LDAP

Autenticazione LDAP e servizi di replica

ESSE3 può autenticare gli utenti interrogando un server LDAP: per dettagli sulla modalità di autenticazione, vedere il relativo documento.

Per rendere possibile l'autenticazione su un server LDAP è necessario attivare un meccanismo di replica, in tempo reale, tra la base dati ESSE3 ed il server LDAP: ESSE3 prevede servizi di replica standard,da configurare in fase di start-up del sistema ed eventualmente estendibile in una fase successiva.

Il servizio di replica alimenta in modalità asincrona il server LDAP configurato: ogni transazione eseguita sulle anagrafiche di ESSE3 viene catturata e memorizzata in una coda al fine di poter eseguire, in un secondo momento, il processo di replica.

ESSE3 supporta due implementazioni standard:

- la prima, basata su linguaggio PL/SQL (per dettagli, vedere i paragrafi di seguito riportati), alimenta una coda Oracle, nella quale vengono memorizzate le coppie attributo/valore da utilizzare durante l'aggiornamento del server LDAP. Il processo viene adeguato alle specifiche richieste dell'Ateneo, parametrizzando l'esecuzione di alcuni dei servizi previsti dal package Oracle (DBMS_LDAP) preposto a tale gestione
- la seconda, basata sui servizi ESSE3 Gateway (per dettagli, vedere il relativo documento), prevede l'alimentazione di una coda (tabella Oracle), nella quale vengono memorizzati di ID dei record oggetto di variazione. Sfruttando le configurazioni del prodotto, è possibile replicare la stessa informazione in formati differenti, tra cui anche un LDAP. Il contenuto delle code viene processato con cadenza regolare, sfruttando lo schedulatore di processi previsto da ESSE3: su richiesta, lo stesso processo schedulato può essere attivato dall'utente amministratore (o abilitato), utilizzando la funzionalità di back-office preposta

I servizi ESSE3 Gateway sono da preferire alle implementazioni PL/SQL per due ragioni:

- esistono limitazioni all'uso del package Oracle DBMS_LDAP, quando il server LDAP da alimentare è Microsoft Active Directory
- il gateway può gestire la replica contemporanea su più sistemi target, anche eterogenei (LDAP, web service, flussi, ...)

Implementazione PL/SQL "add-on"

Le prime integrazioni tra ESSE3 ed un server LDAP sono state rilasciate come "add-on" al prodotto. La presenza di questa verticalizzazione, specifica per ogni Ateneo, è facilmente determinabile da una verifica sugli oggetti presenti nella base dati:

- la vista V_LDAP_USER definisce i criteri con cui filtrare le anagrafiche da replicare su LDAP; la vista viene personalizzata in base alle specifiche di implementazione fornite dall'Ateneo
- il package LDAP_DRIVER espone i comandi (creazione della sessione di lavoro; creazione, aggiornamento o rimozione della entry LDAP; ...; chiusura della sessione di lavoro) con cui avviene l'interazione con il server LDAP; in pratica, è un wrapper del package Oracle DBMS_LDAP
- il package LDAP_UPDATE implementa le logiche di replica richieste dall'Ateneo, le quali possono essere sintetizzate nei seguenti step
  - verifica degli estremi per replicare l'anagrafica: solo le anagrafiche estratte dalla vista V_LDAP_USER vengono replicate sul server LDAP
  - memorizzazione sulla coda Oracle delle coppie attributo/valore con cui sincronizzare il server LDAP
- il package LDAP_UPDATE_QUEUE supporta il servizio di replica nella gestione della coda Oracle

Le transazioni sulle anagrafiche di base (utenti, persone, studenti, matricole e docenti: in generale sono queste le anagrafiche che l'Ateneo decide di monitorare per gestire la sincronizzazione di un server LDAP) vengono monitorate tramite alcuni trigger di database, i quali hanno il compito di intercettare e notificare al servizio di replica le variazioni apportate ai dati.

Come indicato in precedenza, il package LDAP_UPDATE contiene tutte le logiche di gestione e di valorizzazione delle entry LDAP, mentre un job Oracle, eseguito in generale ogni minuto, attiva l'aggiornamento del server LDAP con quanto memorizzato nella coda Oracle.

Su richiesta dell'Ateneo, l'esecuzione della replica può essere effettuata anche in modalità sincrona: in questo caso, il servizio non usa la coda Oracle ma tenda di aggiornare immediatamente il server LDAP con le informazioni calcolate. Anche se questa strada è percorribile, l'aggiornamento sincrono del server LDAP è una opzione da scoraggiare in quanto la indisponibilità del server potrebbe far fallire la transazione su ESSE3 (immatricolazione web o in generale una qualunque operazione tentata dalla Segreteria o altro Ufficio).

I parametri di configurazione del servizio di replica sono tutti quelli identificati dal seguente statement SQL:

```
SELECT par_cod, val_alfa, val_num, des

 FROM par_conf

WHERE par_cod LIKE 'LDAP%' AND par_cod NOT LIKE 'LDAP_AUTH%';
```

Implementazione PL/SQL "a prodotto"

Le esperienze fatte su diverse implementazioni "add-on" hanno permesso di rilasciare, a prodotto, un semilavorato che in ogni caso richiede alcune personalizzazioni. L'impianto architetturale descritto per le implementazioni "add-on" rimane di massima lo stesso, con le differenze di seguito riportate:

- la vista utilizzata per determinare gli estremi delle anagrafiche da replicare è la V18_LDAP_USER
- il package preposto alla interazione con il server LDAP è LDAP
- il package preposto alla gestione ed alla valorizzazione delle entry LDAP è LDAP_CUSTOM

Processo - **Single sign on, ldap**

Visibilita - **tutti**