Prevádzkový opis a pokyny pre servis a údržbu

1. ROZSAH PLATNOSTI A ÚČEL

Tato dokumentace slouží jako provozní popis a pokyny pro servis a údržbu Národního katalogu otevřených dat (NKOD), části projektu OD2.0.

2. DEFINÍCIA POJMOV A SKRATIEK

NKOD
Národní katalog otevřených dat

OCI
Oracle Cloud Infrastructure

LP-ETL
LinkedPipes ETL

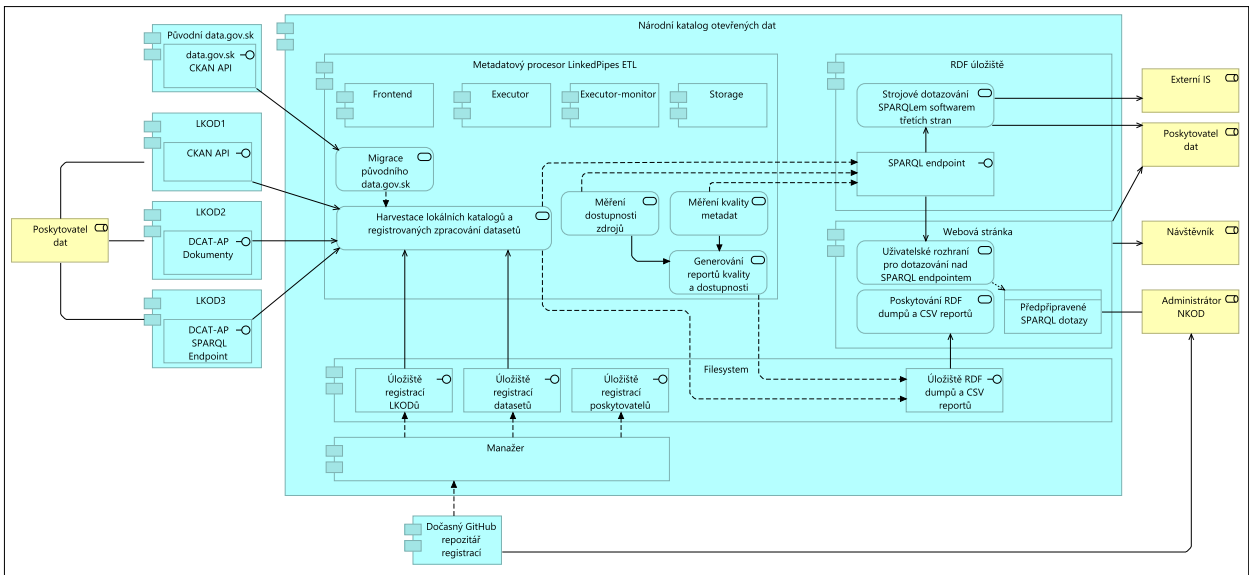
3. POPIS FUNKCIE SYSTÉMU A FUNKCIE APLIKÁCIE

Popis funkcionality a modulů je možné najít v Aplikační příručce. V této sekci tak pouze doplníme informace již obsažené tam.

3.1. Úlohy a funkcionalita IS.

Úlohy a funkcionalita IS je popsána v Aplikační příručce sekce 3. POPIS FUNKCIONALITY IS.

3.2. Popis jednotlivých modulov a väzby.



Popis modulů a jejich vazeb je možné najít v Aplikační příručce sekce 3.2 ZOZNAM A ZÁKLADNÝ POPIS SUBSYSTÉMOV A FUNKCIÍ a 4. POPIS MODULOV.

