

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
2. Analisi domande inviate e analisi dei casi più significativi
3. Comparazione e Approfondimento delle ARP distribuite da IDEM
4. Esempi di SP complessi: Google Suite & Microsoft Office 365
5. Recap conclusivo

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

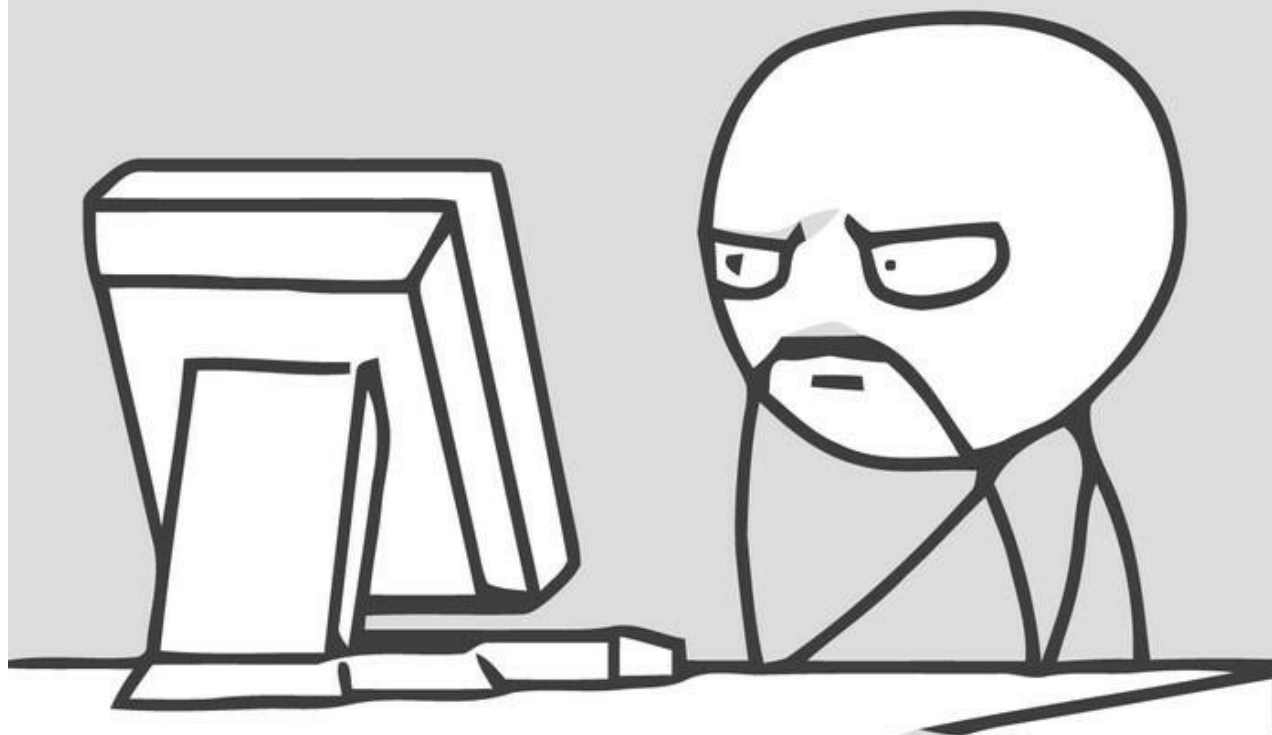
CONSIGLIO:

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](#)



PRONTI?

