

# Installazione di Shibboleth IdP v.3.4

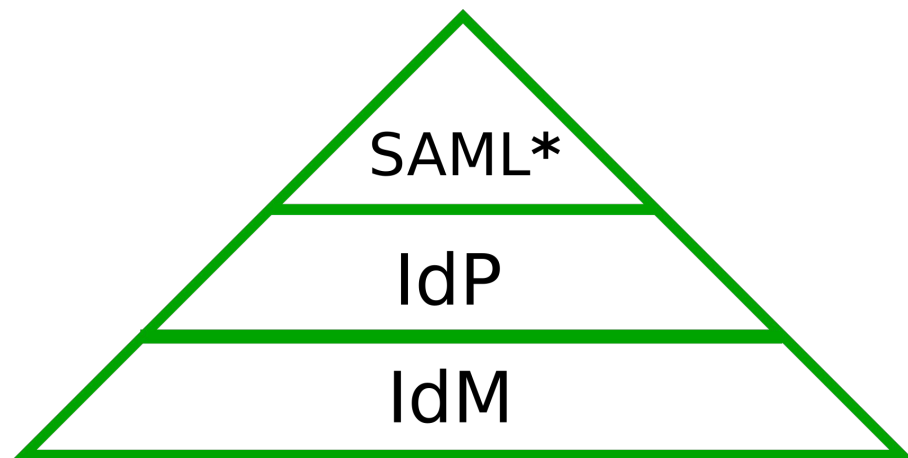
## Introduzione

Corso Shibboleth IdP - 22-23/01/2020

Giuseppe De Marco - [giuseppe.demarco@unical.it](mailto:giuseppe.demarco@unical.it)

# Obiettivi del Corso

1. Conoscenze di base di **IAM**
2. Realizzazione di uno Shibboleth Identity Provider (**IdP**)
3. Introduzione a **SAML2**
4. Utilizzo di **IDEM Registry**
5. Introduzione alle federazioni multilaterali **R&S**
6. Configurazioni note e casi comuni, condivisione esperienze



Identity & Access Management (IAM)

*\*data exchange format (SAML2, OAuth2, OIDC ...)*

# Corso, prima parte - 9:30 / 12:30

- Uso di un'installazione dimostrativa di OpenLDAP con schemi Educational (eduPerson e SCHAC), PPolicy e altri moduli/overlay;
- Un'installazione dimostrativa di Shibboleth IdP 3.4.x (latest);
- Uso di un'installazione dimostrativa di Shibboleth SP 3.

Ambiente operativo: **Debian 10 (buster)**

Materiale didattico:

1. Idem-tutorials: <https://github.com/ConsortiumGARR/idem-tutorials>
2. Idem-playbook: <https://github.com/ConsortiumGARR/Ansible-Shibboleth-IDP-SP-Debian>
3. slapd-playbook: <https://github.com/ConsortiumGARR/ansible-slapd-eduperson2016>
4. GIT Repository: <http://tiny.cc/idem-course>

# Idem-tutorials e playbook

## Idem-tutorials (fonte ufficiale)

1. Sempre aggiornati
2. Descrive setup ShibIdP
3. Richiede circa 4 ore (mezza giornata)
4. Trasparente, aiuta a comprendere i passaggi e le componenti

## Playbook (utilità)

1. Aggiornati occasionalmente
2. ShibIdP con SP di test
3. Richiede 10 minuti
4. Automatico, consigliabile per tests, migrazioni e prototipazioni veloci

# Strumenti utilizzati nel corso

1. VM di test ... server di esempio per ogni partecipante
2. ssh ... connessioni remote al server di esempio
3. Editor di testo ... modifica dei file .properties e .xml
4. ldapsearch ... LDAP client, accesso ai dati (*slapcat -n1*)
5. diff (meld) ... visualizza le differenze tra file
6. git ... storico ed avanzamento della configurazione
7. [aacli](#) ... test di risoluzione e rilascio degli attributi