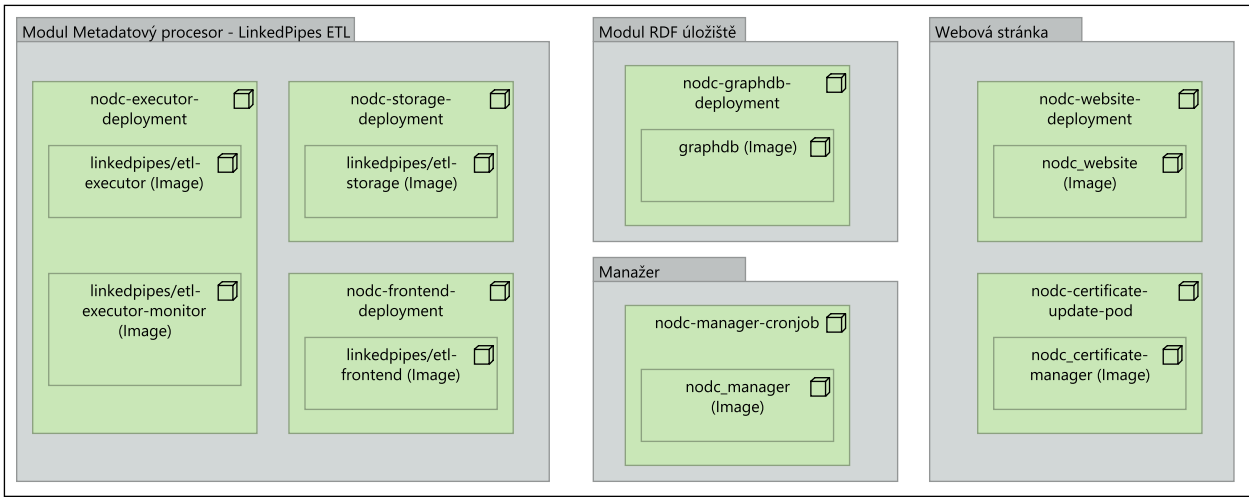


Diagram nasazení komponent do Kubernetes.

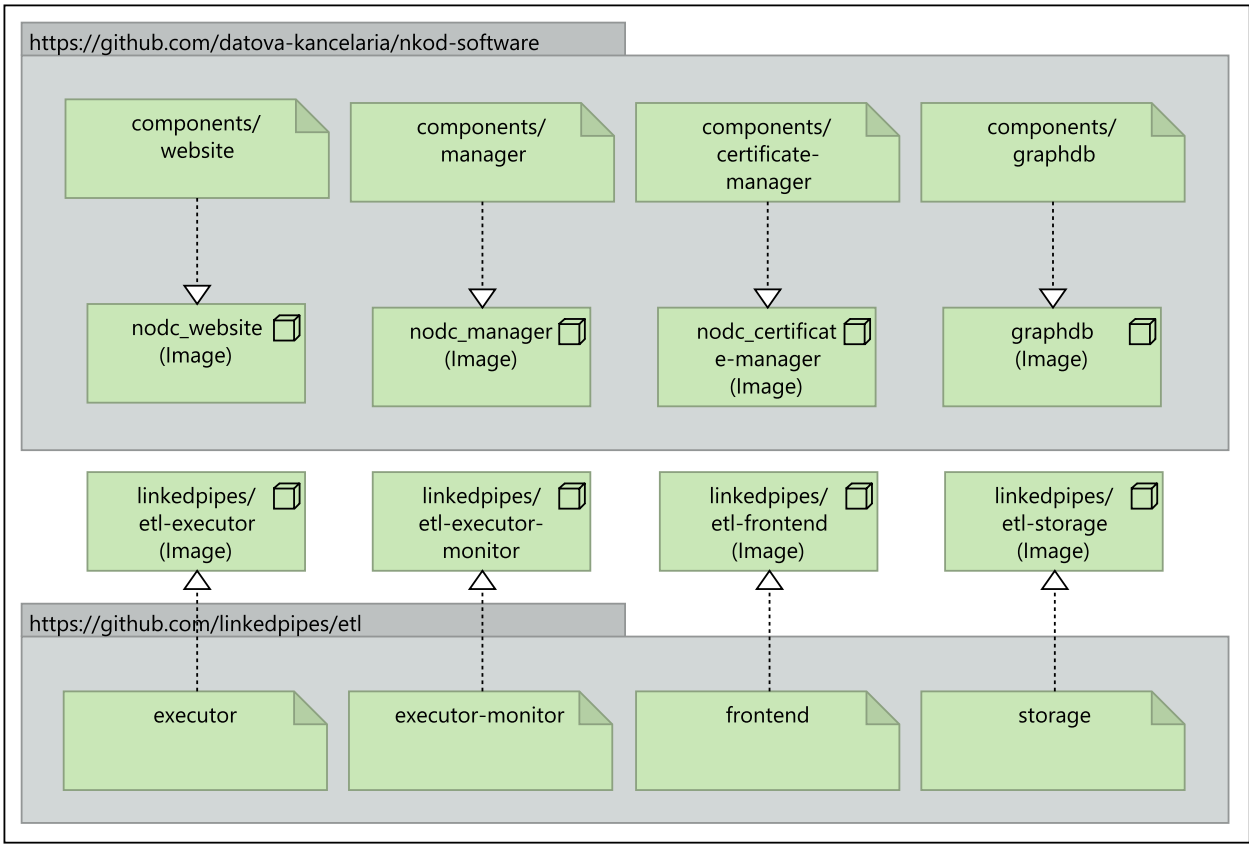


Diagram umístění definic využitých Docker images.

