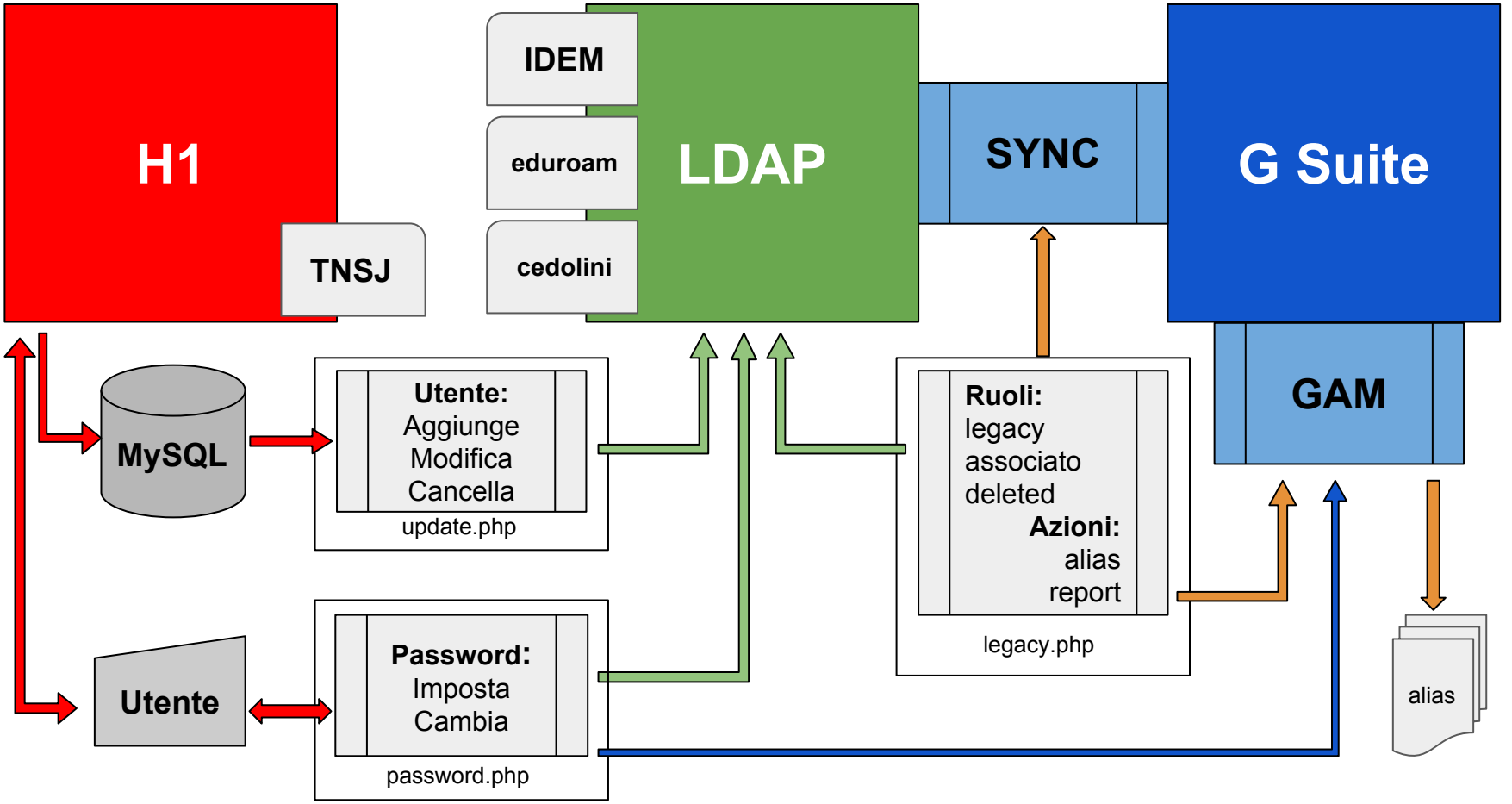
Gsuite - INAF
Procedure di sincronizzazione

