IAM

Specifiche integrazione con LDAP esterni

V 1.2

Indice

Integrazione IAM – LDAP esterni

Il presente documento descrive i passi operativi per la configurazione di una VPN L2L per il dialogo sicuro tra IAM e la rete che ospita l'LDAP.
A seguito dell'instaurazione della VPN occorre abilitare l'accesso anche sul cloud regionale ed infine implementare le opportune configurazioni applicative su IAM.

Step 1 – configurazione VPN

Chiedere la configurazione di una VPN L2L tra la rete esterna ((tipicamente della Struttura Sanitaria, dove risiede l'infrastruttura LDAP da integrare) e i seguenti indirizzi IP di IAM

Hostname	Indirizzo IP
RPU-IAM-WS-L001	172.29.33.42
RPU-IAM-WS-L002	172.29.33.43
RPU-IAM-WS-L003	172.29.33.44
RPU-IAM-WS-L004	172.29.33.46

La VPN configurata servirà per il dialogo tra i sistemi LDAP remoti e gli ambienti IAM test ed esercizio. E' opportuno contattare preventivamente il SOC di InnovaPuglia per tutte le attività inerenti la configurazione della VPN. La richiesta derivata, mediante la compilazione di un modulo messo a disposizione dalla stessa struttura SOC, dovrà pervenire all'indirizzo mail: info@soc.innova.puglia.it

E' consigliabile utilizzare (ove presente) un LDAP di test; in mancanza di questo occorre seguire gli accorgimenti descritti nello Step 3

Step 2 – abilitazioni Cloud

Chiedere la modifica dei permessi del cloud:

WS to LDAP	SG-RPU-IAM-WS	<IP LDAP da VPN L2L>	Tcp/389 tcp/636 (o altra porta sicura concordata)

La richiesta viene fatta modificando il documento di onboarding sul cloud regionale che va inviato a helpdesk@innova.puglia.it, firmato digitalmente dal referente di IAM.

Step 3 – configurazioni IAM di TEST

Configurazione dell'ambiente di IAM TEST; occorrono i seguenti dati:

1. *url di connessione ldap*; possibilmente ldaps su porta 636
2. *user DN*: è il distinguished name di un utente con permessi sufficienti a leggere i dati
3. *user password*: la password dell'utente di cui sopra
4. *search base*: un DN context sotto cui sono memorizzate le entry degli utenti; ad es: ou=People,dc=my.domain, dc=it
5. *attributo per lo username*: l'attributo che contiene lo username per il login degli utenti; ad es cn
6. *search filter*: una query criterio per filtrare gli utenti, ad es: (&(objectClass=person)(cn=?))
7. *list filter*: una query per ottenere la lista di utenti; ad es: (objectClass=person)

Stabilita la connessione con ldap occorre configurare in IAM gli attributi dell'ldap per il mapping con gli attributi restituiti da IAM; questo deve essere fatto volta per volta a seconda della struttura dell'ldap e delle esigenze delle applicazioni che utilizzano i dati in esso presenti.

La richiesta comprensiva dei dati va inviati a spid@regione.puglia.it da parte dei referenti tecnici che gestiscono l'LDAP

Per l'ambiente di IAM test, in mancanza di un LDAP di test, occorre fare in modo che l'utente le cui credenziali sono definite ai punti 2 e 3 acceda NON a tutto l'ldap di esercizio, ma a un ramo con utenze di test; in questo caso per il test occorre quindi definire una searchbase (punto 4) opportuna e diversa da quella di esercizio.
Per l'ambiente di test e per quello di esercizio è opportuno inoltre che l'utente possa accedere solo al set di dati richiesto dal servizio integrato con IAM che utilizza l'ldap.

Step 4 – integrazione in esercizio

Richiedere l'integrazione in esercizio tramite mail a spid@regione.puglia.it; i dati di accesso a ldap (Step 3 punti 2, 3 e 4) devono essere opportunamente modificate per l'accesso ai dati di esercizio.

Il titolare dei dati presenti in LDAP deve nominare il fornitore di IAM Responsabile del Trattamento dei dati a titolo non oneroso.