Sommario

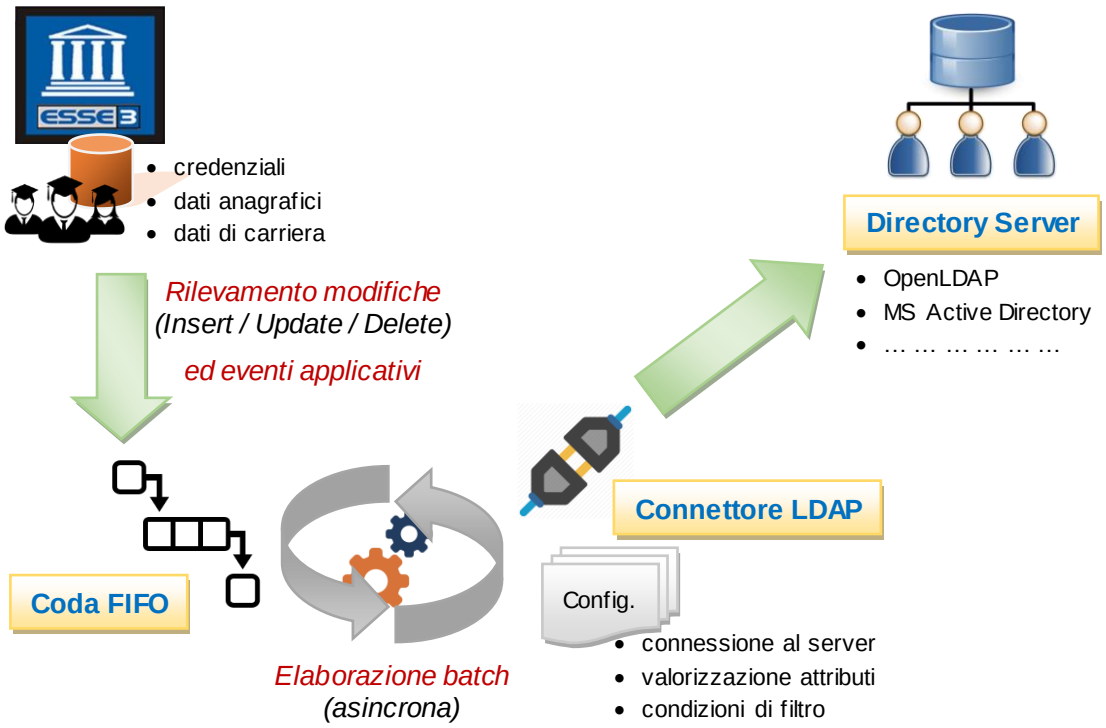
Introduzione

Questo documento descrive la soluzione offerta del sistema di segreteria Esse3 per effettuare provisioning di utenze (tipicamente studenti) su un Directory Server LDAP esterno.

L'implementazione fa uso del motore Esse3 Gateway, sistema configurabile tramite il quale più genericamente è possibile gestire integrazioni tra Esse3 ed altri sistemi esterni mediante flussi di replica/import dati e, nel caso specifico oggetto di questo documento, permette di interfacciarsi al Directory Server tramite un apposito connettore LDAP.

Architettura del sistema

L'architettura del sistema di provisioning utenti su LDAP server, implementato in Esse3, viene esemplificata nella figura seguente.



Nei successivi paragrafi vengono descritti in dettaglio tutti i principali elementi costituenti.

Si evidenzia comunque da subito come i due sistemi, Esse3 ed il Directory Server oggetto del provisioning, non siano strettamente interconnessi ma la propagazione dei dati avvenga invece tramite un ***processo asincrono***.

Per quel che riguarda i tipi di Directory Server supportati basta che si tratti di un server accessibile tramite interfaccia standard ***LDAP***, come ad esempio OpenLDAP o Active Directory di Microsoft.

Tipologie di utenze sincronizzate

In Esse3 sono presenti i dati anagrafici, di carriera e credenziali di accesso di studenti e persone registrate a sistema.

Più in particolare possiamo individuare varie tipologie di utenze che vanno ad alimentare il processo di provisioning verso LDAP:

- studenti attivi (aventi carriera in ateneo in stato attiva o sospesa)
- studenti laureati
- studenti cessati (per motivo diverso da conseguimento titolo)
- studenti pre-immatricolati
- prospect, ovvero studenti solo registrati (che non hanno proceduto ancora ad alcun tipo di immatricolazione).

Da configurazione, su Esse3, è possibile stabilire se prendere in considerazione qualsiasi tipo di utenza o restringere invece solo su alcune.

L'ordine con cui sono elencate tali tipologie al tempo stesso rappresenta anche la priorità a loro assegnata ed utilizzata, nel caso di studente con più carriere in ateneo, per determinare quella 'prevalente' ai fini della sincronizzazione su LDAP (che presuppone di individuare una ed una sola carriera).

Ad esempio una carriera attiva viene privilegiata rispetto ad un'altra già chiusa ed una chiusa per conseguimento titolo (laurea) viene privilegiata rispetto ad un'altra chiusa per altro motivo.

A parità di priorità viene considerata la carriera più recente (ciò vale, di base, anche nell'eventualità di carriere compatibili, ovvero più carriere attive per lo stesso studente).

Rilevamento ed accodamento modifiche/eventi

Alla base del processo di provisioning c'è l'intercettare qualsiasi evento che potenzialmente potrebbe dar luogo ad una sincronizzazione di dati verso LDAP.

