Design e Sviluppo di un Sistema Distribuito Avanzato per Verifiche di Security Assurance

Alex Della Bruna

16 Luglio 2024

Relatore: Prof. Marco Anisetti
Correlatori: Dott. Nicola Bena, Dott. Filippo Berto

Contesto

I sistemi software hanno subito un cambiamento radicale

- sistemi distribuiti moderni altamente dinamici
- cloud-computing
- Machine Learning e cloud-edge

Necessità di verificare il comportamento ed il supporto continuo a requisiti non-funzionali $\Longrightarrow$ assurance e certificazione

Motivazioni

Questa rivoluzione ha impattato anche le tecniche di assurance stesse, richiedendo di definire nuovi approcci teorici ed implementazioni pratiche

Moon Cloud

- piattaforma cloud per l'assurance e la certificazione di sistemi
  - garanzia di compliance per sistemi e infrastrutture ICT
  - valutazione di assurance basata su raccolta di evidenze

Obiettivi

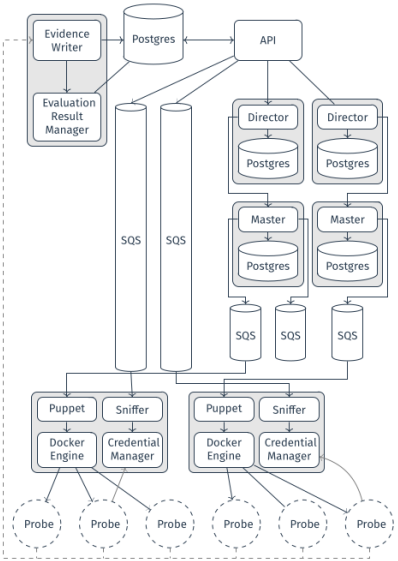
Ri-definire la piattaforma di assurance di Moon Cloud secondo le peculiarità dei sistemi distribuiti moderni

- realizzazione di un'architettura modulare facilmente installabile nelle modalità managed, hybrid, e on-premise
- architettura cloud-native
- garanzia di affidabilità, scalabilità, e replicabilità
- migliore gestione dei risultati

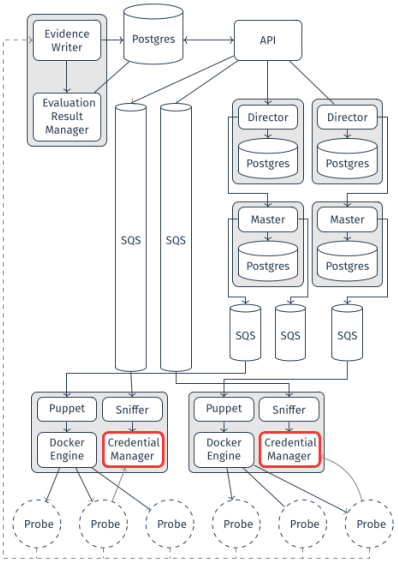
Migrazione

1. progettazione di un piano di migrazione con focus su
   - individuazione criticità
   - architettura multi-cluster
   - tecnologie cloud-native
2. implementazione
3. validazione

