obrázok 11 : Technology Viewpoint Developmnent CI/CD DEV

Diagram znázorňuje proces buildu a nasadenia novej verzie balíka v podobe Docker image do DEV prostredia. Diagram je využitelný pre prípad vlastných balíkov, pre ostatné existujúce sa využíva verejný DockerHub zdroj.

Popis používaných prvkov:

Build and Upload Docker Image

Build proces s následným nahratím Docker Image do Docker Registry je štandardný krok, ktorý zabezpečuje automatizované zostavenie aplikačného kontajnera, jeho označenie a publikovanie do centralizovaného repozitára, odkiaľ môže byť nasadený do vývojových, testovacích alebo produkčných prostredí.

Download Docker Image

Uloženie Docker image do Docker Registry začína vytvorením image z Dockerfile pomocou príkazu docker build. Následne sa image označí podľa názvu a verzie cieľového registry. Po autentifikácii sa image nahrá príkazom docker push a stáva sa dostupným pre ďalšie nasadenie.

Nový build

Spustenie nového build procesu predstavuje inicializáciu a konfiguráciu automatizovaného reťazca úloh, ktorého cieľom je zostavenie, testovanie a príprava softvérového artefaktu na ďalšie spracovanie alebo nasadenie.

Run Docker Container

Spustenie Docker kontajnera začína stiahnutím alebo výberom existujúceho Docker image, z ktorého sa vytvorí inštancia aplikácie. Kontajner sa spúšťa príkazom docker run, kde možno definovať parametre ako porty, volume mounty, premenné prostredia či sieťové nastavenia. Po spustení beží kontajner ako izolovaný proces, pripravený na komunikáciu so službami alebo používateľom.

Save Docker Image

Proces uloženia Docker image do Docker Registry zahŕňa vytvorenie image pomocou príkazu docker build, jeho označenie s cieľovou adresou registry a verziou. Následne prebehne autentifikácia do registry a samotný upload cez príkaz docker push. Výsledkom je, že image je uložený v centrálnom repozitári, odkiaľ ho možno nasadiť do ľubovoľného prostredia.

DEV prostredie

Predstavuje interné DEV a TEST prostredie

Brain:IT

Lokalita Brain:IT

Deployment configuration

Reprezentácia Kubernetes Deployment artifaktu. Kubernetes Deployment artefakt je konfiguračný súbor, ktorý definuje želaný stav nasadenia aplikácie v Kubernetes klustri – vrátane počtu replík, Docker imagu, portov a stratégií aktualizácie. Tento artefakt slúži ako vstup pre kubectl alebo CI/CD pipeline, ktoré ho aplikujú do klastru na zabezpečenie deklaratívneho a opakovateľného nasadenia.

Docker Image

Reprezentácia Docker Image artifaktu, Docker Image ako artefakt je výsledný balík aplikácie zostavený počas build procesu, ktorý obsahuje všetky potrebné vrstvy, závislosti a konfiguráciu na spustenie v kontajnerovom prostredí. Tento artefakt sa ukladá do Docker Registry, odkiaľ môže byť opakovane použitý na nasadenie v rôznych prostrediach.

GitLab

Predstavuje inštaláciu GitLab. Inštancia GitLab predstavuje samostatné nasadenie platformy GitLab, ktoré môže bežať ako cloudová služba (GitLab.com) alebo ako self-managed verzia na vlastnej infraštruktúre. Obsahuje všetky komponenty potrebné na správu repozitárov, CI/CD pipeline, issue tracking a DevOps workflow v jednom integrovanom prostredí. V rámci organizácie umožňuje úplnú kontrolu nad projektmi, používateľmi, bezpečnosťou a prístupovými právami.

GitLab Worker

Predstavuje insštanciu GitLab Worker, inštancia GitLab Worker (nazývaná aj GitLab Runner) je samostatná služba, ktorá vykonáva úlohy definované v CI/CD pipeline, ako je build, testovanie alebo nasadenie aplikácií. Beží na vyhradenom prostredí (Kubernetes) a komunikuje s centrálnym GitLab serverom, kde prijíma joby na spracovanie.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Nexus

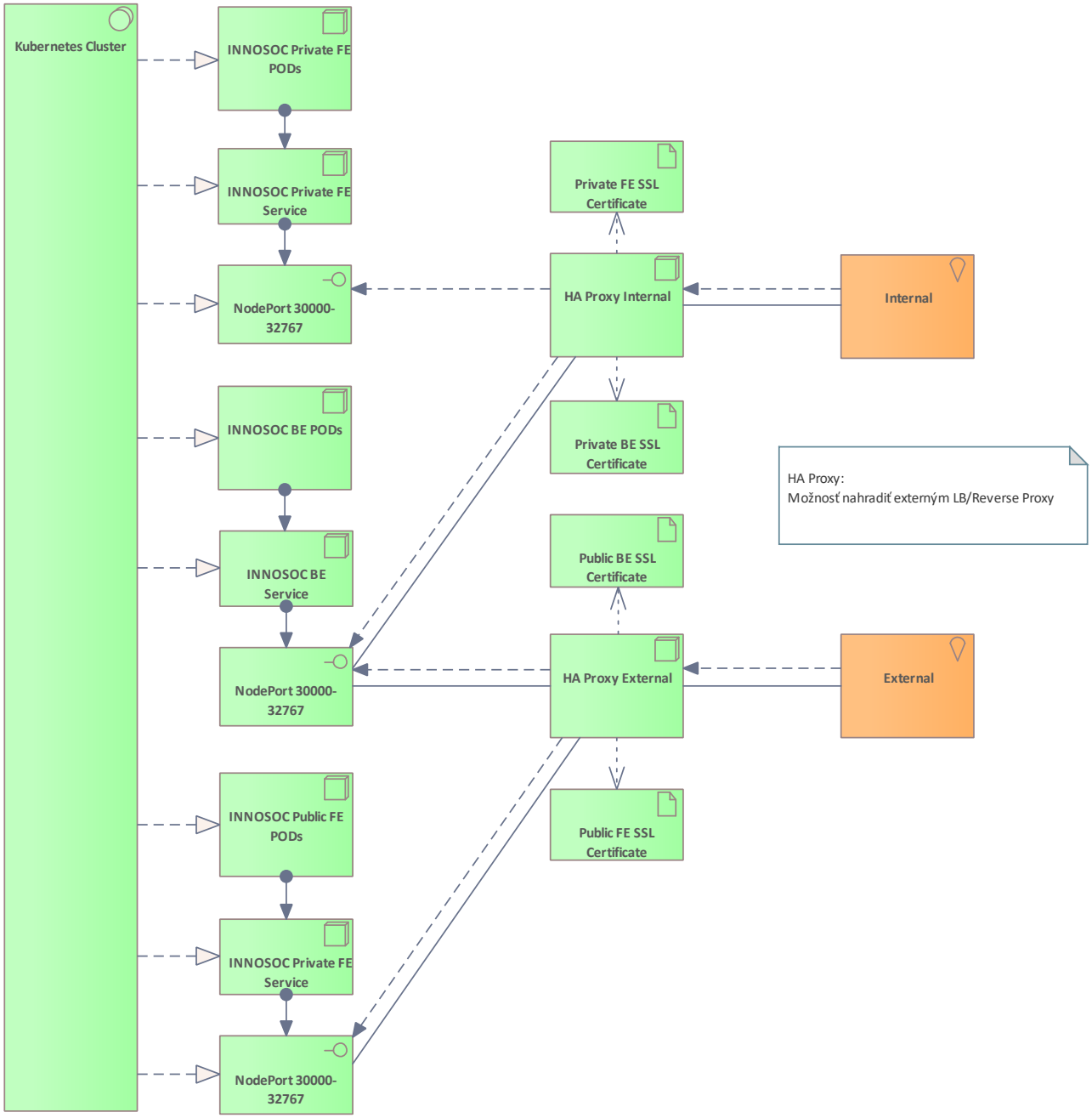
Predstavuje private Docker Registry. Private Docker Registry je súkromné úložisko pre Docker imagy, ktoré umožňuje organizáciám bezpečne ukladať a spravovať kontajnerové obrazy mimo verejných služieb ako Docker Hub. Poskytuje kontrolu nad prístupom, verziami a distribúciou image-ov, a je často integrovaný s CI/CD pipeline pre automatizované buildy a nasadenia.

GitLab CI/CD Pipelines

GitLab CI/CD Pipelines je séria úloh zabezpečujúca kompiláciu, testy, konfiguráciu, nasadenie a iné v rámci GitLabu.

Pod

Predstavuje inštanciu Podu, v rámci ktorej je spustený nový Docker Image v podobe Docker Containera



Obrázok 12 : Technology Viewpoint Interconnect

Diagram znázorňuje deployment a prepojenie vystavených služieb kubernetes a LB/Reverse Proxy pre dve zóny.

Popis používaných prvkov:

External

Predstavuje externé prostredie Internet

HA Proxy External

Predstavuje Externú reverse proxy postavenej na HA Proxy. Externá reverse proxy postavená na HAProxy je sprostredkovateľská vrstva, ktorá sa nachádza na hranici siete a slúži na prijímanie požiadaviek z internetu, ktoré následne presmerováva na interné backend služby. HAProxy v tejto úlohe zabezpečuje TLS termináciu, load balancing, ochranu cez ACL pravidlá, a tiež možnosť filtrovania alebo prepúšťania prevádzky na základe definovaných bezpečnostných politík. Táto architektúra zvyšuje bezpečnosť, škálovateľnosť a dostupnosť verejne prístupných služieb, pričom oddeľuje externú vrstvu od vnútornej infraštruktúry.

HA Proxy Internal

Predstavuje Internú reverse proxy postavenej na HA Proxy. Interná reverse proxy postavená na HAProxy je sprostredkovateľská služba, ktorá prijíma prichádzajúce požiadavky v rámci internej siete a presmerováva ich na príslušné backend služby podľa konfigurovaných pravidiel. HAProxy v tomto prípade zabezpečuje load balancing, TLS termináciu, health checking a možnosť centrálne riadiť tok dát medzi mikroslužbami alebo internými aplikáciami.

INNOSOC BE Service

Predstavuje INNOSOC BE Service. Beží ako súčasť predkonfigurovaného PODu, často vo forme kontajnera alebo virtuálneho stroja, a aktualizuje sa cez riadený CI/CD proces.

INNOSOC Private FE Service

Predstavuje INNOSOC FE Private Service. Beží ako súčasť predkonfigurovaného PODu, často vo forme kontajnera alebo virtuálneho stroja, a aktualizuje sa cez riadený CI/CD proces.

