



Contribution ID: 5

Type: **Comunicazione orale**

Realizzazione e gestione di una piattaforma di High Performance Computing

Friday, 15 October 2021 09:40 (30 minutes)

Background

I recenti sviluppi tecnologici in ambito biomedico, hanno portato alla generazione di enormi mole di dati derivanti da tecnologie di high-throughput come microarray e sequenziatori che richiedono la gestione e la possibilità di effettuare diverse analisi computazionali in modo efficiente ed efficace attraverso una infrastruttura in grado di rispondere ai continui sviluppi tecnologici, di metodi e di algoritmi atti all'analisi.

Il primo problema che si riscontra, è quello derivante dalle richieste fisiche per la loro gestione; in particolare, la richiesta di storage capienti per il salvataggio e i backup dei dati e al contempo la necessità di mantenere un accesso veloce a tali informazioni durante il loro utilizzo.

In questo contesto si inserisce l'infrastruttura di High Performance Computing realizzata in quanto presta particolare attenzione ai sistemi e alle tecniche per:

- Installazione e provisioning dei servers
- Gestione degli utenti e principali servizi di rete (DNS,NTP)
- Gestione e mantenimento dei diversi Software

Installazione e provisioning dei servers

Per l'installazione del Sistema Operativo viene sfruttato il Preboot Execution Environment (PXE) che permette di eseguire il boot di un sistema operativo tramite rete ethernet automatizzandone il deployment distribuito. Successivamente la configurazione dei diversi sistemi è effettuata tramite un software di provisioning che si occupa di automatizzare le procedure di configurazione e gestione.

Un server PXE permette ai client di avviare e installare un sistema in rete senza avere necessariamente un supporto fisico; a differenza dei tradizionali metodi di installazione, si può installare qualsiasi sistema nella rete senza dover usare l'unità CD-ROM o USB.

L'ambiente PXE ha successivamente bisogno di un server DHCP che distribuisce gli indirizzi IP per i sistemi client e un server TFTP da dove scaricare i file di installazione nel quale vengono definite le prime impostazioni inerenti alla lingua di sistema, l'interfaccia di rete e l'accesso remoto per l'interazione con il server di automazione.

Il Configuration Management è un processo automatico e prevedibile utilizzato per definire la configurazione dei server e dei servizi in modo consistente, possibilmente sotto controllo di versione. In particolare, nella realizzazione di questa infrastruttura è stato utilizzato Ansible.

Ansible per sua definizione è configurato per essere idempotente, questo implica che applicando le regole di configurazione diverse volte il risultato finale è sempre lo stesso.

La configurazione del provisioning tramite Ansible può essere racchiusa in 5 aspetti chiave:

- Task: le operazioni che devono essere svolte sui diversi server per configurare il sistema
- Moduli: piccoli programmi messi a disposizione da Ansible che permettono di effettuare e semplificare i task
- Ruolo: rappresenta un insieme di task che permettono di configurare una funzione precisa
- Playbook: organizza i vari ruoli per portare a termine il compito.
- Inventory: è un file che contiene al suo interno dei gruppi che a loro volta contengono gli identificatori dei server. Questi server sono quelli che verranno influenzati durante l'esecuzione dalle istruzioni contenute nei playbook.

Gestione degli utenti e principali servizi di rete

Nell'infrastruttura si è deciso di implementare FreeIPA quale soluzione integrata nella gestione della sicurezza in quanto combina Linux, 389 Directory Server, MIT Kerberos, NTP, DNS e un sistema di certificati gestibile tramite command line o Web GUI.

Nella gestione degli utenti un ruolo fondamentale è dato dall'autenticazione. Essa deve permettere di identificare in modo sicuro ed efficace i diversi utenti e permettere l'utilizzo dei soli servizi disponibili per lo specifico utente.

L'autenticazione viene gestita tramite protocollo Kerberos che permette di autenticarsi nella rete provando la propria identità e cifrando i dati.

Kerberos previene attacchi quali l'intercettazione e i replay attack ed assicura l'integrità dei dati. I componenti Kerberos KDC / Kadmin sono implementati utilizzando il software Kerberos MIT e forniscono i servizi di autenticazione per l'intero dominio di FreeIPA che è utilizzato per i servizi, per gli utenti e per le altre componenti del sistema.

Gestione e mantenimento dei diversi Software

Risulta poi importante l'installazione e la gestione dei software utilizzati. In particolare, è importante poter fornire le diverse versioni al fine di poter riprodurre le analisi con diverse configurazioni. Questo aspetto è molto cruciale perché spesso i software sono dipendenti dalle librerie di sistema e potrebbero suscitare conflitti tra differenti versioni.

Per questa ragione è stato deciso di utilizzare una gestione basata su container che permette di isolare i diversi software; in particolare, è stato scelto di utilizzare Singularity, una piattaforma container open source progettata per essere semplice, veloce e sicura.

La creazione dei container si basa sulla realizzazione di un file di recipes che contiene le istruzioni per la creazione e la realizzazione dell'applicazione.

Per rendere le applicazioni ancora più facilmente utilizzabili ed intuitive è stato integrato il sistema Environment Modules. Questo sistema è uno strumento che aiuta gli utenti a gestire il proprio ambiente shell Unix o Linux, consentendo di creare o rimuovere dinamicamente gruppi di impostazioni relative alle variabili d'ambiente correlate. In particolare, vengono esposti i comandi presenti nei container singularity come alias e quindi richiamabili come comandi base del sistema operativo host.

Conclusione

L'infrastruttura descritta si basa sull'utilizzo di un sistema di provisioning per l'installazione dei diversi servizi, un sistema di identity Management in cui vengono immagazzinate e gestite le informazioni relative agli utenti e ai servizi e un sistema di Environment Modules in grado di fornire l'accesso a specifici software nascondendo la complessità di interazione con il sistema operativo.

Questo rende l'infrastruttura eterogenea e modulare in quanto indipendente dalla tipologia di server e facilmente estendibile nel tempo.

Inoltre, eventuali modifiche e aggiornamenti alle configurazioni della gestione dei sistemi operativo o dei servizi sono facilmente propagabili all'interno dell'intera infrastruttura senza creare disservizi agli utenti.

Primary author: MOSCATELLI, MARCO (CNR - ARMi4)

Co-author: GNOCCHI, MATTEO (CNR-ITB)

Presenter: MOSCATELLI, MARCO (CNR - ARMi4)

Session Classification: Infrastruttura server

Track Classification: Infrastruttura Server