A tale proposito in Esse3 vengono rilevati eventi di diversa natura, più in dettaglio:

- qualsiasi inserimento/modifica/cancellazione di dati anagrafici, di carriera ed utenza – ciò avviene tramite appositi ***trigger di DB***
- eventuali altre ***notifiche applicative*** legate al compimento di processi o al verificarsi di specifiche condizioni (come ad esempio utenze da disabilitare su LDAP, o da ricollocare di posizione/gruppo, una volta trascorso il periodo di franchigia previsto a seguito della cessazione carriera).

In entrambi i casi viene tenuta traccia dell'evento che si è verificato, inserendo un relativo record all'interno di un'apposita ***coda di tipo FIFO*** (First In First Out).

Le principali informazioni contenute nel record accodato sono:

- tipologia di modifica o evento verificatisi (su Esse3 corrisponde al Tipo Replica, come censito a DB sulla tabella `EPI_REPLICA`)
- chiave identificativa del dato variato o al quale si riferisce l'evento notificato (es.: anagrafica, carriera studente, utenza)
- tipo di operazione verificatasi: Inserimento/Modifica/Cancellazione (questa informazione ha senso in particolare nel caso in cui si tratti di variazione di un preciso dato)
- campi di dettaglio che sono stati modificati, solo nel caso in cui si tratti di un aggiornamento dati intercettato da un trigger a DB (es.: modifica dell'indirizzo di residenza in anagrafica, cambio della password per l'utenza, ecc..)
- data/ora di registrazione della modica/evento (e conseguente accodamento).

Si fa notare come tra le informazioni accodate siano presenti solo gli ***estremi identificativi dell'entità oggetto della modifica/evento*** e non venga mantenuta alcuna copia dei valori dei dati e campi interessati presenti in quel momento.

Esempio: a fronte di una modifica di qualche dato anagrafico di uno studente viene accodato un record che tiene traccia del fatto che è avvenuta tale modifica, non vengono invece memorizzati i valori dei diversi campi che costituiscono l'anagrafica in questione (ovvero lo stato né prima né dopo la modifica).

La struttura che implementa e gestisce gli ***accodamenti*** si compone in realtà di ***due livelli***:

- una coda di primo livello dove viene tenuta traccia delle modifiche e degli eventi intercettati, come descritta in precedenza (la cui tabella di riferimento sul DB di Esse3 è `EPI_DATO_REPLICA`, assieme alla tabella collegata `P99_ENTITA` che memorizza gli estremi identificativi del dato oggetto di replica)
- una coda di secondo livello per gestire la replica dati verso uno specifico sistema esterno (nel caso in questione, oggetto di questo documento, un Directory Server LDAP) a fronte della modifica o dell'evento intercettati (la tabella di riferimento sul DB di Esse3 è la `EPI_CODA_REPLICA`).

Tale struttura a due livelli è dovuta al fatto che genericamente tramite il motore Esse3 Gateway (di cui il provisioning LDAP può essere considerato una specifica applicazione) è possibile gestire integrazioni con diversi sistemi esterni, con la possibilità di indicare tramite configurazione su quali sistemi debbano o meno propagarsi i dati a fronte di una data modifica o la notifica di un evento applicativo.

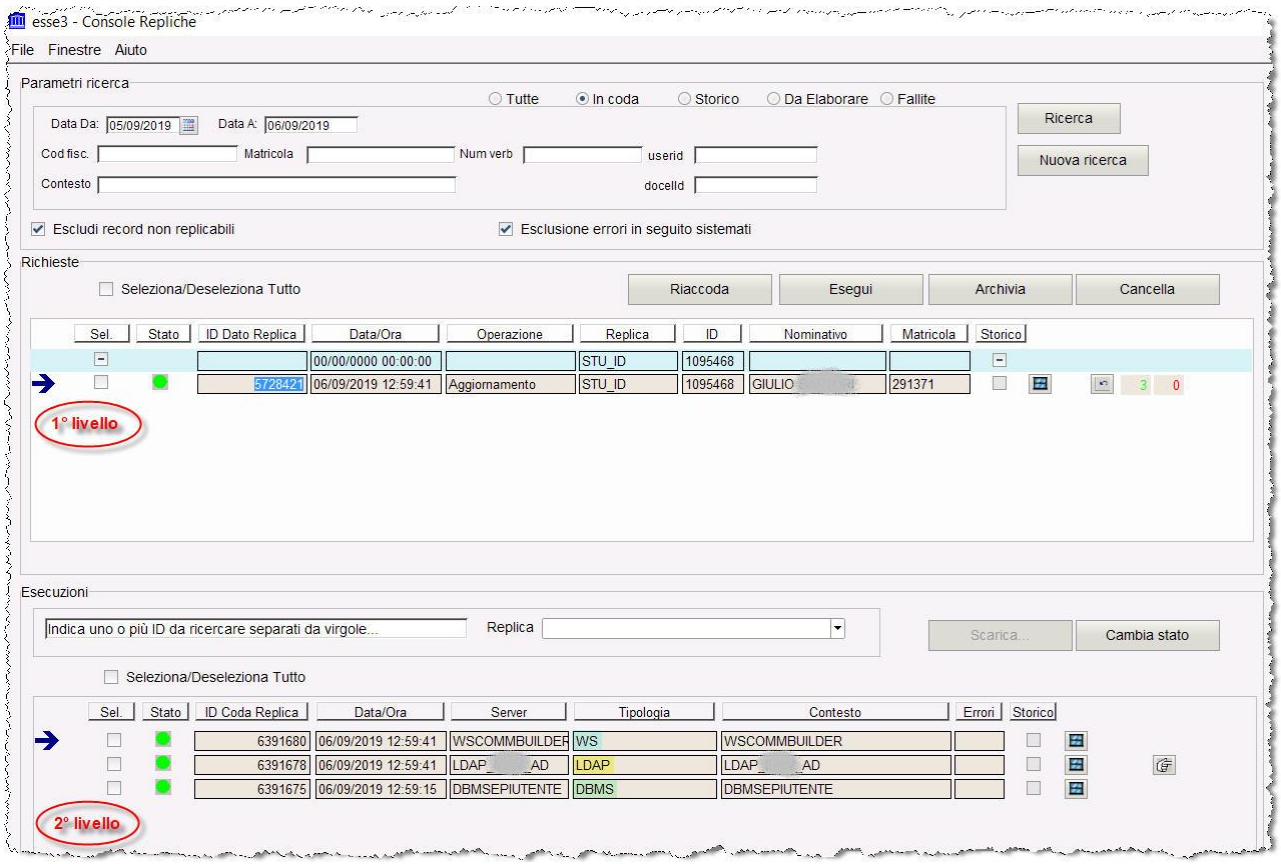
Quindi, ad esempio, a fronte di una modifica di un dato anagrafico o di carriera di uno studente in Esse3 potrebbe darsi che sia necessario sincronizzare più sistemi esterni:

- un Directory Server, tramite connettore LDAP
- un applicativo di ateneo (es.: sistema di biblioteca, sistema documentale, ecc..), tramite appositi Web Service da questo esposti
- un altro DataBase, accedendo via JDBC.

In tal caso in Esse3 saranno presenti:

- un record nella coda di primo livello (su `EPI_DATO_REPLICA`) relativo alla modifica intercettata
- tre record nella coda di secondo livello (su `EPI_CODA_REPLICA`), uno per ognuno dei sistemi esterni interfacciati, consentendo di gestirne la sincronizzazione in maniera indipendente e dedicata.

Da client Esse3 tali concetti sono riscontrabili all'interno della maschera "Console Repliche", come esemplificato nella seguente screenshot.



Elaborazione asincrona

L'elaborazione vera e propria delle modifiche e degli eventi accodati avviene in maniera asincrona tramite l'esecuzione periodica su Esse3 di un'apposita ***elaborazione batch***: per il processo di provisioning utenti su LDAP si tratta dell'elaborazione ***REPLICHE_LDAP***.

La fase di rilevamento ed accodamento di modifiche ai dati e/o notifiche di eventi applicativi è infatti volutamente disaccoppiata dall'esecuzione delle relative operazioni di sincronizzazione verso i sistemi esterni interfacciati da Esse3.

Questo per evitare dipendenze indesiderate da tali sistemi, quali ad esempio il rischio di bloccare o comunque impattare in un qualche modo sui processi applicativi di Esse3 a causa di un eventuale problema su altri applicativi integrati.

Ad ogni esecuzione dell'elaborazione batch vengono effettuate le seguenti operazioni:

- viene letta la coda di primo livello estraendone eventuali record ancora da elaborare (come detto in precedenza la coda è di tipo FIFO, quindi le repliche dati seguiranno l'ordine di accodamento)
- per ogni record estratto, sulla base delle opportune configurazioni presenti in Esse3, si determina quanti e quali sono i sistemi esterni su cui è necessario propagare i dati collegati all'evento scatenante
- per ogni sistema da sincronizzare viene generata una coda di secondo livello dedicata
- viene letta la coda di secondo livello estraendone eventuali record ancora da elaborare e, per ognuno di questi, viene attivato il connettore appropriato per il sistema a cui ci si deve interfacciare (nel caso in questione, oggetto di questo documento, il Connettore LDAP)
- vengono reperiti tutti i dati oggetto di replica (a partire dalla chiave identificativa memorizzata sulla coda di primo livello), nella forma di *n* accoppiate del tipo *<nome campo; valore>*, e vengono passati al connettore invocando infine l'operazione di replica sul sistema esterno.

I dati che vengono sincronizzati su LDAP, in termini di campi e loro valori, sono quindi reperiti solo in ultima istanza nel momento in cui viene eseguita l'elaborazione batch REPLICHE_LDAP – in precedenza, quando viene intercettato l'evento scatenante per la replica, viene accodata solo la chiave identificativa dell'entità di riferimento (es.: identificativo dell'anagrafica, carriera studente o utenza).