INNOSOC Private FE Service

Predstavuje INNOSOC FE Public Service. Beží ako súčasť predkonfigurovaného PODu, často vo forme kontajnera alebo virtuálneho stroja, a aktualizuje sa cez riadený CI/CD proces.

Internal

Predstavuje interné prostrednie BRAIN:IT

Private BE SSL Certificate

Predstavuje validný Private SSL certifikát pre potreby HTTPS. Validný BE SSL certifikát pre potreby HTTPS je bezpečnostný certifikát nainštalovaný na backendovej (BE) vrstve systému, ktorý umožňuje šifrovanú a autentifikovanú komunikáciu medzi službami alebo medzi frontendom a backendom. Certifikát musí byť vydaný dôveryhodnou certifikačnou autoritou (CA) alebo internou PKI infraštruktúrou a zabezpečovať integritu a dôvernosť dát prenášaných cez HTTPS.

Private FE SSL Certificate

Predstavuje validný SSL certifikát pre potreby HTTPS. Validný FE SSL certifikát pre potreby HTTPS je dôveryhodný digitálny certifikát, nainštalovaný na frontendovej (FE) vrstve aplikácie, ktorý zabezpečuje šifrovanú komunikáciu medzi používateľským prehliadačom a frontend serverom. Tento certifikát musí byť vydaný akreditovanou certifikačnou autoritou (CA), byť platný pre konkrétnu doménu a nesmie byť expirovaný ani neplatný.

Public BE SSL Certificate

Predstavuje validný Public SSL certifikát pre potreby HTTPS. Validný BE Public SSL certifikát pre potreby HTTPS je certifikát nainštalovaný na backendovej službe, ktorá je dostupná z verejnej siete, a slúži na zabezpečenie šifrovanej a overenej komunikácie cez HTTPS. Musí byť vydaný dôveryhodnou verejnou certifikačnou autoritou (CA), byť platný pre konkrétnu verejnú doménu a spĺňať bezpečnostné štandardy.

Public FE SSL Certificate

Predstavuje validný Public SSL certifikát pre potreby HTTPS. Validný FE Public SSL certifikát pre potreby HTTPS je dôveryhodný certifikát nainštalovaný na frontendovej vrstve aplikácie, ktorá je verejne dostupná cez internet, a zabezpečuje šifrovanú komunikáciu medzi klientským prehliadačom a frontend serverom. Musí byť vydaný verejnou certifikačnou autoritou (CA), byť platný pre danú doménu a nesmie byť expirovaný ani zneplatnený, aby bol akceptovaný modernými prehliadačmi.

NodePort 30000-32767

Predstavuje smerovanie typu NodePort z rozsahu 30000-32767

NodePort 30000-32767

Predstavuje smerovanie typu NodePort z rozsahu 30000-32767

NodePort 30000-32767

Predstavuje smerovanie typu NodePort z rozsahu 30000-32767

Note

HA Proxy:

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

INNOSOC BE PODs

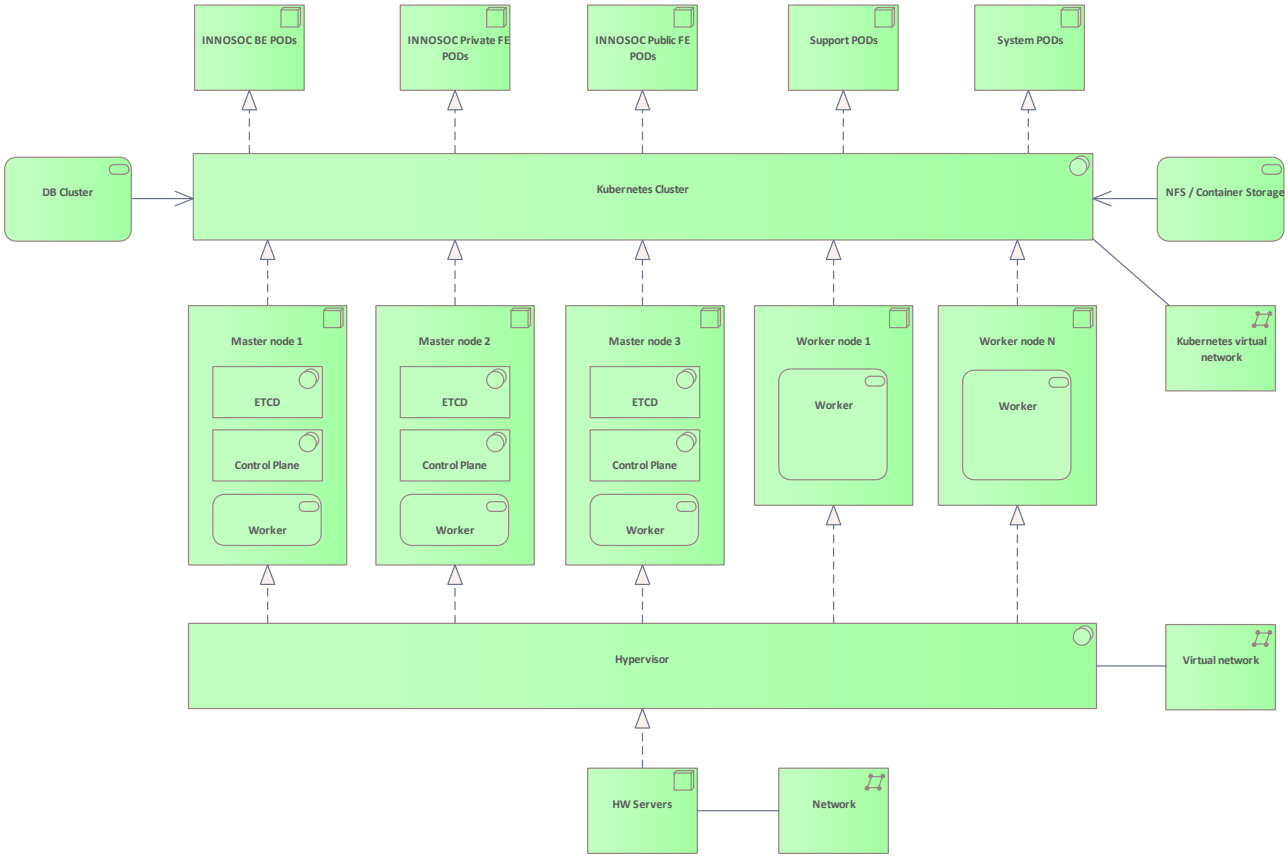
Predstavuje PODy CNM BE. PODy CNM BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému Core Network Management (CNM), ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu CNM architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

INNOSOC Private FE PODs

PODy CNM FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v privátnom prostredí zákazníka. Ide o architektonický prvok vychádzajúci z princípov kontajnerizácie a mikroservisnej architektúry, kde každý POD obsahuje samostatne nasaditeľné prvky prezentačnej vrstvy (FE – frontend), ako sú webové aplikácie, Single Page Applications (SPA), či UI moduly.

INNOSOC Public FE PODs

PODy CNM FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v verejne dostupnom cloudovom alebo hybridnom prostredí, ktoré je spravované poskytovateľom služby alebo centralizovanou infraštruktúrou organizácie. V rámci tejto architektúry sú frontendové komponenty – typicky Single Page Applications (SPA) alebo webové rozhrania – prevádzkované ako súčasť viacnájomného (multi-tenant) systému, dostupného cez verejnú sieť (internet), pričom komunikácia a prístup sú riadené prísnymi bezpečnostnými politikami. Tieto PODy fungujú ako izolované deploymenty v rámci centralizovaného cloudu (napr. Microsoft Azure, AWS, GCP), prípadne v spravovanom Kubernetes clustri. Ich cieľom je zabezpečiť škálovateľné, vysoko dostupné a jednoducho aktualizovateľné rozhranie pre koncových používateľov alebo zákazníkov, ktorí pristupujú k CNM službám bez nutnosti lokálnej inštalácie alebo privátnej infraštruktúry.



Obrázok 13 : Technology Viewpoint Kubernetes Cluster

Predstavuje rolu a službu Worker nodu .

Popis používaných prvkov:

DB Cluster

Predstavuje službu clustrovanej relačnej databázy. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle,

container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

HW Servers

Predstavuje HW serverovú infraštruktúru. HW serverová infraštruktúra predstavuje fyzické výpočtové a sieťové vybavenie, ktoré tvorí základ pre prevádzku IT systémov, vrátane serverov, úložísk, prepínačov, smerovačov a záložných zdrojov napájania. Táto infraštruktúra je nasadzovaná buď on-premise alebo ako súčasť cloudovej platformy, a poskytuje výpočtový výkon, dostupnosť a konektivitu pre virtualizované aj nevirtualizované prostredia.

Hypervisor

Predstavuje Hypervisor 1. alebo 2. typu. Hypervisor 1. typu, známy aj ako "bare-metal" hypervisor, beží priamo na fyzickom hardvéri bez operačného systému, čím poskytuje vysoký výkon a efektivitu virtualizácie; príkladmi sú VMware ESXi, Microsoft Hyper-V (core) alebo Xen. Tento typ hypervisora je určený najmä pre dátové centrá a enterprise prostredia, kde sa kladie dôraz na výkon, stabilitu a bezpečnosť.

Hypervisor 2. typu, nazývaný aj "hostovaný" hypervisor, beží nad existujúcim operačným systémom ako aplikácia, a tým zdieľa systémové zdroje s hostiteľom; príklady zahŕňajú VMware Workstation alebo Oracle VirtualBox. Hoci je jednoduchší na inštaláciu a vhodný na vývoj alebo testovanie, jeho výkon a izolácia sú nižšie v porovnaní s typom 1.

Kubernetes virtual network

Predstavuje virtuálnu sieť/subsieť Kubernetes Clustra. Virtuálna sieť alebo podsieť v Kubernetes clustri je logická sieťová architektúra, ktorá umožňuje komunikáciu medzi podmi, službami a ďalšími komponentmi v klastri bez nutnosti NAT. Každý pod dostáva vlastnú IP adresu v rámci tejto siete, čo zabezpečuje predvídateľnú a plne routovateľnú konektivitu v súlade s princípom "každý pod môže komunikovať s každým iným podom".

Master node 1

Predstavuje Master node Kubernetes Clustra. Master node v Kubernetes clustri je riadiaci uzol, ktorý hostuje komponenty Control Plane, zodpovedné za globálne rozhodovanie, plánovanie workloadov a udržiavanie stavu clustra. Obsahuje kľúčové služby ako kube-apiserver, ETCD databázu, scheduler a controller-managery, ktoré spolu zabezpečujú orchestráciu a správu všetkých Worker nodov a podov.

