UNIVERSITÀ DEGLI STUDI
DI GENOVA

sita centro servizi informatici e telematici di ateneo

simpleSAMLphp in alta disponibilità

Marco Ferrante
Università di Genova/CTS IDEM
marco@csita.unige.it
Quarto Convegno IDEM
4 aprile 2014

UNIVERSITÀ DEGLI STUDI
DI GENOVA

sita centro servizi informatici e telematici di ateneo

Sommario

- IdP in alta disponibilità
- simpleSAMLphp
- Memcached
- Deployment
- Problemi

UNIVERSITÀ DEGLI STUDI DI GENOVA

sita centro servizi informatici e telematici di ateneo

Cosa vogliamo da un IdP in HA

- Nel nostro contesto la disponibilità è la probabilità che un utente ottenga il servizio di autenticazione in un determinato momento
  - Guasti hardware, problemi di software, errori umani
    - Virtualizzazione
    - Gestione
  - Connettività
    - Ridondanza
  - Manutenzione e test
    - Le condizioni reali sono sempre replicabili “in vitro”

UNIVERSITÀ DEGLI STUDI DI GENOVA

sita centro servizi informatici e telematici di ateneo

simpleSAMLphp

- simpleSAMLphp (ssp) è una libreria PHP per trattare SAML 2.0 che fornisce anche i servizi per implementare un IdP o un SP
  - https://simplesamlphp.org/
- Sviluppato da Feide/UNINETT
- Multiprotocollo/multistandard
- Perché ssp invece di Shibboleth?
  - Se “mettete le mani nel codice”
  - Più rapido da rendere operativo
  - Per applicazioni PHP portabili

simpleSAMLphp e sessioni

- Tipicamente le applicazioni web PHP sono *stateless*
  - Ogni invocazione dello script è indipendente
  - Al contrario, le applicazioni J2EE che sono solitamente *long running*
- La gestione dello stato di default è delegata ai meccanismi di sessione di PHP

UNIVERSITÀ DEGLI STUDI
DI GENOVA

sita centro servizi informatici e telematici di ateneo

Memcached

- Memcached è una *in-memory* cache distribuita
  - http://www.memcached.org/
- Il sistema è costituito da un server

```
apt-get install memcached
vi /etc/memecached.conf
/etc/init.d/memcached start
```

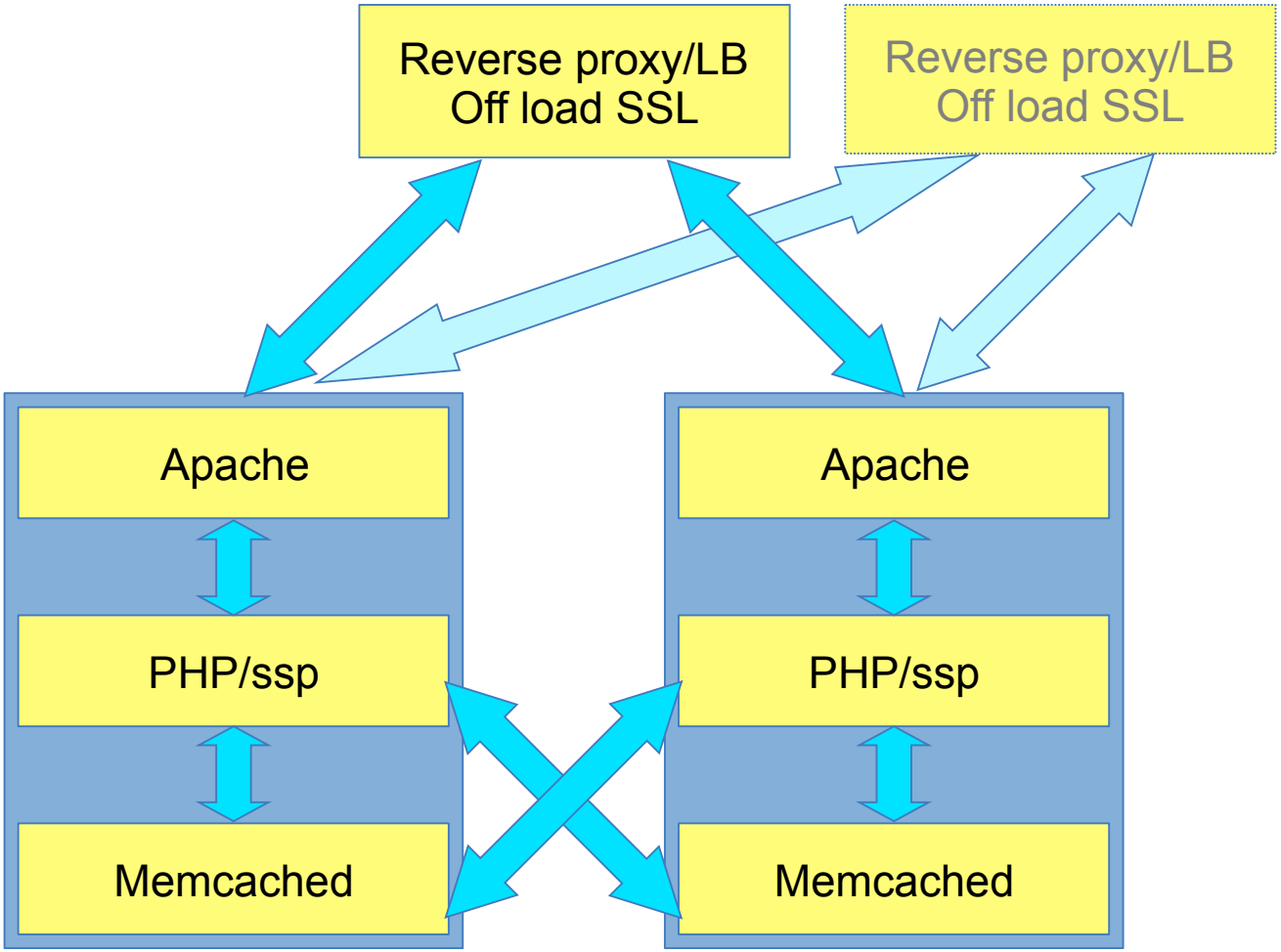
- e da due possibili librerie/interfacce *memcached* e *memcache*

```
apt-get install php5-memcache
```