# Rapido glossario

## SAML2

Standard per lo scambio di dati di autenticazione e autorizzazione (dette asserzioni) tra IdP/SP

## Metadata

Informazioni descrittivo/funzionali di una o più entità (*entityID*)

entityID

Identificativo univoco assegnato ad una entità (IdP, SP o AA)

IdP

Autentica gli utenti a seguito delle richieste (*authn*) degli SP

SP

Servizio web che delega l'autenticazione presso un IdP SAML

NameID

Identificativo univoco di un soggetto (utente) in una sessione

WAYF/DS

Risorsa interna/esterna usata da un SP per selezionare un IdP

Servlet

Container

Contesto HTTP di esecuzione programmi Java (**Jetty**)

# Primo accesso al server: ssh ...

In /etc/hosts: **90.147.x.y shib-sp.aai-test.garr.it shib-idp.aai-test.garr.it**

---

/opt/jetty	... path di installazione di Jetty Servlet Container
/opt/shibboleth-idp	... path di installazione di Shibboleth IdP
/etc/shibboleth	... path di configurazione di Shib SP ( <u>opzionale</u> )

---

## *Primi quesiti*

Come si installa Shibboleth IdP?

1. Come si (ri)avvia Shibboleth IdP?
  - a. */etc/init.d/jetty restart*
  - b. *systemctl restart jetty*
  - c. *touch /opt/jetty/webapps/idp.xml*
2. Visione dei logs (*/opt/shibboleth/logs* e */var/log/jetty/logs*)

# Installazione di ShibIdP - ingredienti

1. Download/installazione Java JDK (suggerito: [Amazon Corretto 1.8](#))
2. [Installazione dipendenze](#) Jetty/Spring/ShibIdP
3. Compilare ed installare Jetty (se si usa Tomcat: pacchetti di sistema)
4. [Scaricare](#) e decomprimere Shibboleth Identity Provider [3.4.x](#)
5. Eseguire l'installazione di Shibboleth IdP:

```
root@idp:/usr/local/src/shibboleth-identity-provider-3.4.x# ./bin/install.sh
```

```
Source (Distribution) Directory: [/usr/local/src/shibboleth-identity-provider-3.4.x]
```

```
Installation Directory: [/opt/shibboleth-idp]
```

```
Hostname: [shib-idp.aai-test.garr.it]
```

```
SAML EntityID: [https://shib-idp.aai-test.garr.it/idp/shibboleth]
```

```
Attribute Scope: [garr.it]
```

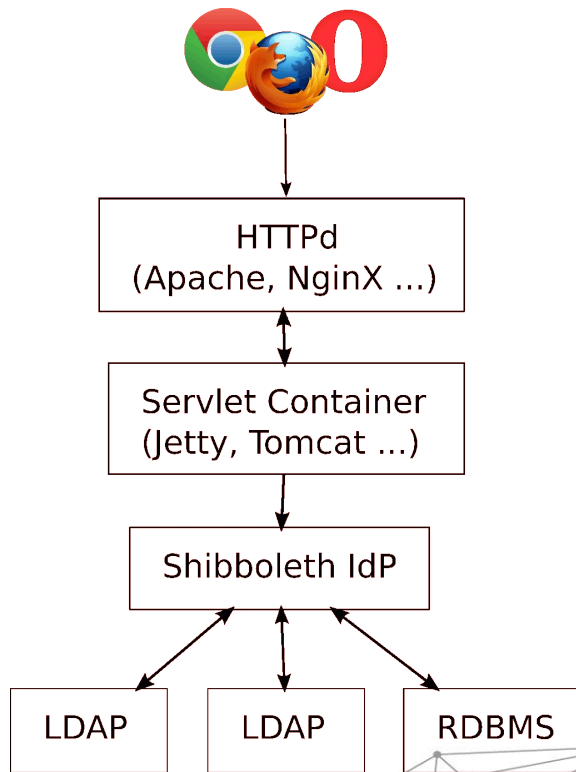
```
Backchannel PKCS12 Password: ###PASSWORD-FOR-BACKCHANNEL### (re-enter password)
```

```
Cookie Encryption Key Password: ###PASSWORD-FOR-COOKIE-ENCRYPTION### (re-enter password)
```