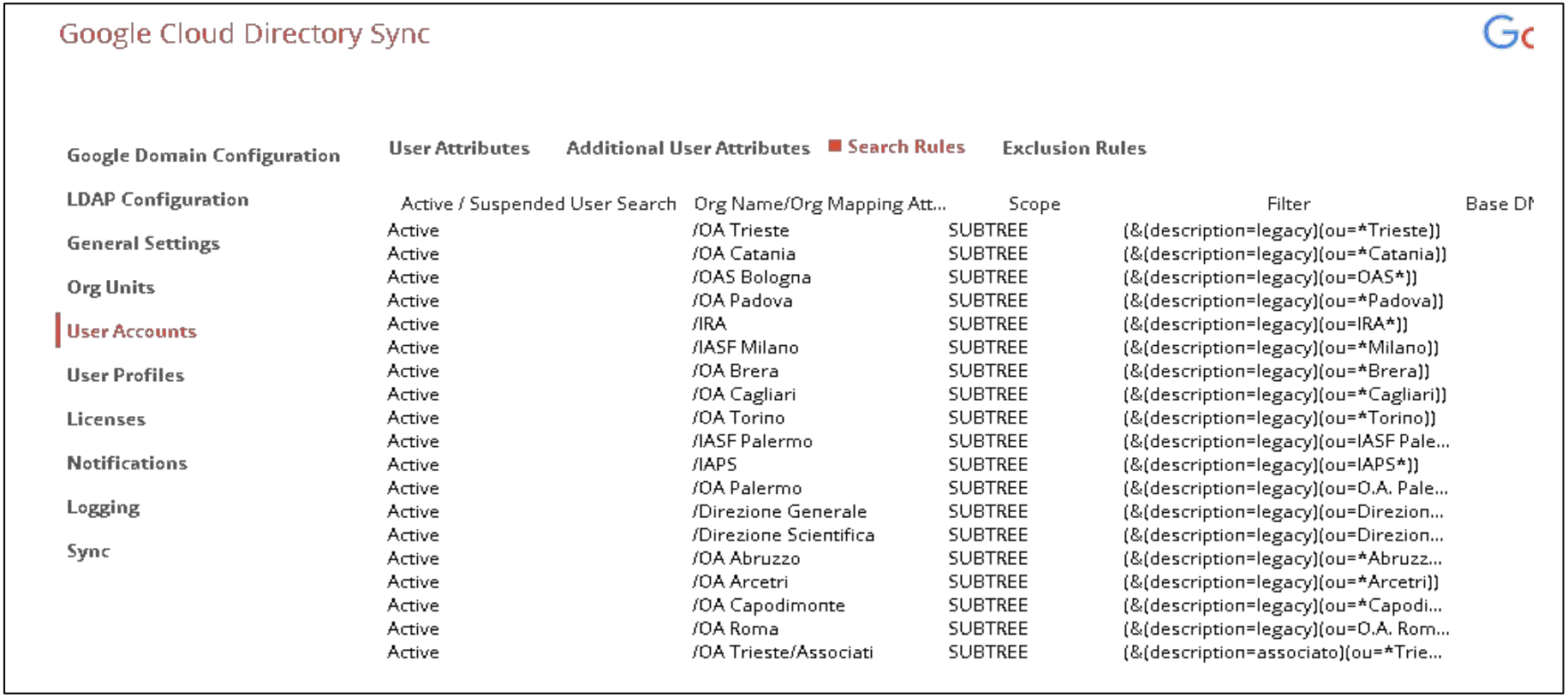
Franco Tinarelli - ICT Catania 2018



GoogleCloudDirSync

Google Cloud Directory Sync è il software che permette di definire le regole di sincronizzazione tra il server LDAP di INAF e la G Suite.

È composto da un applicativo grafico (config-manager) che permette di definire i ruoli per l'assegnazione degli utenti all'organizzazione appropriata:



GoogleCloudDirSync

e da un programma eseguibile da linea di comando (sync-cmd) che viene utilizzato dalle procedure automatiche (crontab) che gestiscono la creazione, la modifica e la cancellazione degli utenti in LDAP e di conseguenza nella G Suite.

```
// Sincronizza il DB Google con LDAP
    $gsync = "/opt/GoogleCloudDirSync/sync-cmd -a -c /root/scripts2/INAF_SYNC";
    $status = exec( $gsync );
```

Le tre righe precedenti appartengono alla procedura legacy.php che gestisce i parametri utente, specifici per la G Suite, in LDAP.