UNIVERSITÀ DEGLI STUDI
DI GENOVA

sita centro servizi informatici e telematici di ateneo

Deployment



UNIVERSITÀ DEGLI STUDI DI GENOVA

sita centro servizi informatici e telematici di ateneo

Deployment

- La coerenza delle sessioni memorizzare sui due server dipende strettamente dall'ora di sistema: sincronizzate gli orologi!
- Il *load balancing* non sembra fondamentale
  - 1 server 255.000 auth/mese (oltre 8000/giorno)
    - Servizi on line studenti, Moodle di Ateneo
    - Sessioni lunghe, un utente tipico al più un paio al giorno
  - l'algoritmo sembrerebbe soggetto a *race condition*
- Più utile il *failover* (anche per motivi di gestione)
  - Configurazione di Apache come *reverse proxy* in *failover (e* debug per i gestori)
  - Vedere la presentazione di Fabio Spelta del

Configurazione

- config.php:

```
'store.type' => 'memcache',
'memcache_store.expires' => ttl della entry, > di session.duration
    'memcache_store.servers' => array(
      array(
        array('hostname' => 'idp1',
           'port' => …, 'weight' => …, 'timeout' => …,
        ),
        //array('hostname' => 'memcache-backup'),
      ),
      array(
        array('hostname' => 'idp2'),
      ),
    ),
```

Altro

- In php.ini

  memcache.allow_failover = Off

- Il meccanismo di *failover* di Memcached richiede è in conflitto con l'algoritmo di *failover* di ssp
- Il server Memcached non ha alcun meccanismo di controllo dell'accesso via rete
  - intervenire a livello di firewall

UNIVERSITÀ DEGLI STUDI DI GENOVA

sita centro servizi informatici e telematici di ateneo

Modo d'intervento

- Se idp1 non risponde, il *reverse proxy* (con timeout) passa la richiesta a ipd2
- Idp2 cerca la sessione (con timeout) su tutti i server Memcached e prova ad aggiornarla
- Ritardo totale:
  - reverse proxy timeout + *n* * memcached down * 2
- Nessun problema nei test a secco
- Sperimentato un solo incidente in produzione
  - Gli aggiornamenti sono controllati

UNIVERSITÀ DEGLI STUDI DI GENOVA

sita centro servizi informatici e telematici di ateneo

Problemi

- Il subentro di idp2 a idp1 ha funzionato senza problemi, ma ci sono invece stati numerose segnalazioni di asserzioni duplicate al riavvio di idp1
  - Non è chiaro da cosa siano state generate
  - Non abbiamo replicato l'evento
- Non permette di gestire ePTID memorizzati che richiedono un DB SQL
- Eventuale ridondanza dei DB per Consent
  - È possibile usare i cookie