Status report infrastruttura

Guido Guizzunti, Stefano Bovina

Agenda

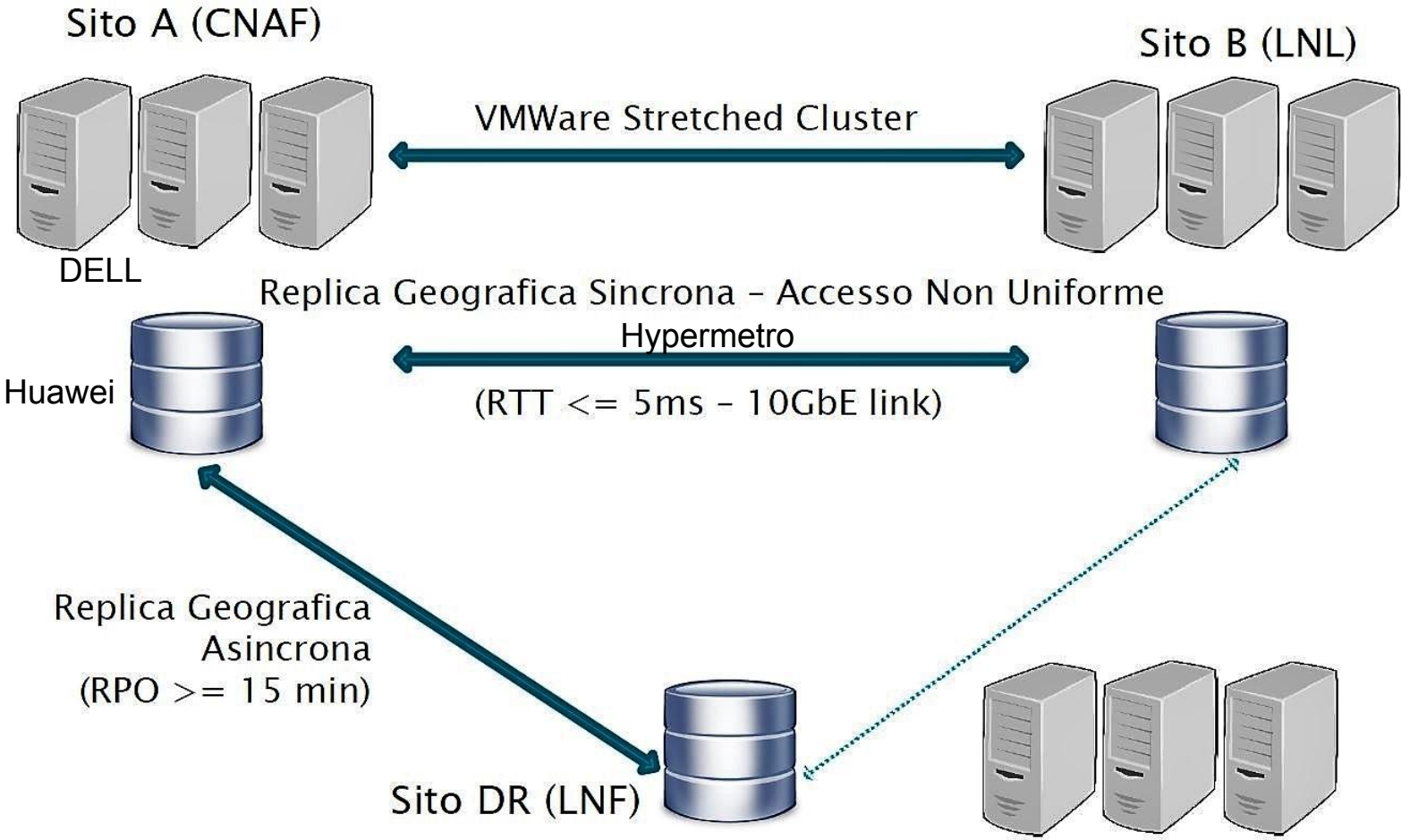
Parte 1

- Panoramica infrastruttura DSI
- Riflessioni su BC
- Stato DR
- Problemi infrastrutturali

Parte 2

- Recap organizzativi
- Attività 2021
- Panoramica nuovi servizi
- Attività 2022 (parziale)
- Report security e criticità

Panoramica infrastruttura DSI



Business continuity INFN (BC)

Richiesta per aumentare affidabilità e disponibilità di dati e applicazioni core

- In caso di manutenzione programmata di uno dei due siti
- In caso di down non programmato di uno dei due siti
- Con un RPO ~ 0
- Con un RTO -> 0

Soluzione implementata a livello HW, avendo in mente applicazioni

- monolitiche, che non hanno interazioni/dipendenze con altri servizi
- non progettate per l'HA a livello applicativo

Vantaggi e svantaggi della BC INFN

1. Razionalizzazione delle risorse
2. Azzerati tempi per acquisti e manutenzioni HW per personale SI
3. Aumento performance in lettura
4. Nessuna interruzione di servizio in caso di manutenzione programmata di uno dei due siti
5. Breve interruzione di servizio in caso di down non programmato di uno dei siti

1. Non progettata tenendo conto dei requirements tecnici del SI
   a. considerevole calo performance in scrittura
2. Svariati problemi di stabilità
   a. vengono meno punto 4 e 5
3. Aumento tempi di risoluzione problematiche e mancanza di comunicazione
4. Mancanza di autonomia gestionale
5. Latenze di rete non costanti e spesso oltre i 5ms
6. Aggiunge la complessità di un sistema distribuito senza nessun beneficio tangibile
7. Una reale BC non è realizzabile a livello HW
8. Maggiori implicazioni di sicurezza