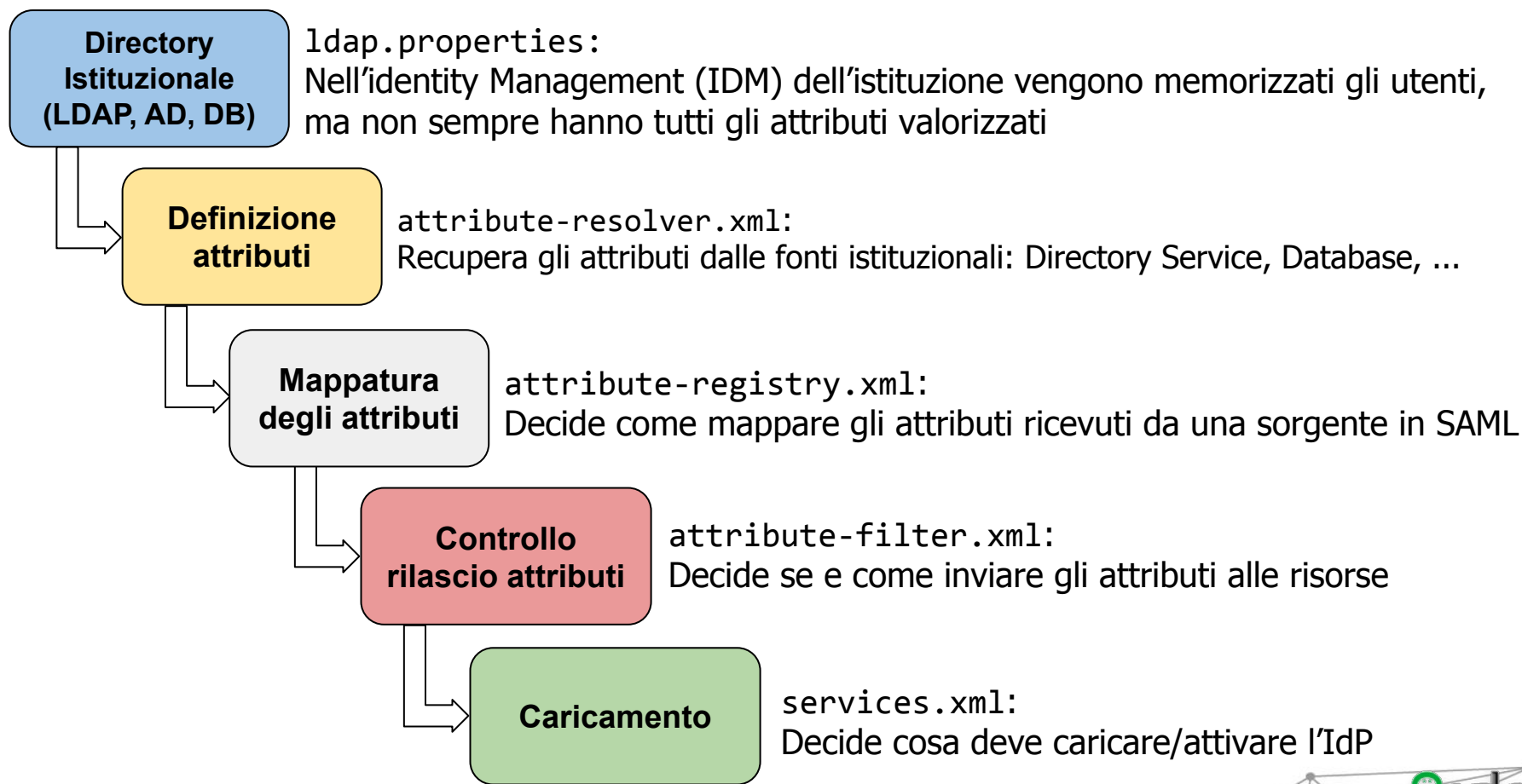


OBIETTIVO DEL GIORNO

Consolidare i contenuti trattati nei giorni precedenti approfondendo le regole che stabiliscono il rilascio degli attributi e analizzare alcuni casi complessi di interesse generale

Attribute Release Policy (con Attribute Registry)

La Politica per il rilascio degli attributi è il modo con cui un IdP decide **cosa, come e a chi rilasciare gli attributi** dei suoi utenti e prevede:



Confronto delle ARP fornite da IDEM

Shibboleth IdP V3	Shibboleth IdP V4
<u>IDEM Default Resources</u>	<u>IDEM Default Resources</u>
<u>IDEM Required</u>	<u>IDEM Required</u>
<u>IDEM Entity Category Resources</u>	<u>IDEM Entity Category Resources</u>
	<u>IDEM Special Resources</u> (NEW)
<u>IDEM Requested</u>	<u>IDEM Requested</u> (NEW)

Google Suite

Microsoft Office 365

Cosa abbiamo imparato (Recap)

- Che dobbiamo modificare eventuali script per la raccolta delle statistiche sugli accessi basati sull'idp-audit.log perchè il numero dei campi e i valori sono cambiati o riportare la sua forma a come era prima
- Che è migliorata la sicurezza per l'autenticazione utente grazie alla protezione contro il Cross-Site Request Forgery abilitata di default
- Che sono stati risolti i problemi legati ai <TAG> vuoti inseriti nei metadata che rompevano il funzionamento dell'IdP

