

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

Docente

- **Nome:**

Marco Malavolti

- **Ruolo:**

IDEM Help &
Development/Operations

- **Hobby:**

Improvvisazione Teatrale



Andate su <https://menti.com/>

e inserite il codice: **20 14 44 5**

OBIETTIVO DEL GIORNO

Conoscere le novità e le modifiche introdotte dalla nuova versione di Shibboleth Identity Provider V4 e prepararsi adeguatamente alla migrazione

Indicazioni per una corretta lettura delle slide

- 1. I file e le cartelle sono indicate con il colore arancione scuro**

A dicembre 2020...



PER FARE DOMANDE

Andate su <https://menti.com/>

e inserite il codice: **12 66 75 5**

News

Shibboleth IdP versione 4 - NEWS

- Imposta la trasmissione dei Cookie via SSL/TLS di default
- Il formato dei log inseriti in `log/idp-audit.log` è cambiato e sono stati aggiunti i seguenti campi:
 - Generici: **ST** (Timestamp for start of flow), **DEST** (Destination URL of outgoing msg), **ROP** (Requested authentication operator), **RPRIN** (Requested authentication principals),
 - SAML: **SPQ** (NameID SPNameQualifier), **pf** (NameIDPolicy required format), **PSPQ** (NameIDPolicy required SPNameQualifier), **XX** (Signed inbound messages), **XA** (Encryption algorithm)
 - Il timestamp del record (%T) ora riporta l'intero date/time: 2020-10-15T13:33:58.510242Z e non più 20201015T133358Z
 - Il formato del tempo è modificabile in "`conf/audit.xml`" alla voce "`shibboleth.AuditDateTimeFormat`", mentre la voce "`shibboleth.AuditFormattingMap`" permette di modificare i campi inseriti nella linea scritta nel log

Shibboleth IdP versione 4 - NEWS

- Incentivata la propagazione del SAML Logout
- Rimossi i profili a supporto di SAML 1.1 e di SAML 2.0 AttributeQuery tra quelli abilitati di default nel **relying-party.xml**
- Cross-Site Request Forgery ([CSRF](#)) Protection abilitato di default
- **! WARNING !**
L'algoritmo di criptazione delle asserzioni predefinito è passato da "AES128-CBC" a "**AES128-GCM**". Tutti gli SP che non espongono gli algoritmi di criptazione nei metadata, riceveranno asserzioni criptate con tale algoritmo e potrebbero fallire la loro decrittazione e, quindi, l'autenticazione utente

Shibboleth IdP versione 4 - NEWS

- La presenza nei metadata dei tag quali: `<md:ServiceName/>`, `<md:ServiceDescription/>` o figli vuoti di `<md:Organization>` non sono più considerati dai `<MetadataProvider>` configurati in `"metadata-providers.xml"` prevenendo l'insorgere di errori
- Sono stati deprecati i seguenti *built-in* `<bean>` per un bug di Spring non risolto (se usati generano dei Warning. Rimossi nella V5):
 - `shibboleth.NonCachingHttpClient`
 - `shibboleth.FileCachingHttpClient`
 - `shibboleth.MemoryCachingHttpClient`

al loro posto sono nati:

- `shibboleth.HttpClientFactory`
- `shibboleth.FileCachingHttpClientFactory`
- `shibboleth.MemoryCachingHttpClientFactory`

Shibboleth IdP versione 4 - NEWS

- L'installer dell'IdP V4 è stato riscritto in Java mantenendo le stesse funzionalità della V3, quindi l'installazione non interattiva (silent-mode) è ancora supportata
- Il [Password Login Flow](#) (default authn flow) ha subito una re-implementazione che ne ha migliorato la flessibilità semplificando l'aggancio dei propri back-end grazie all'implementazione dell'interfaccia [CredentialValidator](#). Flow da adattare se modificato
- Introdotto il nuovo "[SAML proxy login flow](#)" per poter usare l'IdP come SAML proxy. Ciò permette di autenticare un utente mediante un secondo IdP

Andate su <https://menti.com/>

e inserite il codice: **38 56 89 2**

Shibboleth IdP versione 4 - NEWS

- Introdotto il parametro "exportAttributes" nel <DataConnector> "LDAPDirectory" per generare IdPAttribute "Simple" senza la necessità di un <AttributeDefinition>
- L'intestazione di `conf/metadata-providers.xml` è stata aggiornata con nuovi namespaces e nuove location schema per supportare le nuove funzionalità dell'IdP 4
- Tutti i valori temporali utilizzati per LDAP (`ldap.properties`) devono essere convertiti in sintassi ISO (e.g.: Da "2000" a "PT2S") perchè i millisecondo generano un'eccezione di parsing sul DateTime
- Utilizzare funzionalità deprecate e rimosse genera warning nei log



PER FARE DOMANDE

Andate su <https://menti.com/>

e inserite il codice: **12 66 75 5**

Shibboleth IdP versione 4 - NEWS

- [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

Shibboleth IdP versione 4 - NEWS

- `<AttributeEncoders>` privati dell'attributo XML "*friendlyName*" che conteneva il valore dell'attributeID usato nell'attribute-filter
Unica soluzione per riaverlo: usare il nuovo `AttributeRegistry`
- `edu.internet2.middleware.shibboleth.common.attribute.provider.BasicAttribute` - **DEPRECATO** - verrà rimosso completamente nella V5 di Shibboleth IdP.
Sostituito da [ScriptedIdPAttribute](#) e valorizzato con quanto trovato negli `AttributeDefinition/AttributeRegistry`
- Rimosso definitivamente il deprecato `<SourceAttribute>` dal tipo "Template" di `<AttributeDefinition>`.
Enumerare gli attributi sorgente nell' `<InputDataconnector>`
- Nella generazione degli attribute di tipo "Scripted", non è più disponibile il metodo universale `getValue()`, ma è stato sostituito da `getNativeValue()`. Per i valori "scoped" la `getNativeValue()` restituisce una coppia di valori evitando perdite di conversione