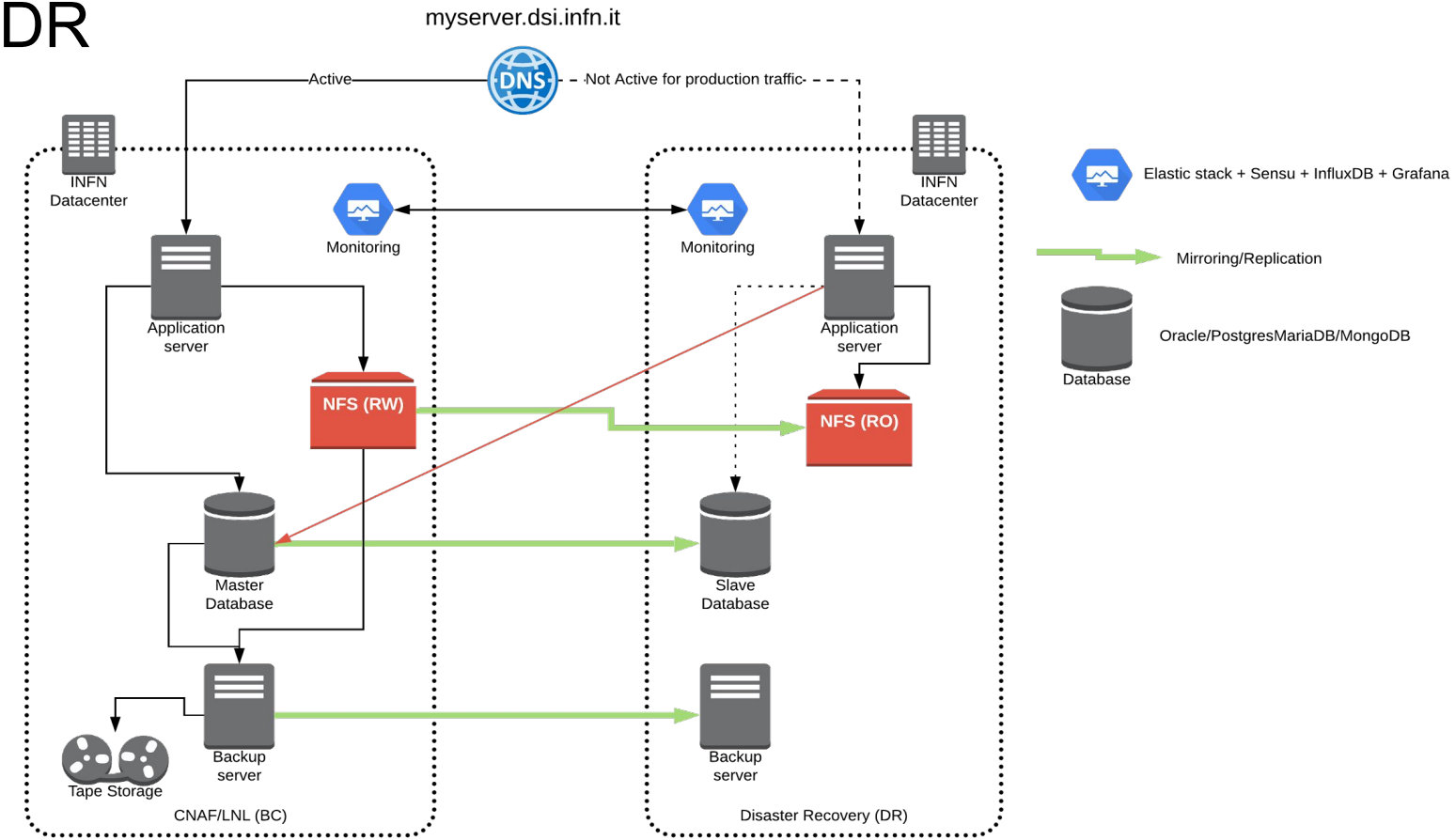
Migrazione dei servizi su BC

- Iniziata a fine 2019
- Complicata per:
  - elevato numero di servizi (~100)
  - adeguamento dei servizi legacy agli standard di sviluppo e sicurezza
  - dismissione AFS
  - mancanza di documentazione e di sistemi automatici di configurazione/provisioning (LNF)
  - dipendenze hard-coded tra le applicazioni
  - aggiornamenti vari (release DB, versione SO, ecc.)
  - cambio di indirizzamento IP (192.135.23.0/24 -> 131.154.56.0/24)
- **~50** i servizi già migrati, **~40** i servizi da migrare (alcuni verranno dismessi o saranno riscritti/accorpati)

Disaster recovery (DR)

- I servizi sono installati e configurati in maniera totalmente automatica (es.: mediante Foreman e Puppet)
- Le VM in fase di deployment vengono istanziate sia sul sito principale che su quello di DR
- A seconda del contesto e della criticità:
  - il backup viene eseguito ed inviato sul sito di DR una o più volte al giorno
  - il dato viene replicato tramite funzionalità "native" (es.: replica del database)
- Alcuni servizi (es.: monitoraggio e analisi dei log) sono locali al singolo sito (ed indipendenti dagli altri siti) e il dato viene aggregato a livello di dashboard
- In caso di disastro, viene attuata la procedura di disaster recovery (cambio record DNS, elezione DB a master, ecc.)