V této sekci tento popis rozšíříme o nasazení popsaných komponent do prostředí Kubernetes. Jedná se o následující moduly:

- RDF úložiště
- Metadatový procesor - LinkedPipes ETL
- Webová stránka
- Manažer

3.2.1. Modul `RDF úložiště`

Module je implementován nasazením Ontotext GraphDB Free z `graphdb Docker image` . Tento modul je následně nasazen `nodc-graphdb-deployment` . Neb v použité verzi GraphDB nepodporuje běh v clusteru, je nasazena právě jedna instance.

Pro uložení dat je využito `nodc-registration-pvc` . Ten definuje úložiště jako `Block Storage` , který je spravován OCI na požadavek Kubernetes. `Block Storage` je zvolen z důvodu výkonu a je používán výhradně `nodc-graphdb-deployment` . Nasazený Docker Image je pak definovaný v NKOD-SW.

S modulem je komunikováno výhradně skrze HTTP rozhraní. Zápis do modul RDF úložiště provádí `nodc-executor-deployment`, který je součástí modulu Metadatového procesoru. K zápisu dochází v rámci procesu harvestace. Současně modul RDF úložiště poskytuje SPARQL endpoint, který je přístupný skrze `nodc-website-deployment` ze sítě Internet.

Pro potřeby řešení chyb v NKOD se dále počítá s přístupem pro administrátora skze VPN, která v době psaní dokumentace ještě nebyla k dispozici.

3.2.2. Modul `Metadatový procesor - LinkedPipes ETL`

Modul je realizován nasazením LinkedPipes ETL (LP-ETL). Nástroj LP-ETL se skládá z několika komponent, které mohou běžet samostatně: executor, executor-monitor, storage a frontend. Oproti původnímu záměru však nejsou komponenty nasazeny v různých Kubernetes Deploymentech. Důvodem je prodleva synchronizace sekundárního úložiště mezi komponentami `executor` a `executor-monitor`. Tato prodleva je způsobena implementací sdíleného `File Systemu` pomocí NFS. Řešením je nasadit obě komponenty v rámci jednoho Podu.

Jednotlivé komponenty jsou tedy nasazeny následovně:

- `nodc-executor-deployment` : executor, executor-monitor
- `nodc-storage-deployment` : storage
- `nodc-frontend-deployment` : frontend Ačkoliv není komponenta frontend přístupná z venku, je nutná pro spouštění harvestace. Dále je pak skrze VPN přístupná pro administrační účely.

Z hlediska komunikace není žádná z komponent Metadatového procesoru veřejně dostupná. O spouštění harvestace se stará komponenta Manažer, která komunikuje s `nodc-frontend-deployment` skrze HTTP. Harvestace pak probíhá dle pipeline dostupných na `nodc-linkedpipes-storage-pvc`. Ten je napojen na `OCI File System`.

Z hlediska komunikace je pak zásadní `nodc-executor-deployment`, který je zodpovědný za samotný proces harvestace. Z tohoto důvodu provádí čtení registračních záznamů z `nodc-registration-pvc`, který je napojen na `OCI File System`. Pracovní data z průběhu harvestace a logy o jejím průběhu jsou pak ukládány na `nodc-linkedpipes-executor-pvc`. Ten je definován jako `Block Storage` úložiště, které automaticky spravuje OCI dle definice v Kubernetes. Důvodem je urychlení harvestace, neb `Block Storage` je výkonnějším úložištěm proti `File Systemu`. Na závěr harvestace jsou pak data nahrána do modulu RDF úložiště pomocí HTTP komunikace s `nodc-graphdb`. Soubory, které mají být veřejně dostupné pro stažení, jsou pak uloženy do sdíleného úložiště `nodc-website-pvc`. Toto úložiště je napojeno na `OCI File System`.

