Aggiornamenti DataCloud

Claudio Grandi

Personale

Dopo quasi 1 anno dall'assunzione, necessaria una valutazione del contributo dei neoassunti e una eventuale riassegnazione

- Valutazione da parte dei WP leader
- Interazioni con i responsabili delle strutture
- Proposta di revisione

Necessario un maggiore coinvolgimento

Interazioni in ambito PNRR

Discussioni con CINECA e GARR sul middleware per la federazione italiana (ICSC, TeRABIT)

- Documenti su architettura e middleware per deliverable TeRBIT e ICSC

Deve partire il lavoro per il PoC in cui dimostriamo di poter accedere a siti INFN e CINECA (Galileo 100) (giugno 2024)

WP1 - Operations

- Interazioni con in Tier-2 su integrazione delle risorse
  - Avviato un GdL per chi vuole sperimentare l'uso di Kubernetes invece che OpenStack – comunque necessario lavoro di sviluppo
  - Su richiesta dello steering del C3SN preparato il mandato del GdL e approntata una matrice di funzionalità in funzione del back- end (vedi slide successive)
- Federazione di infrastrutture cloud
  - Oltre a CNAF, Bari, CloudVeneto, completata Catania e in fase di completamento Napoli
- Da definire il modello di deployment di IAM

WP1 - Operations

- Urgente un potenziamento del backbone
  - Previsto l'utilizzo di risorse dall'AQ TeRABIT
  - In fase di definizione le policy di utilizzo del backbone e la migrazione dei dati sperimentali alle cloud federate
- Nuovi servizi core stanno entrando in produzione (FTS, RUCIO, …)
- Necessario migliorare monitoring e accounting
- Come evidenziato nella riunione con lo steering, necessario definire policy di allocazione di risorse non referate a esperimenti
  - Da discutere oggi!!!

Mandato del GdL su Kubernetes (DRAFT) 1/2

Il gruppo di lavoro su Kubernetes (k8s) è un sottogruppo del WG DataCloud del C3SN, con lo scopo di creare una comunità di persone dell'INFN interessate all'utilizzo della piattaforma per la gestione delle risorse dei siti, con l'intento primario, ma non esclusivo, di facilitare l'accesso da parte delle applicazioni Cloud. La supervisione del gruppo di lavoro è del PMB di DataCloud.

In generale, gli scopi sono:

- condividere pratiche per l'installazione e la gestione della piattaforma;
- individuare un gruppo di persone che abbiano o acquisiscano il know-how che gli permettano di essere in grado di gestire cluster k8s anche per i servizi centrali di DataCloud
- identificare persone nei siti in grado di contribuire allo sviluppo di configurazioni e componenti specifiche, anche ad alto livello, utili a consentire l'utilizzo di risorse su k8s da parte delle applicazioni Cloud.

Mandato del GdL su Kubernetes (DRAFT) 2/2

Nello specifico scopi sono:

- Avere installazioni di k8s ai siti (che non hanno OpenStack) capaci di fornire risorse tramite un approccio cloud, sia rispetto agli utenti locali sia tramite i servizi centrali di INFN Cloud;
- Avere un team per le operation di cluster di k8s per ospitare servizi centrali di Datacloud
- Implementare le componenti (connettori) dell'orchestratore di INFN Cloud in grado di accedere alle risorse gestite da k8s.

Le attività specifiche e le priorità sono definite dal PMB di DataCloud, in funzione dei benefici e dei costi di implementazione anche nel confronto con soluzioni che utilizzano backend diversi (OpenStack, batch system).

Matrice – Work in progress!

