

ÚDZS Integračná platforma

Prevádzková dokumentácia

Príručka administrátora



- úrad pre
- dohľad nad
- zdravotnou
- starostlivosťou

Autor	<i>Informácia vyňatá</i>
Vytvorené dňa	12. september 2022
Ukončené dňa	
Referencia	UDZS-Prirucka_administratora_IP_v1.0.docx
Verzia	1.0
Schválené	

KONTROLA DOKUMENTU

Záznam o zmene

Dátum	Autor	Verzia	Popis zmeny
18.08.2022	<i>Informácia vyňatá</i>	0.1	Vytvorený dokument
12.09.2022	<i>Informácia vyňatá</i>	1.0	Prvá publikovaná verzia

Distribúcia

Č. kópie	Meno	Funkcia
1	Úrad pre dohľad nad zdravotnou starostlivosťou (ÚDZS)	-
2	<i>Informácia vyňatá</i>	-
3		-

ZOZNAM POJMOV A SKRATIEK

Skratka	Popis
AD	Active Directory – implementácia adresárových služieb LDAP firmou Microsoft
CA	Certifikačná autorita
CSR	Certificate Sign Request
DB	Databáza
DN	Distinguished Name (jednoznačná identifikácia entity v LDAP)
DNR	Detailný návrh riešenia
DR	Disaster recovery – obnova systému po výpadku
FMW	Oracle Fusion Middleware (rodina produktov Oracle)
http	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol – Secure
IP	Integračná platforma
LDAP	Lightweight Directory Access Protocol
OS	Operačný systém
OSB	Oracle Service Bus
PROD	Produkčné prostredie
SOA	Servisne Orientovaná Architektúra
SOA Suite	Sada aplikácií od firmy Oracle na implementovanie integračných služieb a procesov
SSL	Secure Sockets Layer – bezpečnostný protokol
TEST	Testovacie prostredie
ÚDZS	Úrad pre dohľad nad zdravotnou starostlivosťou
WL	Weblogic
WLS	Weblogic Server
WSM	Web Services Manager (komponent SOA Suite)

ZOZNAM PRÍLOH A ODKAZOV

Zoznam príloh

Č. prílohy	Názov a popis

Zoznam odkazov

Č. odkazu	Názov a popis
1.	<u>Dokumentácia Oracle Service Bus (OSB)</u> https://docs.oracle.com/en/middleware/soa-suite/service-bus/12.2.1.4/index.html
2.	<u>Administrátorská príručka Oracle Service Bus (OSB)</u> https://docs.oracle.com/en/middleware/soa-suite/service-bus/12.2.1.4/administer/administering-oracle-service-bus.pdf
3.	<u>Dokumentácia Oracle SOA Suite</u> https://docs.oracle.com/en/middleware/soa-suite/index.html
4.	<u>Administrátorská príručka SOA Suite</u> https://docs.oracle.com/en/middleware/soa-suite/soa/12.2.1.4/administer/administering-oracle-soa-suite-and-oracle-business-process-management-suite.pdf
5.	<u>Dokumentácia Enterprise Manager</u> https://docs.oracle.com/en/enterprise-manager/

1. ÚVOD

Zámer a ciele dokumentu

Dokument vznikol v rámci projektu implementácie novej integračnej platformy (IP) na Úrade na dohľad nad zdravotnou starostlivosťou (ÚDZS). V rámci projektu ÚDZS plánuje zmodernizovať a zefektívniť integračné prostredie IS ÚDZS, ktoré bolo vybudované v roku 2005 a dnes už nevyhovuje potrebám užívateľov, ale ani platným bezpečnostným a technologickým postupom a štandardom.

Dokument je určený pre zamestnancov ÚDZS a externých dodávateľov, ktorí sa budú podieľať na prevádzke a rozvoji IP na testovacích a produkčných prostrediach ÚDZS.

Čitateľ tohto dokumentu by mal mať znalosti o architektúre a dizajne IP, ktoré sú popísané dokumente „Detailný návrh riešenia“ vytvoreného v rámci projektu implementácie IP. Cieľom dokumentu nie je vysvetliť princípy integrácie, SOA alebo komponentov IP, ale popísať ich fungovanie z pohľadu prevádzky a najčastejšie vykonávaných úloh pre podporu prevádzky.

Rozsah a platnosť dokumentu

Dokument popisuje bežné, rutinné aktivity, ktoré súvisia s prevádzkou Integračnej platformy. Je rozdelený do niekoľkých častí, z ktorých každá rieši iný aspekt prevádzky riešenia:

- Administrácia
- Dostupnosť riešenia
- Bezpečnosť
- Retencia dát a čistenie
- Diagnostika
- Dohľad

Dokument obsahuje návody, postupy a odporúčania, avšak nenahrádza štandardnú Oracle dokumentáciu k produktom, ktorá by mala byť hlavným zdrojom informácií.

2. ADMINISTRÁCIA

Z pohľadu administrácie Integračnej platformy na úrovni aplikačnej vrstvy rozlišujeme tzv. domény, ktoré zoskupujú samostatné aplikačné servre (inštancie) do logických celkov s jednotnou administráciou a konfiguráciou.

Integračnú platformu tvoria v každom z prostredí dve nezávislé domény, SOA doména a OSB doména.

Informácia o doménach vyňatá

Riadenie behu aplikačného servera

Node Manager

Pre riadenie behu inštancií aplikačného servra je potrebný beh tzv. Node Manager (NM) procesu. Jeho automatický štart je zabezpečený systemd službou vytvorenou na úrovni OS.

