INFN Sezione di Roma, pagine *Web* personali.

Le pagine web personali sono disponibili solo per utenti AFS.

Gli utenti della Sezione INFN di Roma possono pubblicare pagine web personali raggiungibili tramite uno dei seguenti due indirizzamenti:

- `http://www.roma1.infn.it/~$USER`
- `http://www.roma1.infn.it/people/$USER`

Cosa deve fare l'utente:

1. Creare un nuova directory `www` nella sua home-directory in AFS:

```
$ cd ~
$ mkdir www
```

2. Definire opportune ACL (Access Control List) per quella directory, in particolare abilitare la lettura di quella zona AFS al server Web e disabilitare l'accesso al resto del "mondo":

```
$ cd ~
$ fs setacl www rm1admin:www-nodes read
$ fs setacl www system:anyuser     none
```

3. Preparare un file `index.html` nella stessa directory `$HOME/www`. Tale file sarà letto di default nell'accedere alla URL `http://www.roma1.infn.it/~$USER`
   Per motivi di sicurezza, in mancanza del file `index.html` NON sarà fornito un elenco del contenuto della directory.

Come scrivere pagine Web

Il linguaggio necessario per scrivere pagine Web e' HTML (HyperText Markup Language).
Documenti introduttivi al linguaggio HTML sono disponibili alle seguenti URL (Uniform Resource Locator):

- http://www.w3.org/html/
- https://it.wikipedia.org/wiki/HTML

Indexing

Come già detto l'indexing di una directory via web è disabilitato per default e deve essere esplicitamente consentito dall'utente. Per fare ciò è sufficiente creare un file, nella directory in questione, che si chiami .htaccess e che contenga il seguente record:

```
Options Indexes
```

Una volta creato il file, nel sottoalbero a partire da quella directory è consentito il listing via web.

Accesso regolato da password

La attuale implementazione consente la pubblicazione di informazioni il cui accesso sia limitato ad uno o più utenti. È possibile controllare l'acesso attraverso apposite coppie di username e password oppure abilitare utenti della cella nazionale AFS (REALM Kerberos5 "INFN.IT").

Accesso attraverso username e password locali

È possibile definire una apposita username e password per controllare l'accesso ad un sottoalbero della propria area web.

Nella directory che ospita informazioni riservate dovrà essere presente un file `.htaccess` che conterrà l'indirizzo del repository (file **`.htFILE`**) contenente la coppia *username:password* per l'accesso a quel ramo dell'albero www.

- File `.htaccess`

Di seguito è riportato un template del file `.htaccess`

---------- inizio file `.htaccess` ----------

```
AuthUserFile /DIRECTORY/.htFILE
AuthGroupFile /dev/null
AuthName "SHORT_DESCRIPTION"
AuthType Basic

<Limit GET PUT POST>
order allow,deny
allow from all
require valid-user
</Limit>
```

---------- fine file `.htaccess` ----------

Le stringhe indicate in **bold** vanno sostituite con il valore corretto:

FILE = parte variabile del nome che si è voluto dare al file contenente le coppie username:password. Per motivi di sicurezza è importante che il nome di questo file inizi con **`.ht`** ;

DIRECTORY = path completo della directory in cui è stato creato il file `.ht`**FILE**.
La directory scelta dovrà soddisfare i seguenti requisiti:
- dovrà risiedere in zona AFS;
- non dovrà essere visibile via web (quindi non potrà essere, ad esempio, una sottodirectory di `/afs/infn.it/roma1/project/www/htdocs`, né di `/afs/infn.it/roma1/$USER/www`;
- dovranno essere definite opportune ACL che consentato la lettura dello spazio disco al server web e neghino l'accesso al resto del mondo.

Es:
```
$ cd ~
$ mkdir myhtpw
$ fs setacl myhtpw rm1admin:www-nodes read
$ fs setacl myhtpw system:anyuser     none
```

SHORT DESCRIPTION = breve descrizione del contenuto di quella directory.

es: `AuthUserFile` **`/afs/infn.it/roma1/user/pippo/myhtpw/`**`.ht`**`plutopw`**
`AuthName` **`"Internal Information"`**

- File **`.ht`**`FILE`

Di seguito è riportato un esempio del file `.ht`**`FILE`**

---------- inizio file `.ht`**`FILE`** ----------
```
admin:XSR7RbCDFAdcI
ospite:PdpinzuHWnyFg
```
---------- fine file `.ht`**`FILE`** ----------

Come fa supporre l'esempio sovrastante, le username dovranno essere scritte in chiaro, mentre le password dovranno essere **crittate**.
Per ottenere la stringa crittata corrisponde alla password scelta è disponibile una form sul sito del SICR:

https://www.roma1.infn.it/sicr/

SERVIZI
- **MyWebCrypt**

Accesso ad utenti della cella nazionale AFS (REALM K5 INFN.IT)

E' altresì possibile consentire l'accesso ad un sottoalbero della propria area web ad uno o più utenti REALM Kerberos5 nazionale "INFN.IT", che si autentichino con le proprie credenziali.

Nella directory che ospita informazioni riservate dovrà essere presente un file `.htaccess` che conterrà l'elenco dei principal (<username>@INFN.IT) degli utenti autorizzati.

- File `.htaccess`

Di seguito è riportato un template del file `.htaccess`

---------- inizio file `.htaccess` ----------

```
SSLRequireSSL

AuthType Kerberos
AuthName "<SHORT_DESCRIPTION>"
KrbAuthRealms INFN.IT
KrbServiceName host
KrbMethodK5Passwd On
KrbMethodNegotiate Off
Krb5KeyTab /etc/httpd/conf/keytab
require user <USERNAME_1>@INFN.IT <USERNAME_2>@INFN.IT
```

---------- fine file `.htaccess` ----------

Le stringhe indicate in **bold** vanno sostituite con il valore corretto:

`SHORT DESCRIPTION` = breve descrizione del contenuto di quella directory.

es: `AuthName "Internal Information"`

`USERNAME_x` = username dell'utente autorizzato