Schema DR



NOTA: schema non aggiornato con tutte le nuove componenti (vedi slide stefano), ma la logica rimane la stessa

Problematiche infrastrutturali aperte (1)

- Saturazione indirizzi IPv4
  - 246 usati, considerando lavori già preventivati
  - 131.154.56.0/**24** in esaurimento
  - richiesto ampliamento subnet: 131.154.56.0/**23**
    - seguirà una riconfigurazione generale
- Saturazione delle risorse HW
  - riscontrati problemi di memory spike per carenza di memoria (risolti dopo aumento di risorse)
  - risorse HW attuali: RAM=1.7TB, Disco totale=65TB
  - richiesto aumento risorse HW: RAM=2.2TB, Disco totale=65TB -> non prima dell'estate 2022
- Carenza di autonomia gestionale
  - impossibile definire policy adeguate a garantire gli standard di HA e performance
  - richiesta di un cluster riservato alle applicazioni SI (se non si trova soluzione al problema sopra)
    - necessario acquisto di blade dedicati -> non prima dell'estate 2022

Problematiche infrastrutturali aperte (2)

- Sistema di virtualizzazione vecchio: vSphere 6.5 (2016)
- Sistema VPN inadeguato
  - non è sotto la gestione di personale SI -> infattibile attivare/disattivare account in autonomia
  - manca mapping con LDAP/Godiva per gestione credenziali e permessi
  - manca corrispondenza tra utente/IP-utilizzato -> difficile risalire a chi si è collegato
  - manca possibilità di compartimentare la rete -> ditte esterne accedono a tutto
  - manca logging adeguato con possibilità di invio ai sistemi di analisi/conservazione dei log del SI
  - manca possibilità di delegare ad altri la gestione di singoli account/gruppi
  - non in HA -> prediligere soluzione software messa su BC (es. pfsense)
- Problematiche firewall
  - Manca autonomia nella gestione delle regole (ACL) -> maggiori tempi di intervento
  - Manca definizione di object group -> creazione/gestione policy complicata e calo performance
  - Next generation firewall Palo Alto: spento per problematiche di connettività
- Dipendenza dal gruppo net@CNAF per gestione entry DNS

Parte 2

Recap organizzativi

Dal 2019 la wiki sysinfo è disponibile qui

Nella wiki trovate anche tutte le informazioni sui tool che vedrete nelle prossime slide/presentazioni e indicazioni per lo sviluppo software.

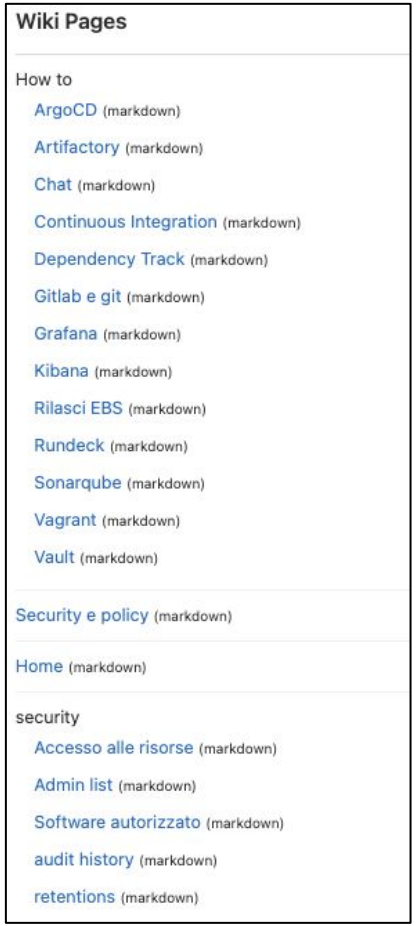
Per dubbi potete consultare anche la sezione F.A.Q qui.

In caso di problemi potete aprire una issue come indicato qui nella wiki.

Per vedere le issues aperte potete consultare questo link (le issues sono collegate ad ogni progetto software).

Invito tutti a:

1. pianificare le nuove attività per tempo (i task “infrastrutturali” vengono concordati per i prossimi 3 mesi e poi schedulati con sprint di 1 o 2 settimane); da questo sono escluse ovviamente le attività di manutenzione “ordinaria” e le emergenze
2. non progettare/implementare senza coinvolgere tutti gli attori
3. non porsi obiettivi/task/scadenze su attività che non sono al 100% di vostra competenza senza concordare nulla con gli altri interessati
4. non lavorare in maniera affrettata additando pretesti (es: “c’è fretta”, “ho questa attività come obiettivi entro l’anno”, ecc): se il lavoro fatto non risulta conforme agli standard verrà rigettato in attesa di fix (tenetene conto nel calcolo dei tempi)
5. quando viene fatta una richiesta da parte degli utenti, cercare di distinguere **reali** emergenze da capricci o attività differibili (vedi anche punti precedenti)