Cosa abbiamo imparato (Recap)

- Che le asserzioni vengono cifrate con l'algoritmo "**AES128-GCM**" di default e che ciò potrebbe comportare problemi di autenticazione sugli SP che non espongono gli algoritmi di cifratura supportati nei metadata

AES128-CBC è insicuro e in alcuni casi permette la decriptazione delle asserzioni contenenti i dati utente, quindi la scelta di Shibboleth di usare un diverso algoritmo di criptazione per le asserzione è dettato dalla volontà di fornire un sistema sicuro. Se nei metadata del SP non è specificato l'<EncryptionMethod> per il precedente algoritmo "AES128-CBC":

```
<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
```

le asserzioni a lui inviate saranno criptate con:

```
<EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
```

Per i Service Provider che non dovessero supportare AES128-GCM è possibile forzare l'utilizzo di AES128-CBC tramite una lista di eccezioni: [AlgorithmFilter-Examples](#)

Se invece volete fare un override dalla politica di default e disabilitare AES128-GCM, commentate il parametro 'idp.encryption.config' in '[conf/idp.properties](#)' e riavviare Jetty/Tomcat

Cosa abbiamo imparato (Recap)

- [AttributeRegistry](#) (controlla il modo in cui gli IdPAttribute interni vengono rappresentati in SAML, CAS e nel futuro OpenID Connect):
 - implementato come soluzione a:
 - proxying di attributi provenienti da fonti esterne
 - mappatura di dati come <RequestedAttribute> dei metadata
 - <AttributeDefinition> di tipo "Simple"
 - **!WARNING!**
Usare contemporaneamente <AttributeDefinition> (con <AttributeEncoder>) e AttributeRegistry causa un rilascio doppio degli attributi !!!
 - La codifica degli attributi avviene con i nuovi Transcoder Types:
 - SAML2StringAttributeTranscoder,
 - SAML2ScopedStringAttributeTranscoder,
 - SAML2ByteAttributeTranscoder,
 - SAML2XMLObjectAttributeTranscoder

Cosa abbiamo imparato (Recap)

- Che l'attributeID usato nei filtri per il rilascio degli attributi assume il valore degli identificativi (id) definiti dall'AttributeRegistry che a sua volta segue la nomenclatura fornita dagli standard (schema)
- Che la direzione di Shibboleth è quella di incentivare il logout e disincentivare l'uso di SAML V1 (deprecato e insicuro) e SAML2 AttributeQuery
- Che possiamo usare l'IdP come SAML Proxy senza aver bisogno della parte SP (Service Provider)

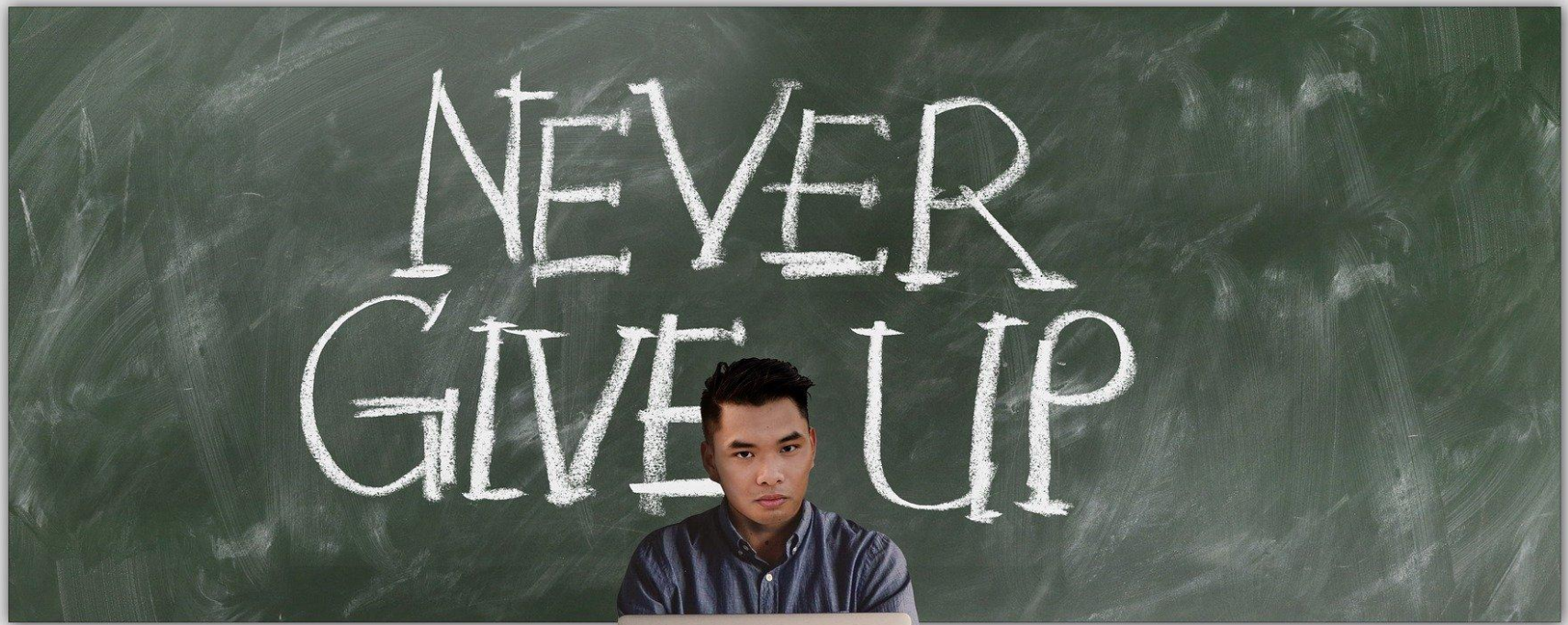
Cosa abbiamo imparato (Recap)