3.2.3. Webová stránka

Webová stránka slouží jako vstupní brána k aplikaci NKOD. Z tohoto důvodu je `nodc-public` realizován jako `Load Balancer`.

Za běžného provozu je nasazen pouze `nodc-website-deployment`. Tento Deployment obsahuje Docker image nakonfigurovaného `nginx`. `nginx` pak slouží jako proxy pro `nodc-graphdb`, poskytuje statické soubory klientská části aplikace a současně zajistuje přístup k souborům vytvořeným harvestací uložených v `nodc-website-pvc`.

`nginx` v `nodc-website-deployment` provádí HTTPS terminaci. Certifikát pro terminaci je uložený na `nodc-certificate-pvc`. Důvodem nevyužití `Secret` je nemožnost měnit obsah `Secret` z Podu, certifikát by tak bylo třeba vkládat do `Secret` ručně. Získání a případné obnovení certifikátu zajišťuje `nodc-certificate-update-pod`. Ten je nutné spouštět manuálně se zastavením `nodc-website-deployment`. Důvodem je způsob ověření certifikátu Let's Encrypt skrze HTTP, z tohoto důvodu musí projít požadavky na `nodc-certificate-update-pod` a nikoliv `nodc-website-deployment`.

3.2.4. Manažer

Modul Manažer je nasazený pomocí `nodc-manager-cronjob` a je zodpovědný za:

- aktualizaci definic pipeline pro harvestování
- aktualizaci registračních záznamů Modul je spouštěn periodicky dle konfigurace, ve výchozím nastavení jednou za den.

Původním záměrem provádět úpravu registračních záznamů v reakci na webhook. Problémem tohoto řešení je nutnost vystavit další komponentu mimo prostředí NKOD. Pokud navíc služba neběží v době změny v externím úložišti registrací, tak by se změna neprojevila, neb webhook není volán opakovaně. Z těchto důvodů bylo rozhodnuto o zjednodušení, registrace jsou aktualizovány před každou harvestací. Neb je harvestace aktuálně plánována denně, nejedná se o významnou výpočetní zátěž. Zdrojem pro aktualizaci dat jsou externí GitHub repozitáře: NKOD-SW, NKOD-REG.

Aktualizace registračních záznamů je prováděna do `nodc-registration-pvc`. Aktualizace pipeline je prováděna do `nodc-linkedpipes-storage-pvc`. Po aktualizaci pipeline je nutné skrze HTTP a `nodc-frontend` notifikovat `nodc-storage-deployment` o potřebě načtení upravených pipeline. Následně je možné pomocí HTTP provést spuštění harvestace přes `nodc-frontend`.

Ačkoliv je možné skrze `nodc-frontend` a VPN pustit tedy harvestaci přímo, je třeba mít na paměti, že takové spuštění nepovede k aktualizaci dat. Pro aktualizaci dat je třeba provést manuální vytvoření jobu z `nodc-manager-cronjob`.

