Status report infrastruttura

Guido Guizzunti, Stefano Bovina

Agenda

- Stato rispetto a plenaria precedente:
  - attività in corso
  - attività in stallo
  - criticità
- Stato dell’arte dei nuovi servizi
- Deadline varie e attività/criticità annesse
- Prossimi upgrade ed attività
- Varie
- Altre comunicazioni

Legenda colori nella slide:

Attività non iniziata/tutto invariato

Attività parzialmente fatta/in risoluzione

Attività conclusa/problematica risolta

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 **(NEW)**
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. Rifiniture aggiuntive infrastruttura K8s
15. Major upgrade vari Safety
16. Ampliamento pool indirizzi IP **(NEW)**
17. Refresh certificati interni k8s **(NEW)**
18. Espansione cluster K8s **(NEW)**
19. Keycloak dedicato al sistema informativo + migrazione app
20. Major upgrade Rundeck + porting su BC **(NEW)**
21. Upgrade a PHP 8 **(NEW)**
22. Migrazione su BC di quanto rimasto su vecchia infra (dev env) ---> serve upgrade HW su BC
23. Upgrade Jasperserver (?TBD?)
24. Dismissione hardware@CNAF (vecchia infrastruttura)
25. Upgrade vamweb **(NEW)**
26. Major upgrade Wazuh **(NEW)**
27. Major upgrade infrastruttura K8s
28. Analisi per soluzione alternativa a VPN **(NEW)**
29. Possibile porting SPID/CIE **(NEW:** ?TBD?**)**
30. Wazuh GA

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 troppi 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)
- Librofirma 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: 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
    - richiede una pensata per il futuro:
        - iniziati primi ragionamenti a riguardo (molto teorici)
        - evoluzione verso una “piattaforma di analytics” (simile a quella dei log): attività a lungo termine ancora da schedulare (in primis è infrastruttura)
        - soluzione breve/medio periodo: tutta da studiare/implementare (da fare con tecnologie/tool già “in produzione” e/o con il minor utilizzo di risorse hardware aggiuntive)

Altre problematiche/task in stallo

1. Bonifica grant: in stallo per applicazioni legacy (es: presenze, godiva 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
   c. mysql: ancora da fare
   d. mongo (wf-engine): da sistemare
3. Bonifica password applicative: bloccato da punto 2
4. Reset automatico password presenze: non chiaro/non implementato
5. Riscrittura/riprogettazione applicazioni (vedi prossime slide): manca ancora pianificazione dettagliata

Stato dell’arte per i nuovi servizi e criticità

- L’utilizzo di nuovi framework e modalità di sviluppo è ormai consolidato
- L’adozione di database “moderni” ed utilizzati correttamente è ormai consolidato
- Per le nuove applicazioni i database di riferimento sono solo MongoDB ed eventualmente PostgreSQL e per i file Minio (S3): migrazione dato “storico” ancora da studiare
- L’utilizzo di servizi “legacy” (es: PHP) adeguati con API REST **deve** essere una soluzione **momentanea** per favorire la migrazione:
    - problemi preesistenti rimangono (problemi di manutenibilità, bug, mancanza di test ecc ecc)
    - vecchia infrastruttura con “limitazioni” e “problemi” annessi (gestione dei secret vecchio stile, gestione dei db vecchio stile, file su NFS, circuit breaking/retry policy inesistenti, ecc)
    - rischio di impatto anche sui nuovi servizi
    - sarebbe bene convergere su Springboot/Angular
- Valutare l’utilizzo dei nuovi “framework” e modalità di sviluppo prima di iniziare pesanti attività di upgrade (vedi prossime slide)
- E’ necessario consolidare al meglio quando fatto fino ad ora (vedi prossime slide)

Stato nuove applicazioni - part 1

SVC name	TEST	PROD	COVERAGE	PATCH	NOTE
appman	SI	SI	NON OK	OK	“zoppo” causa Keycloak AAI obsoleto
booking	SI	NO	NON OK	OK	
consuntivi	SI	SI	OK	OK	
identity	SI	SI	NON OK	OK	
mail	SI	SI	NON OK	OK	ancora non attivamente usato
preventivi	SI	SI	OK	OK	
progetti	SI	SI	OK	OK	
storage	SI	SI	NON OK	OK	ancora non attivamente usato
titolidistudio	SI	NO	NON OK	NON OK	
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	NO	OK	OK	
concorsi	NO	NO	OK	OK	
ssasdl	NO	NO	OK	OK	

