Autenticazione Esterna Web (Shibboleth)

1 INTRODUZIONE

La maggior parte degli Atenei ha in produzione più applicazioni web che necessitano di autenticazione. WebEsse3 si inserisce in questo contesto come una delle n applicazioni che offrono servizi web agli utenti.

Laddove non vi è un supporto tecnologico e infrastrutturale a modalità di Single Sign On (SSO), all'utente viene chiesto di ripetere l'autenticazione su ogni applicazione web, compresa WebEsse3.

2 OBIETTIVO

Nel corso del 2008 Kion ha messo in piano una evoluzione di prodotto tale da supportare una modalità di autenticazione esterna a WebEsse3.

Il supporto a quei sistemi di SSO nei quali l'autenticazione di diverse applicazioni web è effettuata in un unico punto, esterno alle applicazioni stesse, sarebbe stata una conseguenza diretta di questa evoluzione.

3 RISULTATO

Il risultato ottenuto è stato quindi quello di consentire il deployment di WebEsse3 all'interno di una architettura che prevede un sistema di autenticazione esterno ed in particolare un sistema di SSO.

Per poter far ciò è necessario che il sistema esterno e l'infrastruttura a supporto di esso soddisfino alcuni requisiti di seguito descritti.

4 REQUISITI

4.1 QUALSIASI UTENTE WEB DEVE ESSERE AUTENTICATO ESTERNAMENTE

L'abilitazione dell'autenticazione esterna implica che quasiasi utente appartenente ad un gruppo con accesso su WebEsse3 dovrà effettuare l' autenticazione su sistema esterno. Non è cioè possibile differenziare in base al gruppo, o al singolo utente, se usare l'autenticazione esterna o quella di WebEsse3.

Il requisito corrispondente è:

Non sarà possibile differenziare l'utilizzo del sistema di autenticazione esterno o di quello interno a WebEsse3 in base al gruppo di appartenenza dell'utente. Tutti gli utenti dovranno usare il sistema esterno.

4.2 PROTEZIONE DEGLI URL DI ACCESSO

Tutti gli url delle funzionalità di WebEsse3 che richiedono l'identificazione dell'utente sono stati rimappati sotto il path:

/auth/*

Quindi, per esempio, la pagina dei dati anagrafici dell'utente è raggiungibile tramite l'url:

<host:port>/<ContextPath>**/auth/**studente/Anagrafica/Anagrafica.do

La pagina per il cambio password:

<host:port>/<ContextPath>**/auth/**CambioPasswordForm.do

E chiaramente anche quella della login:

<host:port>/<ContextPath>**/auth/**Logon.do

Il requisito corrispondente è:

Il web server deve intercettare qualsiasi richiesta verso WebEsse3 del tipo:

/auth/*

e, qualora l'utente non sia già stato autenticato, ridirigerlo sul sistema di autenticazione esterno per fargli fare la login, al termine della quale verrà ridiretto sulla risorsa inizialmente richiesta.

4.3 INVIO IDENTIFICATIVO UTENTE TRAMITE REMOTE USER

WebEsse3 deve poter riconoscere l'identificativo dell'utente, nel seguito USER_ID, che accede a risorse protette che vengono identificate tramite il path indicato nel paragrafo precedente.

Affinchè ciò possa avvenire è necessario che, a fronte di tutte queste richieste, venga inviato a WebEsse3 lo USER_ID.

Il requisito corrispondente è:

Per ogni richiesta verso path per i quali è richiesta l'autenticazione deve essere presente nella *"request http"* un header con nome REMOTE_USER (o con nome diverso specificato nel modo descritto al successivo paragrafo 5.2) e con valore lo USER_ID dell'utente autenticato.

4.4 CONDIVISIONE UTENTI

Poichè Esse3, pur in presenza di un sistema di autenticazione esterno, necessita di effettuare comunque una *login applicativa* utilizzando lo USER_ID ottenuto nella modalita descritta al punto precedente, è necessario che sia il sistema esterno sia Esse3 abbiano visibilità degli account che utilizzano questo tipo di autenticazione. Ciò può essere ottenuto condividendo il repository di questi account o adottando procedure di replica sincrona o asincrona.

Non è comunque necessario che Esse3 abbia visibilità delle password di questi account, ma è sufficiente la condivisione/sincronizzazione dello USER_ID.

Inoltre è necessario che in Esse3 siano state popolate le anagrafiche di questi account, altrimenti nel momento dell'accesso a WebEsse3 non sarà possibile caricare i dati dell'utente, impedendogli di fatto l'utilizzo delle funzionalità di WebEsse3.

