

Manuale di installazione

January 31, 2014

1 Premessa

Si garantisce la piena compatibilità solo nei sistemi UNIX like (OSX, linux) a causa del path delle immagini uploadate.

E' stato creato un EAR anche per le versioni windows ma non è stato testato, causa mancanza di un computer con installato il sistema operativo citato, e quindi non si garantisce il corretto funzionamento.

2 Consigli

- Per garantire una resa grafica migliore si consiglia di avere almeno 6 pacchetti disponibili a database
- Il database viene creato con già l'utente con privilegi di amministratore con queste credenziali
 - nome utente: admin@gmail.com
 - password: admin
- Il login in homepage fa il redirect sulla home appropriata a seconda del gruppo appartenente alle credenziali possibili. Questo è possibile grazie alla modifica fatta a j_security_check.
- Le varie pagine dello store (parte cliente) non hanno i nomi delle pagine presenti nel codice perchè è stata usata una libreria di url rewriting(pretty-faces)
- Se l'installazione dovesse presentare problemi contattare un membro del gruppo oppure visitare il link travel-dream.rmdesign.it dove è presente una versione funzionante dell'applicazione. Sono stati messi a disposizione 3 utenti(uno per ogni gruppo) così da poter visitare ogni parte del sito. di seguito le credenziali
 - admin: admin@gmail.com password: admin
 - dipendente: dipendente@gmail.com password: dipendente
 - cliente: cliente@gmail.com password: cliente
- L'applicazione per funzionare necessita di un mail server installato e configurato a dovere, nella sezione relativa all'installazione è descritto come configurare postfix su ambiente UNIX, potete però scegliere quello che preferite.
- Per provare le funzioni che prevedono l'invio delle mail da parte dell'applicazione(pacchetto condiviso ed invia lista desideri) cercare le mail in spam (anche se il record DNS è certificato...mistero...)

3 Installazione

1. Clonare la repo di git sul proprio computer
 - `git clone https://code.google.com/p/traveldream-mariani-marchesini-mastellone/`
2. Aprire mysql ed eseguire lo script presente nella cartella, questo creerà il database corretto
3. creare la cartella per l'upload delle immagini
 - (ambiente UNIX)
 - `sudo mkdir /var/uploads`
 - `sudo chmod -R 777 /var/uploads`
 - (ambiente Windows)
 - creare la cartella in `C:/Documents/uploads`
4. creare la JDBC connection pool su glassfish con queste impostazioni:
 - nome: `TravelDreamDB`
 - resource type: `DataSource`
 - nelle impostazioni avanzate cambiare le tuple `URL` e `Url` con il seguente url:
 - `jdbc:mysql://127.0.0.1:3306/TravelDreamDB`
 - cambiare nome utente e password con quelle appropriate
5. creare la JDBC resource e chiamarla `jdbc/TravelDreamDB`
6. creare il reame di sicurezza con queste impostazioni

Realm Name: travelrealm

Class Name: com.sun.enterprise.security.ee.auth.realm.jdbc.JDBCRealm

Properties specific to this Class

JAAS Context: *	<input type="text" value="jdbcRealm"/> Identifier for the login module to use for this realm
JNDI: *	<input type="text" value="jdbc/TravelDreamDB"/> JNDI name of the JDBC resource used by this realm
User Table: *	<input type="text" value="Utente"/> Name of the database table that contains the list of authorized users for this realm
User Name Column: *	<input type="text" value="email"/> Name of the column in the user table that contains the list of user names
Password Column: *	<input type="text" value="password"/> Name of the column in the user table that contains the user passwords
Group Table: *	<input type="text" value="UtenteGruppo"/> Name of the database table that contains the list of groups for this realm
Group Table User Name Column:	<input type="text"/> Name of the column in the user group table that contains the list of groups for this realm
Group Name Column: *	<input type="text" value="gruppo"/> Name of the column in the group table that contains the list of group names
Password Encryption Algorithm: *	<input type="text" value="MD5"/> This denotes the algorithm for encrypting the passwords in the database. It is a security risk to leave this field empty.
Assign Groups:	<input type="text" value="CLIENTE,DIPENDENTE,AMMINISTRATORE"/> Comma-separated list of group names

Figure 1: Reame di sicurezza

7. modificare le impostazioni del pannello security all'interno di server-config come segue

Configuration Name: server-config

Security Manager	<input type="checkbox"/> Enabled Enable the security manager for the domain by adding an option in the JVM Settings
Audit Logging	<input type="checkbox"/> Enabled Enable server to load and run all audit modules specified in the Audit Modules setting
Default Realm	<input type="text" value="travelrealm"/> Default realm used by all applications for authentication
Default Principal	<input type="text"/> User name used by the server when no principal is provided; must contain only alphanumeric, underscore, dash, or dot characters
Default Principal Password	<input type="text"/> Required if Default Principal contains a value
JACC	<input type="text" value="default"/> Name of the jacc-provider element to use for configuring the JACC infrastructure
Audit Modules	<div><input type="text" value="default"/> <input type="text"/></div> List of audit provider modules used by the audit subsystem; Control-click to multiple-select
Default Principal To Role Mapping	<input checked="" type="checkbox"/> Enabled Apply default principal-to-role mapping at deployment when application-specific mapping is not defined; does not affect currently deployed applications
Mapped Principal Class	<input type="text"/> Customize the java.security.Principal implementation class used for default principal-to-role mapping

Figure 2: Impostazioni server-config/security

8. configurare postfix(ambiente unix):

- (a) installare postfix
- (b) editare la configurazione di base
 - sudo vim /etc/postfix/main.cf
 - controllare se sono presenti le seguenti impostazioni
 - mydomain_fallback = localhost
 - mail_owner = _postfix
 - setgid_group = _postdrop
 - aggiungere le seguenti impostazioni
 - relayhost=smtp.gmail.com:587(vale solo per gmail)
 - smtp_sasl_auth_enable=yes
 - smtp_sasl_password_maps=hash:/etc/postfix/sasl_passwd
 - smtp_sasl_security_options=
 - smtp_use_tls=yes
 - smtp_tls_security_level=encrypt
 - tls_random_source=dev:/dev/urandom
- (c) creare il file contenente la password
 - sudo vim /etc/postfix/sasl_passwd

- smtp.gmail.com:587 <vostro_indirizzo>@gmail.com:<vostra_password>
- salvare il file
- sudo postmap /etc/postfix/sasl_passwd

(d) avviare postfix

- sudo postfix start

(e) eventualmente testarlo

- date | mail -s <soggetto> <indirizzo destinatario>
- se la mail arriva è tutto a posto (controllare anche nello spam)

(f) se qualcosa non va controllare i log di postfix

- tail -f /var/log/mail.log

9. deployare l'EAR appropriato in glassfish tramite la pagina di amministrazione

10. ENJOY!