Attività “base” ordinarie

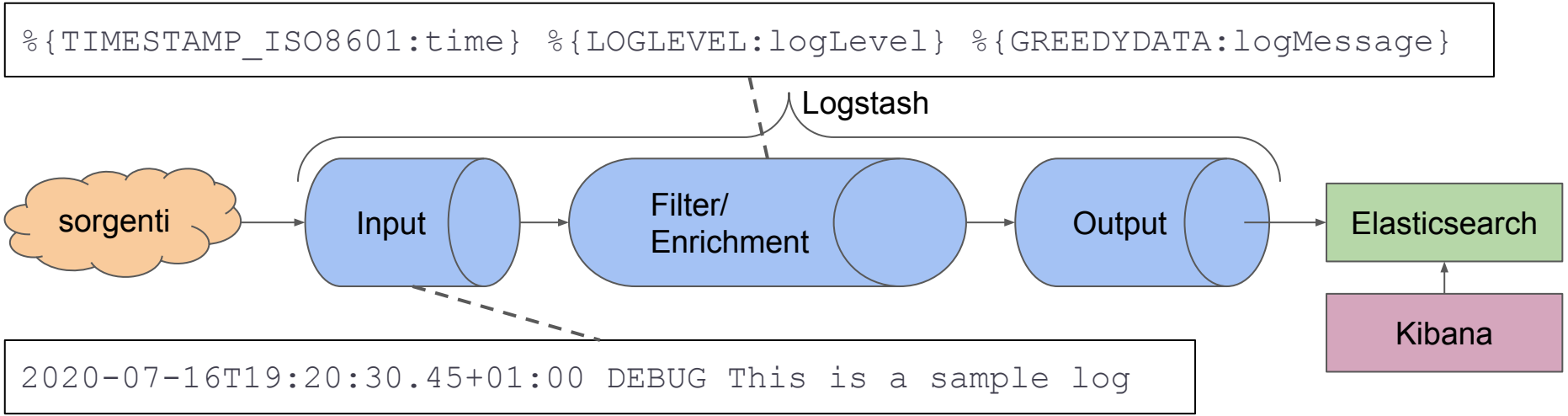
1. Migrazione su BC (fino a quando non avremo finito)
2. Nuove applicazioni sysinfo (standard)
3. Manutenzione ordinaria (minor upgrade, security upgrade, fix vari ecc)
4. Questioni inerenti la “security” e policy collegate
5. Risoluzione di problemi/supporto
6. Verifica sostenibilità/compliance e review dei progetti e soluzioni tecniche adottate (per quanto ci compete..*”a bridge between development and operations”*)

Attività “extra” 2021

1. Major upgrade artifactory + migrazione a versione Pro
2. Major upgrade PostgreSQL a 9.6 o superiore
3. Major upgrade MongoDB (4.2)
4. Major upgrade ELK stack (7.x) + revisione completa architettura cluster
5. Rivista completamente struttura dati su Elasticsearch e logiche di enrichment
6. Plugin Kibana enterprise: workspace personali
7. Upgrade PHP 7.2 a 7.4
8. Wazuh (ossec) in tech preview
9. Aggiunta di Kafka nell'infrastruttura analisi log
10. Major upgrade container registry
11. Supporto a sistema operativo RH8 e derivati (adeguamenti necessari)
12. Acquisto licenze RedHat
13. Aggiunto supporto lato CI per applicazioni NodeJS
14. Inventario (servizio fuori standard: Springboot + NodeJS)
15. Minio (S3)
16. Dependency track (dtrack)
17. Long term preservation dei log su S3
18. Major upgrade vari Safety
19. Password policy e review account EBS
20. Vault
21. Account personali e revisione grant su DB Oracle
22. Ecosistema K8s/Microservizi
23. Inizio setup cluster PostgreSQL
24. Inizio lavori per seminari

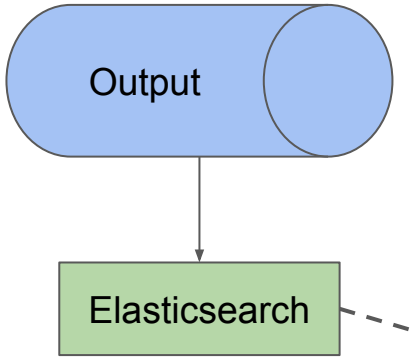
ELK (Elasticsearch - Logstash - Kibana)

- **Elasticsearch**: è il database
- **Kibana**: la dashboard collegata al database
- **Logstash**: “server-side data processing pipeline”



NOTA: è solo un esempio..per dettagli vedi wiki

ELK (Elasticsearch - Logstash - Kibana)