Migrazione: Architettura Originale

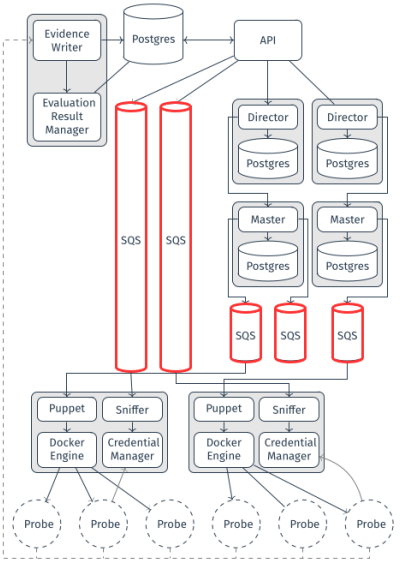


Migrazione: Criticità



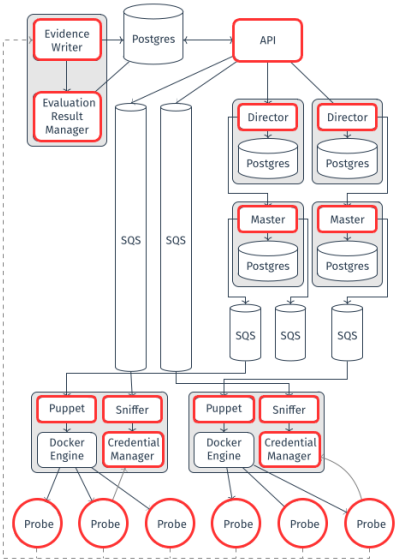
Gestione basica delle credenziali

Migrazione: Criticità



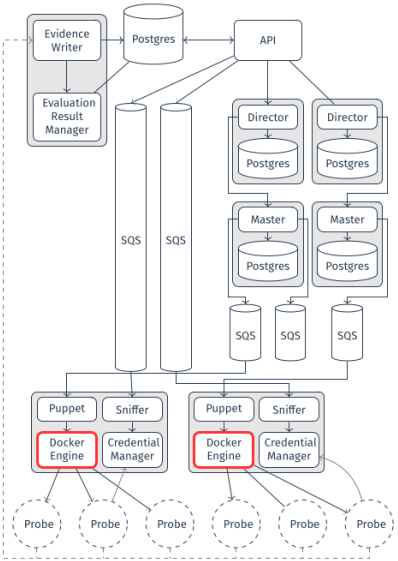
Dipendenza da un sistema pub/sub esterno