Master node 2

Predstavuje Master node Kubernetes Clustra

Master node 3

Predstavuje Master node Kubernetes Clustra

Network

Predstavuje sieť/subsieť HW infraštruktúry. Sieť alebo podsieť HW infraštruktúry je fyzická a logická vrstva prepojenia serverov, úložísk a sieťových zariadení, ktorá zabezpečuje prenos dát, komunikáciu a prístup k službám v rámci dátového centra.

Support PODs

Predstavuje PODy podporných služieb. PODy podporných služieb predstavujú kontajnerové alebo virtuálne jednotky nasadenia, ktoré zabezpečujú neaplikačné funkcie potrebné na chod a správu hlavného systému, ako sú monitoring, logging, autentifikácia či konfigurácia. Tieto služby typicky fungujú ako infrastrukturné komponenty a sú nasadené paralelne s aplikačnými PODmi v rámci rovnakého clustra alebo prostredia.

System PODs

Predstavuje PODy systémových služieb. PODy systémových služieb sú nasadené komponenty v kontajnerizovanom prostredí, ktoré zabezpečujú základnú funkcionalitu a operácie potrebné pre správnu činnosť celej platformy alebo clustra, ako je networking, DNS, storage či orchestrácia. Tieto služby zvyčajne tvoria súčasť základnej infraštruktúry Kubernetes alebo iného orchestrátora a fungujú nezávisle od aplikačných a podporných PODov, pričom zabezpečujú stabilitu a prevádzkyschopnosť systému.

Virtual network

Predstavuje virtuálnu sieť/subsieť Hypervisora. Virtuálna sieť alebo podsieť Hypervisora je logická sieťová infraštruktúra, ktorú hypervisor vytvára na účely prepojenia virtuálnych strojov (VM) medzi sebou, s hostiteľským systémom alebo s vonkajšou sieťou. Umožňuje definovanie virtuálnych switchov, NAT, bridged alebo internal networking režimov, čím poskytuje flexibilitu v izolácii, komunikácii a routovaní dát medzi VM a fyzickým sieťovým prostredím.

Worker node 1

Predstavuje Worker node Kubernetes Clustra. Worker node v Kubernetes clustri je výpočtový uzol, na ktorom sú nasadzované a spúšťané aplikačné Pody, teda reálne workloady systému. Obsahuje základné komponenty ako kubelet, kube-proxy a container runtime (napr. containerd), ktoré zabezpečujú komunikáciu s Control Plane a správne vykonávanie priradených úloh.

Worker node N

Predstavuje Worker node Kubernetes Clustra

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje

nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

INNOSOC BE PODs

Predstavuje PODy CNM BE. PODy CNM BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému Core Network Management (CNM), ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu CNM architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

INNOSOC Private FE PODs

PODy CNM FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v privátnom prostredí zákazníka. Ide o architektonický prvok vychádzajúci z princípov kontajnerizácie a mikroservisnej architektúry, kde každý POD obsahuje samostatne nasaditeľné prvky prezentačnej vrstvy (FE – frontend), ako sú webové aplikácie, Single Page Applications (SPA), či UI moduly.

INNOSOC Public FE PODs

PODy CNM FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v verejne dostupnom cloudovom alebo hybridnom prostredí, ktoré je spravované poskytovateľom služby alebo centralizovanou infraštruktúrou organizácie. V rámci tejto architektúry sú frontendové komponenty – typicky Single Page Applications (SPA) alebo webové rozhrania – prevádzkované ako súčasť viacnájomného (multi-tenant) systému, dostupného cez verejnú sieť (internet), pričom komunikácia a prístup sú riadené prísnymi bezpečnostnými politikami. Tieto PODy fungujú ako izolované deploymenty v rámci centralizovaného cloudu (napr. Microsoft Azure, AWS, GCP), prípadne v spravovanom Kubernetes clustri. Ich cieľom je zabezpečiť škálovateľné, vysoko dostupné a jednoducho aktualizovateľné rozhranie pre koncových používateľov alebo zákazníkov, ktorí pristupujú k CNM službám bez nutnosti lokálnej inštalácie alebo privátnej infraštruktúry.

Worker

Predstavuje rolu a službu Worker nodu. Rola a služba Worker nodu v Kubernetes spočíva v hostovaní a spúšťaní aplikačných podov, pričom zabezpečuje vykonávanie workloadov na základe pokynov z Control Plane.

Control Plane

Predstavuje Control Plane pre správu Kubernetes Clustra. Control Plane pre správu Kubernetes clustra je centrálna riadiaca vrstva, ktorá zabezpečuje globálnu

orchestráciu, plánovanie a správu všetkých komponentov v klastri. Obsahuje kľúčové služby ako kube-apiserver, ETCD databáza, kube-scheduler, kube-controller-manager a prípadne cloud-controller-manager. Control Plane rozhoduje, kde a ako budú aplikácie bežať, monitoruje ich stav a zaručuje, že požadovaný stav (deklarovaný používateľom) zodpovedá aktuálnemu stavu clustra.

ETCD

Predstavuje ETCD databázu. ETCD databáza je distribuovaná, vysoko dostupná kľúč-hodnota databáza, navrhnutá pre ukladanie konfiguračných dát a metadát v reálnom čase. Je základnou súčasťou Kubernetes, kde slúži ako centrálne úložisko stavov clustra, vrátane informácií o pods, konfiguráciách, secret-och a ďalších objektoch. Vďaka mechanizmu konsenzu Raft zabezpečuje spoľahlivosť, konzistenciu a odolnosť voči výpadkom v distribuovaných systémoch.

Worker

Predstavuje rolu a službu Worker nodu

Control Plane

Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD

Predstavuje ETCD databázu

Worker

Control Plane

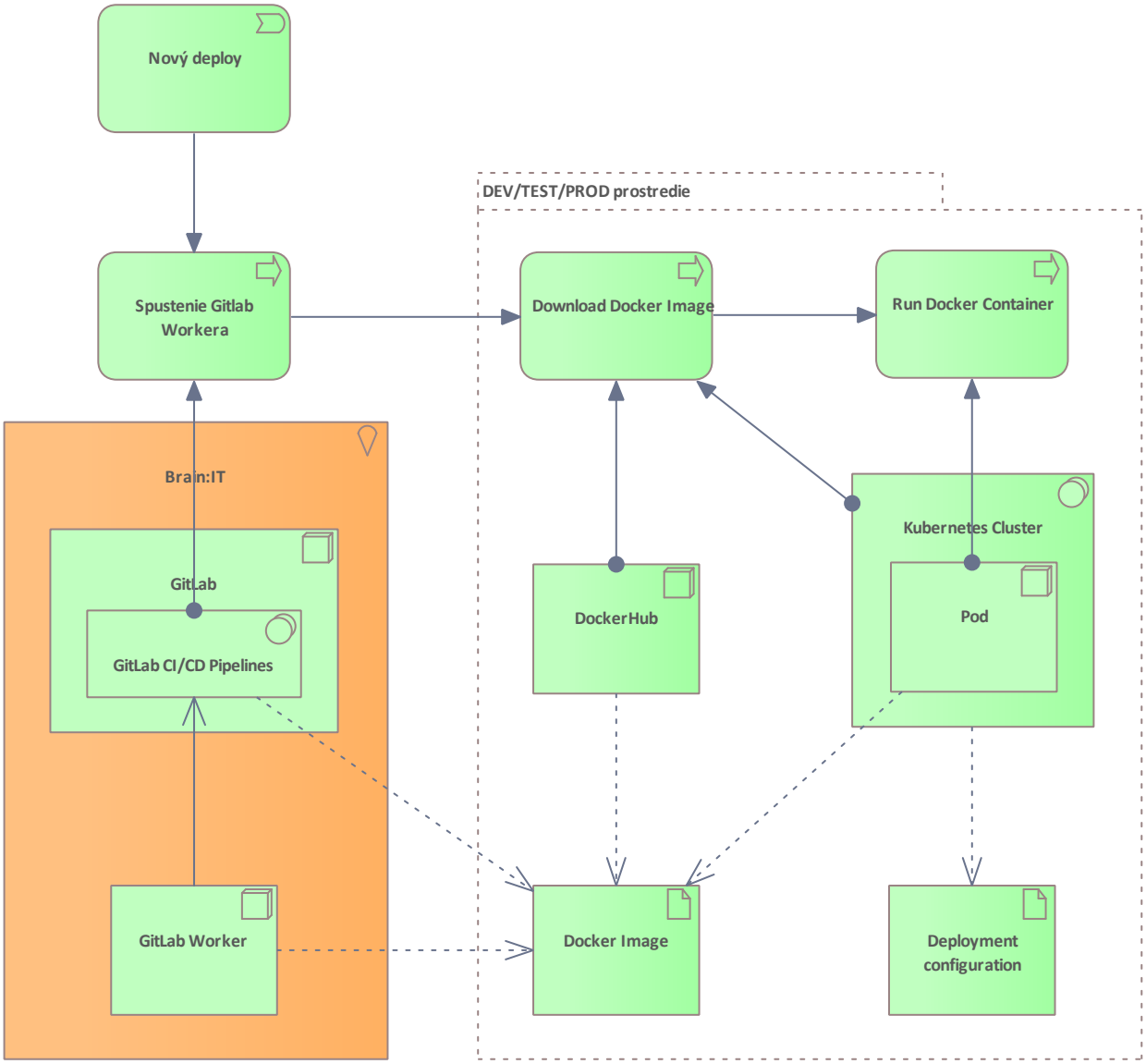
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD

Predstavuje ETCD databázu

Worker

Worker



Obrázok 14 : Technology Viewpoint standard CI/CD DEV/TEST/PROD

Popis používaných prvkov:

Download Docker Image

Uloženie Docker image do Docker Registry začína vytvorením image z Dockerfile pomocou príkazu docker build. Následne sa image označí podľa názvu a verzie cieľového registry. Po autentifikácii sa image nahrá príkazom docker push a stáva sa dostupným pre ďalšie nasadenie.

Nový deploy

Spustenie nového deploy procesu je akcia, pri ktorej sa nová verzia aplikácie alebo služby automatizovane nasadí do cieľového prostredia na základe definovanej CI/CD pipeline.

Run Docker Container

Spustenie Docker kontajnera začína stiahnutím alebo výberom existujúceho Docker image, z ktorého sa vytvorí inštancia aplikácie. Kontajner sa spúšťa príkazom docker run, kde možno definovať parametre ako porty, volume mounty, premenné prostredia či sieťové nastavenia. Po spustení beží kontajner ako izolovaný proces, pripravený na komunikáciu so službami alebo používateľom.