Služba OS je pomenované podľa konvencií:

```
<názov domény>_nodemanager.service
```

Napr. na TEST prostredí sú dostupné tieto NM služby:

- osbt_domain_nodemanager.service
- soat_domain_nodemanager.service

Spustenie alebo zastavenie NM je prostredníctvom systemctl príkazu (pod „root“ používateľom):

```
systemctl start <názov NM služby>  
systemctl stop <názov NM služby>
```

Štart/stop inštancií WLS

Popis použitia štandardných skriptov dodávaných s inštaláciou WLS je súčasťou Oracle dokumentácie:

<https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/start/overview.html>

Pre jednoduchšie riadenie behu aplikačných serverov Integračnej platformy sú nad rámec štandardných skriptov dostupné tieto skripty:

- startAdmin.sh – spustenie Admin servra
- stopAdmin.sh – zastavenie Admin servra
- startManaged.sh – spustenie Managed servra
- stopManaged.sh – zastavenie Managed servra
- startCluster.sh – spustenie všetkých serverov klastra
- stopCluster.sh – zastavenie všetkých serverov klastra

Skripty sú dostupné v samostatných adresároch pre každú doménu:

```
/oracle/scripts/<názov domény>
```

Signatúra pre jednotlivé skripty je nasledovná:

```
startAdmin.sh  
stopAdmin.sh  
startManaged.sh <názov managed servra>  
stopManaged.sh <názov managed servra>  
startCluster.sh <názov klastra>  
stopCluster.sh <názov klastra>
```

Názvy WL serverov ako aj klastrov v rámci domén sú uvedené na začiatku kapitoly 2.

Pre spustenie serverov OSB domény, napr. v TEST prostredí, je potrebný štart admin servera a serverov jednotlivých klastrov v rámci OSB domény:

```
/oracle/scripts/osbt_domain/startAdmin.sh  
/oracle/scripts/osbt_domain/startCluster.sh osb_cluster  
/oracle/scripts/osbt_domain/startCluster.sh jms_cluster
```

Pre zastavenie OSB domény, napr. v TEST prostredí, je potrebné zastaviť servre v opačnom poradí:

```
/oracle/scripts/osbt_domain/stopCluster.sh osb_cluster  
/oracle/scripts/osbt_domain/stopCluster.sh jms_cluster  
/oracle/scripts/osbt_domain/startAdmin.sh
```

Pre štart serverov SOA domény, napr. v TEST prostredí, je potrebný štart admin servera a serverov klastra v rámci SOA domény:

```
/oracle/scripts/soat_domain/startAdmin.sh  
/oracle/scripts/soat_domain/startCluster.sh soa_cluster
```

Pre zastavenie SOA domény, napr. v TEST prostredí, je potrebné zastaviť servre v opačnom poradí:

```
/oracle/scripts/soat_domain/stopCluster.sh soa_cluster  
/oracle/scripts/soat_domain/stopAdmin.sh
```

Logy

Pre riešenie problémov pri štarte alebo počas behu aplikačného servra je odporúčané skontrolovať logy v adresári dedikovanom pre príslušnú doménu, podľa konvencií:

```
/oracle/logs/<názov domény>
```

Alternatívou pre spustenie a zastavenie inštancií aplikačného servra v rámci domény cez príkazový riadok je použitie grafického používateľského rozhrania - WLS administračnej konzoly. Popis jednotlivých krokov je súčasťou štandardnej dokumentácie:

<https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/wlach/taskhelp/startstop/StartAndStopServers.html>

Štart/stop HTTP servra

HTTP server plní v rámci Integračnej platformy funkcie reverzného proxy a loadbalancera. Na spustenie a zastavenie HTTP servra slúžia príkazy OS:

```
systemctl start httpd  
systemctl stop httpd
```

Logy

Pre riešenie problémov pri štarte alebo počas behu HTTP servra je odporúčané skontrolovať logy v adresári pre príslušnú doménu:

```
/var/log/httpd/soa  
/var/log/httpd/osb
```

Vytvorenie nového dátového zdroja

Pridávanie a konfigurácia dátových zdrojov (angl. Data Source) je popísaná v Oracle dokumentácii:

<https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/wlach/taskhelp/jdbc/ConfigureDatabaseConnectivity.html>

Riadenie životného cyklu služieb

Všetchny služby sú evidované v katalogu služieb. To je excel dokument UDZS_IP-ServiceCatalogue_YYYY-MM-DD.xlsx uložený na sharepoint.

Každá služba je popísaná ve specifikaci služby. Specifikace je dokument MS Word uložený na sharepoint. Specifikace popisuje službu, její rozhraní a chování.

Např. UDZS-SpecRozhrania_SID-029_PokytntutieUdajovRPOpreRPZS-v1.0.docx

Životný cyklus služieb zahrnuje tyto stavy:

- vytvorenie služby
- používání služby
- deaktivace služby

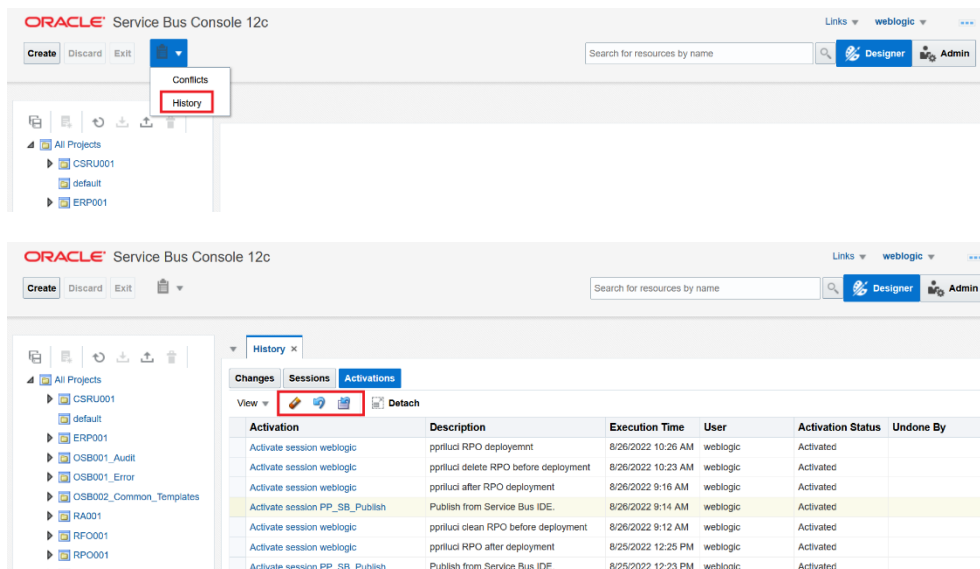
Vytvorenie služby

Služby sa vytvoří v rámci vývoje v nástroji Oracle JDeveloper.

Po otestování se použije Deployment Tool pro nasazení služby na konkrétní prostředí. Typicky se nasazují skupiny služeb v tzv. projektu.