Il requisito corrispondente è:

Il repository degli utenti utilizzato dal sistema di autenticazione esterno deve essero lo stesso utilizzato per la login applicativa di Esse3, eventualmente configurando quest'ultimo. In alternativa è possibile predisporre delle procedure di replica sincrona o asincrona tra i due repository, verificando in sede di progetto le modalità e gli eventuali costi di implementazione.

5 CONFIGURAZIONI

5.1 CONFIGURAZIONE DEL SERVLET CONTAINER TOMCAT

Affinchè il servlet container Tomcat non intercetti, sovrascrivendolo, il valore del REMOTE_USER aggiunto dal web server alla *"request http"*, è necessario modificare un file di configurazione.

NB: è necessario effettuare lo stop di Tomcat

La configurazione corrispondente è:

Il file di configurazione di Tomcat conf/server.xml deve essere modificato nella definizione del *"connector AJP"* per aggiungere l'attributo tomcatAuthentication con valore false.

Esempio relativo al file server.xml distribuito con tomcat 6.0.26:

<!-- Define an AJP 1.3 Connector on port 8009 -->

<Connector port="8009" redirectPort="8443" protocol="AJP/1.3" **tomcatAuthentication="false"**/>

5.2 CONFIGURAZIONE DEL CONTESTO DELLA WEB APPLICATION

Affinchè la web application WebEsse3 si predisponga per accettare l'autenticazione esterna e per recuperare, dalla *"request http"*, lo USER_ID di ogni richiesta effettuata verso una risorsa protetta da autenticazione, è necessario impostare una proprietà, ExternalAuth, sul file descrittore del contesto.

In aggiunta è inoltre possibile valorizzare un altra proprietà, RemoteUserHeaderName, per indicare di utilizzare un header della *"request http"* diverso da quello di default, che è REMOTE_USER, per recuperare lo USER_ID. L'utilizzo di questa proprietà è obbligatorio nel caso di utilizzo di un webserver IIS poichè quest'ultimo non lascia passare l'header REMOTE_USER.

NB: è necessario effettuare lo stop di Tomcat

La configurazione corrispondente è:

Il file di contesto della web application, che normalmente si trova in corrispondenza del percorso conf/catalina/localhost /<ROOT_o_nomewebapp>.xml deve avere la proprietà di nome *"ExternalAuth"* con valore *"1"*, se WebEsse3 deve effettuare al logout la cancellazione dei cookies del service provider, con valore "2", se WebEsse3 NON deve effettuare al logout la cancellazione dei cookies del service provider.

In aggiunta è possibile, ma non obbligatorio se non nel caso di IIS, valorizzare la proprietà di nome *"RemoteUserHeaderName"* con valore corrispondente all'header con il quale viene passato lo USER_ID.

Esempio relativo ad un file di context in cui è configurato l'indirizzo del Jaguar_Server e della proprietà ExternalAuth (con cancellazione dei cookies del service provider alla logout):

<Context path="/esse3" docBase="/war/esse3.war">

<Parameter name="Jaguar_Server" value="jaguar.kion.it:10000;jaguar.kion.it:10001 override="false"/>

<Parameter name="ExternalAuth" value="1" override="false" />

</Context>

Esempio relativo ad un file di context in cui è configurato l'indirizzo del Jaguar_Server e delle proprietà ExternalAuth (senza cancellazione dei cookies del service provider alla logout) e RemoteUserHeaderName, quest'ultima con valore "UTENTEESTERNO":

<Context path="/esse3" docBase="/war/esse3.war">

<Parameter name="Jaguar_Server" value="jaguar.kion.it:10000;jaguar.kion.it:10001 override="false"/>

<Parameter name="ExternalAuth" value="2" override="false" />

<Parameter name="RemoteUserHeaderName" value="UTENTEESTERNO" override="false" />

</Context>

5.3 CONFIGURAZIONE DEI GRUPPI UTENTI SUL DB DI ESSE3

Una ulteriore configurazione necessaria riguarda i gruppi di utenti per i quali abilitare l'autenticazione esterna. I gruppi da modificare sono quelli che hanno accesso a WebEsse3 [cfr. Requisito n.1], non quelli che accedono tramite client di Esse3.

La configurazione corrispondente è:

Per ogni gruppo della tabella P18_GRP abilitato all'accesso tramite WebEsse3, deve essere modificato il valore di "AUTH_PWD_MASTER_LOCATION" impostandolo a "3".