Migrazione: Criticità



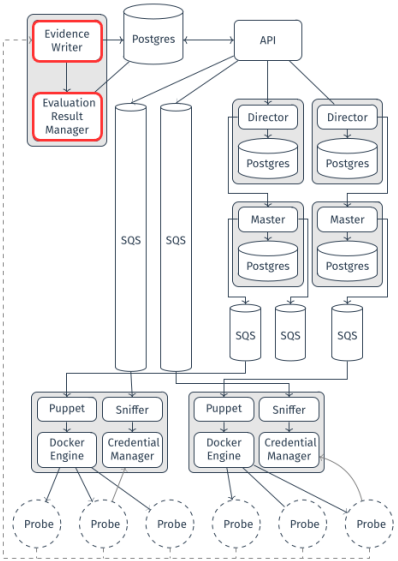
Eccessiva presenza di componenti custom

Migrazione: Criticità



Deployment in un sistema legacy

Migrazione: Criticità



Risultati non puntuali

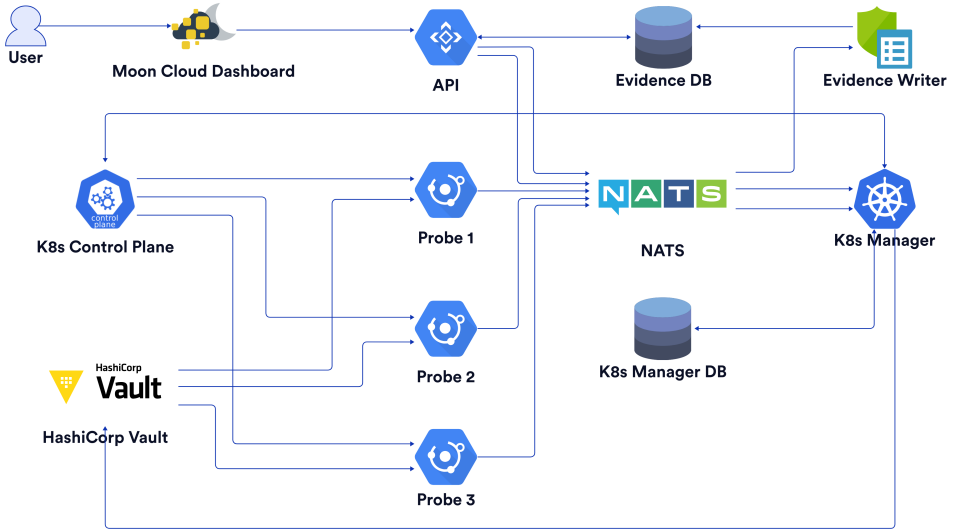
Migrazione: Progettazione

Progettazione di un'architettura multi-cluster

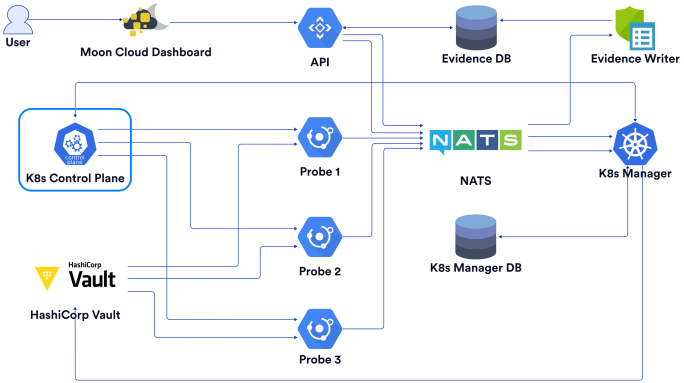
- supporto a diversi tipi di deployment $\Longrightarrow$ managed, hybrid, e on-premise
- risoluzione dei problemi legati alle federazioni
- scalabile, manutenibile, ed estendibile

$\Longrightarrow$ approccio basato su più cluster *Kubernetes* interconnessi tramite *NATS*

Nuova Architettura



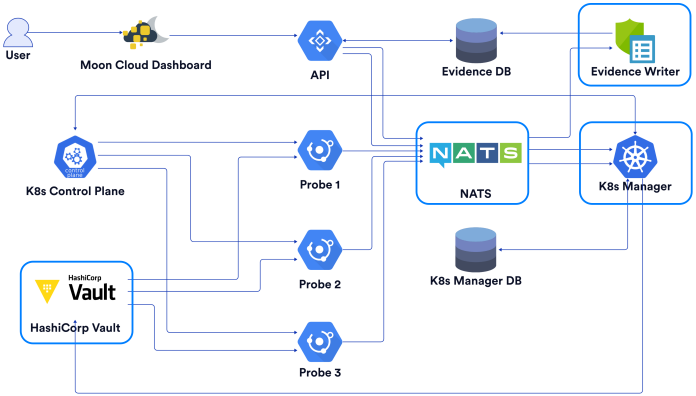
Nuova Architettura



Deployment basato su Kubernetes

- definizione delle varie entità *Kubernetes*
- aggiornamento delle configurazioni di deployment
- installazione e testing con più nodi
- interconnessione e testing multi-cluster

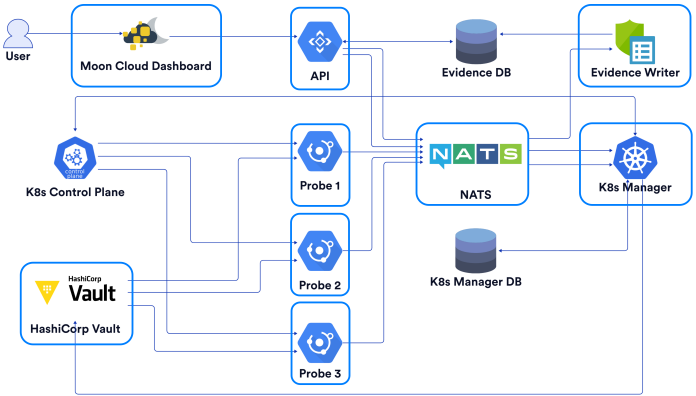
Nuova Architettura



Nuovi componenti

- *K8s Manager* come agent per lo scheduling delle *Probe*
- *Evidence Writer* per la scrittura delle evidenze
- *NATS* come pub/sub interno
- *HashiCorp Vault* per la gestione delle credenziali