Administrátorská konzole [https:// Informácia vyňatá/servicebus](https://informacia.vyňatá/servicebus) umožňuje:

- prehľad historie nasazení. Jméno v popisu nebo v názvu session určuje osobu, která prováděla nasazení.
- roll back nebo opětovné nasazení už provedných změn atp.
- dodatečnou customizaci



Používání služby

Používání služby je nejdelší období, kdy je služba nebo verze služby nasazena na prostředí a vykonává integrace.

Monitoring služeb je popsán v kapitole Dohľad

Deaktivace služby

K deaktivaci služby nebo verzi služby dojde v okamžiku, kdy už danou verzi nebo službu nikdo nepoužívá. V praxi se tento stav zjistí ve dvou krocích:

1. z monitoringu je zřejmé, že služba nebyla volána dlouhé časové období (typicky rok, ale stanoví se podle typu služby)
2. IP tým osloví konzumenty služby s dotazem, jestli danou verzi nebo službu ještě budou používat

Deaktivace služby se provádí ve dvou krocích:

- služba nebo verze se deaktivuje pomocí OEM nebo lokální EM console OSB [https:// Informácia vyňatá/em](https://informacia.vyňatá/em) (Oracle dokumentace) nebo pomocí skriptu
- služba nebo verze zůstane deaktivována po dlouhé časové období pro případ, že by se ji nějaké konzument pokusil zavolat.
- pokud nebyla služba nebo verze volána po dlouhé období, dojde k jejímu odmazání z OSB a undeploy z SOA Suite.

Popis systémových služieb

Systémové služby ODA dôležité z pohľadu administrátora, ich manažovanie (startup, restart, shutdown) a dopad na beh integračnej platformy, napr. DNS, Timserver, LDAP, Mailserver.

Systémové služby, potrebné pre spoľahlivý beh a manažovateľnosť integračnej platformy:

- **interné** (bežiace v prostredí ODA):

- „out of the box“ - štartované, reštartovateľné a vypínateľné, čo najviac automatizované, z prostredia manažmentu platformy = odacli, ODAUI, Enterprise Manager.

- „custom“ - vytvorené počas implementácie riešenia - sem zaraďujeme napr. vytvorenie, inicializáciu a nastavenie automatického pravidelného behu skriptov na backup VM serverov platformy (tieto ďalej využívajú utilitu kvmb). Automatizované spúšťanie je zabezpečené definíciou cyklov, prostredníctvom nastavení programu crontab pre užívateľov root a odaadmin, v operačnom systéme hlavných serverov platformy.

- tiež sem radíme špeciálne použitie služby interného zdieľaného úložiska - tzv. „NFS server“, (resp. „NFS share“), poskytované z hlavných serverov platformy, do konkrétnych virtuálnych serverov, pre potreby zdieľania „cluster“ informácií medzi vybranými virtuálnymi servermi, či pre potreby zdieľania inštalácií softvérového vybavenia. Vytvorenie zdieľaného úložiska je štandardne realizované cez ODA UI, pričom takéto špeciálne použitie NFS share, je ďalej manuálne dodefinované (s nastavením obmedzenia prístupu pre konkrétne virtuálne servre) v /etc/exports na jednotlivých hlavných serveroch, nasledovne:

integracia01:

Informácia vyřatá

integracia02:

Informácia vyřatá

Na základe nastavenia služby interného zdieľaného úložiska - tzv. „NFS server“ z jednotlivých hlavných serverov, sú ďalej definované automatické pripojenia príslušných NFS share v konkrétnych virtuálnych serveroch, vždy v konfiguračnom súbore /etc/fstab - napr. pre VM a1p01:

Informácia vyřatá

Z dôvodu nadesignovaného poskytovania služby interného zdieľaného úložiska - tzv. „NFS server“ z hlavných serverov platformy, je potrebné pri prevádzaní ich prípadného reštartu, či vypínania, vždy tomuto kroku predradiť vypnutie všetkých virtuálnych serverov, ktoré využívajú službu zdieľaného úložiska, poskytovanú príslušnými hlavnými servermi platformy. Tak tiež je odporúčané pred opätovným zapnutím virtuálnych serverov, overiť, že služba interného zdieľaného úložiska -

tzv.“ NFS server“ je po reštarte hlavných serverov platformy, už opäť dostupná.
Typicky používané príkazy pre overenie:

```
Showmount -e „IP_ADRESA_NFS_servra  
ps -ef | grep nfs
```

-**externé** (bežiacie v ostatnom prostredí, v rámci infraštruktúry zákazníka):

- DNS služba – dostupnosť nutná pre zabezpečenie spoľahlivého prekladania názvov komponentov sieťových spojení, na konkrétne adresy sieťových provkov. Definovali sme a vo všetkých komponentoch používame servre 10.51.17.10 , 10.51.17.11 .

- NTP služba – používanie a pravidelná synchronizácia systémového času jednotlivých komponentov integračnej platformy, voči jednému zdroju, sú potrebné z dôvodu zabezpečenia správneho fungovania platformou poskytovaných služieb. Definovali sme a vo všetkých komponentoch používame server 10.51.19.200 .

- LDAP služba – použité pre autentifikáciu a autorizáciu prístupov do jednotlivých komponentov platformy, či voči externým dátovým zdrojom.

- mailserver služba - bude použité po inicializácii funkcií notifikácie o aktuálnych, či neštandardných stavoch komponentov platformy, v prostredí Enterprise Manager, pre monitoring (10.51.19.29). Použitie v iných častiach platformy ako je Monitoring, nepredpokladáme.

- NFS služba – použité pre korektné fungovanie Oracle DB Data Guard (+ ako sekundárne úložisko pre zálohy databáz) a ako úložisko pre zálohy aplikačných virtuálnych serverov. Definovali sme a používame server

10.51.19.30 .

- EM monitoring a manažment systém – popis v kapitole 7. Dohľad

Záplaty a upgrade

Dôležitým aspektom pre posúdenie potreby aktualizácie Integračnej platformy je trvanie podpory zo strany Oracle, ktorá sa viaže na konkrétnu verziu (release) produktu. V prípade dostupnosti novej verzie niektorého z komponentov Integračnej platformy (ako napr. SOA Suite, OSB) odporúčame preveriť dátum ukončenia podpory pre staršiu verziu produktu a aktualizáciu (upgrade) na jej novšiu verziu. Postup pre upgrade je špecifický pre daný komponent a je popísaný v štandardnej Oracle dokumentácii pre novšiu verziu.