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:

- upgrade PHP 7.4 → 8.x (probabilmente 8.1): **entro novembre 2022**
- upgrade PHP 5.x → 8.x (probabilmente 8.1): **vedi deadline per RH8**
- 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**
- 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. Nessun feedback ricevuto su ambiente Apex**
- Stipendiale —> **“dismissione” ad inizio anno ma non abbiamo ancora ricevuto comunicazioni “ufficiali” su dismissione ambienti**

Stato applicazioni PHP - 5.x

Da riscrivere in springboot/nodejs o adeguare per php 8 con **deadline per installazione RH8**:

- bandi
- circolari
- cofound
- conferences
- consulenze
- curriculum
- cvonline
- disposizioni
- eventi
- formazione
- gestassprev
- jobs
- portalephp **(difficilmente aggiornabile: framework in EOL da anni)**
- reportgodiva
- servizidac
- sussidi
- vamweb **(software fornito da ditta esterna)**
- isidownloader **(batch host)**

host condiviso - gruppo 1

host condiviso - gruppo 2

NOTA: se non evidenziato è su host dedicato

NOTA: valutare se fare upgrade di PHP su EL7 o passare anche a EL8

ATTENZIONE: vedi note su “servizi legacy” nella slide “stato dell’arte dei nuovi servizi” prima di procedere con upgrade

Stato applicazioni PHP - 7.x

Da riscrivere in springboot/nodejs o adeguare per php 8 con **deadline novembre 2022:**

- assegnazioni
- beneficiassistenziali
- cedolino **(stipendiale???)**
- cu **(stipendiale???)**
- dbprogetti **(in dismissione)**
- pubblicazioni
- seminari **(software fornito da ditta esterna)**
- timesheet
- safety **(software fornito da ditta esterna)**

host condiviso - gruppo 1

host condiviso - stipendiale only

NOTA: se non evidenziato è su host dedicato

NOTA: valutare se fare upgrade di PHP su EL7 o passare anche a EL8

ATTENZIONE: vedi note su “servizi legacy” nella slide “stato dell’arte dei nuovi servizi” prima di procedere con upgrade

Proposta per progetti PHP

1. Predisporre server “vuoto” con PHP 8.x e RH8 così da fare 2 upgrade in un colpo solo: **max inizio settembre 2022**
2. Mano a mano che le applicazioni sono pronte, vengono spostate su questi nuovi server: **vedi EOL nelle precedenti slide, in test ASAP**
3. Una volta spostati tutti i servizi (produzione compresa), i vecchi server PHP 5.x e 7.x vengono dismessi: **vedi EOL nelle precedenti slide**
4. Da questo punto in avanti, tutti i progetti devono essere tenuti aggiornati secondo gli EOL PHP

NOTA: Se il software è fornito da una ditta esterna, chiederemo ok a procedere

NOTA: Se possibile valuterei migrazione ad OIDC (dismissione shibboleth) per facilitare lo sviluppo locale senza macchina remota PHP

NOTA: Ovviamente sono esclusi quelli in dismissione ed in “riscrittura”

Stato applicazioni java “legacy” - Vaadin

Da riscrivere con **deadline per installazione RH8**:

- alfred
- assegniricerca
- associazioni
- contratti
- datipersonali
- determine
- gestioneamministrativa
- gestioneaziende
- organigramma
- portale
- postaac
- reclutamento

Stato applicazioni java “legacy” - Altro framework

Da riscrivere e/o adeguare pesantemente con **deadline per installazione RH8**:

- finengine
- rda
- wfengine

….

….

….

