Status report infrastruttura

Guido Guizzunti, Stefano Bovina

Agenda

- Stato rispetto a plenaria precedente:
  - attività in corso e
  - attività in stallo
  - criticità
- Stato nuove applicazioni
- Deadline varie e attività/criticità connesse
- Prossimi upgrade ed attività

Legenda colori nella slide:

Attività non iniziata/tutto invariato

Attività parzialmente fatta/in risoluzione

Attività conclusa/problematica risolta

Attività conclusa alla scorsa plenaria

Attività “extra” 2022 (parziale)

1. Lavori per Seminari
2. Finalizzare cluster PostgreSQL
3. Consolidamento base infrastruttura K8s
4. Major upgrade Artifactory
5. Major upgrade Sonarqube LTS
6. Major upgrade Puppet (5 → 7)
7. Migrazione provisioning infrastructure su BC
8. Major upgrade PostgreSQL a 10 o superiore
9. Minor upgrade infrastruttura K8s
10. Major upgrade infrastruttura K8s
11. Finalizzazione proxy user + cambio password DB Oracle + bonifica grant (da fare a 4 mani) ---> **cruciale anche per attività relative a microservizi**
12. Messa in produzione delle applicazioni sysinfo su K8s
13. Applicazione seminari in produzione
14. Finiture aggiuntive infrastruttura K8s
15. Major upgrade vari Safety (**never ending task**)
16. Ampliamento pool indirizzi IP
17. Refresh certificati interni k8s
18. Espansione cluster K8s
19. Keycloak dedicato al sistema informativo + migrazione app
20. Major upgrade Rundeck + porting su BC
21. Upgrade a PHP 8 (manca safety)
22. Migrazione su BC di quanto rimasto su vecchia infra (DEV + varie)
23. Upgrade Jasperserver (?TBD?)
24. Dismissione hardware@CNAF (vecchia infrastruttura)
25. Upgrade vamweb (?TBD?)
26. Major upgrade Wazuh (?TBD?)
27. Major upgrade infrastruttura K8s
28. Analisi per soluzione alternativa a VPN (?TBD?)
29. Possibile porting SPID/CIE (?TBD?) **—> NO**
30. Wazuh GA (?TBD?)

Criticità (note e segnalate) - Parte 1

- Memory leak MySQL (ogni X giorni si satura la memoria, bug MySQL noto e non risolto)
- Molte query SQL (Oracle) durano secoli (grosso impatto sul DB)
- Slow query presenti anche in altre DB engine (es: MySQL), ma meno rilevanti
- Applicazioni che bloccano table/row per tanto tempo (OracleDB)
- Connection leak vari verso i database (OracleDB)
- Applicazioni che generano “cascade failures” (auto DOS)
- Applicazioni che non reggono a down/riallineamento db (OracleDB)
- Applicazioni con memory leak problematici

Criticità (note e segnalate) - Parte 2

- Stato “security” applicazioni legacy ampiamente migliorabile (vedi Sonarqube e report lato CI)
- Sistema di monitoraggio in EOL (farming@CNAF in avanscoperta)
- Infrastruttura di provisioning da aggiornare e migrare urgentemente
- Ancora servizi a LNF (?)
- Presenza di servizi a LNF (gestiti da noi e non) che richiedono accesso a DB@BC
- Avviati incontri periodici con Sviluppatori per pianificazione attività trasversali (c'è margine di miglioramento)

Criticità (note e segnalate) - Parte 3

- LibroFirma
  - stato patch sicurezza non conforme al capitolato (troppe poche release)
  - ogni tanto va in errore senza fornire feedback all'utente e senza errori particolari nei log
  - non prevede purge documenti + non verranno commissionate ulteriori modifiche al SW a causa di tempi e costi sproporzionati
- Stato security stipendiale: critico; lavori di security hardening e migrazione bloccati per cause di forza maggiore (in maniera indefinita?)
- Impianto EBS
  - Application: obsoleto e NON aggiornabile/mantenibile
  - Oracle DBs: versione obsoleta (per attività di upgrade/futuro vedi fine prossima presentazione)
- Sistema Presenze: obsoleto e NON aggiornabile/mantenibile
- "Ecosistema BI":
  - vari problemi da risolvere (es: pesantezza generazione risorse ETL su contabilità, jasperserver obsoleto, ecc.)
  - richiede una pensata per il futuro

Altre problematiche/task in stallo

1. Bonifica grant: in stallo per applicazioni legacy (es: presenze, godiva, alfred, ecc.)
2. Account personali sui DB:
   a. alcune persone hanno fatto richiesta di account e non hanno nemmeno fatto 1 accesso
   b. per sviluppo su EBS (form/report) non è fattibile usare proxy user (troppo vecchio)
   c. mysql: parzialmente fatta
   d. mongo (wf-engine): da sistemare
3. Bonifica password applicative: bloccato da punto 2
4. Reset automatico password presenze: non implementato
5. Riscrittura/riprogettazione applicazioni (vedi prossime slide): manca ancora pianificazione dettagliata

Recap deadline

Entro giugno 2024 (deadline) dobbiamo reinstallare tutti i sistemi Centos 7 (240 host) a RH8 (ad oggi 80 host):

- non è un problema per servizi “aggiornabili” e compatibili con il sistema operativo: li gestiamo in completa autonomia
- da aggiungere supporto nei rispettivi moduli Puppet ma la procedura di reinstall è completamente automatizzata (a parte la migrazione del dato)
- per i servizi scritti in casa da valutare cosa ha senso reinstallare e cosa verrà riprogettato/riscritto (**richiede pianificazione**)

Note e criticità:

- upgrade PHP 7.4 → 8.x (probabilmente 8.1): **entro novembre 2022 —> fatto: manca safety**
- upgrade PHP 5.x → 8.x (probabilmente 8.1): **vedi deadline per RH8 (vedi slide plenaria giugno 2020)**
- Adeguamento Java “legacy” basate su Vaadin e/o OpenJDK 8 (e simili): **vedi deadline per RH8 (*per pochi casi particolari, fine 2025)**
- Adeguamento Sistemi con OracleJDK 7/Tomcat 7: **deadline passata → aggiornare ASAP (presenze/jasperserver)**
- LibroFirma: **blackbox (la ditta non fornisce upgrade + futuro incerto)**
- Oracle —> **vedi deadline per RH8 —> non chiaro destino a causa di dipendenze**
- EBS —> **vedi deadline per RH8 —> non chiaro destino**
- Stipendiale —> **“dismissione” ad inizio 2023 ma non abbiamo ancora ricevuto comunicazioni “ufficiali” su dismissione ambienti**

Stato nuove applicazioni - part 1

SVC name	TEST	PROD	COVERAGE	PATCH	NOTE
appman	SI	SI	NON OK	NON OK	
booking	SI	NO	NON OK	OK	
consuntivi	SI	SI	OK	NON OK	
identity	SI	SI	NON OK	NON OK	
mail	SI	SI	NON OK	NON OK	
preventivi	SI	SI	OK	OK	
progetti	SI	SI	OK	OK	
storage	SI	SI	NON OK	NON OK	
titolidistudio	SI	NO	NON OK	NON OK	**da capire destino progetto
inventario	SI	SI	NON OK	NON OK	Da dismettere e/o adeguare e portare su k8s

Stato nuove applicazioni - part 2

SVC name	TEST	PROD	COVERAGE	PATCH	NOTE
fondipersonale	SI	SI	OK	OK	
concorsi	SI	SI	OK	OK	
ssasdl	SI	NO	OK	OK	in test ma ancora non finalizzato/validato
ratp	SI	NO	OK	OK	appena messo in test, ancora da validare

Note varie

- Stato con coverage “NON OK”:
  - messa regola, più di un anno fa, per evitare blocco lato CI (solo warning) e per permettere adeguamento
  - entro marzo 2023* verrà tolta la regola ed i progetti non conformi verranno bloccati
- Stato patch indicato come “OK”
  - non ci sono vulnerabilità alte/critiche ma potenziali altri livelli
  - 172 vulnerabilità attive <= medium —> controllare stato applicazioni su dtrack (dipendenze vulnerabili, anche medium/low)
- Altre analisi (vedi sonarqube) spesso ignorate:
  - segnalano bug ed aiutano a prevenire problemi (di sicurezza e non)
  - nel corso del prossimo anno, avere uno stato “dignitoso” su sonarqube sarà obbligatorio e bloccante lato CI
- Progetti (es.: titolidistudio, identity, mail, ecc.) con destino incerto, oggi su un cluster NON della DSI (AAI) che devono essere dismessi e/o migrati (attività concordata da tempo, ma nessun feedback/piano a riguardo noto)

Prossimi upgrade ed attività

Dicembre

- Upgrade cluster k8s 1.22 → 1.23
- Finalizzare progetti SW con modifiche in corso: poi se ne riparla a nuovo anno
  - es: comunicazione via sftp con zucchetti (validazione conf)
  - app su k8s, da terminare ASAP (vedi upgrade k8s):
    - booking?
    - ratp?
    - portale unico v2?
- Finire verifiche su Keycloak dev + rispettivi adeguamenti su progetti SW (a 4 mani con devs)
- Setup Keycloak in test e prod
- Upgrade Keycloak >= 20
- Security scan e follow up security
- Preparazione migrazione a nuovo setup Keycloak

Gennaio-Febbraio

- Produzione progetti SW vari (es: ssasdl)
- Inizio spostamento applicazioni su keycloak DSI
- Inizio lavori Jasperserver (anche prima se avanza tempo) + analisi authZ/authN
- Preparazione migrazione/installazione safety php 8.x/EL8 + major upgrade
- Upgrade cluster k8s 1.23 → 1.24
- Formazione nuovo personale

Marzo-Aprile

- Security upgrade massivo
- Mongodb: EL8 + major upgrade (entro marzo)
- Mysql: EL8 + major upgrade (entro Aprile)
- Upgrade Kafka
- Upgrade ELK
- Upgrade Vam+ (se arriva persona nuova)
- Finalizzazione setup base Jasperserver + inizio lavori porting report su Jasperserver(*)

Argomenti di discussione per oggi

- Dato che le applicazioni salvano/salveranno i **documenti** non su alfresco (o altri sistemi proprietari difficilmente sfruttabili) ma sempre su altri sistemi (es: microservizi di storage -> s3), come intendiamo affrontare i temi quale conservazione, gestione metadati, ecc.?
- Quale sarà il destino delle **EBS**?
- Quale sarà il destino del Sistema delle **Presenze**?
- Riusciamo a mantenere con costanza almeno i **progetti nuovi**?
- Come migliorare il coordinamento (sviluppo software, tempo del personale, ecc.) dei **progetti “terzi**” (es.: booking, ssasdl, safety, ecc.)?

Altri argomenti da affrontare a breve

- Quale sarà il destino del **LibroFirma**? Come gestiamo le applicazioni che già si stanno interfacciando ad esso? Continuiamo a collegarci applicazioni che poi andranno riadeguate?
- Abbiamo una roadmap/pianificazione per adeguamento di tutto quello che è **php5/java legacy** che deve essere riscritto/adeguato (es.: migrazione da oracle, upgrade impianto, risoluzione problemi esistenti, ecc.)?
- Quale sarà il destino di **Siper/Cezanne/OneService** e risorse collegate (db, cedolino, cu, ecc.)