Je dobrou praxou, aj vzhľadom na nové objavujúce sa bezpečnostné riziká, udržiavať jednotlivé komponenty riešenia aktuálne. Oracle informuje o rizikách, kritických chybách a vydaných záplatách na štvrt'-ročnej báze prostredníctvom stránky, ktorú odporúčame sledovať:

<https://www.oracle.com/security-alerts/>

3. DOSTUPNOSŤ RIEŠENIA

Zálohovanie a obnova

Zálohovanie a Obnova sú veľmi detailne popísané v dokumente Detailný Návrh Riešenia – kapitola 16 (copy+paste s opravou niektorých preklepov):

a. POPIS RIEŠENIA PRE ZÁLOHOVANIE

i. Zálohovanie databázy

Zálohovanie databázy je automaticky spustené po deployi DB VM resp. po vytvorení DB inštancie. Realizuje sa databázovými jobmi, prostredníctvom RMAN utility, ale definovaný je výhradne prostredníctvom ODACLI príkazov (doplnené do defaultov je okrem umiestnenia DB backupov do ASM – do FastRecoveryArea, aj umiestnenie backupov, na *informácia o umiestnení vyňatá*).

DB backupy sú automaticky nastavené na pravidelné inkreментy level1 a pravidelnú zálohu archívnych logov - cieľom je možnosť PointInTimeRecovery 10 dní.

Priebeh a históriu backupov je okrem RMAN výpisov možné zobrazíť aj cez ODACLI výpisy alebo prehľadnejšie aj napr. v prostredí Enterprise Manager.

Pre produkčné DB prostredie okrem pravidelného backupu máme zabezpečenú aj vysokú dostupnosť prostredníctvom technológie Oracle DataGuard (opäť definované výhradne cez ODACLI príkazy). Toto v skratke spočíva v okamžitom aplikovaní DB redo logov z aktívnej (štandardne na ODA1) na standby stranu (štandardne bežiacu na ODA2).

Stav DataGuard je možné zobrazíť cez ODACLI výpisy, alebo prehľadnejšie aj napr. v prostredí Enterprise Manager.

Upozorňujeme že použitá konfigurácia DataGuard, zahŕňa passive standby stranu, t.j. do DB sa na tejto strane nedá pripojiť – beží v read-only móde.

ii. Zálohovanie virtuálnych serverov

VM backup je nadefinovaný na ODA serveroch, ako cron job a využíva funkcionality utility kvibr. Backupy sa umiestňujú na *informácia o umiestnení záloh je vyňatá*.

Backup VM sa spúšťa výhradne pod užívateľom ODAADMIN – najskôr sa skriptom vytvára token, pre korektné použitie odacli commandov a následne sa v skripte spúšťa backup VM cez kvibr, ktorý vykoná:

- kontrolu, že VMka beží na danom systéme

- kontrolu, že sa aktuálne táto VM nebackupuje
- suspend VMky
- snapshot diskov VMky v ASM
- odpauzovanie VMky
- backup diskov VMky zo snapshotu do *informácia vyňatá* s ich súčasnou kompresiou
- vymazanie snapshotu diskov z ASM

Čo sa týka restorov VM - využije sa funkcionálna kvmb. Upozorňujeme, že z dôvodu použitia backup stratégie bez zbierania obrazu aktuálne bežiacich dát z RAM, pri suspende VM (keďže táto operácia by spomaľovala backup proces), VM po restore bude v stave novo naštartovaná.

Tiež upozorňujeme, že pre backup VM, používame komprimovaný backup - najmä z dôvodu nižších nárokov na potrebné voľné miesto a na zníženie nárokov na nutný sieťový prenos *informácia o umiestnení je vyňatá*. V dôsledku tohoto faktu kópia a kompresia dát trvá rádovo hodiny pre každú VM. Vyhodou je však krátkodobá nedostupnosť VM (potrebná len na odloženie snapshotu diskov VM) pohybujúca sa rádovo v jednotkách sekúnd; čiže s VM sa dá aj počas backupu ďalej pracovať takmer bez výpadku. Aktualizácia systémového času (1-3 sekundový rozdiel vznikajúci počas pauzy VM v suspend stave) je vyriešená automatickou synchronizáciou systémového času zo zákazníkom poskytnutého NTP servera.

b. POPIS RIEŠENIA PRE OBNOVU

V rámci obnovy (alebo restore) je rozdielny prístup pre DB inštalácie (DB VM) a aplikačné inštalácie (APP VM).

Obnova DB VM prostredí je realizovateľná prostredníctvom ODACLI príkazov, alebo prostredníctvom RMAN utility či DBADMIN príkazov – podľa závažnosti výpadku a nedostupnosti konkrétnych prostredí. Nutnou podmienkou je buď existujúce, alebo možnosť vystaviť nové, prázdne DB prostredie s inštalovanou DB v príslušnej verzii a dostupnosť všetkých potrebných záloh (Level0, Level1 a Archivne logy db). Konkrétny postup môže byť tak jednoduchý ako "FLASHBACK TABLE username.table1 TO TIME STAMP (SYSTIMESTAMP - INTERVAL '25' MINUTE);", ale aj tak zložitý ako sú uvádzané príklady v dokumentácii na stránke:

<https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/user-managed-recovery-advanced.html>

Odporúčaním je preto vždy kontaktovať DB Administrátora (ideálne certifikovaného Oracle pre správu databáz), pokiaľ by vyvstala potreba obnovy zálohovaných dát DB.

Obnova APP VM prostredí je iná operácia ako obnova DB VM. Pri restore APP VM sa v skratke najčastejšie jedná buď o pripojenie obrazu odloženého disku do inak

fungujúcej VM (čiastočný restore), alebo o vystavanie novej VM, použitím obnovy niektorých, alebo všetkých zálohovaných diskov (tzv. kompletný restore).

Najjednoduchší spôsob pre kompletný restore, je vytvoriť novú VM s príslušnými konfiguráciami (počet a veľkosť diskov, meno a sieťová konfigurácia servera), následne túto VM je potrebné vypnúť a vo vypnutom stave rozbaľiť a prekopírovať odložené obrazy diskov.

Všeobecným odporúčaním je opäť pri výpadku VM a strate dát kontaktovať systémového administrátora, ktorý po vyhodnotení stavu zvolí vhodnú stratégiu obnovy dát.