Funzionalità	Posix-shared (GPFS-like)	Xrootd/webdav	S3-object	Block-storage in cloud	Tape
Accesso da applicazione	Si tutte le applicazioni	Si ma solo applicazioni scientifiche	mostly-Not la maggior parte delle app hanno bisogno di fare il download dei dati	Si tutte non parallelo/scalabile: usabile per piccoli use-case	
Tipo di federazione implementabile (remote access)	Tramite protocollo remoto: xrootd/webdav	Già dimostrato	Da indagare	Tramite protocollo remoto: xrootd/webdav	
Trasferimento out-of-site x(third-party) (orchestrato via RUCIO o simile)	Tramite protocollo remoto: xrootd/webdav/gridftp	Si	Si	Tramite protocollo remoto: xrootd/webdav/gridftp	
Automatic cache management	Può essere sia la sorgente (via protocolli remoti) sia usato per avere dati in cache vicino alle CPU	Può essere la sorgente da cui popolare una cache oppure un servizio “volatile” di storage sul sito popolato da un “repo” remoto.	Può essere la sorgente da cui popolare una cache	Si	

Funzionalità	Openstack	Kubernetes	Batch System di qualunque natura (include grid site e HPC External centers)
Accesso diretto a Docker Orchestrators	Ok, previo deployment via PaaS Ok attraverso API Openstack (i.e. Magnum)	Ok nativamente con accesso diretto al cluster con AAI federata	No
Deployment di Virtual Machine o cluster di Virtual Machines con accesso privilegiato (root) (i.e. per la gestione di servizi NON containerizzati)	Si. Funziona con l'attuale versione di PaaS-Orchestrator. "production ready" -Monitoring -Accounting -Storage	No (non in senso assoluto ma non per ora)	No
Servizio Containerizzato Long Running Service (con o senza accesso privilegiato) (LRS) - Esempi un DB, Web Page, Code Repository, etc	Si. Funziona con l'attuale versione dell'Orchestratore. "production ready"	Si. supportabile con deployment diretto da PaaS Orchestrator. Non production ready. Analisi dei costi work in progress (WP5)	No
Servizio Containerizzato: Esempi - JupyterHub, Dask, Serverless, MLFlow (e altri nodi dinamici per WF Manager)	Si. Funziona con l'attuale versione di PaaS Orchestrator. "production ready" **Data:** oggi supportiamo questo genere di servizi usando cluster k8s deployati su VM istanziate su Openstack	Si. Non ancora in produzione con deployment diretto da PaaS Orchestrator. Analisi dei costi per lo sviluppo production level: work in progress (WP5) Si. Accessible in Offloading (come target). Attività in valutazione a Padova (WP6)	Si, per la parte di compute (i.e. il worker node) acquisito e integrato nel servizio attraverso meccanismo di Offloading. La componente LRS è intesa essere deployata su Cloud nativo (PaaS Orchestrator, both k8s or OpenStack). Analisi dei vantaggi e svantaggi Work In Progress (WP6)
Batch processing Classico	Fattibile e abbiamo una implementazione ma ha dei costi rispetto all'uso nativo che vanno stimati e quantificati. Necessario valutare pro/contro	Fattibile ma non ancora supportabile con deployment diretto da PaaS Orchestrator. Anche in questo caso ha dei costi rispetto all'uso nativo che vanno stimati e quantificati. Se si usa k8s bare metal si annulla l'overhead di performance e scalabilità. Necessario valutare pro/contro	Si: fa questo mestiere. Tipo di backend non federato con PaaS Orchestrator

WP2 - User & Project support

Gestione dei ticket

- Non solo incident response, anche supporto per l'utilizzo di cloud

Organizzazione di corsi

- A breve necessario concentrarsi su quelli legati a EPIC

Necessario organizzare a breve un incontro con CIENCA per lo user support dell'infrastruttura nazionale

Sito web (stile, contenuti, accessibilità, …)