3.2.5. Komunikačný model

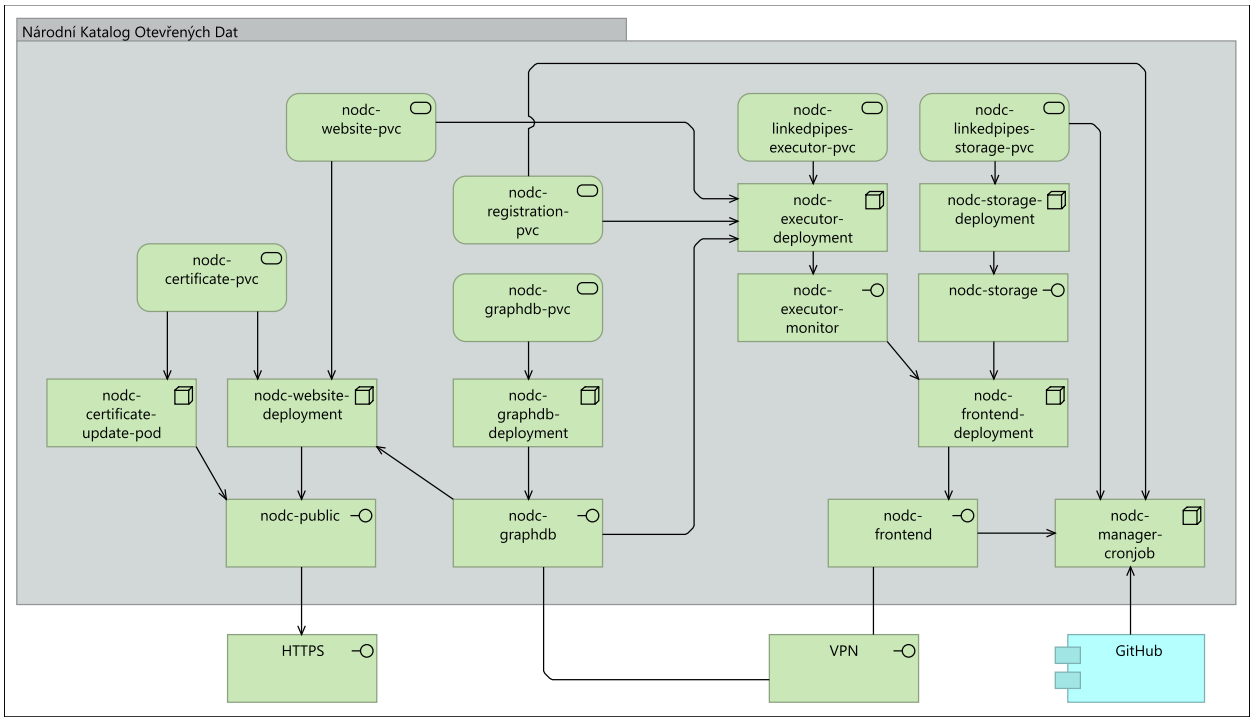


Diagram komunikace komponent.

Komunikace mezi komponentami probíhá dvojím způsobem.

1. pomocí HTTP protokolu,
2. pomocí sdílení dat na disku.

Komunikace mezi moduly je popsána u jednotlivých modulů výše a znázorněna na diagramu komunikace komponent.

3.2.6. Dátový model

Dátový model je popsaná v Aplikační příručce sekce 3.3 DÁTOVY MODEL APLIKÁCIE.

4. POPIS TECHNICKÉHO VYBAVENIA

4.1. Serverová časť / Cloud

Nasazení NKOD počítá s existujícím Kubernetes clusterem verze `1.24.1` v prostředí OCI.

4.2. Klientska časť

Klientská část aplikace běží jako webová stránka ve webovém prohlížeči. Zdrojový kód je součástí modulu Webové stránky a v NKOD-SW v adresáři `./components/website/www/`. Pro sestavení a transpilaci je využitý nástroj Parcel. Oproti větším projektům jako například Webpack vyžaduje Parcel menší množství konfigurace. Seznam podporovaných pohlížečů je specifikován v souboru `package.json` v konfiguraci

```
"browserslist": "> 0.5%, last 2 versions, not dead",
```

Tato konfigurace zajišťuje podporu prohlížečů které:

- > 0.5% - prohlížeče se alespoň 0.5% globálním zastoupením dle
- last 2 version - poslední dvě verze od podporovaných prohlížečů
- not dead - prohlížeče, jejichž podpora neskončila dříve než před dvěma lety Oficiální dokumentaci je možné najít na stránkách browserslist.

4.4. Komunikačné rozhrania

Komunikační rozhraní jsou popsána v Konfiguračná príručka a pokyny pre diagnostiku sekce 3.1. Komunikačné rozhrania.

4.5. Umiestnenie technického vybavenia a zariadení

NKOD běží v Kubernetes pod OCI.

5. UMIESTNENIE ZAKLADNEJ DOKUMENTÁCIE

https://github.com/datova-kancelaria/nkod-dokumentacia

6. ZMENOVÉ KONANIE A SPOSOB INFORMOVANIA O ZMENÁCH V IS

TODO: vlastník/provozovatel

7. ZODPOVEDNOSŤ ZA PREVÁDZKU JEDNOTLIVÝCH ČASTÍ IS

TODO: vlastník/provozovatel

7.1. Zodpovednosť za jednotlivé vrstvy IS

TODO: vlastník/provozovatel

7.2. Zodpovednosť prevádzkovateľa IS

Provozovatel IS je odpovědný za periodické obnovování HTTPS certifikátu. Tento postup je popsán v Konfiguračná príručka a pokyny pre diagnostiku sekce 4.1.2 Obnova či získání HTTPS certifikátů.