Systémový administrátor by mal ovládať správu Linux prostredí, poznať KVM a poznať prostredie Oracle Database Appliance.

Štandardné postupy pre backup a restore APP VM sú zdokumentované v dokumente myhelp.oracle.com - "Backup of KVM guests on ODA 19.9 BM and later (Doc ID 2779329.1)".

Postup zahŕňajúci vyššie uvedené technikálie, použitý v UDZS pre backup VM (s možnosťou restore) predstavuje použitie utility "kvmb", zdokumentované v myhelp.oracle.com - "kvmb - Tool to backup/restore KVM domains (Doc ID 2688239.1)".

Switchover (produkčné prostredie)

V prípade neplánovaného výpadku, ktorého príčina znemožňuje reštart služieb Integrovačnej platformy na primárnom HW uzli (integracia01), alebo jeho dlhšie-trvajúcej plánovanej odstávky, je potrebné zabezpečiť dostupnosť služieb Integrovačnej platformy ich migráciou na sekundárny HW uzol (integracia02).

Topológiu produkčného prostredia, ktorá je východiskom pre migráciu služieb, zachytáva nasledovný obrázok.

Informácia o topológii vyňatá

Nevyhnutným predpokladom pre úspešnú migráciu služieb Integrovačnej platformy je funkčné riešenie pre:

- replikáciu dát DB na druhý záložný HW uzol, ktorá je zabezpečená technológiou Oracle Active Data Guard, a
- replikáciu súborového systému, ktorá je riešená prostredníctvom „rsync“ replikácie na úrovni virtualizovaných uzlov:
 - a1p01 → a1pdr01
 - a1p02 → a1pdr02

V ďalšom je popísaný postup manuálnej migrácie služieb pri nedostupnosti primárneho HW uzla:

1. Pozastavenie vývojového a testovacieho prostredia na sekundárnom uzli je potrebné vzhľadom na obmedzené HW zdroje a kapacitné požiadavky PROD prostredia.

Na druhom HW uzli (integracia02) pod „root“ používateľom:

```
# kontrola bežiacich VM
odacli list-vms
# zastavenie DEV prostredia
odacli stop-vm -n Informácia vyňatá
# zastavenie TEST prostredia
odacli stop-vm -n Informácia vyňatá
odacli stop-vm -n Informácia vyňatá
```

2. Prehlásenie stand-by za primárnu DB a štart DB na sekundárnom HW.
3. Zodvihnutie virtuálnych IP adries.

Na prvom uzli PROD DR klastra (*Informácia vyňatá*) pod „root“ používateľom:

```
ip add show dev eth0
nmcli con mod eth0 +ipv4.address Informácia vyňatá
nmcli con down eth0 && nmcli con up eth0
ip add show dev eth0
```

Na druhom uzli PROD DR klastra (*Informácia vyňatá*) pod „root“ používateľom:

```
ip add show dev eth0
nmcli con mod eth0 +ipv4.address Informácia vyňatá
nmcli con down eth0 && nmcli con up eth0
ip add show dev eth0
```

4. Štart NM komponentov.

Na oboch uzloch PROD DR klastra (*Informácia vyňatá*) pod „root“ používateľom:

```
systemctl start soap_domain_nodemanager
systemctl start osbp_domain_nodemanager
```

5. Štart aplikačných serverov na sekundárnom HW uzli.

Na jednom z uzlov PROD DR klastra (a1pdr01 alebo a1pdr02) pod „oracle“ používateľom:

```
# štart SOA domény
/oracle/scripts/soap_domain/startAdmin.sh
/oracle/scripts/soap_domain/startCluster.sh soa_cluster
# štart OSB domény
/oracle/scripts/osbp_domain/startAdmin.sh
/oracle/scripts/osbp_domain/startCluster.sh osb_cluster
/oracle/scripts/osbp_domain/startCluster.sh jms_cluster
```

6. Preverenie úspešnosti štartu všetkých serverov cez administračnú konzolu WL domény. Všetky servre by mali byť v stave RUNNING.

OSB doména: [http:// *Informácia vyňatá*/console/](http://<i>Informácia vyňatá</i>/console/)

SOA doména: [http:// *Informácia vyňatá*/console/](http://<i>Informácia vyňatá</i>/console/)

4. BEZPEČNOSŤ

SSL/TLS certifikáty

Integračná platforma používa serverové certifikáty dvoch skupín:

1) Certifikáty vydané pre služby

Všetky služby vystavené pre interných ako aj externých konzumentov (v kontexte UDZS) sú zabezpečené na úrovni transportného protokolu s použitím TLSv1.2. Certifikáty pre takúto komunikáciu sú vystavené a podpísané komerčnou dôveryhodnou CA:

C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig R2I2 Certification Service

Aktuálne sú to certifikáty vystavené na mená:

C=SK, L=Bratislava, O=Urad pre dohľad nad zdravotnou starostlivosťou, CN=*Informácia vyňatá*

C=SK, L=Bratislava, O=Urad pre dohľad nad zdravotnou starostlivosťou, CN=*Informácia vyňatá*

C=SK, L=Bratislava, O=Urad pre dohľad nad zdravotnou starostlivosťou, CN=*Informácia vyňatá*

Certifikáty vydané pre služby sú vystavené na úrovni predradeného HTTP servra, cez ktorý je zabezpečená komunikácia (na transportnej vrstve) od konzumentov voči službám Integračnej platformy. HTTP server terminuje SSL spojenie.

2) Certifikáty na interné použitie

Interná komunikácia v rámci komponentov riešenia Integračnej platformy je taktiež zabezpečená na úrovni transportného protokolu. Na podpísanie certifikátov pre internú komunikáciu je použitá interná CA spravovaná administrátorom Integračnej platformy:

CN=IP Internal CA

Privátny kľúč, ako aj self-signed certifikát internej CA je uložený v zabezpečenom repozitári (PKCS#12):

Informácia vyňatá

Certifikáty pre interné použitie podpísané internou CA sú uložené v zabezpečených repozitároch (WLS keystore, truststore) a sú využívané výlučne na internú komunikáciu.