La procedura è eseguita tutte le mattine alle ore 05:00 dopo la procedura di update che sincronizza H1 con LDAP.

se la procedura di update aggiunge, modifica o cancella utenti in LDAP, la procedura di sync aggiunge, modifica o sospende gli stessi utenti in G Suite, in base al parametro “description”:

description: legacy	aggiunge o mantiene l’utente con licenza Business
description: associato	aggiunge o mantiene l’utente con licenza Basic (*)
description: deleted	sospende l’utente (l’utente esiste ma non appartiene più alle categorie precedenti)

Se l’utente viene eliminato in LDAP, sono passati 6 mesi dalla cessazione dal servizio, l’utente viene cancellato dalla G Suite.

GAM (Google Apps Manager)

"GAM is a command line tool that allows administrators to manage many aspects of their Google Apps Account."

Questa è la descrizione di GAM che trovate nel Wiki di GitHub: **https://github.com/jay0lee/GAM/wiki**

Contrariamente alla procedura di sync che viene utilizzata solo dalle procedure automatiche, GAM è il comando da utilizzare per gestire la vostra utenza.

Con GAM potete fare le stesse cose che fareste con la console di G Suite, ma potendo utilizzarlo all'interno di procedure diventa ricorsivo, può generare array d'informazione scrivibili su files, può usare gli stessi files per modificare, aggiungere, o cancellare attributi a utenti e gruppi (es.)

```
// Legge le informazioni degli utenti dal server LDAP e usa GAM per
// aggiungere l'email istituzionale come mail alias all'utente G Suite
if( $users = allLDAPusers() ) {
   $maxUsers = $users['count'];
   for( $i=0; $i<$maxUsers; $i++ ) {
        if( $users[$i]['description'] == "legacy" ) {
            $GamStatus = "";
            $GamArray = array();
            $GamCommand = "/opt/gam/gam create alias ".$users[$i]['mail']." user ".$users[$i]['username']."@inaf.it\n";
            $GamReturn = exec( $GamCommand, $GamArray, $GamStatus );
        }
    }
}
```

La procedura usa il comando "**gam create alias** *mail-alias* **user** *gsuite-username"* e in un unico run di pochi secondi aggiunge circa 1500 mail alias.

GAM (Installazione)

Per installare GAM su di un vostro computer servono:

Il **Software**. esiste per Linux, Mac e Windows.

- Potete copiarlo dal Google Drive nella directory: Team Drives ⇨ GSuite INAF ⇨ Applicativo - INAF
  (un ringraziamento va ad Amedeo Petrella e Danilo Selvestrel per aver creato e popolato la directory.)

- Potete scaricarlo seguendo le istruzioni del Wiki di GitHub: **https://github.com/jay0lee/GAM/wiki**

I **Files di Progetto** client_secrets.json e oauth2service.json. Questi due files sono stati già creati e dovete utilizzarli **senza ricrearli** (il Wiki spiega come) e **senza modificarli.** Li trovate sul Drive nella stessa directory da dove copiate il software, nella subdir Chiavi Applicative.
(Grazie a Sara Cipolletti e Stefano Mongardi di Ingenja per averli generati.)

Il **File di Autorizzazione** oauth2.txt. Questo file viene generato durante la fase di configurazione del software. Se avete già utilizzato GAM con altri progetti dovete rinominare o cancellare questo file prima di riconfigurare il software.

Trovate nel Drive anche un file **Istruzioni.gdoc** che contiene una guida veloce all'installazione:

- copiare l'eseguibile adatto al proprio S.O. in una cartella insieme ai file qui contenuti
- lanciare il comando
  gam oauth2 create
- Premere **c**
- Seguire le istruzioni

GAM (Installazione)

Di default GAM viene installato nella sub directory **bin** della vostra **home directory**, la configurazione crea un file di autorizzazione associato al vostro account di amministratore. Potete installare in un'altra directory facendo mente locale al fatto che **chiunque sia in grado di eseguire GAM lo farà con le vostre credenziali**.