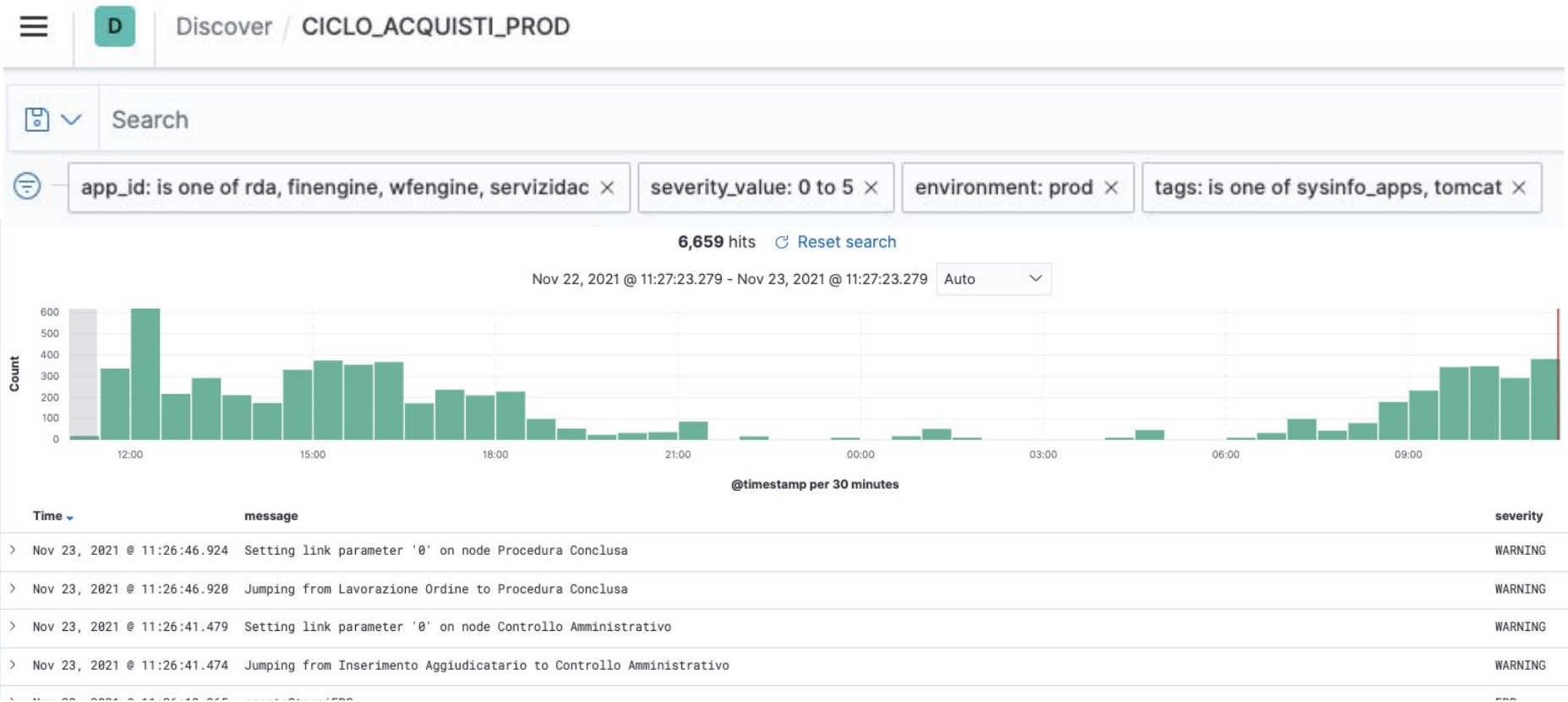


Esempio di dato memorizzato su Elasticsearch

```
{
  "time": [
    [
      "2020-07-16T19:20:30.45+01:00"
    ]
  ],
  "logLevel": [
    [
      "DEBUG"
    ]
  ],
  "logMessage": [
    [
      "This is a sample log"
    ]
  ]
}
```

Campi di ricerca su Kibana

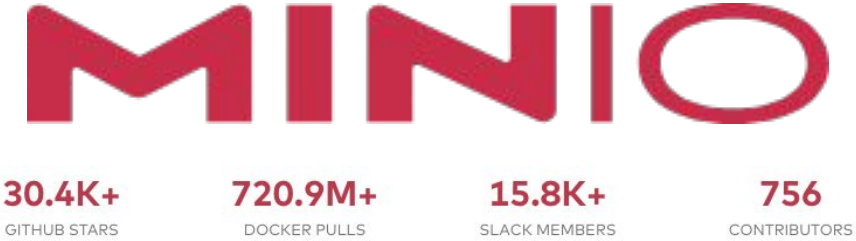
ELK (Elasticsearch - Logstash - Kibana)



Grafana

Dashboard di monitoraggio...circa 70 dashboard totali

Minio



Software-defined high performance object storage

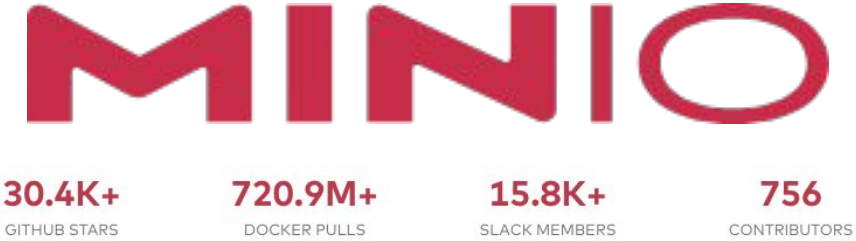
Features:

- Highly available and horizontally scalable
- API compatible with Amazon’s S3 (de-facto standard API for business applications to store unstructured data)
- Bucket Versioning
- Object Lock and Immutability - Write-Once Read-Many (WORM)
- Bucket Notifications (i.e. Kafka)
- Server-Side Bucket Replication (BC/DR)
- Object Lifecycle Management (Transition/Expiration)
- Encryption
- Ransomware protection

Perchè?

- ad oggi, qualunque software che necessita di storage per ospitare file è tipicamente compatibile esclusivamente con storage ad oggetti e sicuramente con le API S3, non Alfresco o filesystem
- facilità di utilizzo in locale
- le feature indicate sono necessarie per questioni tecniche, security e compliance