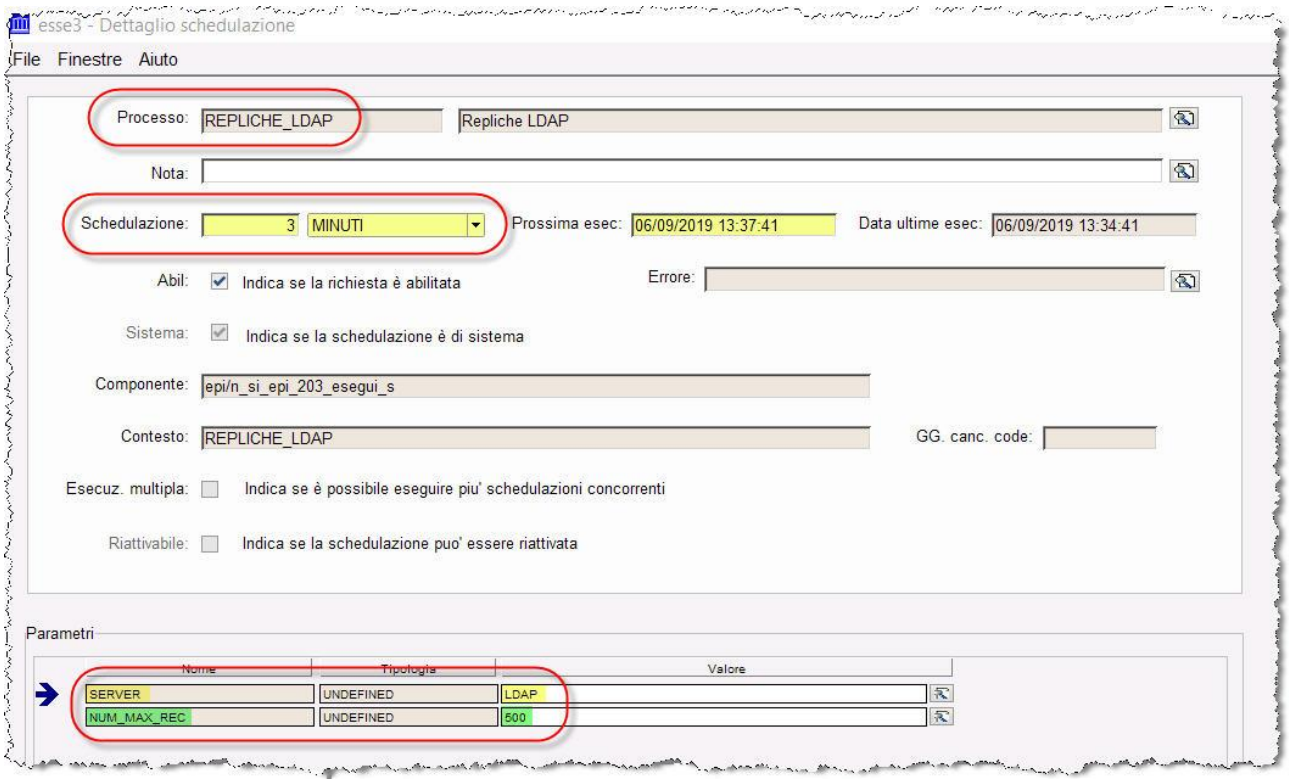
Da client Esse3, tramite la maschera "Elaborazioni batch", è possibile individuare il processo REPLICHE_LDAP e consultarne le ultime esecuzioni.

È inoltre possibile variare alcune configurazioni, ovvero:

- la schedulazione (di default impostata con una frequenza di un'esecuzione ogni 3 minuti)
- il numero massimo di record da elaborare ad ogni esecuzione (parametro `NUM_MAX_REC`).

Infine il parametro `SERVER` valorizzato a 'LDAP' è ciò che caratterizza l'elaborazione REPLICHE_LDAP: infatti tale impostazione fa sì che vengano elaborati dalla coda di secondo livello solo i record relativi ad

un contesto di replica LDAP (esiste anche un processo REPLICHE generico che elabora tutti i rimanenti record per i quali non esistono elaborazioni batch dedicate).



Connettore LDAP

Il connettore LDAP è il componente di Esse3 che si occupa dell'effettiva interazione con il Directory Server, effettuando su di questo le operazioni di inserimento e modifiche delle utenze a seguito degli eventi intercettati su Esse3.

Nello specifico il connettore è implementato, come il resto del backend Esse3, in tecnologia Java e si interfaccia al Directory Server tramite ***protocollo LDAP***: sono quindi supportati tutti i server compatibili con tale standard (es.: OpenLDAP, Microsoft Active Directory, ecc.).

Il connettore va parametrizzato per interfacciarsi al Directory Server voluto ed implementare le logiche desiderate; a tale scopo sono disponibili diverse configurazioni, suddividibili principalmente in:

- ***configurazioni di base***
- ***mapping tra dati Esse3 ed attributi LDAP***.

Configurazioni di base

Tra le configurazioni di base del connettore LDAP troviamo:

- l'indicazione della vista di DB per estrarre da Esse3 i dati oggetto di replica ed eventuali filtri da applicare
- gli estremi di connessione al Directory Server
- le credenziali dell'utenza amministratore per accedere in lettura/scrittura al Directory Server
- il percorso di base che determina la porzione di albero LDAP all'interno della quale opera il provisioning (Distinguished Name di base)
- i sotto contesti all'interno dei quali collocare le utenze
- eventuale gestione di gruppi a cui associare le utenze.

La tabella seguente riporta il set completo delle configurazioni attualmente gestite.

Configurazione	Descrizione
EPI_SQL_VIEW	Vista di DB utilizzata per reperire i dati oggetto di replica Per il provisioning LDAP tipicamente è `V_EPI_REPLICA_UTENTE_LDAP`
EPI_SQL_WHERE	Eventuale condizione di filtro da applicare alla query di reperimento dati (sulla vista indicata con EPI_SQL_VIEW)
LDAP_ADAPTER	Classe di backend Esse3 utilizzata per la comunicazione con il server LDAP: - it.kion.esse4.epi.utils.ldap.LdapAdapter - it.kion.esse4.epi.utils.ldap.AdLdapAdapter (per *Active Directory*)