Spustenie Gitlab Workera

Proces spustenia GitLab Workera pre nasadenie novej verzie balíka začína prijatím jobu z CI/CD pipeline definovanej v .gitlab-ci.yml, ktorý obsahuje kroky pre deployment. Worker následne vykoná inštrukcie ako sťahovanie artefaktu, pripojenie na cieľové prostredie a nasadenie novej verzie aplikácie, pričom celý priebeh je logovaný a spätne sledovateľný.

DEV/TEST/PROD prostredie

Predstavuje interné DEV a TEST prostredie

Brain:IT

Lokalita Brain:IT

DockerHub

Predstavuje verejný Docker Registry DockerHub. DockerHub je verejný Docker Registry poskytovaný spoločnosťou Docker Inc., ktorý umožňuje vývojárom zdieľať, ukladať a sťahovať kontajnerové image prostredníctvom cloudovej platformy. Podporuje verejné aj súkromné repozitáre, verziovanie image-ov, automatické buildy a integráciu s CI/CD nástrojmi.

Deployment configuration

Reprezentácia Kubernetes Deployment artifaktu. Kubernetes Deployment artefakt je konfiguračný súbor, ktorý definuje želaný stav nasadenia aplikácie v Kubernetes klustri

– vrátane počtu replík, Docker imagu, portov a stratégií aktualizácie. Tento artefakt slúži ako vstup pre kubectl alebo CI/CD pipeline, ktoré ho aplikujú do klastru na zabezpečenie deklaratívneho a opakovateľného nasadenia.

Docker Image

Reprezentácia Docker Image artifaktu, Docker Image ako artefakt je výsledný balík aplikácie zostavený počas build procesu, ktorý obsahuje všetky potrebné vrstvy, závislosti a konfiguráciu na spustenie v kontajnerovom prostredí. Tento artefakt sa ukladá do Docker Registry, odkiaľ môže byť opakovane použitý na nasadenie v rôznych prostrediach.

GitLab

Predstavuje inštaláciu GitLab. Inštancia GitLab predstavuje samostatné nasadenie platformy GitLab, ktoré môže bežať ako cloudová služba (GitLab.com) alebo ako self-managed verzia na vlastnej infraštruktúre. Obsahuje všetky komponenty potrebné na správu repozitárov, CI/CD pipeline, issue tracking a DevOps workflow v jednom integrovanom prostredí. V rámci organizácie umožňuje úplnú kontrolu nad projektmi, používateľmi, bezpečnosťou a prístupovými právami.

GitLab Worker

Predstavuje insštanciu GitLab Worker, inštancia GitLab Worker (nazývaná aj GitLab Runner) je samostatná služba, ktorá vykonáva úlohy definované v CI/CD pipeline, ako je build, testovanie alebo nasadenie aplikácií. Beží na vyhradenom prostredí (Kubernetes) a komunikuje s centrálnym GitLab serverom, kde prijíma joby na spracovanie.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

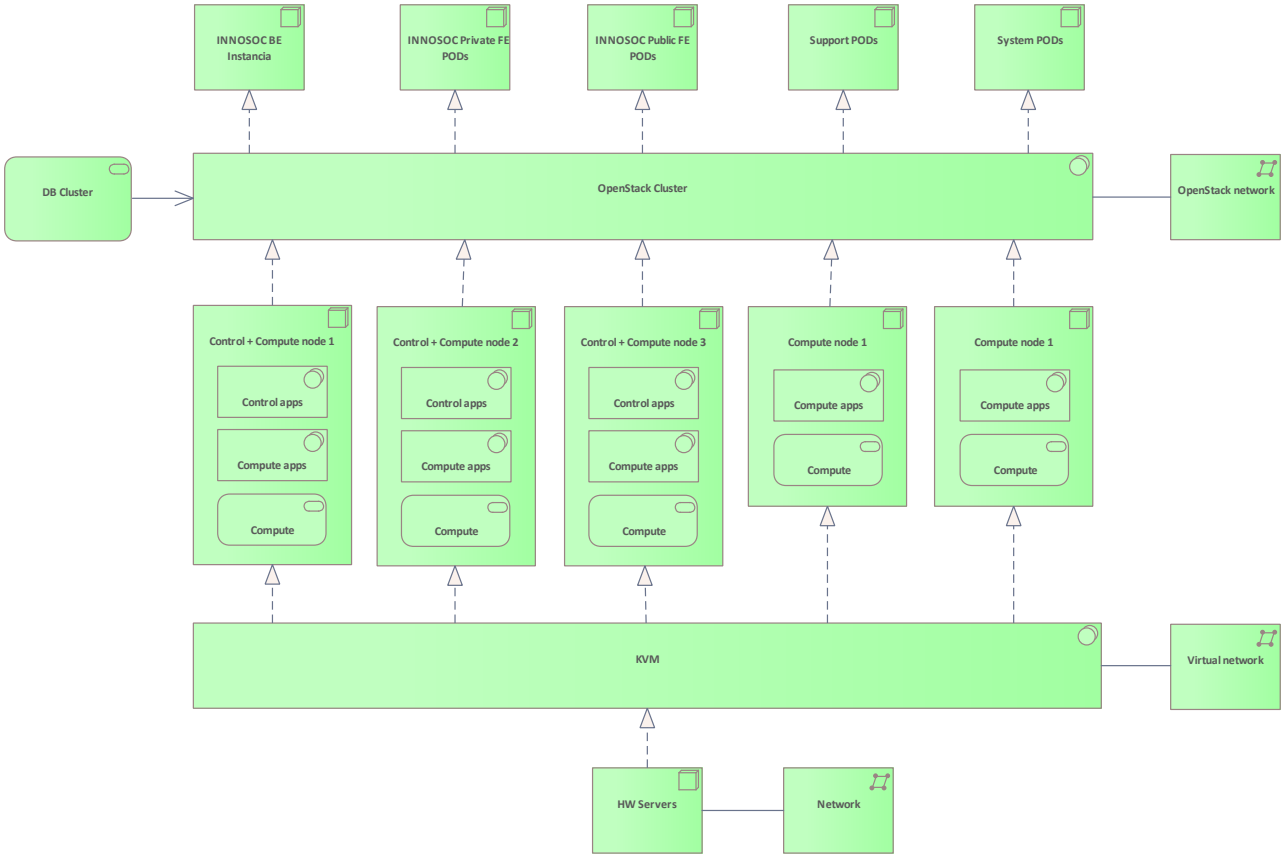
GitLab CI/CD Pipelines

GitLab CI/CD Pipelines je séria úloh zabezpečujúca kompiláciu, testy, konfiguráciu, nasadenie a iné v rámci GitLabu.

Pod

Predstavuje inštanciu Podu, v rámci ktorej je spustený nový Docker Image v podobe Docker Containera

1.6. Technology Viewpoint OpenStack



Obrázok 15 : Technology Viewpoint OpenStack Cluster

Popis používaných prvkov:

DB Cluster

Predstavuje službu clustrovanej relačnej databázy

Compute node 1

Predstavuje Compute node OpenStack Clustra

Compute node 1

Predstavuje Compute node OpenStack Clustra

Control + Compute node 1

Predstavuje Control a Compute node 1 OpenStack Clustra

Control + Compute node 2

Predstavuje Control a Compute node 2 OpenStack Clustra

Control + Compute node 3

Predstavuje Control a Compute node 3 OpenStack Clustra

HW Servers

Predstavuje HW serverovú infraštruktúru

KVM

Predstavuje KVM Hypervisor 1. typu.

Network

Predstavuje sieť/subsieť HW infraštruktúry

OpenStack Cluster

Predstavuje OpenStack Cluster

OpenStack network

Predstavuje sieť/subsieť OpenStack Clustra, konkrétne:

Corporate network

OpenStack Tenant Data Network

OpenStack Internal Admin / API Subnet

Support PODs

Predstavuje PODy podporných služieb

System PODs

Predstavuje PODy systémových služieb

Virtual network

Predstavuje virtuálnu sieť/subsieť Hypervisora

INNOSOC BE Instancia

Predstavuje inštanciu OpenStacku VM alebo kontajner. Inštancia OpenStacku vo forme VM alebo kontajnera predstavuje virtuálny výpočtový zdroj (compute instance), ktorý je nasadený v rámci cloudovej platformy OpenStack prostredníctvom komponentu Nova. Môže ísť o klasickú virtuálnu mašinu (VM) alebo o ľahšiu kontajnerovú inštanciu, v závislosti od použitého hypervisora a integrácie s kontajnerizačnými technológiami ako Kubernetes alebo Docker.