WP3 - Risorse, Data Lake, Sostenibilità

- Organizzazione delle gare per le risorse finanziate dai progetti PNRR
  - Incluso technology tracking e definizione capitolati con il WG tecnologie
- Tracking delle procedure sull'infrastruttura dei siti
  - Valutazione dei siti per definire la capacità di ospitare le risorse
- Valutazione dei servizi ospitabili dai siti (pledged, HPC, …)
- Definizione dei costi di esercizio delle risorse per le esigenze di ICSC
- Analisi delle richieste degli utenti ICSC nel Technical Board di Spoke-0
- Urgente determinare le risorse da mettere a disposizione e le modalità di accesso per gli utenti ICSC
- Attivita' urgente: sistema di monitoraggio delle risorse installate e utilizzate

Coordinamento diretto di Carlino e CG

WP4 - Security, Policies

Attività co-gestita con la CCR, che ha la responsabilità della sicurezza informatica per tutto l'Ente

Gestione CERT, SOC

Scansioni di vulnerabilità

In previsione piccolo acquisto di SW e appliances su fondi ICSC(?)

Sarà necessario concordare politiche comuni con CINECA e GARR per la gestione della federazione italiana

WP5 - Middleware, Nuovi Servizi

- Sviluppo e mantenimento di IAM, Orchestratore, servizi PaaS
  - IAM critico per l'accesso alle risorse; discussioni con CINECA e GARR per la gestione dell'infrastruttura di Autenticazione e autorizzazione
  - Orchestratore è la componente che implementa l'accesso trasparente ai servizi – critico per gli impegni che ci siamo presi in molti progetti
- Definizione dei processi per lo sviluppo e l'inclusione di servizi PaaS
- Strumenti per la gestione del software e del ciclo di produzione
- Indispensabile un inventory di middleware e servizi
  - con l'identificazione degli owner

WP5 - Middleware, Nuovi Servizi

- Critica la carenza di risorse «esperte» per lo sviluppo software
  - Gli sviluppi indispensabili per l'implementazione della federazione nazionale con CINECA e GARR e per la certificazione ISO, si innestano su una situazione non consolidata
  - La gran parte del nuovo personale non ha esperienza sufficiente per dare un contributo positivo nel breve-medio termine
  - Prevista la riscrittura dell'orchestratore in python per allargare la base di sviluppatori
    - Su richiesta dello steering del C3SN, in preparazione un piano di lavoro
- Presto un workshop in presenza con tutti gli sviluppatori

Sviluppo orchestratore

- Critica la sostenibilità della versione attuale in Java
  - Pochi sviluppatori nell'INFN
  - Stratificazioni di codice rendono difficile anche solo l'aggiornamento delle dipendenze
- Per ampliare la base degli sviluppatori e per «svecchiare» il codice, proposta la riscrittura completa in Python
  - In fase di valutazione le librerie da usare. La decisione finale sarà presa dagli sviluppatori nelle prossime settimane e sarà definito il piano di lavoro
  - Contemporaneamente, adozione del processo per lo sviluppo sicuro del software, indispensabile per l'uso su EPIC

Sviluppo IAM

IAM è in produzione per molte comunità fra cui WLCG

Necessario prioritizzare le attività:

- Porting ai nuovi OS
- Sviluppi per supportare l'uso condiviso sulla Cloud nazionale di ICSC/TeRABIT
- Adozione del processo per lo sviluppo sicuro del software per l'uso su EPIC
- …

Nota: al momento su EPIC si usa un prodotto alternativo in attesa che IAM sia compatibile con l'uso sui dati critici (MFA, …)

WP6 - R&D, Testbed, Use Cases

Data management: test del DataLake basato su RUCIO+FTS

Software management: prototipo basato su CVMFS

Storage S3 del backbone: necessaria migrazione a nuovo software per obsolescenza di quello in uso – test con CYGNO

Workload offloading: in collaborazione con InterTwin, su use case CMS e AI_INFN

Previste attività per l'integrazione dei sistemi HPC (CINECA, HPC bubbles di TeRABIT, …). Da definire l'architettura