Configurazione	Descrizione
LDAP_SCHEMA_BUILDER	Classe di backend Esse3 utilizzata per valorizzare gli attributi LDAP: - it.kion.esse4.epi.utils.ldap.LdapBuilder - it.kion.esse4.epi.utils.ldap.AdLdapBuilder (per *Active Directory*)
LDAP_VENDOR	Vendor del server LDAP – è utilizzata solo come nota descrittiva, ad esempio: OpenLDAP, MS Active Directory
LDAP_PROVIDER_URL	URL utilizzato per stabilire la connessione al server LDAP, espresso nel formato 'ldap://<host>:<port>'
LDAP_ADMIN	Utenza amministratore utilizzata per accedere al Directory Server Indicare qui solo il nome relativo, ad esempio: cn=LdapAdmin
LDAP_ADMIN_PWD	Password dell'utenza amministratore
LDAP_BASENAME_0_ID	Primo livello della gerarchia del server LDAP (per comporre il DN di base) Esempio: ou
LDAP_BASENAME_0_VALUE	Valore del primo livello di gerarchia del server LDAP (per comporre il DN di base) Esempio: utenti
LDAP_BASENAME_1_ID	Secondo livello della gerarchia del server LDAP (per comporre il DN di base) Esempio: dc
LDAP_BASENAME_1_VALUE	Valore del secondo livello di gerarchia del server LDAP (per comporre il DN di base) Esempio: unidemo
LDAP_BASENAME_2_ID	Terzo livello della gerarchia del server LDAP (per comporre il DN di base) Esempio: dc
LDAP_BASENAME_2_VALUE	Valore del terzo livello di gerarchia del server LDAP (per comporre il DN di base) Esempio: it
LDAP_SECURITY_PRINCIPAL_INFO	Percorso (relative rispetto a quello base dato da LDAP_BASENAME_*) dove è collocata l'utenza amministratore (esempio: 'OU=Users' per Active Directory)
LDAP_USER_SEARCH_INFO	Filtro LDAP per ricercare l'utente su LDAP (se già esistente – esempio: uid=@USER_ID@)
LDAP_USER_SEARCH_SUBCONTEXT	Percorso su cui restringere la ricerca dell'utente da aggiornare (es.: OU=People) – ha senso solo in congiunzione a LDAP_USER_SEARCH_INFO
LDAP_SUBCONTEXT_NAME	Informazioni utilizzate per determinare il nome del contesto LDAP dove collocare le utenze (ad esempio: 'cn=@USER_ID@, ou=Studenti')
LDAP_USER_APPEND_WHEN_NOTFOUND	Indica se creare l'utente se non viene trovato dall'operazione di modifica
LDAP_USER_APPEND_INACTIVE	Indica se creare l'utente anche se non più attivo (ad esempio studenti con carriera cessata), nel caso non venga trovato dall'operazione di modifica
LDAP_USER_MOVE_ENABLED	Indica se consentire la move dell'utente su LDAP, nel caso in cui il DN individuato da LDAP_USER_SEARCH_INFO sia differente da quello di LDAP_SUBCONTEXT_NAME
LDAP_USER_REMOVE_DUPLICATES	Indica se rimuovere eventuali entry utente duplicate su LDAP, nel caso in cui il criterio dato da LDAP_USER_SEARCH_INFO ritorni piu' risultati
LDAP_ENTRY_DISABLE_MODE	Modalità con cui eseguire la disabilitazione della entry sul server LDAP

Configurazione	Descrizione
	Valori ammessi: disable – delete
LDAP_ENTRY_DISABLE_DELAY	Giorni di ritarno previsti per inoltrare la richiesta di disabilitazione della entry sul server LDAP
LDAP_LINKED_ENTRIES_SEARCH	Filtro di ricerca per individuare eventuali entry collegate all'entry principale, nell'intero sottoalbero dato dal DN di base

Gestione dei gruppi

Tramite alcune configurazioni dedicate è possibile fare in modo che la procedura di provisioning gestisca anche l'attribuzione dell'utente a uno o più gruppi.

In particolare, a seconda della versione di Esse3 installata, sono disponibili due gestioni differenti (con relative configurazioni distinte):

- una nuova gestione, a partire dalla versione 21.03.00 di Esse3, che risulta essere quella più flessibile
- una precedente gestione, per le versioni di Esse3 antecedenti, applicabile solo ad Active Directory e con alcune limitazioni.

Versione precedente

La gestione presente nelle versioni di Esse3 antecedenti la 21.03.00 impone le seguenti limitazioni:

- è disponibile solo per Active Directory
- i gruppi su LDAP devono essere presenti tutti al medesimo percorso (ad esempio all'interno della stessa OU)
- è possibile associare al massimo 5 gruppi ad un utente; si tratta di quelli indicati nei seguenti campi della vista di DB configurata sul contesto di replica (tipicamente la V_EPI_REPLICA_UTENTE_LDAP):
    - GRUPPO
    - GRUPPO_FAC
    - GRUPPO_CDS
    - GRUPPO_STU
    - GRUPPO_ATTIVI.

La tabella seguente riporta le configurazioni su cui è basata tale gestione ed il loro significato.

Configurazione	Descrizione
LDAP_USER_GROUPS	Nomi dei gruppi utente per i quali gestire l'appartenenza, separati da pipe (|) - se un nome termina per asterisco (*) viene interpretato come prefisso. Esempio: WiFi|Studenti_*|Docenti_*
LDAP_USER_GROUPS_SUBCONTEXT	Percorso (relative rispetto a quello base dato da LDAP_BASENAME_*) dove sono collocati i gruppi utente per i quali gestire l'appartenenza. Esempio: OU=Groups

Nuova versione

La nuova gestione è caratterizzata da maggiore flessibilità:

- non ha vincoli sul tipo di Directory Server (quindi non è limitata al solo Active Directory)
- non ha limiti sul numero di gruppi gestibili e sulla loro collocazione all'interno dell'alberatura LDAP
- consente di effettuare il provisioning automatico di un gruppo, se ancora non esistente.

La tabella seguente riporta le configurazioni su cui è basata tale gestione ed il loro significato.