INNOSOC Private FE PODs

Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs

Predstavuje PODy CNM FE Public

Compute

Predstavuje rolu a službu Compute nodu

Compute apps

Predstavuje súbor Compute aplikácií

Control apps

Predstavuje súbor aplikácií pre Control node potrebných pre správu clustra

Compute

Predstavuje rolu a službu Compute nodu

Compute apps

Predstavuje súbor Compute aplikácií

Compute

Predstavuje rolu a službu Compute nodu

Compute apps

Predstavuje súbor Compute aplikácií

Control apps

Predstavuje súbor aplikácií pre Control node potrebných pre správu clustra

Compute

Predstavuje rolu a službu Compute nodu

Compute apps

Predstavuje súbor Compute aplikácií

Control apps

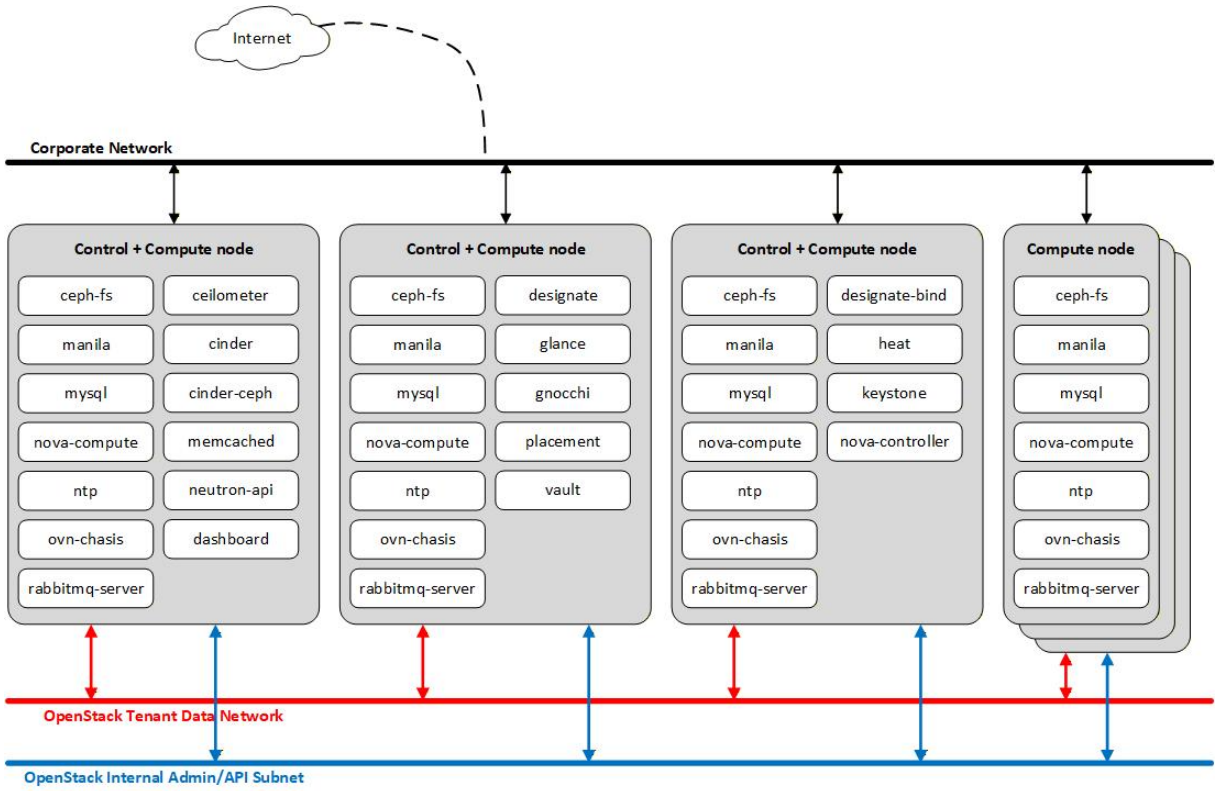
Predstavuje súbor aplikácií pre Control node potrebných pre správu clustra

Compute

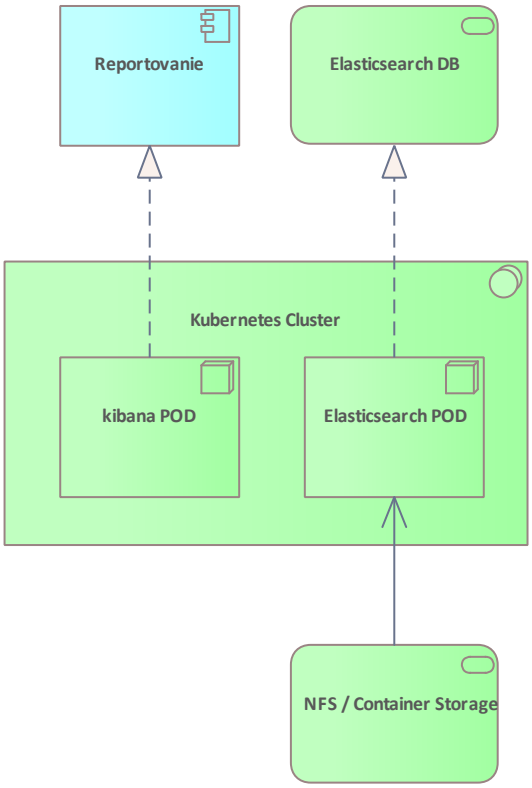
Predstavuje rolu a službu Compute nodu

Compute apps

Predstavuje súbor Compute aplikácií



1.7. Technology Viewpoint Reportovanie



Obrázok 16 : Technology Usage Viewpoint Reportovanie alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1 predstavuje využitie Elasticsearch databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databázy pre Elasticsearch.

Popis používaných prvkov:

Reportovanie

Komponent reportovania v rámci SOCaaS architektúry slúži ako centrálny prostriedok na agregáciu, vizualizáciu a distribúciu bezpečnostných informácií. Jeho úlohou je zabezpečiť pravidelné aj ad-hoc výstupy o stave kybernetickej bezpečnosti pre rôzne cieľové skupiny – od SOC analytikov, cez vedúcich tímov, až po vedenie organizácie alebo klientov. Takýto reportovací systém musí pokrývať:

• Generovanie metriky incidentov, výstrah, SLA a KPIs,

- Prehľady trendov v čase a hodnotenie výkonnosti bezpečnostných opatrení,
- Prispôsobenie obsahu podľa úrovne detailu (technické vs. strategické),
- Automatizáciu a plánovanie distribúcie výstupov,
- Spätnú analýzu a archiváciu historických údajov.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB

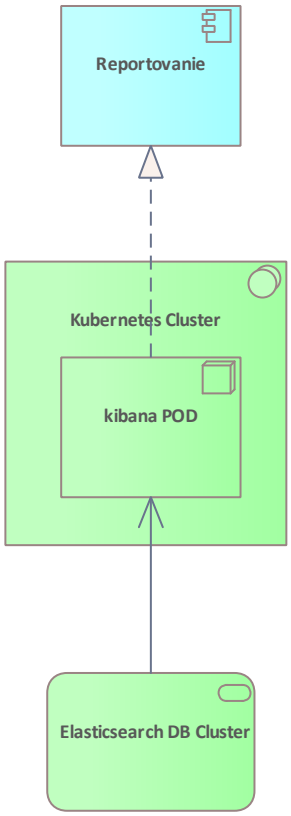
Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

kibana POD

Predstavuje POD Kibana pre Reportovanie.



Obrázok 17 : Technology Usage Viewpoint Reportovanie alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 2 predstavuje využitie Elasticsearch Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

Reportovanie

Komponent reportovania v rámci SOCaaS architektúry slúži ako centrálny prostriedok na agregáciu, vizualizáciu a distribúciu bezpečnostných informácií. Jeho úlohou je zabezpečiť pravidelné aj ad-hoc výstupy o stave kybernetickej bezpečnosti pre rôzne

cieľové skupiny – od SOC analytikov, cez vedúcich tímov, až po vedenie organizácie alebo klientov. Takýto reportovací systém musí pokrývať:

- Generovanie metriky incidentov, výstrah, SLA a KPIs,
- Prehľady trendov v čase a hodnotenie výkonnosti bezpečnostných opatrení,
- Prispôsobenie obsahu podľa úrovne detailu (technické vs. strategické),
- Automatizáciu a plánovanie distribúcie výstupov,
- Spätnú analýzu a archiváciu historických údajov.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

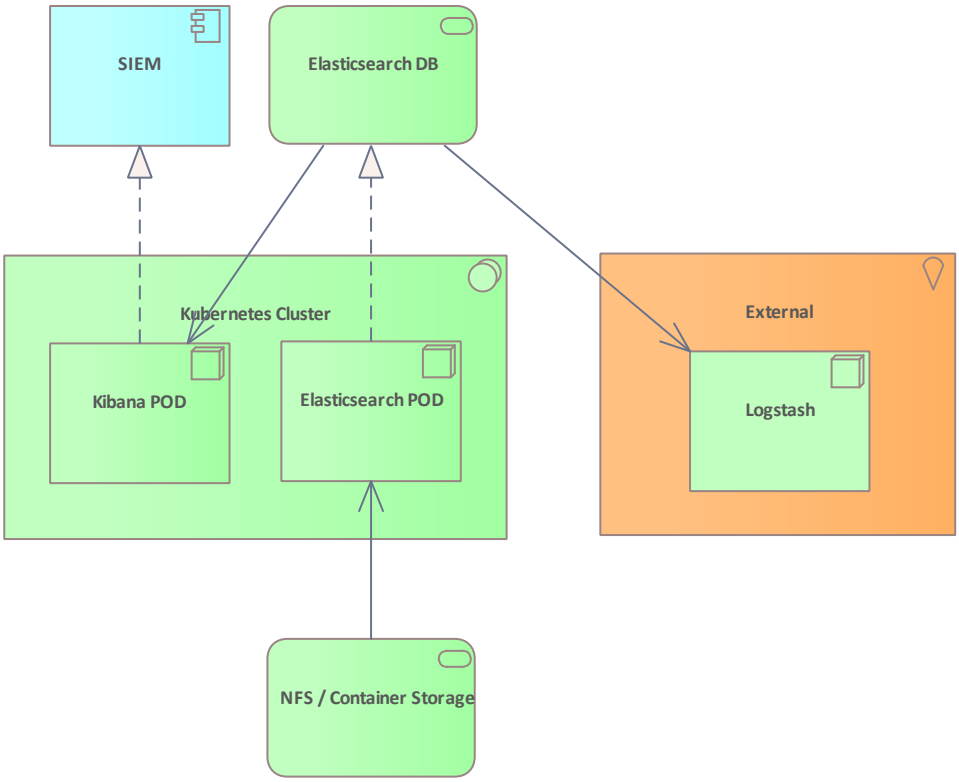
Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

kibana POD

Predstavuje POD Kibana pre Reportovanie.

1.8. Technology Viewpoint SIEM



Obrázok 18 : Technology Usage Viewpoint SIEM alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1 predstavuje využitie Elasticsearch databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databáz pre Elasticsearch.

Popis používaných prvkov:

SIEM

SIEM je srdcom SOCaaS riešenia. Zabezpečuje agregáciu, spracovanie, koreláciu a analýzu bezpečnostných udalostí z rôznych zdrojov, v reálnom čase. Umožňuje analytikom identifikovať anomálie, generovať upozornenia a eskalovať incidenty, pričom zvyšuje viditeľnosť nad infraštruktúrou klienta.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

External

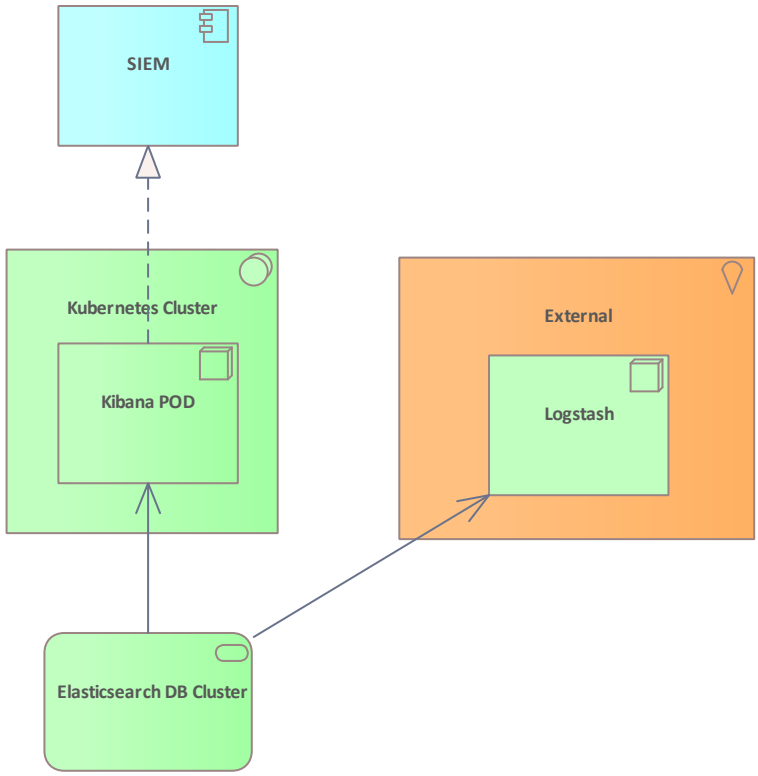
Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

Predstavuje POD Kibana pre SIEM.