WP7 - Sistemi integrati di gestione e Legal Compliance

- Grossa attività su certificazione multisito (CNAF, BA, CT)
  - A parte i siti, si certificano i processi di DataCloud, altrimenti si finisce per partizionare il sistema
  - Impatto su tutto DataCloud
- Sviluppo sicuro del software per la certificazione della PaaS
  - Assessment del codice di IAM e orchestratore
  - Coinvolti WP5 e WP4
- Sviluppo di policy per l'accesso di utenti esterni all'INFN
  - Critico per le attività ICSC e TeRABIT
  - Richiede un ripensamento radicale delle regole altrimenti siamo a rischio di blocco (formazione, idoneità al ruolo di system admin, …)

Attività del Program Officer

Necessario definire milestone dettagliate per il WG

Per iniziare analisi delle scadenze di TeRABIT e ICSC-Spoke-0, a seguire i progetti medici e tutti gli altri

Si parte da un lavoro impostato dal GdL della riorganizzazione di DataCloud

Approccio pragmatico: file excel *live*

Necessario coordinamento con il WG progetti

Il risultato del lavoro sarà una serie di milestone/deliverable (da concordare poi con il PMB) per definire il piano di lavoro dettagliato

Milestone – work in progress

Project	Deliverable/Milestone	Original Date	Real Date	Type	Datacloud WP (Responsible)	DataCloud WP (Collaborating)	C3SN WG (Collaborating)	Breakdown	Note
ICSC-S0	Publication of tenders for the upgrade of the data centres and for the acquisition of IT resources (M5)	30 April 2023		HW	WP3		Technolgy Tracking		
ICSC-S0	Aactivities and working group setup	30 April 2023			Data Cloud Coordination Team				Cosa significa realmente ?
ICSC-S0	Setup User Support	31 August 2023			WP2				Non è una vera milestone ma dobbiamo dare supporto e consulenza per tutto il progetto
ICSC-S0	Publication of tenders for the upgrade of the data centres and for the acquisition of IT resources (M6)	31 August 2023		HW	WP3		Technolgy Tracking		
ICSC-S0	Collection of user requirements and identification of the middleware stack	31 August 2023		Only Document	Data Cloud Coordination Team	PMB			
ICSC-S0	Publication of tenders for the upgrade of the data centres and for the acquisition of IT resources (M7)	29 February 2024		HW	WP3		Technolgy Tracking		
ICSC-S0	HAMMON D1.2 Use case requirements gathering	29 February 2024		Only Document	LNGS ?				
ICSC-S0	Publication of tenders for the upgrade of the data centres and for the acquisition of IT resources (M8)	30 June 2024		HW	WP3		Technolgy Tracking		
ICSC-S0	Activation of a PoC for resource federation	30 June 2024		Integration/devel				BD1	
ICSC-S0	HAMMON D1.3 Implementation of the first PoC of the Cloud Platform	30 June 2024		Integration/devel				BD_H_1	
ICSC-S0	Publication of tenders for the upgrade of the data centres and for the acquisition of IT resources (M9)	31 October 2024		HW	WP3		Technolgy Tracking		
ICSC-S0	HAMMON D1.4 Implementation of the first integrated version of the Cloud Platform	31 October 2024		Integration/devel				BD_H_2	
ICSC-S0	End of project: all hardware in production	31 August 2025		HW	WP3				
ICSC-S0	End of project: infrastructure in production	31 August 2025		Integration/devel				BD2	
ICSC-S0	HAMMON D1.5 Implementation of the fully featured high-available Cloud Platform	31 August 2025		Integration/devel				BD_H_3	
TeRABIT	Setup User Support	31 August 2023			WP2				Non è una vera milestone ma dobbiamo dare supporto e consulenza per tutto il progetto
TeRABIT	D4.1 - Documentation for the tender issued for the acquisition of hardware resources	31 August 2023		HW	WP3		Technolgy Tracking		
TeRABIT	D4.2 - Publication of the WP4 detailed architecture	31 August 2023		Only Document					
TeRABIT	Deadline (from the call) for provider's identification	31 December 2023		HW	WP3				
TeRABIT	D4.3 - Report on the deployment of PoC applications over multiple HPC Bubbles	31 December 2023		Integration/devel				BD_T_1	Per me è come BD_1. Questa milestone si pospone dato che non ci sono bubble ancora verrà rimandata (ma poi cisono i tempi per fare tutto) o si emulano?
TeRABIT	D4.4 - Report on the deployment of a PoC for dynamic caches	31 March 2024		Integration/devel				BD_T_2	
TeRABIT	TeRABIT D4.5 - First report on the integration with the WP2 and WP3 infrastructures	31 March 2024							
TeRABIT	D4.6 - Report on the final installation of all purchased hardware	31 October 2024		HW	WP3				
TeRABIT	D4.7 - Second report on the integration with the WP2 and WP3 infrastructures	31 December 2024							
TeRABIT	End of project: all hardware in production	30 June 2025			WP3				
TeRABIT	End of project: infrastructure in production	30 June 2025		Integration/devel				BD_T_3	

