

# OpenSSO Web GUI



**OSSTech**

オープンソース・ソリューション・テクノロジー株式会社

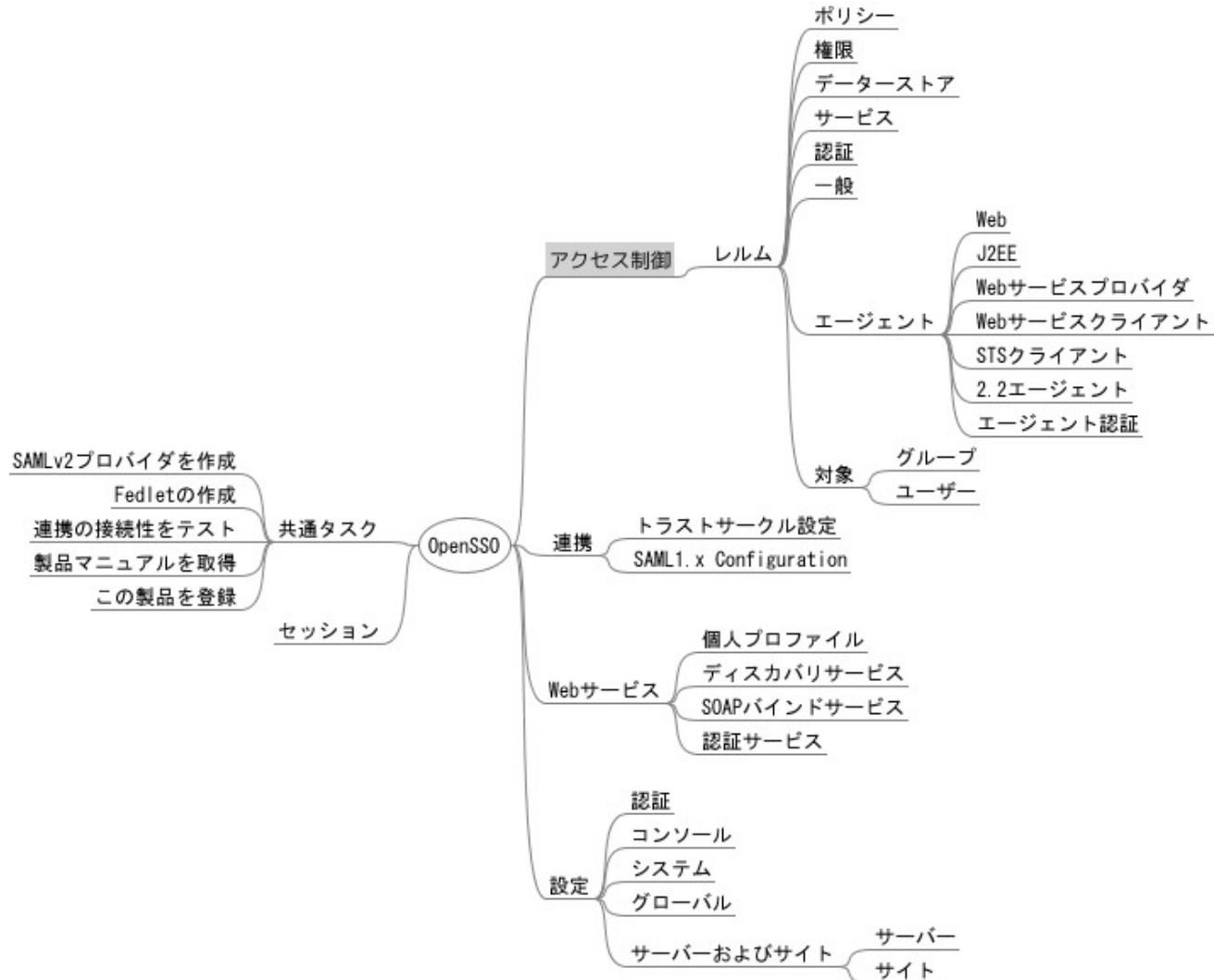
2009/12/22

唐木大介

# 目次

- トップメニュー
- アカウント操作
- バックエンドldap
- おまけ

# メニューリスト



# トップメニュー

- 共通タスク
- アクセス制御
  - アカウント設定
- 連携
  - SAML設定
- Webサービス
  - WSF設定
- 設定
  - OpenSSOサーバー設定
- セッション