Logstash

Predstavuje inštanciu Logstashg pre spracovanie logov a ich zapísanie do Elasticsearch.



Obrázok 19 : Technology Usage Viewpoint SIEM alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 2 predstavuje využitie Elasticsearch Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

SIEM

SIEM je srdcom SOCaaS riešenia. Zabezpečuje agregáciu, spracovanie, koreláciu a analýzu bezpečnostných udalostí z rôznych zdrojov, v reálnom čase. Umožňuje analytikom identifikovať anomálie, generovať upozornenia a eskalovať incidenty, pričom zvyšuje viditeľnosť nad infraštruktúrou klienta.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

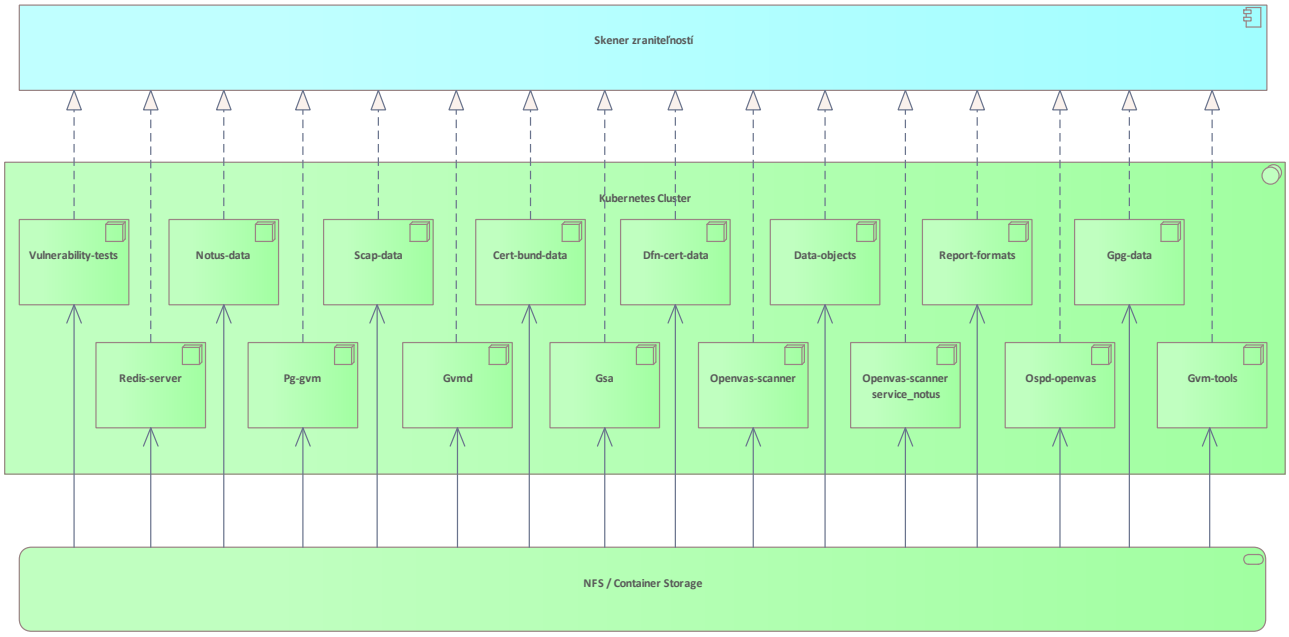
Kibana POD

Predstavuje POD Kibana pre SIEM.

Logstash

Predstavuje inštanciu Logstashg pre spracovanie logov a ich zapísanie do Elasticsearch.

1.9. Technology Viewpoint Skener zraniteľností



Obrázok 20 : Technology Usage Viewpoint Skener zraniteľností

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Popis používaných prvkov:

Skener zraniteľností

Skener zraniteľností je základným stavebným kameňom pre zabezpečenie proaktívneho prístupu v SOCaaS architektúre. Umožňuje pravidelne identifikovať slabé miesta v infraštruktúre, hodnotiť stav aktualizácií, konfigurácií a nastavení, a poskytovať informácie pre ďalšiu prioritizáciu a plánovanie nápravných opatrení. Výstupy skenera sú často zdrojom pre SOAR systémy, SLA metriky, reporting ako aj pre hodnotenie bezpečnostnej úrovne klienta.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Cert-bund-data

Predstavuje POD cert-bund-data.

Data-objects

Predstavuje POD data-objects.

Dfn-cert-data

Predstavuje POD dfn-cert-data.

Gpg-data

Predstavuje POD gpg-data.

Gsa

Predstavuje POD gsa.

Gvmd

Predstavuje POD gvmd.

Gvm-tools

Predstavuje POD gvm-tools.

Notus-data

Predstavuje POD notus-data.

Openvas-scanner

Predstavuje POD openvas-scanner.

Openvas-scanner service_notus

Predstavuje POD openvas-scanner service_notus.

Ospd-openvas

Predstavuje POD ospd-openvas.

Pg-gvm

Predstavuje POD pg-gvm.

Redis-server

Predstavuje POD redis-server.

Report-formats

Predstavuje POD report-formats.

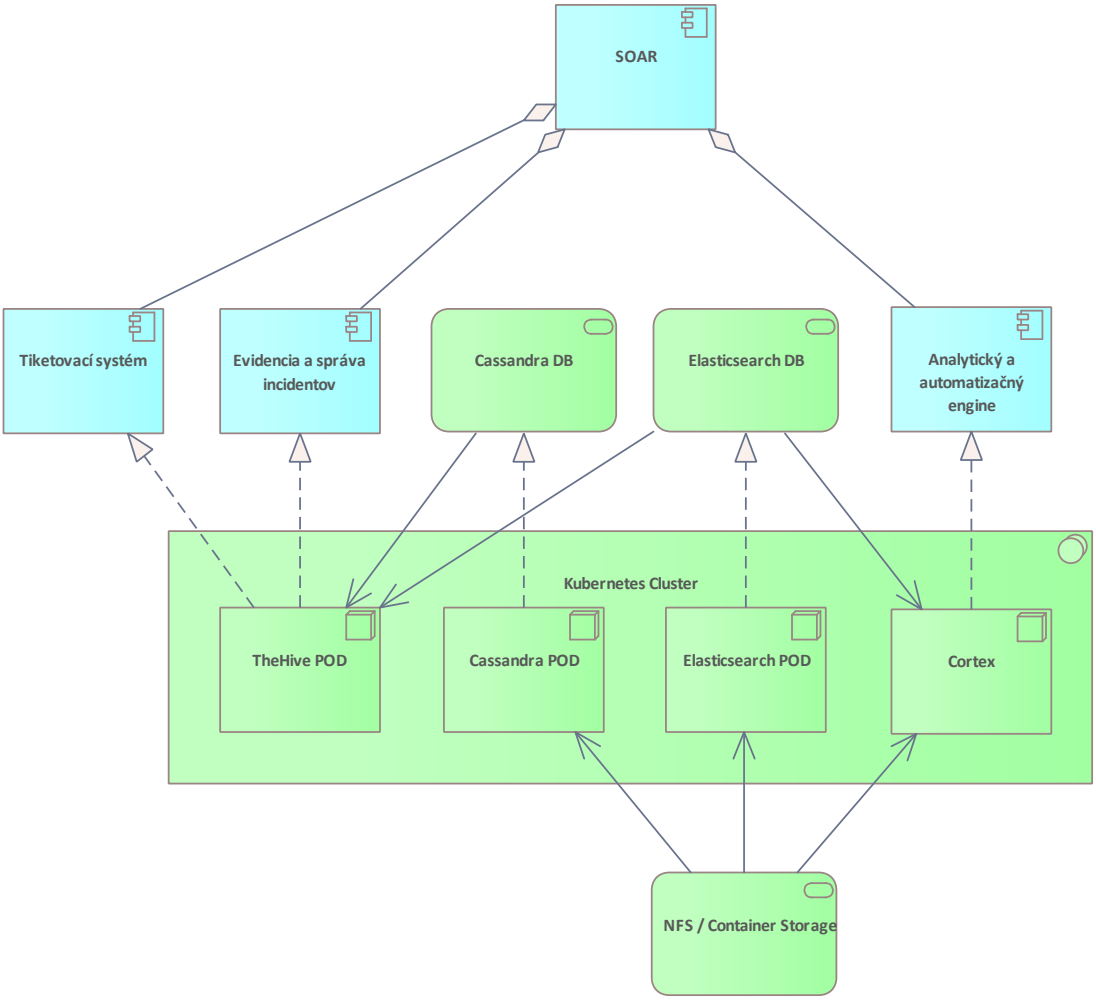
Scap-data

Predstavuje POD scap-data.

Vulnerability-tests

Predstavuje POD vulnerability-tests.

1.10. Technology Viewpoint SOAR



Obrázok 21 : Technology Usage Viewpoint SOAR alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1 predstavuje využitie Elasticsearch databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databáz pre Cassandra a Elasticsearch.

Popis používaných prvkov:

Analytický a automatizačný engine

Evidencia a správa incidentov

Evidencia a správa incidentov je jadrovým prvkom každej bezpečnostnej prevádzky (SOC). Tento podkomponent zaisťuje systematickú dokumentáciu, sledovanie a manažovanie bezpečnostných udalostí a incidentov v priebehu ich životného cyklu – od detekcie cez analýzu až po uzavretie. Kvalitný systém evidencie musí umožniť tímom koordinovane spolupracovať, dokumentovať kroky, evidovať súvisiace artefakty (observables) a prepojiť incidenty

s relevantnými hrozbami, systémami alebo historickými prípadmi. V ideálnom prípade podporuje aj pokročilé obohacovanie údajov, audit, multitenantnosť a možnosť spätného skúmania incidentov.