# Shibboleth IdP - deployment

1. Certificati TLS/SSL richiesti (DigiCERT)
2. Reverse Proxy HTTPd o bilanciatore (HAProxy, NginX ...)
3. Jetty, Tomcat ...
4. Shibboleth IdP
5. Data Store, fonti di dati afferenti all' Identity Management



# Struttura di /opt/shibboleth-idp (aka {idp.home})

conf/	file di configurazione in formato properties (simil yml) e xml
metadata/*	metadati in formato xml (SAML2 md)
credentials/	certificati di firma e criptazione, certificato ldap
logs/*	logs di Shibboleth, configurabili in <i>conf/logback.xml</i>
views/	template html (.vm) la loro modifica non richiede riavvio
edit-webapp/	fogli di stile e js, la modifica richiede l'esecuzione di <i>/opt/shibboleth-idp/bin/build.sh</i> ed il riavvio dell' IdP
messages/	messaggi e localizzazione del software, modificare message.properties oppure aggiungere nuovi (conf/services.xml)

# /opt/shibboleth-idp/logs

idp-audit.log	... request/response da e verso user-agents
idp-consent-audit.log	... messaggi sul consenso al trattamento dei dati
idp-process.log	... messaggi generali di funzionamento sistema
idp-warn.log	... messaggi diagnostici di allerta del sistema

Possono essere configurati in {idp.home}/conf/logback.xml

Guida: <https://wiki.shibboleth.net/confluence/display/IDP30/LoggingConfiguration>

# /opt/shibboleth-idp/conf

ldap.properties	Configurazione connessione LDAP
idp.properties	Variabili di configurazione di base dell'IdP
services.xml	Risorse/Servizi avviati con l'IdP
<a href="#">attribute-resolver</a>	definizione, costruzione, codifica degli Attributi
<a href="#">attribute-filter</a>	Attributi da rilasciare, per relying-party (SP)
<a href="#">metadata-providers</a>	definizione delle fonti di metadata (directory, web)
global.xml	Definizioni (Spring beans) visibili globalmente
saml-nameid.properties	Proprietà generali sulla produzione del <a href="#">NameID</a>
saml-nameid.xml	Ulteriori personalizzazioni e controlli del <a href="#">NameID</a>
relying-party.xml	Configurazioni specializzate per SP

# /opt/shibboleth-idp/metadata

idp-metadata.xml

Metadati dell'IdP, visionabili presso:

<https://shib-idp.aai-test.garr.it/idp/shibboleth>

Ricordiamoci di:

1. rimuovere 'validUntil=["TZ0-9\.\-:\:]+'
2. rimuovere :8443 (SAML1)

Esempio di metadata di produzione:

<https://garr-idp-prod.irccs.garr.it/idp/shibboleth>

# Usare git (conclusione primo slot)

git log	lista dei commit effettuati
git branch	lista dei branch attivi
git stash	undo di tutte le modifiche non committate
git checkout \$branchname	cambio branch
git diff [\$branchname]	diff di tutte le modifiche non committate o delle differenze rispetto ad un branch
<hr/>	
<b>AGGIORNAMENTI DELL'ALBERO</b>	
git status	lista delle modifiche non committate
git add -A	aggiunta di nuovi file nelle modifiche
git commit -am 'descrizione'	commit, rende le modifiche permanenti

# Domande?

[marco.malavolti@garr.it](mailto:marco.malavolti@garr.it)  
[giuseppe.demarco@unical.it](mailto:giuseppe.demarco@unical.it)  
[maurizio.festi@unitn.it](mailto:maurizio.festi@unitn.it)