Oba typy certifikátov sú uložené a spravované na servroch Integračnej platformy v adresároch:

Informácia vyňatá

Sledovanie expirácie SSL certifikátov

Nakoľko v UDZS neexistuje PKI infraštruktúra, ktorá by automaticky sledovala blížiacu sa expiráciu vydaných certifikátov, je potrebné zabezpečiť pravidelnú manuálnu kontrolu ich platnosti.

Certifikáty určené na interné použitie je potrebné najprv vyexportovať z keystore:

```
openssl pkcs12 \  
-in <cesta ku PKCS#12 keystore> \  
-out <cesta a názov výstupného súboru s certifikátom> \  
-passin pass:<heslo ku keystore> \  
-nokeys -clcerts
```

Všetky keystore (udržiavané vo formáte JKS a PKCS#12) sú uložené v adresári podľa menných konvencií:

```
/oracle/config/security/<meno servra>/<meno servra>-keystore.jks  
/oracle/config/security/<meno servra>/<meno servra>-keystore.p12
```

Napr. pre TEST prostredie (1. uzol) je keystore:

```
/oracle/config/security/Informácia vyňatá-keystore.jks  
/oracle/config/security/Informácia vyňatá-keystore.p12
```

Kontrola ukončenia platnosti certifikátu, napr. do 30 dní (2592000 sekúnd):

```
openssl x509 \  
-in <cesta a názov súboru s certifikátom> \  
-checkend 2592000
```

Príklad použitia príkazu pre komerčný certifikát na TEST prostredí:

```
openssl x509 \  
-in /oracle/config/security/Informácia vyňatá \  
-checkend 2592000
```

V prípade, ak certifikát neexpiruje v rámci uvedeného časového intervalu (do 30 dní), príkaz zobrazí túto hlášku, čo značí, že certifikát nie je potrebné aktualizovať:

```
Certificate will not expire
```

V prípade blížiacej sa expirácie certifikátov je potrebné včasne zabezpečiť ich aktualizáciu.

Aktualizácia SSL certifikátov

Aktualizácia SSL certifikátu pozostáva z týchto krokov.

Generovanie CSR

Na vygenerovanie CSR je potrebný privátny kľúč prislúchajúci danému servru. Je uložený v zabezpečenom úložisku (PKCS#12):

```
/oracle/config/security/<meno servra>/<meno servra>-key.p12
```

Generovanie CSR:

```
openssl req -new -sha256 \  
-passin pass:<heslo k privátnemu kľúču> \  

```

```
-key <súbor s privátnym kľúčom> \  
-out <názov CSR súboru> \  
-subj "<DN meno servra>"
```

Vystavenie nového certifikátu a jeho podpísanie CA

Vygenerovaný CSR je potrebné zaslať administrátorovi CA, ktorý na jeho základe vygeneruje a podpíše požadovaný certifikát.

V prípade potreby vystavenia certifikátu internou CA:

```
openssl x509 -req -days 3650 \  
-passin pass:<heslo k privátnemu kľúču CA> \  
-in <názov CSR súboru> \  
-CA <súbor s certifikátom CA> \  
-CAkey <súbor s privátnym kľúčom CA> \  
-CAcreateserial \  
-out <názov súboru s certifikátom servra>
```

Aktualizácia certifikátu na servroch

Certifikáty vydávané komerčnou CA (Disig) je potrebné aktualizovať v mieste ich uloženia, napr. pre TEST prostredie:

/oracle/config/security/*Informácia vyňatá*.pem

Certifikáty vydané internou CA (IP Internal CA) je potrebné aktualizovať v príslušných keystore a truststore repozitároch.

Správa klientských certifikátov

Klientské certifikáty sú certifikáty vydané a podpísané poskytovateľom služieb, ktorých je Integrovaná platforma konzumentom. Sledovanie ich platnosti je v zodpovednosti administrátora Integračnej platformy.

Špecifikácia použitých klientských certifikátov na autentifikáciu Integračnej platformy voči externým službám musí byť súčasťou dokumentácie k integračným komponentom (službám) na Integračnej platforme.

Riadenie prístupových práv

Administrátorské účty

Administrácia používateľských účtov v prostredí WLS aplikačného servra je popísaná v štandardnej Oracle dokumentácii:

<https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/wlach/taskhelp/security/ManageUsersAndGroups.html>

<https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/roles/secroles.html>

Aplikačné účty

Aplikačné účty sú spravované mimo Integračnej platformy. Sú vedené v MS AD infraštruktúre, ktorá je v zodpovednosti ÚDZS. Identitu týchto používateľov overuje Integračná Platforma v rámci autentifikácie voči MS AD. Aplikačné účty sú vedené v podstrome:

`OU=servisne_ucty,OU=UDZS Users,DC=ad,DC=udzs,DC=sk`

Integračná platforma autorizuje aplikačného používateľa na základe jeho príslušnosti k používateľskej skupine v podstrome:

`OU=SKUPINY,OU=UDZS Users,DC=ad,DC=udzs,DC=sk`

Špecifikácia, ktoré skupiny sú oprávnené na volanie ktorých služieb Integračnej platformy by malo byť súčasťou dokumentácie k integračným komponentom (službám).

Integrační účty

Integrační účty se používají pro autentizaci vnitřní komunikace typicky mezi OSB a SOA Suite.

Účty se udržují lokálně v SOA Suite. Administrace je možná přes WebLogic console SOA Suite. [Oracle dokumentace](#).

Zabezpečenie služieb

Informácia o bezpečnosti vyňatá

5. RETENCIA DÁT A ČISTENIE

Auditné záznamy v DB

Komponenty, na ktorých je postavená Integrovaná platforma (Oracle SOA Suite a OSB) ukladajú metadáta ako aj auditné záznamy v relačnej DB. Ich objem rastie priamoúmerne s počtom integračných komponentov a počtom prichádzajúcich požiadaviek. Preto je dôležité zvoliť nielen vhodnú úroveň auditu ale aj pravidlá na odmazávanie starších – nepotrebných záznamov. Výrazný nárast objemu dát v DB má priamy dopad na výkonnosť Integrovaného platformy (napr. pomalé odozvy používateľského rozhrania).

Bližšie informácie k tomu, ako správne nastaviť stratégiu a proces odmazávanie je popísaný v Oracle dokumentácii:

<https://docs.oracle.com/en/middleware/soa-suite/soa/12.2.1.4/administer/developing-database-growth-management-strategy.html>

Retencia auditných dát v DB je aktuálne nastavená 7 dní. Po tomto čase sa záznamy z DB automaticky odmazávajú.