Esempio di script di update:

```
update P18_GRP
set AUTH_PWD_MASTER_LOCATION = 3
where P18_GRP.GRP_ID in (4, 6, 7, 8, 9, 10, 11, 12);
```

ATTENZIONE: Verificare sempre con il gruppo di Esse3 la lista esatta dei gruppi da modificare

5.4 CONFIGURAZIONE DELL'URL PER IL LOGOUT

Se il sistema è configurato per utilizzare l'autenticazione esterna, l'operazione di logout, dopo avere cancellato la sessione utente, effettua un redirect sull' url configurato sulla tabella di Esse3 PAR_CONF_URL, con codice **AFTER_LOGOUT_REDIRECT**, consentendo quindi ulteriori operazioni esterne a WebEsse3.

Se è richiesta l'esecuzione della Logout da WebEsse3 senza redirigere all'url configurato sulla PAR_CONF_URL, è possibile modificare (a cura di Kion) l'url di logout sostituendo /Logout.do con l'url **/LogoutNoRedirect.do.**

Se invece l'invocazione della logout su WebEsse3 è effettuata tramite un link esterno a WebEsse3 stesso (per esempio un link di logout su un portale), è possibile rimuovere il link dal menu di WebEsse3, a cura di Kion, e far invocare il link /Logout.do da parte del sistema esterno, a cura di chi realizza e implementa il sistema esterno.

La configurazione corrispondente è:

Quando WebEsse3 è configurato per accettare l'autenticazione esterna è necessario valorizzare l'url da richiamare in seguito alla logout, sulla tabella PAR_CONF_URL con codice AFTER_LOGOUT_REDIRECT.

NB: se l'url configurato nella PAR_CONF_URL corrisponde al logout del service provider (SP) di Shibboleth, cioè Shibboleth.sso/Logout, lo stesso SP deve essere configurato per fare a sua volta un altro redirect dopo il suo logout, configurazione resa possibile dal SP di Shibboleth. Normalmente quest'altro redirect viene fatto alla home del portale o al logout di un altro sistema configurato in SSO.

6 SHIBBOLETH

Tra i sistemi di SSO più utilizzati, o in via di utilizzo, da parte degli Atenei, vi è sicuramente **Shibboleth**.

Per i dettagli sulla installazione e configurazione di un ambiente Shibboleth si rimanda alla documentazione presente sul sito ufficiale:

http://shibboleth.internet2.edu

Kion non fornisce supporto diretto alla installazione e configurazione di Shibboleth. Eventuale supporto per queste attività può comunque essere richiesto al Cineca tramite Kion che provvederà a mettere in contatto i rispettivi referenti ed a svolgere l'eventuale ruolo di coordinamento.

A grandi linee l'architettura di Shibboleth prevede due componenti principali: un Identity Provider (**IdP**) ed un Service Provider (**SP**). Il primo è dove l'utente viene ridiretto per effettuare la login, il secondo è installato sul web server ed ha il compito di intercettare le richieste verso le risorse protette, verificare se l' utente è già autenticato ed in caso negativo ridirigere sull'IdP e aggiungere il REMOTE_USER. La comunicazione tra IdP e SP avviene tramite scambio di messaggi SAML.

ATTENZIONE: poichè Shibboleth non supporta meccanismi di logout globale (cioè tra i vari sistemi/applicativi messi in SSO), è necessario adottare soluzioni custom per ottenere la stessa funzionalità.

7 OPENSSO

Un altro sistema di SSO di prossima utilizzazione per autenticare in un'architettura in cui è presente anche WebEsse3 è OpenSSO (recentemente rinominato OpenAM e ceduto a ForgeRock dopo che Oracle ne ha deciso l'interruzione dello sviluppo nel febbraio 2010).

La configurazione utilizzata in questo caso prevede una soluzione ibrida con l'utilizzo del Service Provider (SP) di Shibboleth e dell'Identity Provider di OpenSSO.

8 CONCLUSIONI

L'ateneo che intendesse dotarsi di un sistema di autenticazione esterna da integrare anche, o soltanto, con WebEsse3 dovrà valutare attentamente se i requisiti elencati in questo documento sono rispettati dal sistema (protezione degli accessi e valorizzazione del remote_user) e dalla struttura organizzativa o infrastruttura in generale (condivisione account in termini di user_id).

Nel caso venisse scelto Shibboleth, Kion ne garantisce la compatibilità architetturale ed è in grado di interfacciare il cliente con il Cineca per l'eventuale supporto alla installazione e configurazione.

E' necessario comunque attivare un progetto specifico sia per il coordinamento di tutte le attività e gli attori eventualmente coinvolti, sia per le eventuali implementazioni da effettuare per la condivisione degli account e, nel caso di Shibboleth, per la gestione del logout globale.

Processo - **Autenticazione e autorizzazione**

Visibilita - **tutti**