- Che non abbiamo più la necessità di definire attributi “Simple” il cui valore è direttamente reperibile dal Directory Service (LDAP/AD)
- Che il nostro IdP rilascia solo il “transient” NameID sei, nei metadata del Service Provider, viene inserito il <NameIDFormat>:

`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`

- Che il filtro per il rilascio degli attributi (attribute-filter) è cambiato, anche se di poco
- Che per aggiornare un IdP in produzione non è necessario interrompere bruscamente il servizio

idem-ws2020@garr.it



Materiali Utili

1. Repository GitHub:

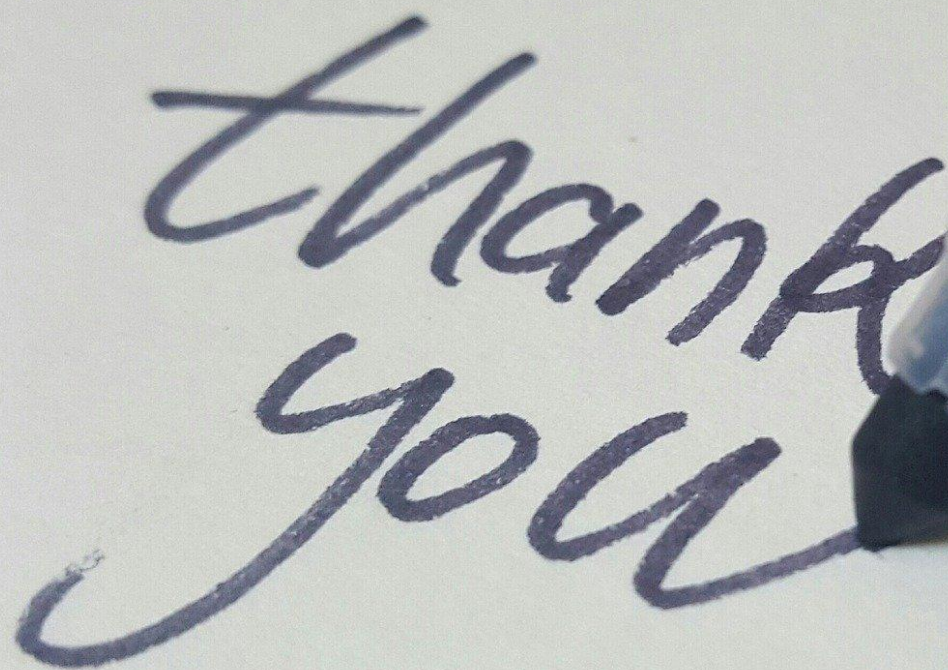
- <https://github.com/ConsortiumGARR/idem-shib-idp-course>

2. IDEM Tutorials:

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

3. IDEM Wiki:

- <https://wiki.idem.garr.it>



thank
you