Nuova Architettura



Architettura cloud-native

- passaggio ad approccio pub/sub
- nuovi pattern cloud-native (es. injection di credenziali)

Caso di Studio - Probe ML

Target: applicazione basata su Machine Learning

- verifica delle performance basata su metriche $\Longrightarrow$ accuracy, precision, e recall
- test dell'intera architettura

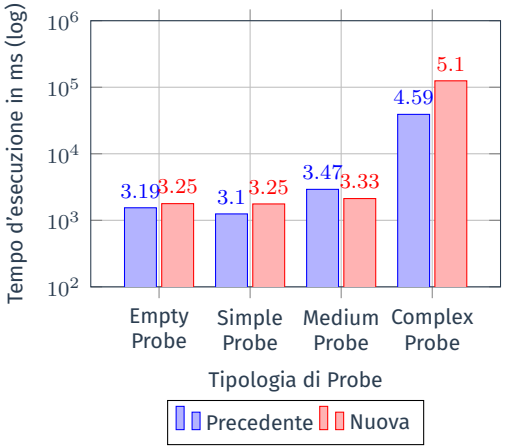

```
{
    "integer_result": 0,
    "pretty_result": "Declared metrics match the model status",
    "extra_data": {
        "detected_accuracy": 0.9525909592061742,
        "detected_recall": 0.9586206896551724,
        "detected_precision": 0.9434389140271493
    }
}
```

Esperimenti

Valutazione delle performance e dei tempi d'esecuzione

- overhead del framework $\Longrightarrow$ Empty Probe
- performance end-to-end $\Longrightarrow$ Simple Probe, Medium Probe, e Complex Probe
- media di 10 ripetizioni per ogni *Probe*

$\Longrightarrow$ overhead trascurabile in relazione ai vantaggi della nuova architettura



Conclusioni

Riprogettazione e implementazione di un'architettura di assurance per sistemi distribuiti moderni

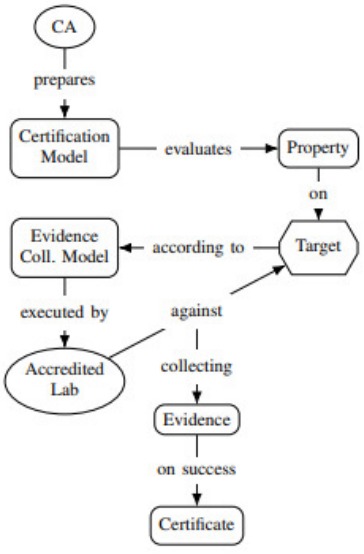
- utilizzo in ambienti cloud, hybrid, e on-premise
- semplificazione generale del funzionamento, aggiornando i componenti al cloud-native
- scalabilità, affidabilità, e replicabilità

Lavori futuri

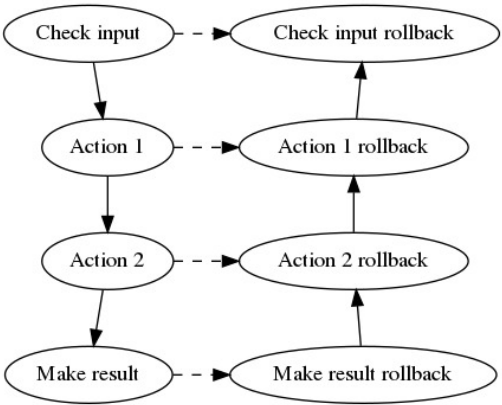
- passaggio ad un modello a credenziali effimere
- implementazione di un orchestratore avanzato per la scelta del nodo di deployment delle *Probe* basato su metriche

