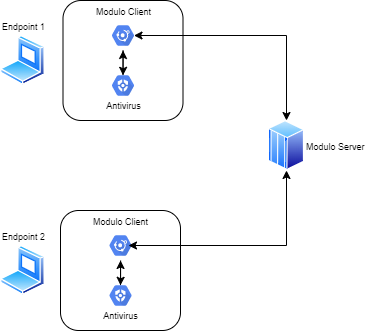
**CEPMS (Cloud Endpoint Protection Management System)**

CEMPS è un’applicazione server il cui obiettivo è riuscire a gestire in modo centralizzato molteplici client (endpoint) in merito all’individuazione di software malevolo.

Esistono quindi due moduli dell’applicazione:

* modulo server (CEPMS)**:** Effettua la gestione degli antivirus installati sugli endpoint.
* modulo client (endpoint): applicativo installato sugli endpoint, che mette in comunicazione antivirus e modulo server.



**Modulo Server**

Il modulo server consente di interfacciarsi al modulo client per programmare scansioni su due basi temporali:

* ripetute (periodiche)
* una tantum

Inoltre una scansione può avvenire in due modalità:

* rapida (secondo policies dell’AV locale)
* completa (secondo plicies dell’AV locale).

Il modulo server dovrà quindi fornire un’interfaccia di login agli amministratori di sistema per accedere alla gestione della protezione degli endpoint e consentire di aggiungere o rimuovere amministratori dal sistema. Deve inoltre permettere di associare e disassociare gli endpoint (moduli client) al server CEPMS e fornire informazioni sulla programmazione delle scansioni e creazione di report che specifichino in sintesi il numero di minacce bloccate, ignorate, rilevate per ogni endpoint associato.

I dati dell’applicazione vengono fatti persistere su database tramite JDBC.

**Modulo Client**

Il modulo client ha la responsabilità di gestire la comunicazione tra modulo server e antivirus, agendo da interfaccia tra i due applicativi. Questo modulo quindi possiede in memoria la programmazione delle scansioni gestite tramite modulo server. La comunicazione con AV locale viene gestita tramite fake implementation.

Una volta finalizzata la scansione dell’AV locale, quest’ultimo generera’ ed inviera’ il report della scansione e la lista degli eventuali file in quarantena al modulo client (endpoint) che a sua volta li inviera’ al modulo server.