IdP 3.2.x
–
Clustering

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

Shibboleth IdP 3.x Workshop
16./17. Juni 2016, FU Berlin

Clustering – Motivation

- Failover
  - Hardware
  - VM
  - Netzwerk
  - ...
- Load Balancing

High Availability (HA)

- Wartungen
  - Upgrades
  - Extensions
  - Anpassungen CD
  - etc.

Sessions und Storage

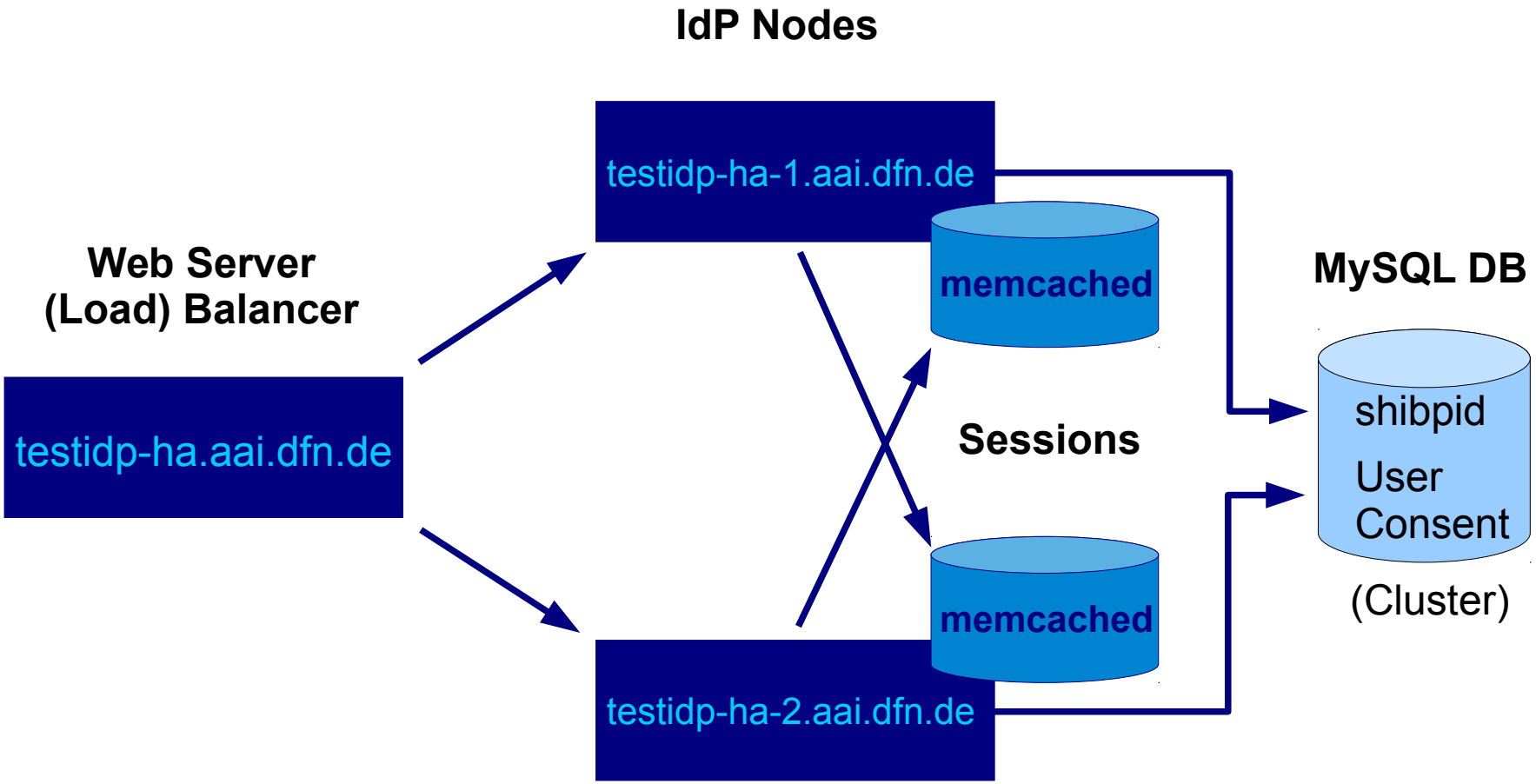
- **Conversational State**
  Spring Web Flow conversational state during profile request processing (essentially a single login, query, or other operation)
- **IdP Session**
  An "IdP session" capturing authentication results (so they can be reused for SSO) and optionally tracking services for logout
  Default: Cookie-Based StorageService Bean (Session Cookies / HTML Local Storage)
- **User Consent**
  Default: Cookie-Based StorageService Bean (Persistent Cookies / HTML Local Storage)
- **Message Replay Cache, SAML Artifact Store**
  Default: In-Memory StorageService Bean

Siehe auch https://wiki.shibboleth.net/confluence/x/uAEUAQ
und https://wiki.shibboleth.net/confluence/x/lYEgAQ

Sessions und Storage → Cluster

- **Conversational State**
  → keine Änderung (möglich)
- **IdP Session**
  → SP Session Tracking (SLO) erfordert zumindest HTML Local Storage (siehe Anmerkung im Shib Wiki), alternativ serverseitige Storage Implementierung
- **User Consent**
  → Vor allem juristische Erwägungen: Information in /logs/idp-consent-audit.log ausreichend? Andernfalls serverseitige Storage Implementierung
- **Message Replay Cache, SAML Artifact Store**
  → Memcached, JPA/Hibernate etc. (falls benötigt)

Versuchsanordnung



Siehe auch

https://wiki.shibboleth.net/confluence/display/IDP30/StorageConfiguration#StorageConfiguration-MemcachedStorageService

Bisherige Erfahrungen

- Scheint prinzipiell zu funktionieren
  (wenig Zeit zum Testen)
- Eine produktive Lösung erfordert weitaus mehr als das in einer solchen Teststellung angewandte Setup
  - Load Balancer, Firewall (→ Memcached), Hardware
  - Zombie-Nodes (→ STONITH)
  - DB Failover / Cluster – auch für LDAP/AD
  - Synchronisierung der IdP-Konfiguration, Templates etc.
  - Secret key management for cookie encryption
  - Monitoring
  - u.a.m.
- Ausführliche Diskussion bei SWITCH, siehe letzte Folie

Nützliche Ressourcen

- Shibboleth Wiki:
  https://wiki.shibboleth.net/confluence/display/IDP30/Clustering
- SWITCHaai - ausführliche Diskussion unter
  https://www.switch.ch/aai/guides/idp/clustering/
- Shibboleth Wiki - Storage Configuration:
  https://wiki.shibboleth.net/confluence/x/lYEgAQ
- Memcached
  https://memcached.org/
- Memcached Security
  http://blog.couchbase.com/memcached-security
  und, z.B.
  https://serverfault.com/questions/424324/how-to-secure-memcached/424330

Vielen Dank für Ihre Aufmerksamkeit!

Fragen? Anmerkungen?

Kontakt

www: https://www.aai.dfn.de

eMail: hotline@aai.dfn.de

Tel.: +49 711 63314 215