Logovacie súbory

Integrovaná platforma využíva logovací framework aplikačného servra na logovanie svojich aktivít. Všetky logovacie súbory (s výnimkou HTTP servra) sú umiestnené v spoločnom adresári:

`/oracle/logs/<názov domény>`

Štandardne sú to tieto logy:

Informácia o logoch vyňatá

Logy majú nastavenú rotáciu (odmazávanie/prepisovanie starších logov) podľa retenčných pravidiel:

- Typ A:
 - počet súborov 10
 - rotovanie logov po 24 hodinách
- Typ B:
 - rotovanie po každom reštarte servra
- Typ C:
 - rotovanie po prekročení veľkosti súboru 10 MB s obmedzením sumárnej veľkosti všetkých súborov 100 MB

V prípade zmeny retenčných pravidiel je potrebné upraviť konfiguráciu pre jednotlivé logy prostredníctvom grafického používateľského rozhrania:

- WLS Control administračnej konzoly
<https://docs.oracle.com/en/middleware/fusion-middleware/weblogic-server/12.2.1.4/wlach/taskhelp/logging/ConfigureAndViewLogs.html>
- EM FMW Control konzoly
<https://docs.oracle.com/en/middleware/soa-suite/soa/12.2.1.4/administer/configuring-soa-infrastructure.html>

Je dobrou praxou monitorovať obsadenosť diskového priestoru na servroch pre prípad, že by logy neboli v dostatočnej frekvencii odmazávané alebo rotované. Táto situácia môže nastať pri zapnutom detailnom logovaní (DEBUG) na logoch bez obmedzenia celkovej veľkosti logov (typ A a B horevyššie).

6. DIAGNOSTIKA

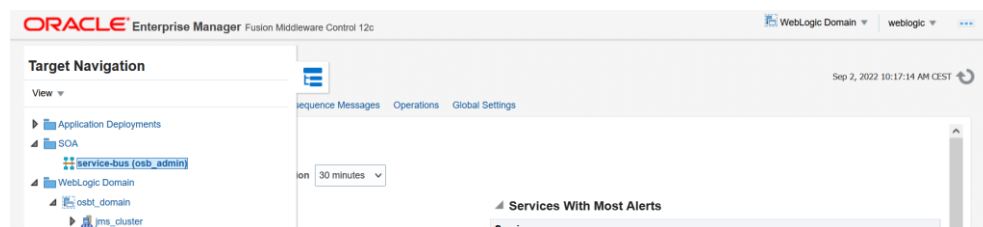
Centrální místo pro monitoring je Oracle Enterprise Manager (OEM): [https:// Informácia vyňatá/em/](https://Informácia vyňatá/em/). Zde je možné monitorovat a ovládat všechny systémy IP na jednom místě. Přes Target vybereme Middleware a pak vlevo jednotlivé systémy. K tomu ještě každý systém přidává své monitorovací konzoly.

Zoznam implementovaných služieb na OSB zobrazuje OEM nebo OSB konzola <https:// Informácia vyňatá/servicebus>

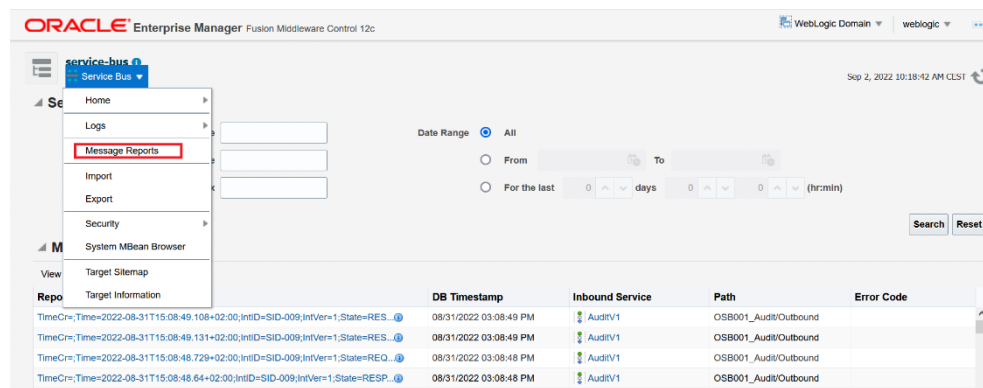
Zoznamu implementovaných procesov na SOA Suite zobrazuje OEM výše nebo EM konzola <https:// Informácia vyňatá/em>

Audit zpráv

Audit zpráv zobrazuje EM konzola OSB: <https:// Informácia vyňatá/em>



Obrázek 1 OSB monitoring

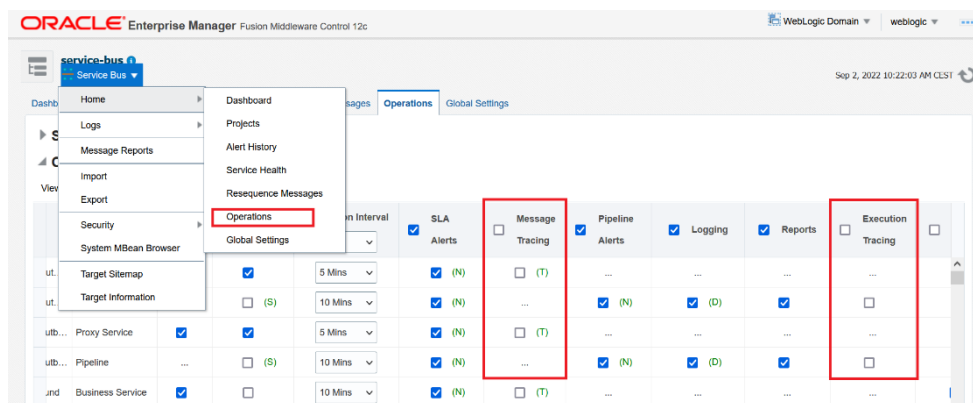


Obrázek 2 audit zpráv detail

Audit obsahuje metadata a obsah zprávy pro dotaz, odpověď a popř. pro poddotazy a pododpovědi u orchestrovaných služieb.