Milestone – work in progress

Activation of a PoC for resource federation
1- Federazione minimale di un provider Openstack
2- Federazione a livello di applicazione via offloading

Involved Areas	Involved Services/Components	Fine grained activities	Date	Priority	Owner	Contributors	NOTE
AAI		IAM PoC/Test inscance Deployment			Wp6		Questo sarà quello usato per tutti i servizi centrali e high level che faranno parte del PoC
		IAM(s) Operations			WP6	WP2/1	
Compute Federation		Deployment of multitenacy dashboard			WP5		Questo breackdonw assume una definizione della matrice già avvenuta o sostanzialmente avvenuta
	PaaS Orchestrator	Orchestrator configuration (i.e. federation registry) - Option 1			WP1	WP5	
	- Option1. Openstack federation, - Option1. Service level offloading (requres Orchestrator at least for the origin)	Federation validation (i.e. high level service deployment)			WP6		Assumo che la federazione debba mostrare che alcuni servizi sono deployabili. Corretto? se si quali ?
		Storage enpoints deployment			WP1		Va defiito un modello per lo storage cloud (s3) per attività ICSC. Non credo che prevediamo di usare il backbone (o si?). Per il PoC possiamo avere un endpoint S3 ad hoc ma poi va definito il modello. Se siamo d'accordo va aggiustato il breakdonw in accordo
		High level service deploybed by Orchestrator automatically configured to offload toward external Provider (batch and other: vm or k8s)			WP6	WP5	Selezionando un servizio k8s puo' essere abilitato l'offloading nelle seguenti condizioni target. - Nodo (fat node) - batch - k8s
Data Federation	RUCIO	Actual Rucio(s) Deployment			WP6	WP1	Puo' essere un servizio dedicato sull'infrastruttura di WP6
	FTS	FTS Deployment (if needed, might reuse the existing one)			WP6	WP1	Suggerirei di usare l'istanza INFN.
		Storage endpoint configuration at site (depend also on external providers specific setup)			WP6	WP1	Assumo che ci siano anche providers esterni NON INFN dove deployare un endpoint

→ A partire dalle *Fine grained activities* si definiscono le milestone

Audit sicurezza

Secondo audit sulla sicurezza il 28/2 – In attesa di report

A causa del periodo senza coordinamento poche azioni correttive sono state applicate

- Fatti l'aggiornamento dei link nella documentazione e la gestione degli asset
- Il documento sulla riorganizzazione è stato considerato molto positivamente per la mitigazione della Non-Conformità principale (NC01-INFN-DataCloud-22-23) sulla mancanza di documentazione sulla struttura di governo e la catena di responsabilità

Presto da approntare il registro del trattamento, valutazione del rischio, documento sulle misure minime, accessibilità dei siti

Inoltre: procedure e policy per backup, cancellazione di dati e servizi