SOAR

SOAR (Security Orchestration, Automation and Response) je komponent zodpovedný za automatizáciu reakcií na incidenty, orchestráciu bezpečnostných nástrojov a podporu rozhodovania analytikov. V SOCaaS predstavuje základnú zložku umožňujúcu škálovanie reakčných kapacít bez nutnosti zvyšovať počet personálu. Je nevyhnutný najmä pri spracovaní veľkého množstva alertov, kde znižuje MTTR a MTTC metriky.

Tiketovací systém

Tiketovací systém slúži ako ústredný komunikačný a organizačný kanál pre správu bezpečnostných incidentov počas ich celého životného cyklu. Umožňuje vytváranie, priraďovanie a sledovanie úloh a komunikáciu medzi analytikmi, pričom podporuje audit, SLA monitoring, eskaláciu a notifikácie.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Cassandra DB

Predstavuje technologickú službu NoSQL Cassandra databázy.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Cassandra POD

Predstavuje POD Apache Cassandra pre NoSQL databázu.

Elasticsearch POD

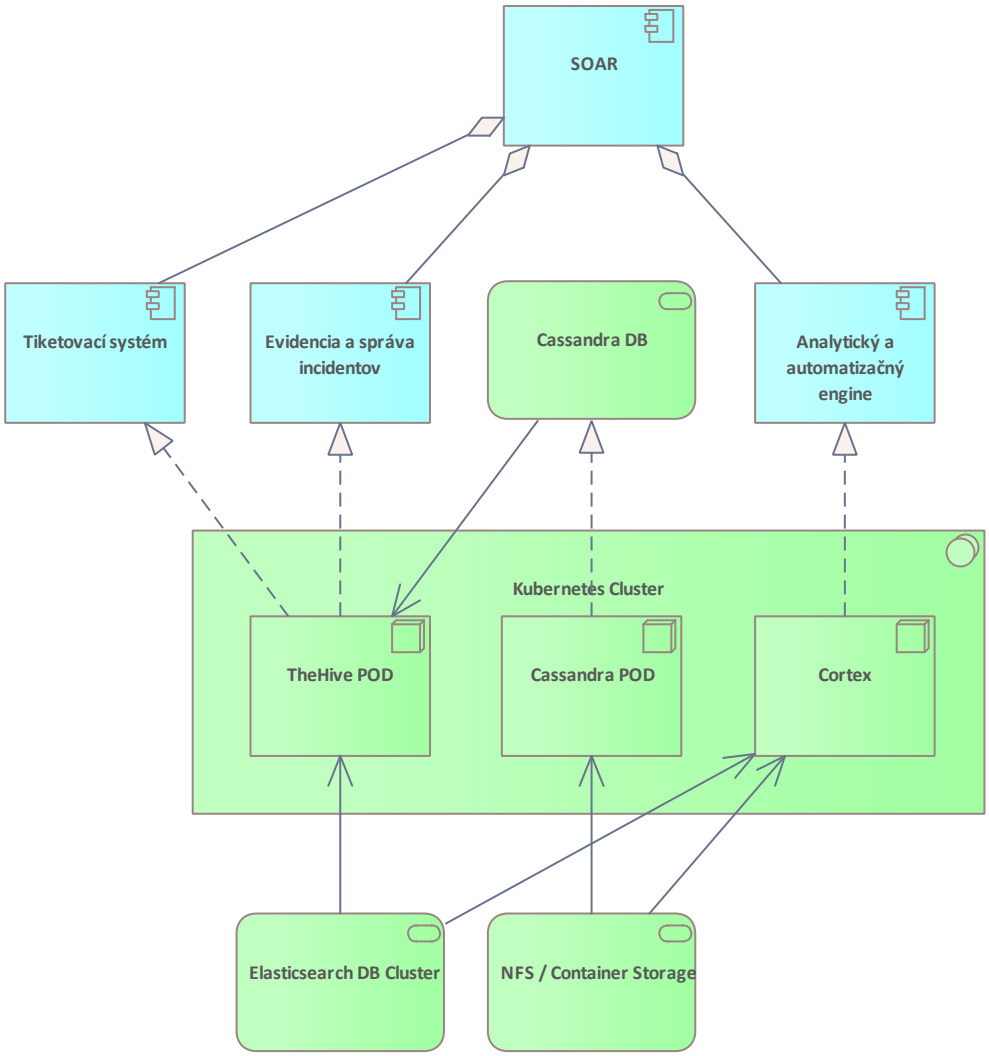
Predstavuje POD Elasticsearch pre NoSQL databázu.

TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.

Cortex

Predstavuje POD Cortex pre SOAR.



Obrázok 22 : Technology Usage Viewpoint SOAR alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 2 predstavuje využitie Elasticsearch Databázy priamo vo forme centralizovaného DB Clustra. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databázy pre Cassandra.

Popis používaných prvkov:

Analytický a automatizačný engine

Evidencia a správa incidentov

Evidencia a správa incidentov je jadrovým prvkom každej bezpečnostnej prevádzky (SOC). Tento podkomponent zaisťuje systematickú dokumentáciu, sledovanie a manažovanie bezpečnostných udalostí a incidentov v priebehu ich životného cyklu – od detekcie cez analýzu až po uzavretie. Kvalitný systém evidencie musí umožniť tímom koordinovane spolupracovať, dokumentovať kroky, evidovať súvisiace artefakty (observables) a prepojiť incidenty

s relevantnými hrozbami, systémami alebo historickými prípadmi. V ideálnom prípade podporuje aj pokročilé obohacovanie údajov, audit, multitenantnosť a možnosť spätného skúmania incidentov.

SOAR

SOAR (Security Orchestration, Automation and Response) je komponent zodpovedný za automatizáciu reakcií na incidenty, orchestráciu bezpečnostných nástrojov a podporu rozhodovania analytikov. V SOCaaS predstavuje základnú zložku umožňujúcu škálovanie reakčných kapacít bez nutnosti zvyšovať počet personálu. Je nevyhnutný najmä pri spracovaní veľkého množstva alertov, kde znižuje MTTR a MTTC metriky.

Tiketovací systém

Tiketovací systém slúži ako ústredný komunikačný a organizačný kanál pre správu bezpečnostných incidentov počas ich celého životného cyklu. Umožňuje vytváranie, priraďovanie a sledovanie úloh a komunikáciu medzi analytikmi, pričom podporuje audit, SLA monitoring, eskaláciu a notifikácie.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie

Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Cassandra DB

Predstavuje technologickú službu NoSQL Cassandra databázy.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

Cassandra POD

Predstavuje POD Apache Cassandra pre NoSQL databázu.

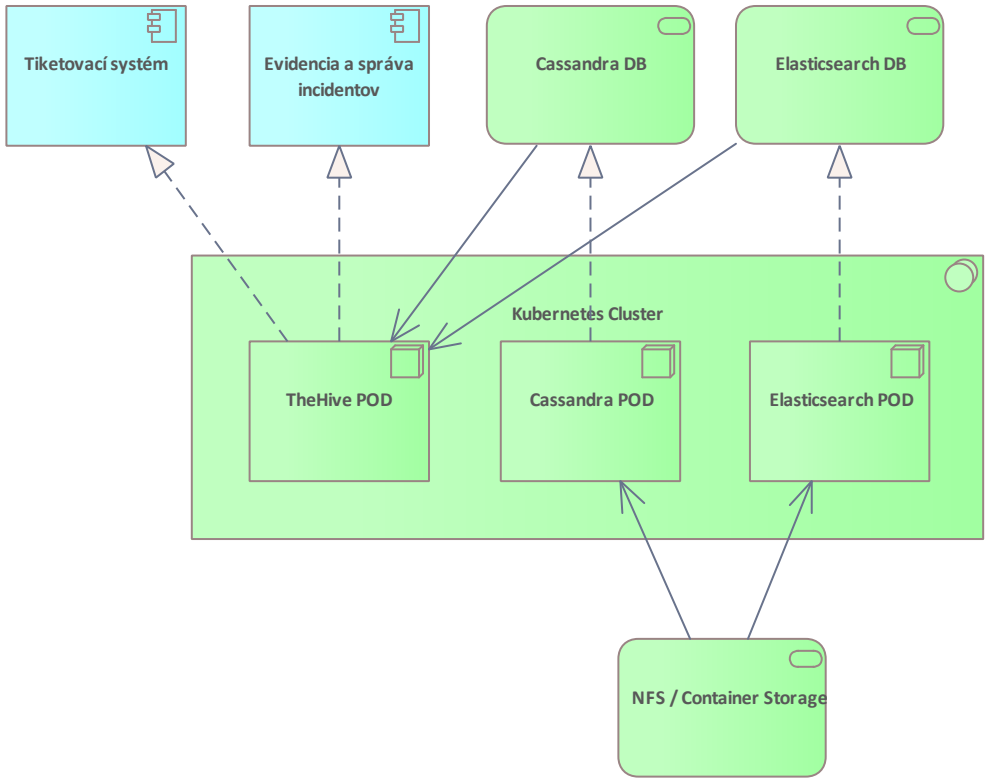
TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.

Cortex

Predstavuje POD Cortex pre SOAR.

1.11. Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov



Obrázok 23 : Technology Usage Viewpoint Tiketovací sytém / Evidencia a správa incidentov alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1 predstavuje využitie Elasticsearch databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databáz pre Cassandra a Elasticsearch.

Popis používaných prvkov:

Evidencia a správa incidentov

Evidencia a správa incidentov je jadrovým prvkom každej bezpečnostnej prevádzky (SOC). Tento podkomponent zaisťuje systematickú dokumentáciu, sledovanie a manažovanie bezpečnostných udalostí a incidentov v priebehu ich životného cyklu – od detekcie cez analýzu až po uzavretie. Kvalitný systém evidencie musí umožniť tímom

koordinovane spolupracovať, dokumentovať kroky, evidovať súvisiace artefakty (observables) a prepojiť incidenty

s relevantnými hrozbami, systémami alebo historickými prípadmi. V ideálnom prípade podporuje aj pokročilé obohacovanie údajov, audit, multitenantnosť a možnosť spätného skúmania incidentov.

