

# Installazione di un server VOMS

\$Id: installazione.txt,v 1.6 2004/12/03 09:22:16 rmurri Exp \$

Queste note descrivono l'installazione del sistema VOMS (server + interfaccia web di amministrazione) su una macchina Scientific Linux CERN 3, fatta per il progetto Grid@TS/EGRID.

## Riferimenti

[VOMS-Admin-Inst] [edg-voms-admin Install Guide, http://edg-wp2.web.cern.ch/edg-wp2/security/voms/edg-voms-admin-install-guide.pdf](http://edg-wp2.web.cern.ch/edg-wp2/security/voms/edg-voms-admin-install-guide.pdf)

[VOMS-Suite] [The VOMS Software Suite: an Installation and Users' Guide, http://infnoforge.cnaif.infn.it/docman/view.php/7/55/software.pdf](http://infnoforge.cnaif.infn.it/docman/view.php/7/55/software.pdf)

[VOMS-Notes] [Notes on VOMS, http://dimou.home.cern.ch/dimou/lcg/voms/REFERENCES-NOTES](http://dimou.home.cern.ch/dimou/lcg/voms/REFERENCES-NOTES)

[VOMS+LCMAPS] [Integration of VOMS+LCAS/LCMAPS, http://grid-it.cnaif.infn.it/fileadmin/sysadm/voms-integration/voms-integration.html](http://grid-it.cnaif.infn.it/fileadmin/sysadm/voms-integration/voms-integration.html)

[VOMS-Deploy] [Deploy a VOMS service, http://grid-deployment.web.cern.ch/grid-deployment/cgi-bin/index.cgi?var=gis/voms-deploy](http://grid-deployment.web.cern.ch/grid-deployment/cgi-bin/index.cgi?var=gis/voms-deploy)

[EDG-SIG] [EDG Security Installation Guide 1.5.3, http://edg-wp2.web.cern.ch/edg-wp2/security/doc/edg-java-security-1.5.3/install-guide/html/security-installguide.h](http://edg-wp2.web.cern.ch/edg-wp2/security/doc/edg-java-security-1.5.3/install-guide/html/security-installguide.h)

[MIG] [LCG Manual Installation Guides, http://grid-deployment.web.cern.ch/grid-deployment/gis/release-docs/MIG-index.html](http://grid-deployment.web.cern.ch/grid-deployment/gis/release-docs/MIG-index.html)

[CE-MIG] [CE Manual Installation Guide \(LCG-2.2.0\), http://www.cern.ch/grid-deployment/gis/release-docs/LCG-2\\_2\\_0/CE/CE.pdf](http://www.cern.ch/grid-deployment/gis/release-docs/LCG-2_2_0/CE/CE.pdf)

## Installazione

L'installazione è stata eseguita su una macchina Scientific Linux CERN 3.0.4.

### 1. Installazione dei certificati host

I certificati host, generati da una CA riconosciuta, devono essere copiati in `/etc/grid-security/`:

```
mkdir -p /etc/grid-security
install -o root -g root -m 0644 hostcert.pem /etc/grid-security
install -o root -g root -m 0400 hostkey.pem /etc/grid-security
```

Il risultato dell'operazione deve essere:

```
rw-r--r--  root  root  hostcert.pem
r-----  root  root  hostkey.pem
```

Nel caso di un host con multipli nomi DNS, occorre scegliere *un* nome per un servizio; si devono quindi copiare i certificati generati col nome host scelto in `/etc/grid-security/` -- per esempio, il server Tomcat (e quindi *tutti* i servizi che girano dentro di esso) usa i file

```
/etc/grid-security/tomcat4cert.pem e
/etc/grid-security/tomcat4key.pem con permessi:
```

```
rw-r--r-- tomcat4 tomcat4 tomcat4cert.pem
r----- tomcat4 tomcat4 tomcat4key.pem
```

## 2. Installare i seguenti pacchetti di LCG-2/EDG::

```
edg-profile edg-profile-umask edg-gpt-profile edg-utils-system voms-server_gcc3_2_2
edg-voms-admin edg-voms-admin-config edg-voms-admin-interface edg-voms-admin-client
edg-java-security-client edg-java-security-test commons-cli MySQL-client
```

La lista *non* è esaustiva, perché `apt-get` si occupa di risolvere le dipendenze; si intende quindi che i pacchetti qui sopra siano installati con una o più invocazioni di `apt-get`.

Durante l'installazione dei pacchetti `MySQL-server` e `tomcat4` si avranno messaggi riguardo ad alcune operazioni di configurazione da effettuare a mano; ignorarli -- le istruzioni opportune sono date più avanti in questo documento.

*Nota:* i seguenti pacchetti non sono probabilmente necessari al funzionamento del sistema e possono forse essere omissi:

```
edg-java-security-client
edg-java-security-test
commons-cli
```

## 3. Configurazione delle librerie aggiuntive

Aggiungere le seguenti righe in fondo al file `/etc/ld.so.conf` (cfr. la sezione 4.2 di [\[CE-MIG\]](#)):

```
/opt/gcc-3.2.2/lib
/opt/globus/lib
/opt/edg/lib
/usr/local/lib
```

E poi eseguire il programma `ldconfig`:

```
ldconfig
```

## 4. Gruppi e utenti necessari

Aggiungere il gruppo `voms` in `/etc/group`:

```
groupadd voms
```

## 5. Installazione dei certificati CA

I certificati delle CA riconosciute devono essere copiati in `/etc/grid-security/certificates`; due metodi sono possibili:

- ◆ per le CA riconosciute in LCG-2, è presente nel repository dei un pacchetto RPM che installa i file necessari;
- ◆ altrimenti è sufficiente copiare i file `hash.0` e `hash.signing_policy` in `/etc/grid-security/certificates`.