- godiva (possibili problemi futuri con JavaWS/altre limitazioni tecniche-tecnologiche)

Stato applicazioni java “legacy che di più non si può”

Utilizzo di OracleJDK 7 + Tomcat 7

- presenze —> ? (problema JavaWS)
- jasperserver —> da aggiornare e rendere setup “standard”

Prossimi upgrade ed attività

Intervento 1 (inizio circa 13 giugno, da terminare entro fine giugno):

- Aumento pool di indirizzi IP (attualmente sono finiti: upgrade da /24 a /23) —> richiede riconfigurazione di tutte le VM
- Security upgrade vari —> **rolling restart di tutto: prima volta "vera" su k8s prod**
- Espansione cluster k8s **—> in valutazione**
- **Keycloak** (se risolvono problemi su nuova versione)

Intervento 2 (inizio luglio):

- refresh certificati interni k8s: **mai provato prima**
- Altri porting AAI:
  - Per quanto riguarda SPID/CIE, al momento **non** è previsto porting a meno di adeguamenti
  - Gli altri servizi dipendono da noi/voi a causa degli adeguamenti necessari

Intervento 3 (luglio-agosto):

- reinstallazione massiva di tutto quello che c'è ancora su vecchia rete (non BC): **da terminare entro massimo fine agosto**
- inizio lavori per test secondo major upgrade k8s —> **da terminare massimo in ottobre**

Altro:

- ferie
- preparazione concorso ed affiancamento nuovo personale
- altri task non elencati (vedi slide precedenti)

Varie

Cosa ci aspettiamo nel periodo estivo:

- nessun nuovo servizio a parte quelli concordati a giugno
- nessuna nuova attività “extra”
- controlli a tappeto su applicazioni esistenti, es:
    - upgrade ad almeno Angular 12 (la 11 è in EOL da 11 May 2022)
    - check stato applicazioni su dtrack (dipendenze vulnerabili, **anche medium/low**)
    - check report su sonarqube: **a tendere diventerà bloccante**
    - controllo/fix coverage **(vedi prossima slide)**
    - finalizzare progetti ancora in test **(vedi prossima slide)**
- inizio controlli/verifiche/valutazioni su progetti PHP per upgrade a PHP 8.x
- definizione scaletta lavori settembre-dicembre (?) da discutere ad inizio settembre

Presentazione fatta in CCR “Microservices and software development infrastructure upgrade”: https://agenda.infn.it/event/30202/contributions/168472/

Backup slide: Altre comunicazioni

- Stiamo cercando/valutando soluzione alternativa al sistema VPN attuale da usare per l'accesso a tutti i servizi interni (le whitelist su base IP per accesso diretto dovranno essere rimosse)
- Utilizzo di infrastrutture cloud:
    - INFN (e non) per sviluppo/test e/o dispiegamento di servizi "interni" (es: database) —> NO
    - Servizi di terze parti SaaS su cloud pubbliche (es: librofirma): valutazione caso per caso
    - **NOTA: le decisioni e/o valutazioni su l'utilizzo di questo tipo infrastrutture sono in primis da parte del reparto infrastruttura**
- Su Gitlab verrà richiesto utilizzo di GPG commit sign: a breve girerà documentazione
- In fase di sperimentazione 2FA per accesso Gitlab
- Iniziata sperimentazione supporto Java 17 (per ora solo lato "infrastruttura": non prendete iniziative)
- Firewall PC personale vs. docker: avete letto quanto ho fatto circolare via email?
- Vogliamo veramente passare a gitlab EE?
    - lato CI/CD non cambierebbe molto, quasi nulla: possiamo però mettere più "controlli" e sblocchiamo cose utili per la gestione —> il costo è giustificato? (https://about.gitlab.com/pricing/self-managed/feature-comparison/)
    - costi e gestione da fronteggiare: deve essere sostenibile negli anni (non come Jira/ServiceDesk/Alfresco)
    - prima dobbiamo risolvere il problema VPN (non lo terrei aperto al mondo vista la frequenza di vulnerabilità)
    - causa tempistiche INFN si andrà a fine 2022/inizio 2023
    - non permette comunque interazioni avanzate con Jira se non paghiamo la ultimate e comunque non è detto che si riesca a fare tutto: ha veramente senso pagare 2 prodotti che si fanno concorrenza?