I files del software GAM dopo una nuova installazione col comando `bash <(curl -s -S -L https://git.io/install-gam)`

$ ls -F bin/gam

GamCommands.txt	gam*	nobrowser.txt
LICENSE	lastupdatecheck.txt	whatsnew.txt

Il file **nobrowser.txt** viene creato durante l'installazione se indicate che state configurando da un computer non in grado di eseguire automaticamente un browser web. Durante la configurazione viene indicata la url da inserire su di un'altro computer e viene richiesto l'inserimento dell'hash generato.

Esistono altri file che inibiscono alcune funzioni che normalmente il software usa durante l'esecuzione:

nochache.txt impedisce di ricordare quanto richiesto nell'ultimo comando e il suo risultato.

noupdatecheck.txt impedisce al software di controllare automaticamente la presenza di nuove versioni. La presenza di una nuova versione blocca l'esecuzione del comando, questo comportamento sarebbe letale per le procedure batch eseguite automaticamente. Dovete ricordarvi di fare l'aggiornamento manualmente controllando le nuove versioni su https://github.com/jay0lee/GAM/releases ela vostra versione col comando gam version e aggiornate con: `bash <(curl -s -S -L https://git.io/install-gam) -l`

GAM (Configurazione)

Se avete installato copiando i file dal Drive ricordatevi di aggiungere al vostro .bash_profile il comando gam() { "/Users/ftinarel/bin/gam/gam" "$@" ; } questo vi permette di eseguire gam senza curarvi del path.

Per configurare **dovete copiare i due file json** nella stessa directory dell'eseguibile e dare il comando:

$ gam create oauth2

Warning corretto il file non deve esistere

… UserWarning: Cannot access /Users/ftinarel/bin/gam/oauth2.txt: No such file or directory

Select the authorized scopes by entering a number.
Append an 'r' to grant read-only access or an 'a' to grant action-only access.

[*] 0) Classroom API - counts as 5 scopes
[*] 1) Cloud Print API
…
...
e) Exit without changes
c) Continue to authorization
Please enter 0-23[a|r] or s|u|e|c: **c**

What is your G Suite admin email address? **nome.cognome@inaf.it**

url da inserire in un browser web

Go to the following link in your browser:

https://accounts.google.com/o/oauth2/v2/auth?redirect_uri=urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&response_type=code&client_id=
…
… login_hint=nome.cognome%40inaf.it&access_type=offline

hash generato dalla url

Enter verification code: 4/Ug……..UJbc
Authentication successful.

La configurazione ha prodotto il file **oauth2.txt** e siete in grado di utilizzare gam da riga di comando o all'interno di procedure batch.

GAM (procedure)

Potete consultare due procedure, create dall'Osservatorio di Padova, per fare pratica con l'utilizzo di gam in modo batch. Le trovate nel Drive nella directory: Team Drives ⇨ GSuite INAF ⇨ Scripts

clone-group.php permette di copiare i settaggi di un gruppo google in un altro gruppo.
Se il gruppo di destinazione non esiste può essere creato.

gam info group *email-gruppo-origine*

```
// Ritorna lo stato del comando eseguito utilizzando PHP (> 0 se fallisce)
$GamStatus = "";
// Conterra tutto il risultato del comando eseguito, conviene azzerarlo puo'
// contenere anche il risultato di altri comandi gam
$GamArray = array();
// Comando gam da passare alla funzione exec()
$GamCommand = "/path/gam info group email-gruppo-origine";
// Ritorna l'ultima riga del l'output comando eseguito nella variabile $GamReturn
$GamReturn = exec( $GamCommand, $GamArray, $GamStatus );
```

gam create group email-*gruppo-destinazione* **name** *nome-gruppo* **description** *descrizione-gruppo*
gam create alias *alias-gruppo* **group** *email-gruppo-destinazione*
gam update group *email-gruppo-destinazione* **attributo valore [attributo valore]**

sincronizza-liste.php aggiorna i gruppi Google di una Sede, inserendo gli utenti contenuti nel DB di H1 nel gruppo adeguato.