7.2.1. Registrácia prístupov do IS

TODO: vlastník/provozovatel

7.2.2. Registrácia požiadaviek na zmenu IS

TODO: vlastník/provozovatel

7.2.3. Monitoring IS

TODO: vlastník/provozovatel

7.2.4. Prístup k vývojovým prostriedkom

Zdrojový kód jednotlivých komponent, mimo GraphDB je veřejný a přístupný v NKOD-SW. Jejich vývoj tedy nevyžaduje přístup do zvláštního prostředí, pouze práva k repozitáři.

V případě GraphDB se jedná o RDF databázi dodanou třetí stranu s neveřejným vývojem.

7.2.5. Prístup k dátam

Vstupní data, tj. registrační záznamy datových sad, katalogů a poskytovatelů dat jsou přístupná v NKOD-REG. Výstupní data jsou veřejně dostupná skrz komponentu Webové stránky.

7.3. Zodpovednosť používateľa IS

NKOD je užíván přes veřejnou webovou stránku a API v podobě SPARQL endpointu. Uživatelé jsou tedy anonymní veřejnost bez zodpovědností vzhledem k IS.

8. ČINNOSTI REALIZOVANÉ POČAS PREVÁDZKY IS

8.1. Postup pri zálohovaní údajov

Kompletní obsah NKOD je generován při každém harvestování, není tedy třeba provádět jeho zálohu.

8.2. Kontrola správnosti nahratia záloh

Kompletní obsah NKOD je generován při každém harvestování, není tedy třeba provádět jeho zálohu.

8.3. Monitoring prevádzky systému

TODO: vlastník/provozovatel

8.4. Postup pri zabezpečení 24 hod. pohotovostných služieb

24 hod. pohotovostní služby nejsou požadovány.

9. DISTRIBÚCIA A PUBLIKOVANIE APLIKÁCIE

Řešení NKOD je distribuováno jako:

- Definice nasazení do Kubernetes a specifických softwarových komponent NKOD-SW
- Definice pipeline pro harvestaci dat NKOD-PIPELINE

- Definice DCAT-AP-SK 2.0

Mimo tyto zdroje navíc využívá NKOD dalšího softwaru:

- LinkedPipes ETL
- Ontotext GraphDB Free

10. VERZIOVANIE APLIKÁCIÍ (dotýka sa iba správy aplikácií)

Zdrojové kódy všech komponent jsou uložené v Git repozitářích, který poskytuje verzování. Přehled repozitářů je v sekci 9. DISTRIBÚCIA A PUBLIKOVANIE APLIKÁCIE.

GraphDB je zveřejňováno se sémantickým verzováním.

11. VYKONÁVANIE ZMENY V PREVÁDZKOVÝCH DÁTACH

Data tvořící NKOD jsou kompletně přebírána z externích zdrojů a s každou harvestací tvořena znovu. Není tedy potřeba do takto tvořených dat zasahovat.

12. ARCHIVÁCIA ÚDAJOV

Není vyžadována archivace dat NKOD. Jediná data, která je potřeba archivovat, jsou registrační záznamy. Ty jsou ale v NKOD řešeny pouze dočasně přes GitHub repozitář NKOD-REG a v rámci dalšího rozvoje bude řešení změněno. Archivace registrací je tak mimo NKOD.

13. PLÁNOVANIÉ A NEVYHNUTNÉ ODSTÁVKY IS

13.1. Popis pravidelných odstávok

Systém vyžaduje plánovanou odstávku za účelem obnovy HTTPS certifikátu. Tuto odstávku je třeba provést dle expirace certifikátu, v případě využitého Let's Encrypt pak jednou za tři měsíce.

13.2. Popis nepravidelných (nevyhnutných) odstávok.

Dle rozsahu a urgentnosti je možné odstavit NKOD nekolika způsoby.

Plánovaná odstávka by měla probíhat v době mimo harvestaci. V takovém případě je možné bezpečně smazat všechny deploymenty, nebo nastavit počet replik v deploymentu na 0. Tímto dojde k odstavení všech výpočetních kapacit. V případě nutnosti odstavení harvestace, je možné toto učinit smazáním `nodc-manager-cronjob`, který je zdopovědný za spouštění harvestace. Pokud je zapotřebí odstavit NKOD od veřejného přístupu je vhodné tak učinit skrze `nodc-website-deployment`.