Appendice

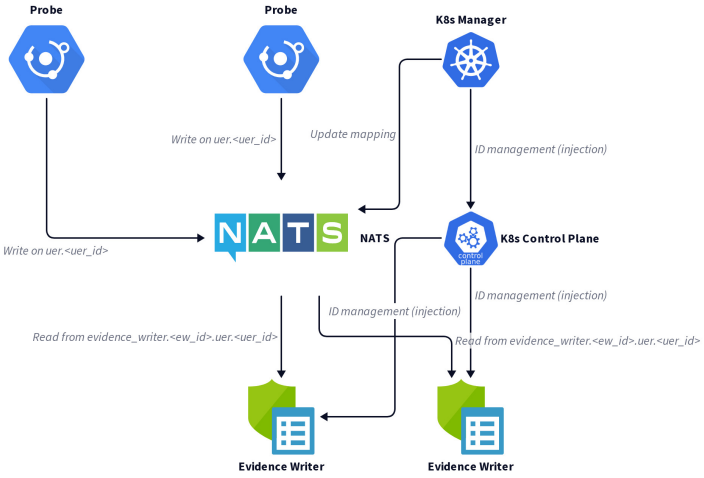
Extra: Modello di Certificazione



Extra: Macchina a Stati Finiti Probe



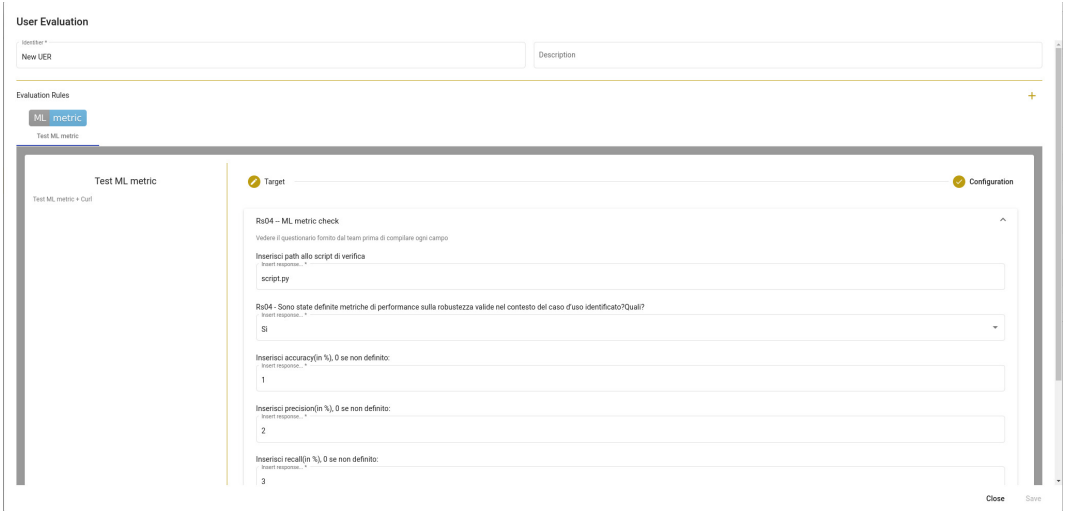
Extra: Architettura NATS



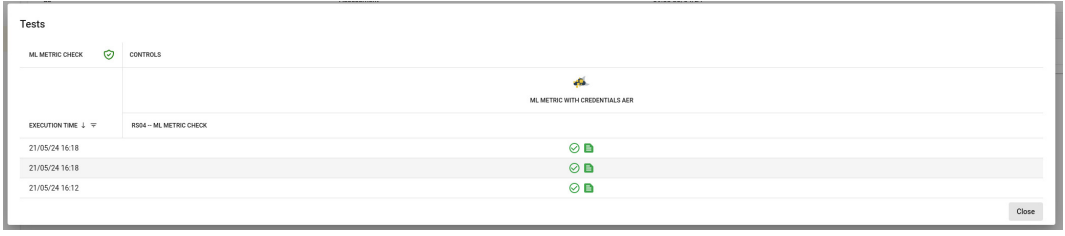
Extra: Mapping NATS

Input subject	Output subject(n=3)
uer.1	evidence_writer.1.uer.1
uer.2	evidence_writer.1.uer.2
uer.3	evidence_writer.2.uer.3
uer.4	evidence_writer.1.uer.4
uer.5	evidence_writer.2.uer.5
uer.6	evidence_writer.2.uer.6
uer.7	evidence_writer.0.uer.7