Tracing

OEM výše nebo EM konzola OSB: <https:// Informácia vyňatá/em> umožňuje zapnutí tzv. tracing u jedné nebo více služieb. Tracing umožňuje zapnout/vypnout detailní log pro danou službu v runtime. V diagnostic log souboru pak najdeme detailní záznam každého volání této služby.



Obrázek 3 zapnutí a vypnutí OSB tracing

Statistiky

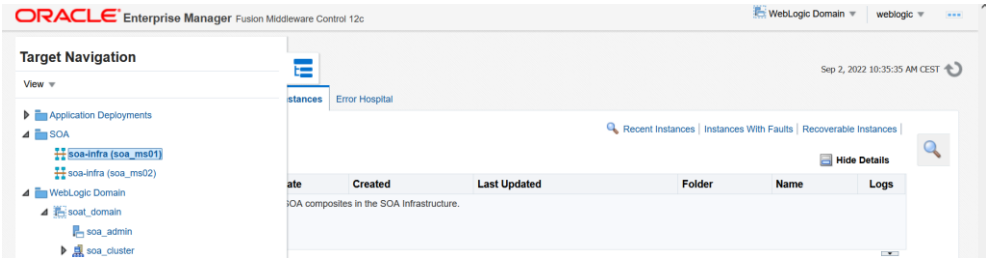
OEM zobrazuje statistiky služeb včetně počtu chyb, počtu volání, času odezvy atp.

Service	Aggr Interval(min.)	Avg. Resp. Time(msecs)	Messages	Errors	SLA Alerts	Pipeline Alerts
ust/Outbound	5	16	2966	2	0	---
rron/Outbound	5	37	104	1	0	---
ietconsoroadic... CSR0001/Outbound	5	2184	257	13	0	---
OznacenieZaujmo... RFO001/inbound	5	1784	151	0	0	---
OznacenieZaujmo... RFO001/inbound	5	1857	191	0	0	0
PoskytnutieRefere... RA001/inbound	5	10928	18	0	0	---
PoskytnutieRefere... RFO001/inbound	5	99	114	0	0	---
PoskytnutieRefere... RFO001/inbound	5	168	160	0	0	0

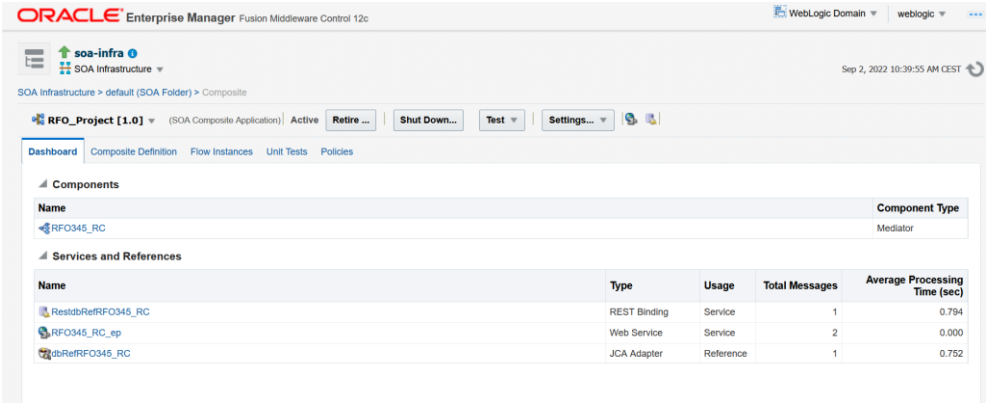
Obrázek 4 OSB statistiky

SOA Suite audit

EM konzola SOA Suite: <https:// Informácia vyňatá/em> zobrazuje detailní audit SOA Suite procesů.



Obrázek 5 SOA Suite EM



Obrázek 6 SOA Suite audit

Logy

Aktivity IP se zaznamenávají do logu.

Umístění logu:

- OSB: /oracle/logs/<jméno domény>
- SOA Suite: /oracle/logs/<jméno domény>

Název souboru	Popis
<jméno serveru>_access.log	http access log. Obsahuje záznamy http komunikace do OSB nebo SOA Suite.
<jméno serveru>.out	obsahuje standard out
<jméno serveru>.err	obsahuje standard error
<jméno serveru>.log	obsahuje zprávy z nižších vrstev IP, typicky aplikační server WebLogic a jeho komponenty
<jméno serveru>-diagnostic.log	obsahuje zpráv z integračné platformy včetně např. OSB tracing

Tabulka 1 typy logu

7. DOHL'AD

Popis monitoringu z dokumentácie Oracle Service Bus (OSB):

<https://docs.oracle.com/en/middleware/soa-suite/service-bus/12.2.1.4/administer/monitoring-oracle-service-bus.html>

Popis monitoringu z dokumentácie Oracle SOA Suite:

<https://docs.oracle.com/en/middleware/soa-suite/soa/12.2.1.4/administer/monitoring-oracle-soa-infrastructure.html>

7.1 EM monitoring a manažment systém

Pre spoločný monitoring integračnej platformy používame Oracle Enterprise Manager 13.5 (= tzv. „OMS server“), aktualizovaný na verziu 13.5.0.6. Klientské komponenty (= tzv. „EMAgent“) zabezpečujúce zbieranie informácií, prevádzanie požadovaných operácií, teda – všeobecnú komunikáciu s hlavným serverom, sú inštalované a spustené vo všetkých virtuálnych serverov (spúšťajú sa automaticky pri štarte serverov, no ich beh sa dá spravovať prostredníctvom „emctl“ príkazov na jednotlivých serveroch). Je dôležité povedať, že beh tohto komponentu nie je pre celkový beh platformy nevyhnutný, no je veľmi odporúčaný (integruje do jedného celku, inak atomizovaný monitoring jednotlivých komponentov integračnej platformy).

Systém beží na servri *Informácia vyňatá*

Spúšťanie a zastavovanie systému sa realizuje vždy pod užívateľom oracle:

-za OMS server, skriptami /home/oracle/scripts (pre vypnutie:

stop_oms.sh, stop_db.sh, pre štart: start_db.sh, start_oms.sh)

-za jednotlivé EMAgent časti – pod užívateľom oracle, použitím „emctl“ príkazov (vypnutie: /u01/app/oracle/EMAgent/agent_inst/bin/emctl stop agent, zapnutie: /u01/app/oracle/EMAgent/agent_inst/bin/emctl start agent)