Tiketovací systém

Tiketovací systém slúži ako ústredný komunikačný a organizačný kanál pre správu bezpečnostných incidentov počas ich celého životného cyklu. Umožňuje vytváranie, priraďovanie a sledovanie úloh a komunikáciu medzi analytikmi, pričom podporuje audit, SLA monitoring, eskaláciu a notifikácie.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Cassandra DB

Predstavuje technologickú službu NoSQL Cassandra databázy.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Cassandra POD

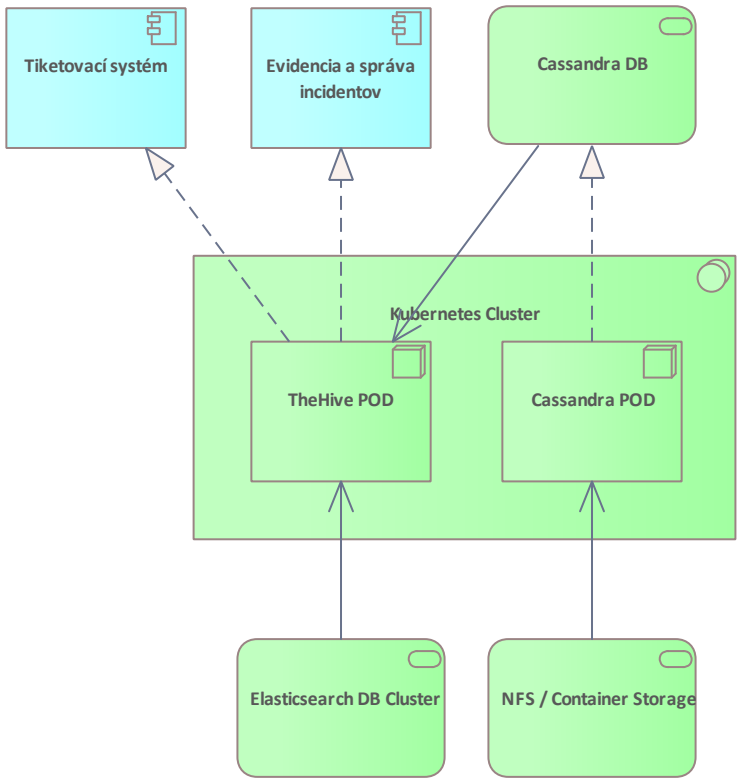
Predstavuje POD Apache Cassandra pre NoSQL databázu.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.



Obrázok 24 : Technology Usage Viewpoint Tiketovací sytém / Evidencia a správa incidentov alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 2 predstavuje využitie Elasticsearch Databázy priamo vo forme centralizovaného DB Clustra. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databázy pre Cassandra.

Popis používaných prvkov:

Evidencia a správa incidentov

Evidencia a správa incidentov je jadrovým prvkom každej bezpečnostnej prevádzky (SOC). Tento podkomponent zaisťuje systematickú dokumentáciu, sledovanie a manažovanie bezpečnostných udalostí a incidentov v priebehu ich životného cyklu – od detekcie cez analýzu až po uzavretie. Kvalitný systém evidencie musí umožniť tímom koordinovane spolupracovať, dokumentovať kroky, evidovať súvisiace artefakty (observables) a prepojiť incidenty

s relevantnými hrozbami, systémami alebo historickými prípadmi. V ideálnom prípade podporuje aj pokročilé obohacovanie údajov, audit, multitenantnosť a možnosť spätného skúmania incidentov.

Tiketovací systém

Tiketovací systém slúži ako ústredný komunikačný a organizačný kanál pre správu bezpečnostných incidentov počas ich celého životného cyklu. Umožňuje vytváranie, priraďovanie a sledovanie úloh a komunikáciu medzi analytikmi, pričom podporuje audit, SLA monitoring, eskaláciu a notifikácie.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Cassandra DB

Predstavuje technologickú službu NoSQL Cassandra databázy.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

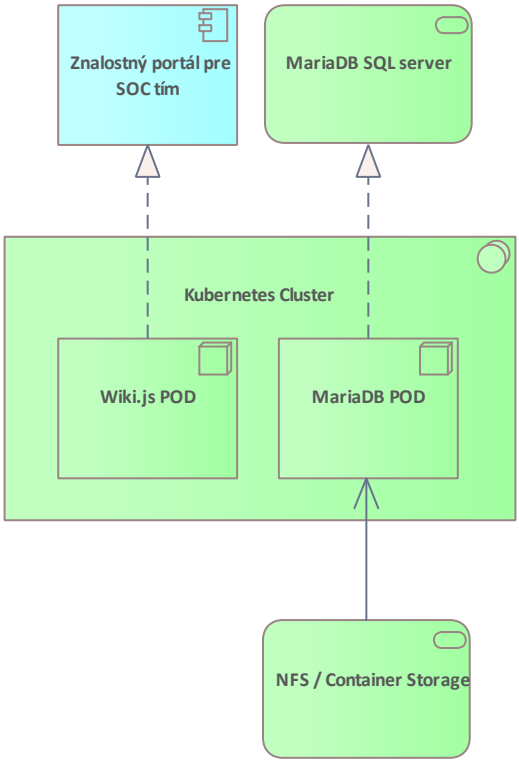
Cassandra POD

Predstavuje POD Apache Cassandra pre NoSQL databázu.

TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.

1.12. Technology Viewpoint Znalostný portál pre SOC tím



Obrázok 25 : Technology Usage Viewpoint Znalostný portál pre SOC tím alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1 predstavuje využitie Databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou SQL servera.

Popis používaných prvkov:

Znalostný portál pre SOC tím

Znalostný portál pre SOC tím je dôležitým stavebným kameňom každého moderného bezpečnostného operačného centra. Slúži ako centrálny repozitár know-how, playbookov, postupov, odporúčaní, analytických návodov a často aj historických lekcií (lessons learned) z incidentov. Znalostný portál:

• Zvyšuje efektivitu a konzistentnosť reakcie na incidenty,

• Umožňuje rýchle zaškolenie nových členov tímu,

• Podporuje štandardizáciu procesov a metodík,

• Umožňuje tímu uchovávať a zdieľať overené postupy a vlastné analytické skúsenosti,

• Posilňuje schopnosť kolektívne sa učiť z incidentov a budovať interné "threat intel" vedomosti.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

MariaDB SQL server

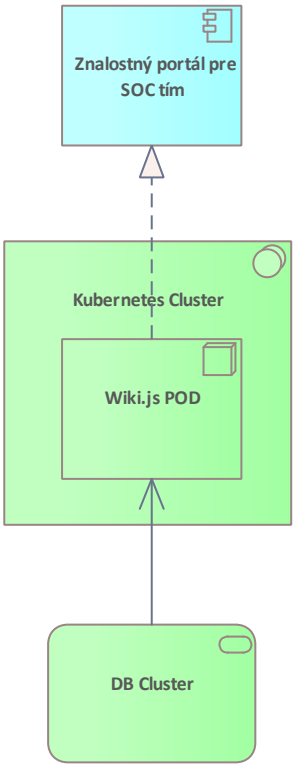
Predstavuje technologickú službu relačnej MariaDB SLQ databázy.

MariaDB POD

Predstavuje POD MariaDB pre relačnú SQL DB.

Wiki.js POD

Predstavuje POD Wiki.js pre Znalostný portál pre SOC tím.



Obrázok 26 : Technology Usage Viewpoint Znalostný portál pre SOC tím alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 2 predstavuje využitie Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

Znalostný portál pre SOC tím

Znalostný portál pre SOC tím je dôležitým stavebným kameňom každého moderného bezpečnostného operačného centra. Slúži ako centrálny repozitár know-how, playbookov, postupov, odporúčaní, analytických návodov a často aj historických lekcií (lessons learned) z incidentov. Znalostný portál:

• Zvyšuje efektivitu a konzistentnosť reakcie na incidenty,

• Umožňuje rýchle zaškolenie nových členov tímu,

• Podporuje štandardizáciu procesov a metodík,

• Umožňuje tímu uchovávať a zdieľať overené postupy a vlastné analytické skúsenosti,

• Posilňuje schopnosť kolektívne sa učiť z incidentov a budovať interné "threat intel" vedomosti.

DB Cluster

Predstavuje službu clustrovanej relačnej databázy. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Wiki.js POD

Predstavuje POD Wiki.js pre Znalostný portál pre SOC tím.

3. ZÁVER

Navrhnuté riešenie v rámci projektu INNOSOC predstavuje komplexný a inovatívny prístup k budovaniu multitenantného operačného centra kybernetickej bezpečnosti poskytovaného ako cloudová služba. V práci boli detailne popísané technologické komponenty, architektonické vrstvy a podporná infraštruktúra, ktoré spoločne tvoria základ pre vysoko škálovateľné, bezpečné a flexibilné prostredie. Nasadenie prvkov automatizácie v kombinácii s integráciou metód strojového učenia, predovšetkým hlbokých neurónových sietí, významne zvyšuje schopnosť systému reagovať na aktuálne hrozby a efektívne identifikovať anomálie v reálnom čase.

Zvolený technologický prístup reflektuje súčasné požiadavky na moderné bezpečnostné architektúry a zároveň umožňuje ďalší rozvoj systému s dôrazom na modularitu, interoperabilitu a prevádzkovú efektivitu. Výsledkom je robustné riešenie, ktoré dokáže pružne reagovať na meniace sa podmienky v oblasti kybernetickej bezpečnosti, pri zachovaní vysokej úrovne automatizácie, pozorovateľnosti a správy viacerých klientských domén v rámci jedného centralizovaného prostredia.

Vytvorená architektúra rešpektuje princípy moderného DevSecOps prístupu, čo zaručuje integráciu bezpečnostných mechanizmov priamo do životného cyklu vývoja a prevádzky služieb. Dôraz na kontajnerizáciu, využitie orchestrácie cez Kubernetes a riadenie CI/CD procesov zaručuje opakovateľnosť, spoľahlivosť a konzistenciu nasadenia služieb v prostrediach s vysokými nárokmi na dostupnosť a bezpečnosť.

Z hľadiska infraštruktúry bolo riešenie navrhnuté s cieľom podporiť vysoký stupeň izolácie, multitenantnú správu a jednoduchú rozšíriteľnosť prostredníctvom škálovateľných deploymentov a privátnych či verejných integračných vrstiev. Technologické prvky ako privátne a verejné Docker Registry, validné SSL certifikáty, HAProxy reverse proxy vrstvy a centralizovaná kontrola cez GitLab CI/CD poskytujú stabilný a bezpečný základ pre prevádzku citlivých bezpečnostných služieb.

Záverom možno konštatovať, že navrhovaná architektúra systému zodpovedá požiadavkám na moderné operačné centrum kybernetickej bezpečnosti, pričom spája vysokú technickú vyspelosť s dôrazom na efektivitu, spoľahlivosť a udržateľnosť v dynamickom kybernetickom prostredí. Systém je pripravený na ďalšie rozšírenie o pokročilé analytické moduly, priame napojenie na externé bezpečnostné zdroje a rozvoj autonómnych reakčných mechanizmov, čím vytvára silný základ pre budúce inovatívne bezpečnostné riešenia.