Není doporučeno smazání `nodc-public`, neb při vytvoření by došlo k přiřazení nové IP adresy a bylo by nutné upravit příslušný DNS záznam.

Poslední krok je pak možné využít i k rychlému odstavení veřejného přístupu k NKOD.

V případě běžící harvestace je možné její zastavení po aktuálně běžící komponentě v pipeline možné skrze uživatelské rozhraní LinkedPipes ETL, nebo jeho API. Toto rozhraní je přístupné administrátorovi skrze VPN a service `nodc-frontned`.

Neb je NKOD nasazený v prostředí OCI nemělo by dojít k neplánovanému a omakžitému ukončení všech podů. V případě, že by se tak stalo, může dojít o opoždění harvestace.

14. SPOSOB PRIDEĽOVANIA PRÍSTUPOVÝCH PRÁV

TODO: vlastník/provozovatel

14.1. Postup pri podávaní žiadostí o prístup

14.2. Prideľovanie žiadateľov do rolí

15. IDENTIFIKÁCIA VLASTNÍKA ÚDAJOV

TODO: vlastník

16. SPRAVOVANIE ČÍSELNÍKOV(platí len pre APL)

V NKOD se používají číselníky z EU Vocabularies, konkrétně File types a Frequencies. Ty se aktualizují cca jednou za tři měsíce. Pokud je třeba pracovat s nejnovější verzí těchto číselníků, stačí spustit servisní pipline `00 - Cache`.

17. POVINNÁ ZMENA POUŽÍVATEĽSKÉHO HESLA

NKOD nespravuje uživatelské účty, u kterých by bylo potřeba řešit změnu hesel.

18. POSTUP RIEŠENIA PORUCHOVÝCH A HAVARIJNÝCH STAVOV

Bežnou součástí řešení problému je nahlédnutí do logů systémů. Tento dokument uvažuje pouze logy NKOD, nikoliv logy generované na úrovni Kubernetes či OCI.

Za modul `Webové stránky` generuje logy z hlavního procesu NginX. Logy jsou generovány dle výchozího nastavení a ukládány do:

- `/var/log/nginx/error.log`
- `/var/log/nginx/access.log` Kde druhý slouží pro logování přístupů. V případě využitého NginX image jsou tyto soubory jen symbolické linky na `/dev/stderr` a `/dev/stdout` . Logy tedy nejsou uloženy do trvalého úložiště ale pouze zobrany na chybový a standartní výstup.

Modul `RDF úložiště` implementovaný GraphDB je konfigurován pomocí logback.xml. Ten je možné najít v NKOD-SW `components/graphdb/conf/logback.xml` . Ve výchozí konfiguraci se logy uchovávají po dobu 14 dní. Velikost jednoho logovacího souboru je 500MB, což při počtu 10 logovacích souborů vyžaduje 5GB místa pro logy. Logy jsou uloženy v `nodc-graphdb-pvc` který má velikost 16GB.

Modul `Metadatový procesor - LinkedPipes ETL` provádí logování na úrovni svých komponent. Komponenta `frontned` neukládá logy an disk a dává je pouze na standartní výstup. Ostatní komponenty ukládají logy do adresáře `/data/lp-etl/logs` s týdenní rotací. Zde je vhodné připomenout, že tato cesta je mapována různé. Pro komponentu `storage` je cesta namapována do File Storage skrze `nodc-linkedpipes-storage-pvc` . Pro komponenty `executor` a `executor-monitor` pak do Block Storage skrze `nodc-linkedpipes-executor-pvc` . Rotace logů pro tyto komponenty je nastavena na jeden týden.

Kromě těchto logů jsou ukládány i logy k jednotlivým spuštěním pipeline. Tyto logy jsou opět ukládány skrze `nodc-linkedpipes-executor-pvc` . Při testovacím provozu byla velikost logů pod 100MB, velikost adresářů se spuštěními pipeline pak 16GB. Je nicméně třeba zdůraznit, že velikost adresářů poroste s množstvím zpracovávaných dat.

