

Shibboleth IdP v3 è End Of Life! e ora?

SERVIZIO IDEM GARR AAI

Marco Malavolti

Barbara Monticini

Davide Vaghetti

Migrare a Shibboleth IdP versione 4

28-29-30 Ottobre 2020

Agenda

1. Verifica degli esercizi dati + Domande sorte
2. Analisi dei casi più significativi inviati
3. Installazione Shibboleth IdP v4.x (Breve)
4. Configurazione e Migrazione
5. Esercizi a casa

Esercizi

1. Analizzare la configurazione installata per il proprio IdP v3 annotando eventuali criticità per una migrazione (attributi dinamici, chaining, attribute definition, data connector, ecc.)
2. Preparare un archivio contenente tutti i file necessari per la migrazione dell'IdP e depositarlo sulla nuova VM che ospiterà il nuovo IdP v4.x.y
3. Segnalateci tutti i dubbi e gli eventuali problemi incontrati a <idem-ws2020@garr.it>



OBIETTIVO DEL GIORNO


Installare e Configurare un Identity Provider Shibboleth V4 funzionante con rilascio del "persistent" e del "transient" NameID, di eduPersonTargetedID e di tutti gli attributi reperibili direttamente/senza script dal proprio Directory Service (LDAP/AD) come indicato negli IDEM Tutorials

Premessa

Le slide fanno riferimento ai seguenti HOWTO di Installazione e Configurazione distribuiti dal Servizio IDEM GARR AAI:

1. [HOWTO Install and Configure a Shibboleth IdP v4.x on Debian-Ubuntu Linux with Apache2 + Jetty9](#)
2. [HOWTO Install and Configure a Shibboleth IdP v4.x on CentOS with Apache2 + Jetty9](#)

Indicazioni per una corretta lettura delle slide

1. Aprire la presentazione con **FireFox**:
Chrome non gestisce bene gli anchor link inseriti agli IDEM Tutorials
2. I file e le cartelle sono indicate col colore arancione scuro
3. Le raccomandazioni del Servizio IDEM GARR AAI sono in verde scuro
4. L'icona  indica che il docente si sposterà sul terminale di un vero IdP

Installazione Shibboleth IdP (in breve)

- Caricare quanto necessario alla migrazione sulla nuova macchina per l'IdP in una cartella di appoggio (e.g.: `/var/local/backups` o `/home/<nomeutente>`)
- [Installare i pacchetti richiesti e Amazon Corretto JDK](#)
- [Configurare l'environment della nuova macchina IdP:](#)
 - `JAVA_HOME`
 - `/etc/hosts` (inserire il FQDN dell'idp di produzione al posto di quello della macchina)

Installazione Shibboleth IdP (in breve)

- [Installare Shibboleth IdP v4.X.Y](#)
inserendo 'entityID' e 'scope' dell'IdP in Produzione:

```
bash /usr/local/src/shibboleth-identity-provider-4.X.Y/bin/install.sh  
-Didp.host.name=$(hostname -f) -Didp.keysize=3072
```

```
Buildfile: /usr/local/src/shibboleth-identity-provider-4.x.y/bin/build.xml
```

```
install:
```

```
Source (Distribution) Directory (press <enter> to accept default):  
[/usr/local/src/shibboleth-identity-provider-4.x.y] ?
```

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

```
Backchannel PKCS12 Password: ###PASSWORD-FOR-BACKCHANNEL###
```

```
Cookie Encryption Key Password: ###PASSWORD-FOR-COOKIE-ENCRYPTION###
```

```
SAML EntityID: [https://idp.example.org/idp/shibboleth] ?
```

```
Attribute Scope: [example.org] ?
```

Installazione Shibboleth IdP (in breve)

- [Installare il Java Servlet Container Jetty e configurarlo](#)
- [Attribuire la giusta ownership alle cartelle di Shibboleth](#)
- Caricare il certificato e la chiave server (HTTPS) dell'IdP in produzione nelle opportune cartelle della nuova macchina
- [Configurare Apache Web Server \(front-end di Jetty\) facendo attenzione nel riportare le proprie personalizzazioni](#)

Configurazione e Migrazione

1. Sostituire, dopo averne salvata una copia, la cartella `"/opt/shibboleth-idp/credentials"` con quella presa dall'IdP di produzione
2. Configurare la gestione dei dati relativi ai consensi e alle sessioni degli utenti, scegliendo la Strategia utilizzata per l'IdP in produzione:
 - a. Strategia A: per chi non ha usato un database
 - b. Strategy B: per chi usa un database (la tabella StorageRecords non ha subito modifiche rispetto a quella usata dalla V3 e può essere importata adattando i passi indicati dall'HOWTO alla voce "[Appendix D: ...](#)")

Configurazione e Migrazione

3. Configurare il collegamento al Directory Service:

a. In chiaro:



- i. configurare la connessione alla Directory Service in `ldap.properties` prendendo come riferimento quanto fatto per l'IdP in produzione e indicare gli attributi recuperabili direttamente dalla Directory (`exportAttributes`)

b. Cifrato:

- i. aprire la porta 389(STARTTLS) o 636(TLS) verso l'IdP
- ii. caricare il certificato in:
`/opt/shibboleth-idp/credentials/ldap-server.crt`
e assegnargli come owner l'utente 'jetty'
(Servlet Container che esegue l'applicazione "`idp.war`")
- iii. configurare la connessione alla Directory Service in `ldap.properties` prendendo come riferimento quanto fatto per l'IdP in produzione e indicare gli attributi recuperabili direttamente dalla Directory (`exportAttributes`)

Configurazione e Migrazione

4. [Configurare il rilascio del persistent NameID scegliendo la Strategia utilizzata dall'IdP in produzione:](#)
 - a. Strategia A: per chi non ha usato un database (raccomandata e di default)
 - b. Strategy B: con l'uso di un database (la tabella 'shibpid' non ha subito modifiche rispetto a quella usata dalla V3 e può essere importata seguendo i passi indicati dall'HOWTO alla voce "[Appendix D: ...](#)")



5. Ripristinare il valore del salt in `credentials/secrets.properties` e i valori di sourceAttribute e di encoding in `conf/saml-nameid.properties`



6. [Configurare un attribute-resolver.xml di base \(distribuito da IDEM\)](#)

Configurazione e Migrazione



7. [Configurare il rilascio di eduPersonTargetedID seguendo la Strategia \(A o B\) usata per il persistent NameID da cui prenderà il valore.](#)

Dato che eduPersonTargetedID **NON** è definito nel file `eduPerson.xml` introdotto con l'AttributeRegistry perchè **DEPRECATO**, è necessario definirlo attraverso un file `eduPersonTargetedID.properties`

```
# eduPersonTargetedID

id=eduPersonTargetedID
transcoder=SAML2XMLObjectTranscoder
saml2.name=urn:oid:1.3.6.1.4.1.5923.1.1.1.10
displayName.en=Opaque per-service identifier eduPersonTargetedID
displayName.it=Identificatore opaco diverso per ogni servizio eduPersonTargetedID
description.en=Opaque per-service identifier eduPersonTargetedID
description.it=Identificatore opaco diverso per ogni servizio eduPersonTargetedID
saml1.encodeType=false
```

Configurazione e Migrazione



8. Aggiungere "SCHAC" all'Attribute Registry per la risoluzione dei suoi attributi

```
<bean parent="shibboleth.TranscodingProperties">
  <property name="properties">
    <props merge="true">
      <prop key="id">schacHomeOrganization</prop>
      <prop key="transcoder">SAML2StringTranscoder SAML1StringTranscoder</prop>
      <prop key="saml2.name">urn:oid:1.3.6.1.4.1.25178.1.2.9</prop>
      <prop key="saml1.name">urn:schac:attribute-def:schacHomeOrganization</prop>
      <prop key="displayName.en">Institution Domain</prop>
      <prop key="displayName.it">Dominio istituzione</prop>
      <prop key="description.en">Domain of the institution</prop>
      <prop key="description.it">Dominio dell'istituzione</prop>
    </props>
  </property>
</bean>
```

9. Configurare i log dell'IdP per la visualizzazione degli errori di autenticazione

Configurazione e Migrazione

10. Aggiungere la lingua italiana tra quelle supportate dall'IdP per una migliore esperienza utente:
 - Se sono stati aggiunti in produzione dei file *.properties* alla cartella "**messages/**" è necessario riportare non solo i file, ma anche eventuali cambiamenti alla lista "**shibboleth.MessageSourceResources**" presente in "**conf/services.xml**"
11. Ripristinare i metadata dell'IdP in produzione copiando il contenuto di "**/opt/shibboleth-idp/metadata/idp-metadata.xml**" nel nuovo IdP

Configurazione e Migrazione



12. [Mettere al sicuro i cookies e altri dati utilizzati dall'IdP \(sealer.kver\)](#)



13. Configurare l'IdP per l'utilizzo dei filtri distribuiti da IDEM:
- a. [IDEM Default Resources ARP:](#) per IDEM Entity Registry & Test SPs questo filtro rilascia ePTID solo se richiesto (isRequired='true')
 - b. [IDEM Required ARP:](#) per il rilascio dei soli attributi necessari agli SP
 - c. [Special Resources ARP:](#) per SP con restrizioni sui valori degli attributi
 - d. [IDEM Entity Category ARP:](#) per SP che implementano le Entity Category
14. Scaricare il certificato della Federazione IDEM e configurare
"/opt/shibboleth-idp/conf/metadata-providers.xml" per consumare gli
stessi stream di metadata presenti nell'IdP in produzione: edugain2idem + altri

Configurazione e Migrazione

15. Ripristinare la Login Page `/opt/shibboleth-idp/views/login.vm` con quello dell'IdP in produzione



16. Abilitare il CSRF protection sulla Login Page:

- `/opt/shibboleth-idp/conf/idp.properties:`
 - i. `idp.csrf.enabled = "true"`
- `/opt/shibboleth-idp/views/login.vm:`
 - i. `#parse("csrf/csrf.vm")`

Sotto `<form action="$flowExecutionUrl" method="post">`

!WARNING!