Minio



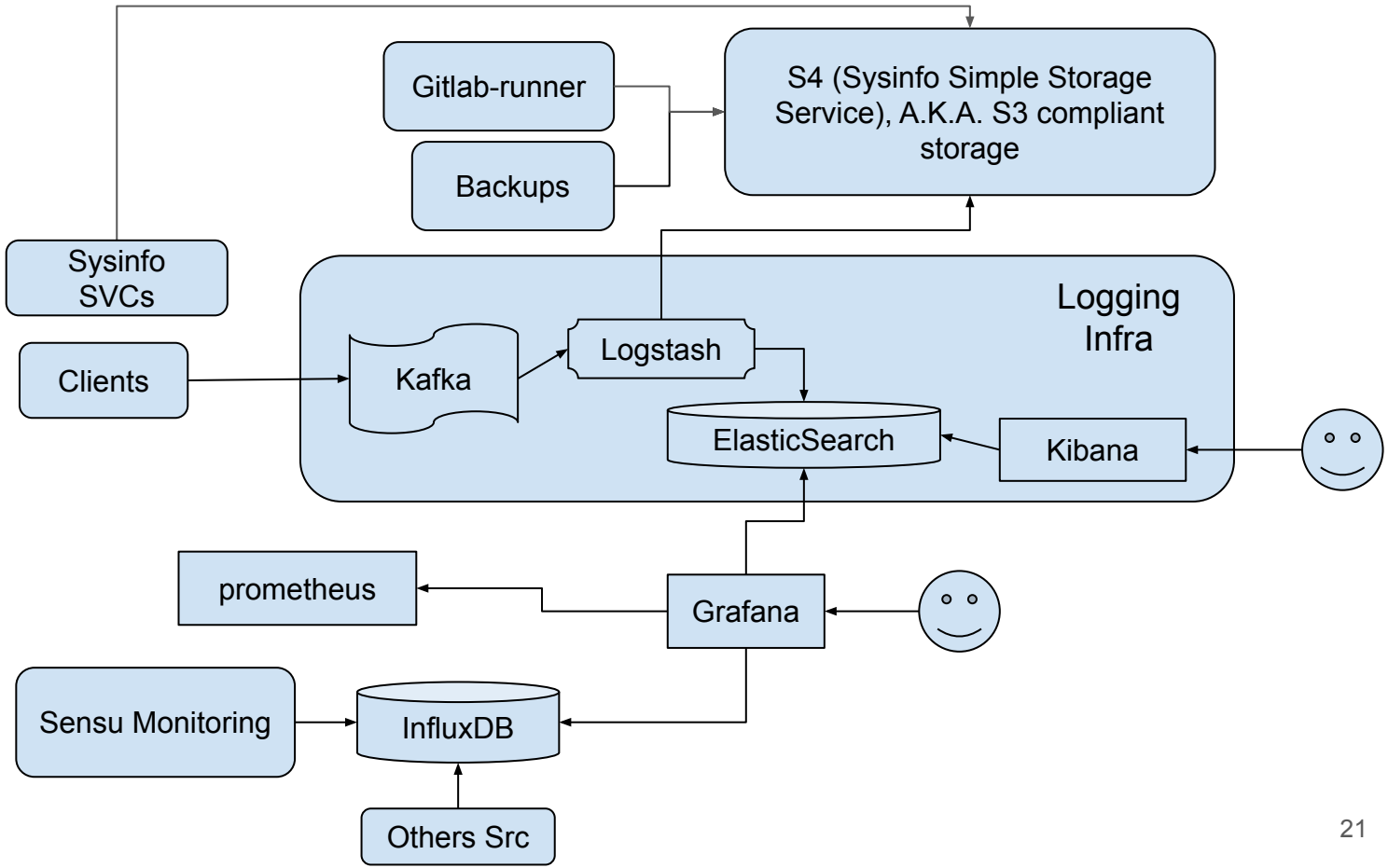
Casi d’uso:

- Backup
- Cache distribuita gitlab-runner
- Long term preservation (es: log)
- Ospitare file prodotti da applicazioni/servizi sysinfo

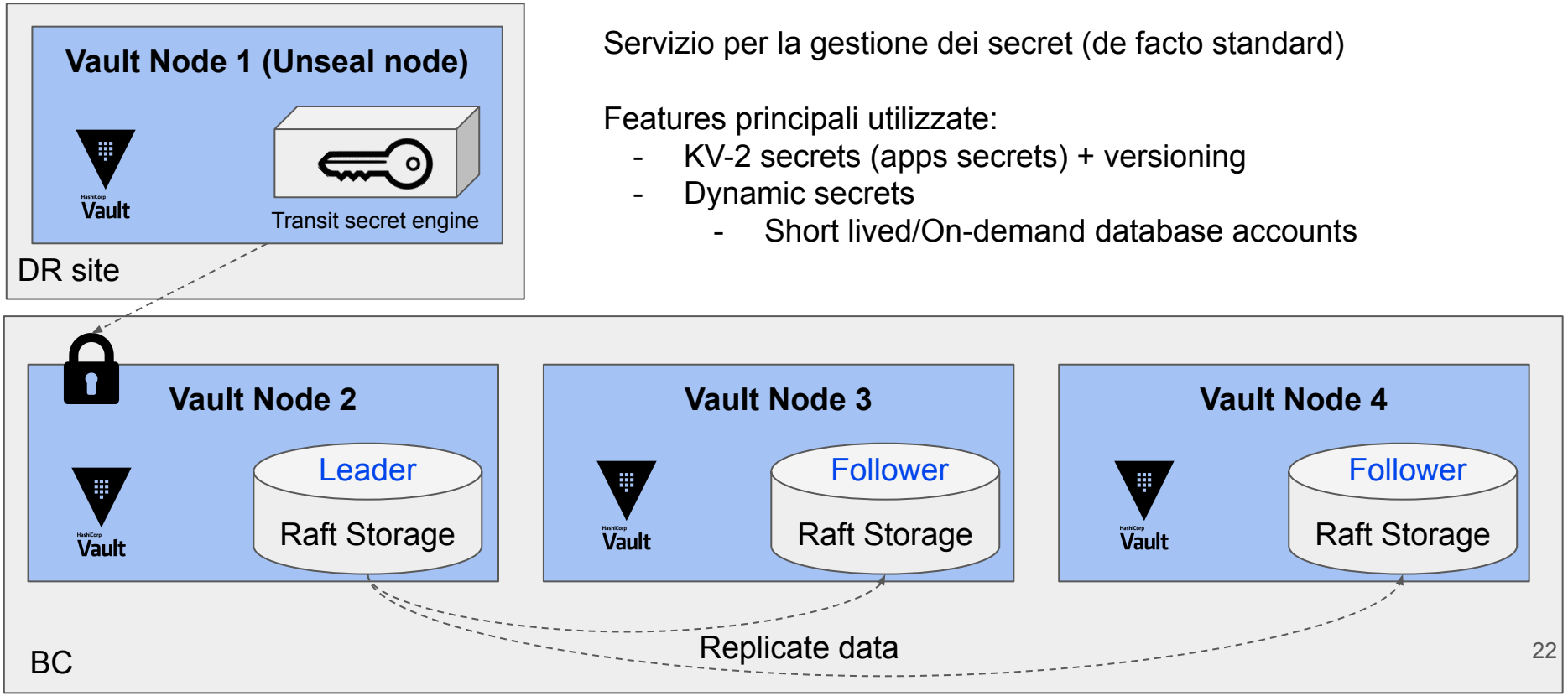
Abbiamo supporto a pagamento:

- Stesso prodotto rispetto alla versione community
- Supporto ottimo (per ora il migliore mai visto): 24/7/365
- SLA < 48h
- Panic button: 1 all’anno

Interazione delle varie componenti monitoraggio/logging/archiving



Vault



Servizio per la gestione dei secret (de facto standard)

Features principali utilizzate:

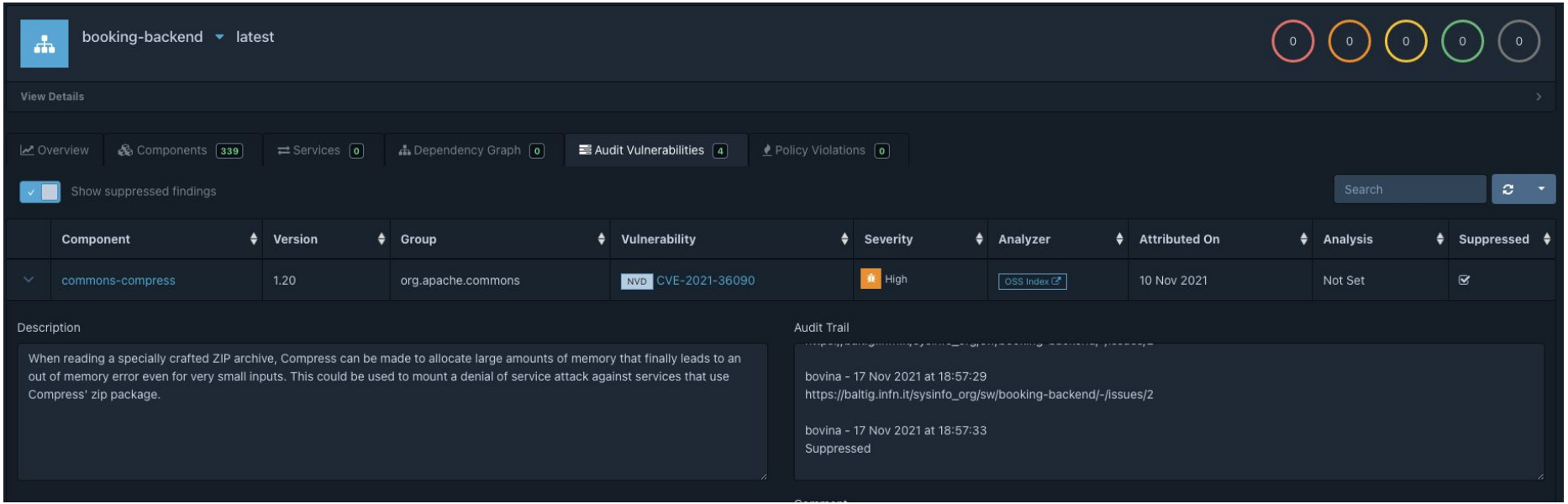
- KV-2 secrets (apps secrets) + versioning
- Dynamic secrets
  - Short lived/On-demand database accounts

Dependency track (dtrack)

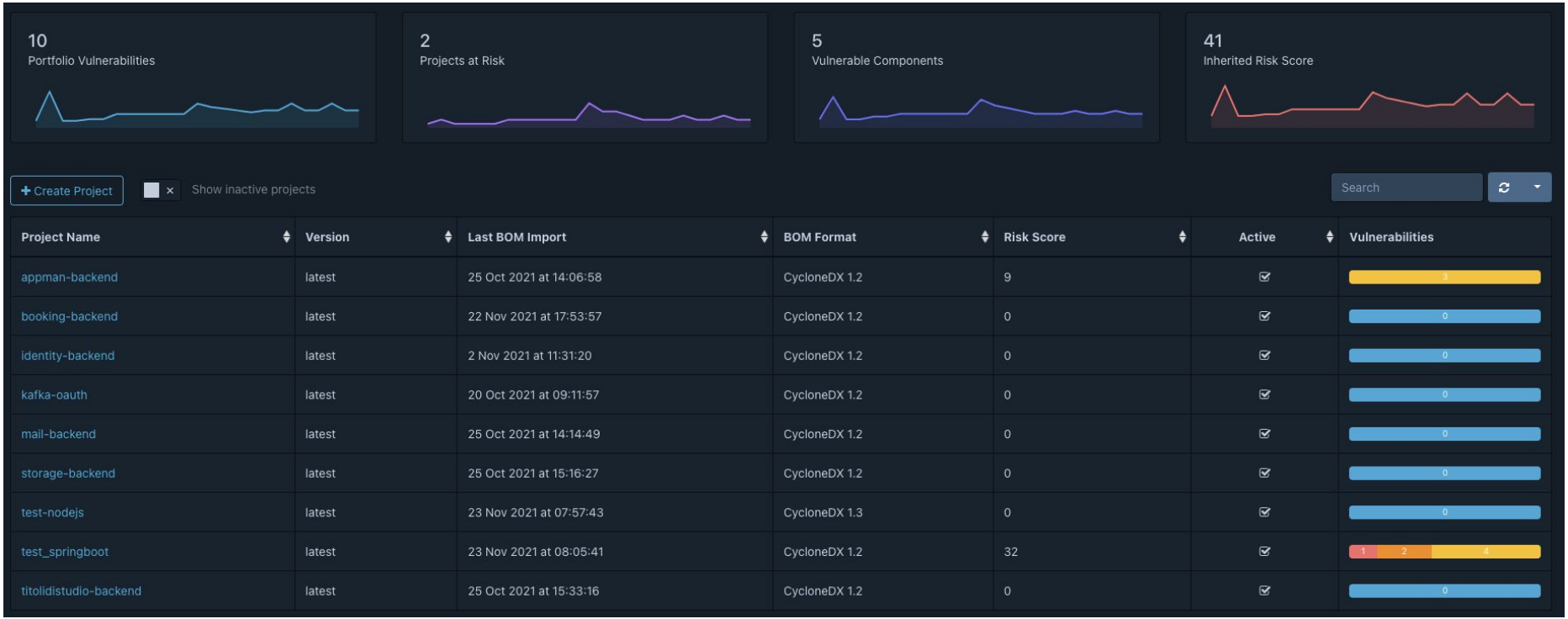
“An intelligent Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain.”