18.1. Registrácia a hlásenie poruchových a havarijných stavov.

TODO: vlastník/provozovatel

18.2. Zásahy na serveri (reštart a pod. správca servera).

Restart kontejnerů je možné provést skrze OCI rozhraní pomocí smazání podů nebo úpravou počtu replik pro Deployment.

18.3. Chybové stavy databázy

Jako databáze se používá Ontotext GraphDB Free. Pro její případné chybové stavy je potřeba konzultovat její dokumentaci.

18.4. Chybové stavy komunikácií

Pro komunikaci ze strany klienta se využívá HTTP prokolu včetně jeho stavových kódů.

18.5. Chybové stavy aplikácie

Chybové stavy lze rozdělit na chyby v/při harvestaci a na chyby v rámci nasazení a provozu infrastruktury.

18.5.1 Chybové stavy harvestace

Pokud dojde při harvestaci k chybě, bude reprezentována jako chybový stav pipeline LP-ETL viditelný v uživatelském rozhraní LP-ETL.

18.5.1.1 Nedostatek operační paměti

Pokud některá z pipeline skončí ve stavu indikovaném červeným otazníkem, je možné, že v průběhu jejího zpracování došla operační paměť, a proces byl zabit operačním systémem. To se může stát v případě řádového nárůstu počtu zpracovávaných datových sad. Je třeba zvýšit dostupnou operační paměť pro `executor`.

18.5.1.2 Chybějící číselníky

Může se stát, že na webu EU Vocabularies dojde ke změně URL používaných číselníků. Pak je třeba URL upravit v pipeline 00 - Cache.

18.5.1.3 Neočekávaná chyba při zpracování registračních záznamů

Pipeline 03 - Harvestace LKOD a registrací zpracovává registrační záznamy z externích zdrojů. I když konfigurace v pipeline předpokládá celou řadu problémů se vstupními daty a řeší je ignorováním takového záznamu, či transformací nevhodných položek na jejich vhodnější hodnotu, může se stát, že některý ze vstupních záznamů bude chybný nepředvídaným způsobem, který způsobí selhání transformace. V takovém případě je třeba z logů exekuce a ladících dat uložených mezi jednotlivými komponentami pipeline zjistit, co je za problém a ošetřit ho v pipeline.

18.5.2 Chybové stavy infrastruktury

Z hlediska infrastruktury, Kubernetes, může dojít k chybám způsobeným konfigurací nebo staven clustru. Špatná konfigurace, například URL NKOD-PIPELINE či NKOD-REG mohou vést k nefunkční harvestaci. Tato chyba se neprojeví v administrativním rozhraní, ale je třeba jí prošetřit srkze log instancí `nodc-manager-cronjob` .

Další chyby mohou být způsobené neuplnou konfigurací. Například chybějícími objekty ConfigMap nebo Secret. V takovém případě nedojde ke spuštění podu. Speciálním případem může být třeba absence služeb pro `nodc-website-deployment` . Kdy `nginx` vyžaduje existenci nodc-graphb při startu.

Dalším důvodem nespuštění podu může být absence nebo nepřipravenost datových úložišť. Z hlediska externích služeb pak může bránit spuštění podu nemožnost stáhnout Docker image z externího repozitáře. Toto platí pro všechny komponenty mimo GraphDB. K nemožnosti stáhnout Docker Image může dojít nedostupností externí služby, nebo vyčerpáním limitu pokusů o stažení. Tyto stavy je opět možné vyžíst skrze rozhraní Kubernetes.

Obecně se jedná o chybové stavy spojené s nasazením do prostředí Kubernetes a tedy nespecifické pro NKOD.

18.6. Prechod na záložný systém

Nepředpokládá se nasazení záložního systému.

19. NÁROKY NA PRESONÁL

19.1. Nároky na správu IS

Administrátor NKOD musí být znalý:

- Kubernetes

- Oracle Cloud Infrastructure (OCI)

19.2. Nároky na používateľov IS

Nároky na uživatele jsou definovány v Aplikační příručka sekce 4. NÁROKY NA POUŽÍVATEĽA.

20. SÚVISIACA DOKUMENTÁCIA

- Aplikační příručka
- Inštalačná príručka a pokyny na inštaláciu (úvodnú/opakovanú)
- Integračná príručka
- Konfiguračná príručka a pokyny pre diagnostiku
- Uživatelská příručka

Give feedback