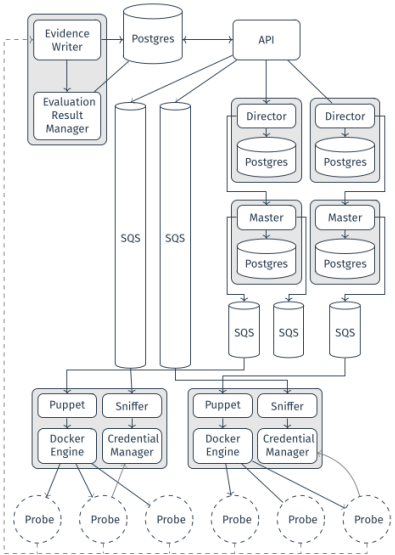
Extra: Creazione UER



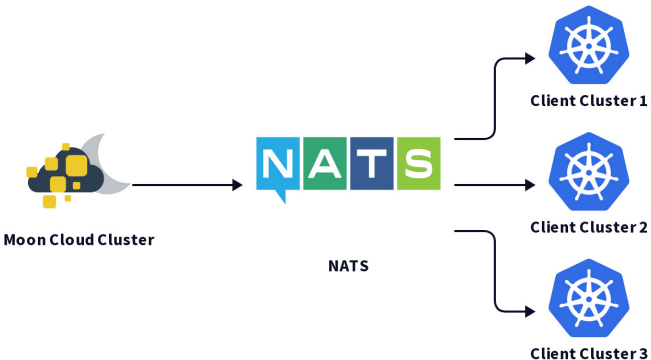
Extra: Risultati UER



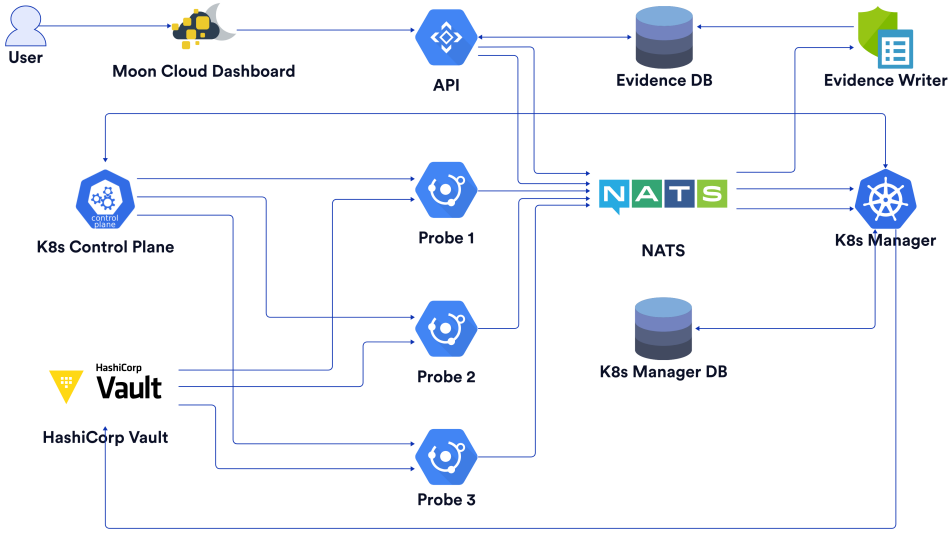
Extra: Architettura Esistente



Extra: Architettura Multi Cluster



Extra: Nuova Architettura



Extra: Risultato Probe ML


```
{
    "integer_result": 0,
    "pretty_result": "Declared metrics match the model status",
    "extra_data": {
        "detected_accuracy": 0.9525909592061742,
        "detected_recall": 0.9586206896551724,
        "detected_precision": 0.9434389140271493
    }
}
```

Extra: Esperimenti