Configurazione	Descrizione
LDAP_GROUPS_SQL_VIEW	Vista di DB da utilizzare per il reperimento dei gruppi di appartenenza dell'utente. Tale vista deve esporre almeno il campo DN, valorizzato con il Distinguished Name del gruppo LDAP (eventualmente a meno di quello base dato da LDAP_BASENAME_*) Esempio: `V_EPI_REPLICA_LDAP_GROUPS`
LDAP_GROUPS_SQL_WHERE	Condizione di filtro per il reperimento dei gruppi di appartenenza dell'utente (si applica alla vista indicata in LDAP_GROUPS_SQL_VIEW). Utile per esprimere il legame tra dati utente (reperiti tramite la vista principale indicata in EPI_SQL_VIEW) e gruppi di appartenenza dell'utente: i parametri presenti in tale condizione (di join) si intendono infatti riferiti ai campi della vista principale. Esempio: `USER_ID = @USER_ID@`
LDAP_GROUPS_SEARCH_1 LDAP_GROUPS_SEARCH_2 LDAP_GROUPS_SEARCH_3 LDAP_GROUPS_SEARCH_4 LDAP_GROUPS_SEARCH_5	Informazioni per reperire su LDAP i gruppi utente da gestire (sono previste fino a 5 casisitiche, esprimibili rispettivamente tramite ognuna delle 5 configurazioni LDAP_GROUPS_SEARCH_*). Sintassi: <percorso base>; <filtro LDAP> Alcuni esempi: - `ou=ServiceGroups[1]; (|(cn=WiFi)(cn=Office365))` indica i gruppi denominati "WiFi" e "Office365" presenti sotto ou=ServiceGroups (un solo livello sotto) - `ou=StudentGroups; (objectClass=group)` indica qualsiasi gruppo all'interno dell'intero sotto-albero avente ou=StudentGroups come radice
LDAP_GROUPS_PROVISIONING	Informazioni per effettuare in automatico il provisioning dei gruppi utente non ancora presenti (oppure lasciare vuota per non applicare tale automatismo). Sintassi: <attributo_1>:<valore_1>; <attributo_2>:<valore_2>; … … … Eventuali parametri si intendono riferiti ai campi della vista di DB per i gruppi utente (quella indicata in LDAP_GROUPS_SQL_VIEW). Esempio: `objectClass:group; cn:@NAME@; description:@DESCR@`
LDAP_GROUPS_REMOVE_EMPTY	Indica se rimuovere il gruppo quando rimane vuoto (ovvero nessun utente appartiene più al gruppo) – valori previsti: 1 (si), 0 (no, default)

Tale gestione avanzata dei gruppi si applica nel momento in cui sono valorizzate, di minima, le seguenti configurazioni:

- LDAP_GROUPS_SQL_VIEW
- almeno una tra le varie LDAP_GROUPS_SEARCH_*

e preclude l'applicazione della precedente gestione (basata sulle configurazioni LDAP_USER_GROUPS e LDAP_USER_GROUPS_SUBCONTEXT, che rimangono comunque disponibili per retro compatibilità).

È possibile fare in modo che i gruppi ancora non esistenti, se necessario, vengano creati sul momento (tramite la configurazione LDAP_GROUPS_PROVISIONING).

Rimane comunque inteso che la struttura nella quale collocare i gruppi (alberatura LDAP composta ad esempio dalle varie OU innestate) debba essere già presente.

Inoltre è possibile pure rimuovere automaticamente un gruppo nel momento in cui da questo viene rimosso l'ultimo suo utente appartenente, evitando di lasciare su LDAP gruppi vuoti (tramite la configurazione LDAP_GROUPS_REMOVE_EMPTY).

Valorizzazione attributi LDAP

In aggiunta alle precedenti configurazioni di base ne esistono altre, di carattere più applicativo, che determinano quali attributi gestire per le utenze che vengono create o modificate dal provisioning su LDAP e come valorizzare tali attributi a partire dai dati presenti su Esse3.

A tale proposito il connettore è in grado di rilevare se l'utenza sul LDAP esiste già oppure no e di conseguenza permette di dettagliare le configurazioni in maniera tale che:

- alcune valorizzazioni di attributi si applichino solo in inserimento di una nuova utenza
- analogamente altre si possono applicare solo in caso di aggiornamento di utenza già esistenza
- è possibile specificare anche impostazioni con validità generica (che si applicano sia in caso di inserimento che di aggiornamento)
- esiste infine la possibilità di specificare quale valorizzazione di attributi adottare per il caso particolare di annullo (essenzialmente riconducibile al caso di studenti con carriera cessata su Esse3).

Nel caso di sincronizzazione di utenza già esistente su LDAP, per quel che riguarda il set di attributi gestiti, il connettore opera nel seguente modo:

- tutti gli attributi per cui, da configurazione, è prevista una valorizzazione da parte di Esse3 vengono sovrascritti (inclusi eventuali valori multipli per uno stesso attributo), a meno che dalla valorizzazione Esse3 non risulti alcun valore per un determinato attributo
- tutti i rimanenti attributi non vengono toccati (manterranno quindi gli eventuali valori già presenti).

Un esempio di configurazione è quello mostrato nella tabella seguente (dove si ipotizza di interfacciarsi ad un server Active Directory).

La colonna "Valorizzazione" indica come viene valorizzato il relativo attributo LDAP: a meno che non si tratti di un valore fisso, la notazione @CampoEsse3@ sta ad indicare che il valore viene preso dal relativo campo della vista di reperimento dati di Esse3 (indicata nella configurazione di base EPI_SQL_VIEW).