Shibboleth IdP versione 4 - NEWS

- **! WARNING !**

Se nei metadata di un Service Provider è presente il NameIDFormat: `"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"` Shibboleth IdP, di default, non considera gli altri NameIDFormat presenti e rilascia il solo transient NameID al Service Provider (SP)

- Nelle `<Rule>` inserite nell'attribute-filter, l'attributo `"ignoreCase"` è stato deprecato in favore di `"caseSensitive"` (default a `'false'`) e `"setIgnoreCase"` passa a `"setCaseSensitive"`.
Usare la versione deprecata produce Warning
- Precluso l'uso di spazi e apici singoli per gli attributeID degli IdPAttribute.
Questo si traduce in: `"non è possibile usare spazi o apici singoli negli identificatori(id) degli attributi definiti con AttributeRegistry"`

Shibboleth IdP versione 4 - NEWS

- JDK pienamente supportati:
 - Amazon Corretto 11 (Linux & Windows) o OpenJDK 11 (Red Hat Enterprise Linux & CentOS 7 and 8)
 - Jetty ≥ 9.4 (raccomandato) o Tomcat ≥ 9

Andate su <https://menti.com/>

e inserite il codice: **37 20 89 6**



Requisiti

Migrare a Shibboleth V4

Requisiti

- Certificati e Chiavi & CA (HTTPS/SSL)
- Contenuto della cartella `/opt/shibboleth-idp`
- Database backups (se sono stati utilizzati)
- Connessione al proprio LDAP/AD funzionante
- Formato username utenti: lowercase, uppercase, mixed
- File vari legati all'interfaccia grafica
- Eventuali personalizzazioni della configurazione di Apache



Requisiti - In dettaglio

- Certificati e Chiavi & CA (HTTPS/SSL)
- IDP Scope
- Contenuto della cartella "**credentials**":
 - **idp-backchannel.crt** , **idp-backchannel.p12** (se utilizzato)
 - **idp-encryption.crt** , **idp-encryption.key**
 - **idp-signing.crt** , **idp-signing.key**
 - **sealer.kver** , **sealer.jks**
- Database backups (se sono stati utilizzati):
 - shibpid (uguale alla V3)
 - StorageRecords (uguale alla V3)
 - Credenziali di accesso (Server, Porta, Username, Password)

Requisiti - In dettaglio

- Connessione al proprio LDAP/AD funzionante:
 - Porta 389/636 aperta verso l'IdP
 - Certificato TLS e contenuto di `conf/ldap.properties`
- Contenuto del file `views/login.vm` e relative dipendenze (immagini, CSS, ...)
- Formato username utenti: lowercase, uppercase, mixed
- Contenuto di "`conf/saml-nameid.properties`":
 - Valore di `idp.persistentId.encoding` (BASE32 o BASE64)
 - Valore di `idp.persistentId.salt`
 - Valore di `idp.persistentId.sourceAttribute`

Requisiti - In dettaglio

- Contenuto di `metadata/idp-metadata.xml`
- Contenuto di `"conf/attribute-resolver*.xml"`
 - Definizione degli attributi dinamici: Scripted, Mapped, Template, ...
- Contenuto degli `"conf/attribute-filter*.xml"` creati per risorse interne o in IDEM
- Contenuto di `"conf/idp.properties"` per recuperare eventuali informazioni non indicate dagli HOWTO diffusi dal Servizio IDEM

Requisiti - In dettaglio

- Contenuto di "`conf/relying-party.xml`" se modificato
- 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`"
- Contenuto di "`conf/global.xml`" se modificato
- Contenuto di "`conf/saml-nameid.xml`" se modificato

Conclusione



Conclusioni

La migrazione a nuova versione di Shibboleth IdP richiede un'attenta valutazione della composizione del proprio ambiente di produzione.

Mantenere il proprio IdP aggiornato nel tempo riduce di molto gli interventi necessari ad una migrazione di versione.

!!! WARNING !!!

- L'algoritmo di criptazione delle asserzioni predefinito è passato da "AES128-CBC" a "**AES128-GCM**". I Service Provider che non dichiarano quali EncryptionMethod supportano riceveranno asserzioni criptate con tale algoritmo.
- Usare contemporaneamente <AttributeDefinition> (con <AttributeEncoder>) e **AttributeRegistry** causa un rilascio doppio degli attributi !!!
- Se nei metadata di un Service Provider è presente il NameIDFormat: "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" Shibboleth IdP, di default, non considera gli altri NameIDFormat presenti e rilascia all'SP il solo transient NameID al Service Provider (SP)

Esercizi per casa

Migrare a Shibboleth V4



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>

Requisiti per il 2° giorno

- Una **nuova macchina virtuale** remota accessibile via terminale/SSH avente le seguenti caratteristiche minime:
 - CPU: **2 Core**
 - RAM: **4 GB**
 - HDD: **20 GB**
 - OS: **Debian 10 / Ubuntu 18.04 o 20.04 / CentOS 7 o 8**
- Accesso all'Identity Provider istituzionale federato in IDEM (produzione)
- Accesso al Directory Service (LDAP/AD) e/o Database relazionali legati all'Identity Provider

Strumenti Utili

1. Cartella condivisa:

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

2. Mailing List Docenti:


- idem-ws2020@garr.it

3. Repository GIT del webinar:

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

4. IDEM Tutorials:

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



thank
you