- Tool OWASP
- Sfrutta i Software Bill of Materials (SBOM) creati in fase di build per analizzare le dipendenze dei vari progetti software (anche a posteriori)
- Permette di identificare vulnerabilità (e non solo) su un progetto software (e non solo) a posteriori ---> caso d’uso: identificare vulnerabilità di un progetto software “fermo”
- Fornisce una panoramica delle licenze utilizzate
- Permette di definire policy e allarmi
- Permette analisi e gestione delle vulnerabilità (analisi, commenti, suppression ecc)

Dependency track (dtrack)



Dependency track (dtrack)



Project Name	Version	Last BOM Import	BOM Format	Risk Score	Active	Vulnerabilities
appman-backend	latest	25 Oct 2021 at 14:06:58	CycloneDX 1.2	9	☑	3
booking-backend	latest	22 Nov 2021 at 17:53:57	CycloneDX 1.2	0	☑	0
identity-backend	latest	2 Nov 2021 at 11:31:20	CycloneDX 1.2	0	☑	0
kafka-oauth	latest	20 Oct 2021 at 09:11:57	CycloneDX 1.2	0	☑	0
mail-backend	latest	25 Oct 2021 at 14:14:49	CycloneDX 1.2	0	☑	0
storage-backend	latest	25 Oct 2021 at 15:16:27	CycloneDX 1.2	0	☑	0
test-nodejs	latest	23 Nov 2021 at 07:57:43	CycloneDX 1.3	0	☑	0
test_springboot	latest	23 Nov 2021 at 08:05:41	CycloneDX 1.2	32	☑	1 2 4
titolidistudio-backend	latest	25 Oct 2021 at 15:33:16	CycloneDX 1.2	0	☑	0

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. Finalizzazione proxy user + cambio password DB Oracle + bonifica grant (da fare a 4 mani) ---> **cruciale anche per attività relative a microservizi**
11. Messa in produzione delle applicazioni sysinfo su K8s
12. Applicazione seminari in produzione
13. Major upgrade infrastruttura K8s
14. Rifiniture aggiuntive infrastruttura K8s
15. Major upgrade vari Safety
16. Upgrade Jasperserver (?TBD?)
17. Porting Keycloak (?TBD?)
18. Wazuh GA
19. Migrazione su BC di quanto rimasto su vecchia infra (dev env) ---> serve upgrade HW su BC
20. Dismissione hardware@CNAF (vecchia infrastruttura)

Note su attività

Le attività su PostgreSQL sono bloccanti per almeno altri 3 task descritti in precedenza

La migrazione/upgrade dell'infrastruttura di provisioning/Puppet è critica (task ormai rimandato di 1 anno per altre "attività più importanti")

Per la produzione delle nuove applicazioni, nonostante sia già possibile, è importante eseguire i task indicati con "Consolidamento base infrastruttura K8s"

Per i nuovi servizi che necessitano della nuova infrastruttura (vedi prossima presentazione) è stato chiesto un prospetto di quali potrebbero/dovrebbero essere pronti nei primi mesi dell'anno; il rispetto di queste previsioni dipenderà da:

- prerequisiti infrastrutturali (vedi sopra)
- rispetto delle policy/prassi (ed in generale dal modo di lavorare dei singoli) indicate in questa e nella prossima presentazione
- eventuali imprevisti/ritardi negli sviluppi
- piano ferie
- vedi altre considerazioni nella prossima presentazione

Status report security scan

Tutto ok a parte:

1. Kernel e annessi non aggiornati di recente (dovremmo fare down globale di tutto ogni mese): ultimo upgrade agosto (rischio accettato da Roberto)
2. Alcune criticità già note che vedrete nelle prossime slide

Criticità (note e segnalate) - Parte 1

Per la prima volta dal 2014 circa, il 13 ottobre 2021 la dashboard di monitoraggio è finalmente “verde” ma…

- 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
- 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
- Pianificazione attività “trasversali” da migliorare

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

Take-home messages

- Dobbiamo cercare di finalizzare il prima possibile il porting su BC del sistema di provisioning
- Dobbiamo riuscire a terminare il porting su BC delle applicazioni e a rimuovere le dipendenze esterne (vedi LNF)
- Dobbiamo dedicare più tempo a manutenzione/risoluzione di problemi frequenti del software
- Alcuni servizi critici andranno ripensati/riprogettati per obsolescenza tecnologica/inadeguatezza
- Per altri servizi critici va chiarito meglio il loro destino (vedi stipendiale, Librofirma)