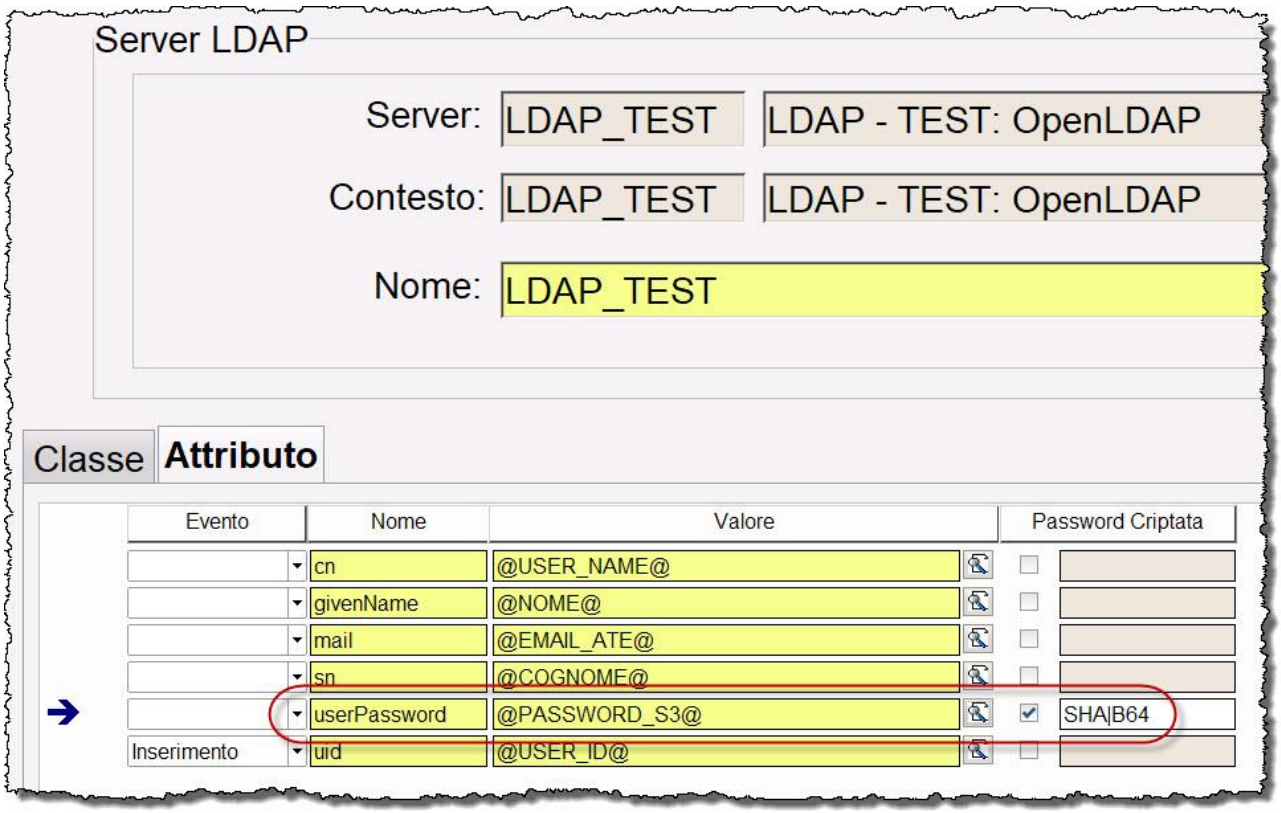
Attributo LDAP	Classe LDAP	Valorizzazione	Note
cn	user	*@USER_ID@*	User ID assegnato in Esse3 *Solo in inserimento (nuovo utente)*
sAMAccountName	securityPrincipal	*@USER_ID@*	User ID assegnato in Esse3 *Solo in inserimento (nuovo utente)*
userPrincipalName	user	*@CUSTOM_2@*	User ID assegnato in Esse3 seguito da "@domain.com" *Solo in inserimento (nuovo utente)*
unicodePwd	user	*@PASSWORD@*	Password
displayName	user	*@NOME@ @COGNOME@*	Nome Cognome
givenName	user	*@NOME@*	Nome
Sn	user	*@COGNOME@*	Cognome
serialNumber	user	*@COD_FIS@*	Codice fiscale
mail	user	*@EMAIL_ATE@*	Email di ateneo assegnata in Esse3
homePostalAddress	user	*@EMAIL@*	Email personale
mobile	user	*@CELLULARE@*	Telefono cellulare
userAccountControl	user	*@CUSTOM_1@*	Valori previsti: - 66048 (normal account + don't expire password) nel caso di account abilitato - 66050 (normal account + don't expire password + account disabled) nel caso di account disabilitato

Gestione delle password e cifratura

Tra le configurazioni di valorizzazione degli attributi sono presenti due impostazioni pensate per la gestione dei campi di tipo password; più in dettaglio si tratta di:

- un flag che consente di dichiarare che un dato attributo memorizza una password, abilitandone così la particolare gestione
- un campo che permette di specificare la cifratura da applicare alla password, nel caso in cui su Esse3 sia disponibile il valore in chiaro.

Un esempio di tale configurazione è quello mostrato nella figura seguente.



La sintassi con la quale indicare la cifratura da applicare alla password (valida solo se è disponibile il suo valore in chiaro ed è impostato il flag password) è la seguente:

`<algoritmo>` oppure `<algoritmo>|<codifica>` oppure `<algoritmo>!<codifica>`

In tale sintassi l'utilizzo di un separatore o un altro determina se il valore cifrato della password (hash) debba essere preceduto da un prefisso che identifica l'algoritmo di cifratura (caso "|") oppure no (caso "!"); nella variante che non fa uso di alcun separatore di default è da intendersi "|" (utilizzo del prefisso).

`<algoritmo>` sta ad indicare l'algoritmo di cifratura da utilizzare ed è possibile specificare uno qualsiasi dei seguenti valori:

- UNIXCRYPT, o semplicemente CRYPT
- AD (valore richiesto da *Microsoft Active Directory* per "unicodePwd" – non si tratta in realtà di una vera cifratura: password in chiaro racchiusa tra doppi apici e codificata in UTF16 Little Endian)
- RSA-BASED
- MD4
- MD5-BASED
- LM (*Microsoft LM hash*)
- NT (*Microsoft NT hash*)
- BCRYPT

- SSHA
- algoritmi standard previsti dalla *Java Cryptography Architecture* (es.: MD5, SHA, SHA-256, SHA-512), come indicato alla relativa sezione MessageDigest
- CLEARTEXT (per forzare il passaggio del valore in chiaro della password, immutato, nel caso il sistema a cui ci si interfaccia lo richieda).

