Shibboleth in hochskalierbaren Umgebungen

Peter Gietz, Martin Haase
DAASI International
{vorname.nachname}@daasi.de

AAI-Forum
64. DFN-Betriebstagung
2. März 2016

Agenda

- DAASI International
- Clustering mit dem IdPv3 - was geht und was geht nicht?
- Konfiguration automatisieren für 100+ Nodes
- White Label Domains - IdP A ist ab *jetzt* auch IdP B

DAASI International

DAASI International

- Ende 2000 als offizielles Spin-Off der Universität Tübingen gegründet
- Forschungsprojekte zu PKI, Grid, Virtuellen Forschungs-infrastrukturen, Digital Humanities, Föderiertes Identity Management
- Wir bieten... Consulting, Design, Implementierung, Programmierung, Schulung, Support
- Technologische Expertise in... Identity Management, Föderationen, LDAP, PKI, RBAC, AAI, Virtuelle Forschungsinfrastrukturen, eHumanities, Web Services, Grid Computing, Hochschulsoftware

DAASI International

Clustering

- IdPv3 bringt von Haus aus Cluster-Fähigkeit mit
  - per Default wird alles in Cookies gespeichert: Sessions und Consent
    - Problem 1: wenn der Client keine Cookies persistiert, muss der User bei Consent JEDES mal zustimmen
    - Problem 2: Persistente NameIDs gehen nur mit Datenbank
  - Dank der Abstraktionsschicht StorageService kann aber genausogut in Memcached oder DB gespeichert werden
- Alles sogenannenter *Non-Conversational* State
- Problem: Conversational State

DAASI International

Conversational State und Stickiness

- «So, out of the box, the IdP software ***requires that flows involving views start and finish on the same node***, the most common example being a login that requires a form prompt or redirect. This is similar to the way V2 worked, in that requests included a "login context" object that maintained state, but this state is now handled by SWF and is bound to the container session. That is a change, in that V2 did not rely on the container session at any point.
- While some containers do have the capability to serialize session state across restarts or replicate sessions between nodes, and Spring itself is able to leverage that mechanism, the IdP does not support that because the *objects it stores in the session are not required to be "serializable*" in the formal Java sense of that term. This greatly simplifies the development of the software, but makes clustering harder.
- At present, there is no solution provided to replicate the per-request conversational state. This means that 100% high availability is not supported; *a failed node will disrupt any requests* that are in the midst of being processed by the node. It also means that ***some degree of session "stickiness" is required. Clients must***

Anforderungen

- Massives Clustering: Größenordnung von bsp. 100 aktiven Nodes gleichzeitig
- Je nach aktueller Auslastung des Clusters im Minutentakt dynamisch Nodes hinzufügen oder entfernen (über die Cloud)
- ---> Keine Stickiness fürs Login-Formular mehr möglich!
- Alle Konfigurationsänderungen muss sich ein Node selbst von zentraler Stelle ziehen
- "White label Domains" - für Branding des IdPs, je nach SP verhält er sich wie eine ganz andere Organisation
- Bandbreite sparen wo möglich

DAASI International

White Label Domains

- Branding des *gesamten* IdPs (nicht nur via DNS)
- IdPv3 kann mit verschiedenen entityIDs auftreten
- Trigger für entityID Overrides können sein:
  - bestimmter SP,
  - bestimmte Föderation,
  - bestimmte EntityCategory
- Problem: entityID muss a priori konfiguriert sein, bevor der SAMLrequest eines SPs ankommt

DAASI International

White Label Domains

- Lösung: die Relying-Party-Overrides mit einer reloadable Resource kombinieren
- Jede Minute eine Remote-Resource nach Änderungen abfragen (ohne zu holen, Größe=0)
- Nur wenn sich die Domains ändern, holt der IdP sich die Relying-Party-Overrides von zentraler Stelle
- Entity-Kategorien in SP-Metadaten nutzen (RelyingPartyByTag) mit Mapping Domain --> entityID

DAASI International

Weitere Strategien für automatisierte Konfiguration

- Einsatz von ReloadableResources wo möglich
- Metadaten für SPs on-demand vom IdM holen - DynamicHTTPMetadataProvider
- Im JAAS-Modul White Label Domains ergänzen
- Bezug von sämtlichen GUI-Elementen der White-Label-Domains aus dem CDN
- Social Login (OpenID Connect) je nach Domain

DAASI International

Stickiness vermeiden

- Behandlung des Conversational State noch offen
- Möglicher Ansatz: Replay des SAMLrequest zusammen mit Login/PW (so macht es ADFS)
  - Könnte schmerzfrei sein, da der IdP per Default Basic Authentication vor dem Anzeigen des Login-Forms akzeptiert
  - Auch möglich beim "Rausspringen" zum OpenID Connect Provider? Und für Consent Flow?
- Andere Option: SAMLrequest in einem Cookie speichern?
- ...

DAASI International

Vielen Dank für Ihre Aufmerksamkeit.

DAASI International

www.daasi.de

Telefon: 07071 4071090

E-Mail: info@daasi.de