Se abilitato e non inserito nella `"login.vm"` l'autenticazione non funziona!

17. Tutti i cookie dell'IdP sono trasmessi via SSL/TLS (`conf/idp.properties`):
 - `idp.cookie.secure = 'true'`

Conclusioni

- Riavviare Jetty per applicare tutte le modifiche e controllare i log (`logs/idp-process.log`) se il riavvio non avesse esito positivo
- Inserire nell' `/etc/hosts` del vostro PC la seguente linea:
 - `IP.IDP.V4.NEW full.qualified.domain.name.idpV3prod`



- Provare il funzionamento:
 - Dal proprio PC:
Provare l'accesso a un risorsa in IDEM attraverso il browser web
 - Dalla VM del nuovo IdP V4:
 - `sudo export JAVA_HOME= ...`
 - `bash /opt/shibboleth-idp/bin/aaccli.sh -n <USERNAME> -r https://sp-demo.idem.garr.it/shibboleth --saml2`

Esercizi per casa

Migrare a Shibboleth V4



Esercizi

1. Installare Shibboleth IdP V4 sulla nuova macchina seguendo l' HOWTO e le slide
2. Ripristinare i <MetadataProvider> e verificarne il funzionamento
3. Analizzare il seguente attribute-resolver contenente la definizione di diversi attributi generati in modo dinamico e segnalare cosa non è chiaro:
 - [Attribute Resolver Dinamico IdP V4](#)

Esercizi

4. Ripristinare i filtri già in uso **adattandoli** per lo Shibboleth IdP V4 (prendendo spunto da quelli forniti da IDEM) ricordandosi che "ignoreCase" è stato sostituito da "caseSensitive" e che gli attributeID sono quelli uscenti da LDAP/AD:

- email (V3) => mail (V4)
- commonName (V3) => cn (V4)
- surname (V3) => sn (V4)

e testare il funzionamento con AACLI per tutte le risorse che non necessitano di ulteriori modifiche alla configurazione dell'IdP

CONSIGLIO:

utilizzare il già disponibile file "[attribute-filter.xml](#)" per tutti gli SP interni

5. Analizzare il seguente filtro e comprendere quali risorse soddisfa e perchè:
- [attribute-filter-v4-idem.xml](#)
6. Configurare il proprio IdP per rilasciare a "sp-demo.idem.garr.it" l'attributo inventato "role" preso da un database: [README da seguire](#)



Strumenti Utili

1. Cartella condivisa:

- <https://gbox.garr.it/garrbox/index.php/s/4EbO3vnzACZPcj2>

2. Mailing List Docenti:

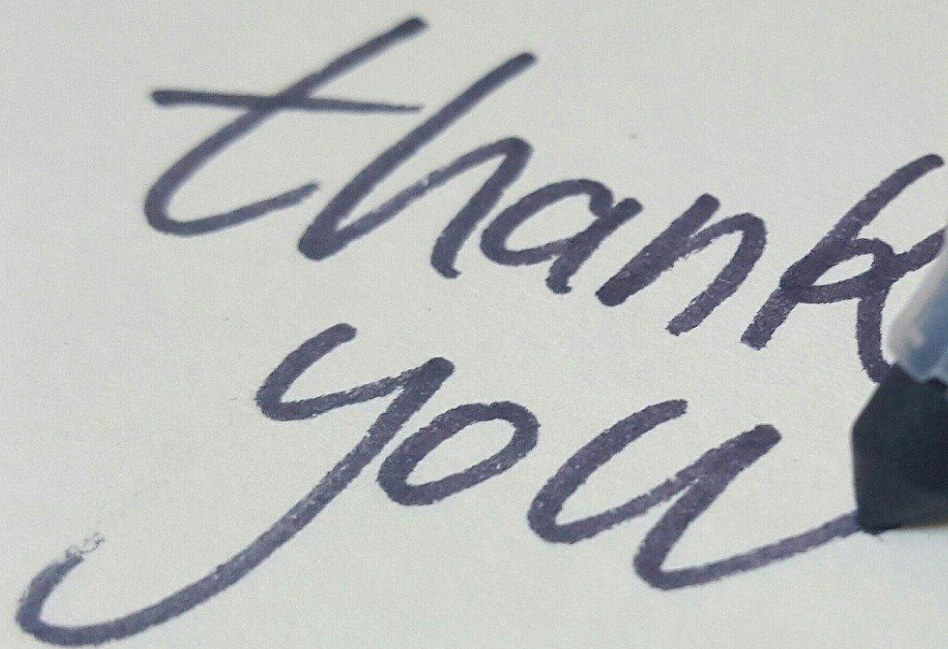
- idem-ws2020@garr.it

3. Repository GitHub:

- <https://github.com/ConsortiumGARR/idem-shib-idp-course>

4. IDEM Tutorials:

- <https://github.com/ConsortiumGARR/idem-tutorials>



thank
you