Se è impostato il flag password ma non è stato specificato alcun algoritmo di cifratura viene adottato un default che varia in funzione di quanto indicato nella configurazione di base LDAP_SCHEMA_BUILDER:

- UNIXCRYPT (se si utilizza `it.kion.esse4.epi.utils.ldap.LdapBuilder`)
- AD (se si utilizza `it.kion.esse4.epi.utils.ldap.AdLdapBuilder`).

Inoltre nell'indicazione dell'algoritmo può anche essere utilizzato il suffisso

`/U8`

per indicare che la password da cifrare deve essere interpretata secondo il set di caratteri UTF-8 (altrimenti di default viene adottato ISO-8859-1).

`<codifica>` sta invece ad indicare una eventuale codifica da applicare all'hash ottenuto dalla cifratura della password, per rappresentarne il valore (binario); può assumere i seguenti valori:

- B64 (rappresentazione Base64 – default nel caso di utilizzo del prefisso)
- HEX (rappresentazione Esadecimale)
- RAW (nessuna codifica, ovvero valore binario dell'hash generato – default nel caso di NON utilizzo del prefisso).

Esempio:

assumiamo che il valore in chiaro della password sia "Test_123", nella seguente tabella vengono mostrati il risultato della cifratura SHA nelle diverse varianti previste.

Configurazione	Risultato
SHA SHA|B64	*valore stringa (sequenza di caratteri)* {sha}Up+rp0g+YFjKl5JHBsvQ0miAvHo=
SHA|HEX	*valore stringa (sequenza di caratteri)* {sha}529FABA7483E6058CA97924706CBD0D26880BC7A
SHA! SHA!RAW	*valore binario (sequenza di byte)* 52 9F AB A7 48 3E 60 58 CA 97 92 47 06 CB D0 D2 68 80 BC 7A
SHA!HEX	*valore stringa (sequenza di caratteri)* 529FABA7483E6058CA97924706CBD0D26880BC7A

Nella tabella seguente vengono invece riportati i prefissi che il connettore aggiunge in testa alla password cifrata, a seconda dell'algoritmo di cifratura utilizzato (nel caso in cui la configurazione preveda di generare tale prefisso).

Cifratura	Prefisso
UNIXCRYPT	{crypt}
MD4	{md4}
MD5	{md5}
SHA-1	{sha}
SHA-256	{sha256}
SHA-512	{sha512}
SSHA	{ssha}
BCRYPT	{crypt}
RSA-BASED	{rsa}
LM	{smblm}
NT	{smbnt}

Sincronizzazione della password in presenza di cifratura su Esse3

Quanto descritto poco sopra si applica in particolare nel caso in cui, a tempo di esecuzione della replica su LDAP, è possibile risalire al valore in chiaro della password (consentendone quindi la cifratura nel modo indicato dalla relativa configurazione).

Se invece su Esse3 la password risulta essere già cifrata, in maniera non reversibile, il connettore LDAP

- ignorerà la configurazione `<algoritmo>`, mantenendo la cifratura già presente su Esse3
- tenterà di applicare le rimanenti configurazioni (tipo di codifica dell'hash ed eventuale prefisso) compatibilmente al tipo di cifratura in questione (in quanto alcune cifrature, come ad esempio AD e CLEARTEXT, per loro natura prevedono un formato fisso senza possibilità di varianti).

Per un corretto funzionamento la vista di riferimento per la replica LDAP (indicata nella configurazione di base EPI_SQL_VIEW) deve esporre una colonna PASSWORD_ENCRYPT con il valore dell'algoritmo utilizzato per cifrare la password (identificativo numerico utilizzato anche per il ParConf PWD_ENCRYPTION).

Una parziale eccezione si ha nel caso in cui la password cifrata memorizzata su Esse3 sia già nella forma

`{<algoritmo>}<password hash codificato Base64>`

in tal caso il connettore LDAP cercherà di rilevare automaticamente la cifratura applicata, per poi ricondursi alle medesime logiche già descritte in precedenza.

Vi sono però alcuni sistemi, quali ad esempio ***Active Directory***, che richiedono necessariamente di passare loro il valore in chiaro della password per i più svariati motivi (Active Directory a partire da tale valore in chiaro genera poi in automatico, internamente, i vari hash di cui ha bisogno).

La procedura di provisioning LDAP per garantire la propagazione della password anche in presenza di cifratura su Esse3 può adottare un apposito ***espediente*** consistente in:

- salvare su Esse3 la password, a fronte di ogni modifica, anche in una ulteriore versione cifrata facendo uso di un algoritmo interno, reversibile e noto solo ad Esse3 (tale funzionalità si abilita valorizzando a 1 il Parametro di Configurazione PWD_LM_NT_FORMAT)
- utilizzare un'apposita sintassi nella valorizzazione della password sulla replica LDAP (del tipo `{S3}<cifratura interna>`) che consente al connettore di riconoscere la cifratura interna fatta da Esse3 e ricostruire da questa il valore in chiaro della password.

Tale valore in chiaro sarà presente in memoria per il solo frangente di tempo necessario per effettuare l'operazione di replica via LDAP, in nessun modo si trova mai memorizzato a DB.

La stessa cifratura 'di appoggio' della password utilizzata per questo espediente, se necessario, può essere rimossa immediatamente dopo la corretta esecuzione della sincronizzazione su LDAP.