# アカウント管理

- アクセス制御
  - データストア
    - 接続先LDAPサーバー設定
  - 対象
    - ユーザー、グループ管理

## ldapへの設定保存

```
ldapsearch -x -W -D "cn=Directory Manager" -b  
"dc=opensso,dc=java,dc=net" -h localhost -p 50389
```

# 設定変更

- アクセス制御
  - レルム
    - データストア
      - openldap(新規データストア作成)

```
ldapsearch -x -W -D "cn=Directory Manager" -b "dc=opensso,dc=java,dc=net" -h localhost -p 50389 -L ou=openldap
```

```
# openldap, default, OrganizationConfig, 1.0, sunidentityrepositoryservice, services, opensso.java.net
dn: ou=openldap,ou=default,ou=OrganizationConfig,ou=1.0,ou=sunidentityreposito
ryservice,ou=services,dc=opensso,dc=java,dc=net
objectClass: sunServiceComponent
objectClass: top
ou: openldap
sunKeyValue: sun-idrepo-ldapv3-config-group-container-name=ou
sunKeyValue: sun-idrepo-ldapv3-config-user-attributes=sunIdentityServerPPCommonNameFN
sunKeyValue: sun-idrepo-ldapv3-config-auth-naming-attr=uid
<略>
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=tonoki101.to-domain.com:389
<略>
sunKeyValue: sun-idrepo-ldapv3-config-authid=cn=Manager,dc=to-domain,dc=com
```

# 設定変更

- アクセス制御
  - レルム
    - エージェント
      - Web

```
ldapsearch -x -W -D "cn=Directory Manager" -b "dc=opensso,dc=java,dc=net" -h localhost -p 50389 -L ou=apache22agent1
```

```
# apache22agent1, default, OrganizationConfig, 1.0, AgentService, services, o  
pensso.java.net  
dn: ou=apache22agent1,ou=default,ou=OrganizationConfig,ou=1.0,ou=AgentService,ou=services,dc=opensso,dc=java,dc=net  
objectClass: sunServiceComponent  
objectClass: top  
ou: apache22agent1  
sunKeyValue: com.sun.identity.agents.config.replaypasswd.key=  
sunKeyValue: com.sun.identity.agents.config.iis.owa.enable.session.timeout.url =  
sunKeyValue: com.sun.identity.agents.config.encode.url.special.chars.enable=false  
sunKeyValue: com.sun.identity.agents.config.domino.ltpa.enable=false  
sunKeyValue: com.sun.identity.agents.config.notenforced.url=[2]=http://tonoki102.to-domain.com:80/test/*
```

# 設定の変更

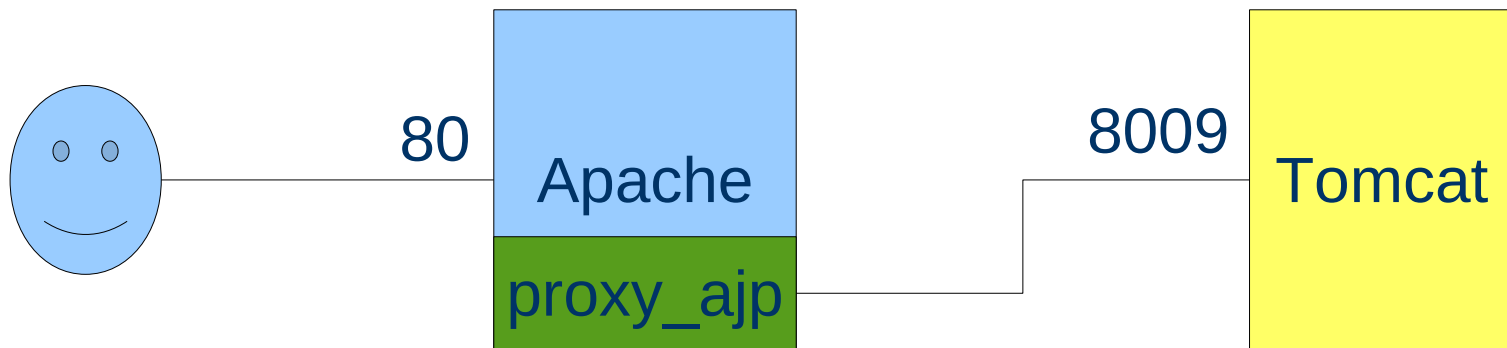
- 連携
  - トラストサークルの作成

```
# TestCOT, default, OrganizationConfig, 1.0, sunFMCOTConfigService, services, opensso.java.net
dn:
ou=TestCOT,ou=default,ou=OrganizationConfig,ou=1.0,ou=sunFMCOTConfigService,ou=services,dc=opensso,dc=java,dc=net
objectClass: sunServiceComponent
objectClass: top
ou: TestCOT
sunKeyValue: sun-fm-cot-status=active
sunKeyValue: sun-fm-cot-description=
sunKeyValue: sun-fm-trusted-providers=http://tonoki102.to-domain.com:8080/opensso|saml2
sunserviceID: cot
sunsmspriority: 0
```

# おまけ1

- Apacheとの連携

- /etc/httpd/conf.d/proxy\_ajp.confに以下記載
- ProxyPass /examples/ ajp://localhost:8009/jsp-examples/
- Apacheとtomcatはajpポート8009を使って通信するのでtomcatの8080は停止しても良い。
- Tomcatを直接外部へ晒さない。



## おまけ2

- Apache にweb Agentを入れリバースプロキシにする場合は。。。apache-tomcatが同一ホストではajp\_proxyを使えない

エージェントのOpenssoへのポリシー確認アクセスがグループ

httpスレッドマックス！