Sul server VOMS del gruppo di sviluppo di StoRM sono stati installati:

```
ca_INFN
ca_CERN
```

dai pacchetti delle CA riconosciute in LCG-2, mentre i file della CA del testbed di EGRID sono stati copiati a mano.

## 6. Sicurezza del server MySQL

Occorre impostare una password per l'utente amministrativo `root` sul server MySQL appena installato::

```
mysqladmin -u root password ***** mysqladmin -u root -h egrid-1.egrid.it password *****
```

*Attenzione!* Gli script di configurazione del servizio VOMS falliranno se la password scelta contiene caratteri speciali per la shell (e.g., `'`, `"`, ``` ecc.) -- si consiglia di limitare la password ai soli caratteri alfanumerici.

*Attenzione!* Gli utenti creati da `edg-voms-admin-configure` per l'accesso ai database hanno accesso da *ogni host in rete*:

```
mysql> select user,host from mysql.user;
+-----+-----+
| user          | host          |
+-----+-----+
| stormdev_adm | %             |
| stormdev_que | %             |
| stormdev_seq | %             |
| stormdev_upd | %             |
|               | egrid-1.egrid.it |
| root          | egrid-1.egrid.it |
|               | localhost     |
| root          | localhost     |
| stormdev_adm | localhost     |
| stormdev_que | localhost     |
| stormdev_seq | localhost     |
| stormdev_upd | localhost     |
+-----+-----+
```

È quindi opportuno proteggere il server MySQL limitando l'accesso tramite un firewall oppure con i *tcp wrappers* (man `hosts.deny`).

*Nota:* Il comando `mysqladmin` sta nel pacchetto 'MySQL-client':

```
apt-get install MySQL-client
```

## 7. Installazione di Java

Gli script di EDG leggono il file `/etc/java/java.conf` per rintracciare la JVM, ma questo file non viene creato automaticamente durante l'installazione del pacchetto. Perciò:

1. Creare il file `/etc/java/java.conf` :

```
mkdir -p /etc/java
echo export JAVA_HOME=/usr/java/j2sdk1.4.2_04 \
>> /etc/java/java.conf
```

2. Si possono anche creare link simbolici alla JVM nel path:

```
for x in /usr/java/j2sdk1.4.2_04/bin/*; do
ln -s $x /usr/local/bin
done
```

*Nota:* Sostituire la stringa `j2sdk1.4.2_04` con la versione di J2SDK effettivamente installata sul proprio sistema.

## 8. Configurazione di Tomcat4 & EDG Java Security

Seguendo le istruzioni di [\[EDG-SIG\]](#),

<http://edg-wp2.web.cern.ch/edg-wp2/security/doc/edg-java-security-1.5.3/install-guide/html/node24.html>

, si eseguono le seguenti operazioni:

```
# edg-java-security-post-install.sh
Doing ln -sf /usr/share/java/bcprov-jdk14.jar /var/tomcat4/server/lib
Doing ln -sf /opt/edg/share/java/edg-java-security.jar /var/tomcat4/server/lib
Doing ln -sf /usr/share/java/log4j.jar /var/tomcat4/server/lib
# edg-java-security-tomcat-configure --verbose --secure
```

## 9. Configurazione del VOMS server

Il server VOMS si attiva e configura con il programma `edg-voms-admin-configure`.

Seguendo le istruzioni di [\[VOMS-Admin-Inst\]](#) e [\[VOMS-Deploy\]](#), si esegue il comando (la manpage `man edg-voms-admin-configure` spiega in dettaglio le varie opzioni):

```
# edg-voms-admin-configure install --vo='stormdev' --port=15000 \
--smtp-host=localhost --mail-from='stormdev@egrid-1.egrid.it' \
--dbapwd='*****' \
--password='*****'
```

che produce come output::

```
/opt/edg/sbin/edg-voms-admin-configure uses the following settings:
EDG_LOCATION           /opt/edg
EDG_LOCATION_VAR       /opt/edg/var
EDG_TMP                /tmp
VO name                storm-dev
VO alias               storm_dev
vomsd port number      15000
X509 certificate       /etc/grid-security/hostcert.pem
CA certificates        /etc/grid-security/certificates
config userid          0
config group tomcat    91
config group voms      10001
smtp host              localhost
mail from              voms@egrid-1.egrid.it
Database name          voms_storm_dev
Creating the database...
...loading the scheme
...creating the roles
...inserting the initial values
...saving the settings ...processing template
/opt/edg/etc/edg-voms-admin/voms.database.properties.template
to
/opt/edg/var/etc/edg-voms-admin/storm_dev/voms.database.properties
Installing vomsd configuration ...
/opt/edg/etc/voms/storm-dev/voms.pass
/opt/edg/etc/voms/storm-dev/voms.database.properties
Service properties ... processing template
/opt/edg/etc/edg-voms-admin/voms.service.properties.template
to
/opt/edg/var/etc/edg-voms-admin/storm_dev/voms.service.properties
context block ... processing template
/opt/edg/etc/edg-voms-admin/context.xml.template
to
/opt/edg/var/etc/edg-voms-admin/storm_dev/edg-voms-admin-storm-dev.xml
Installation complete.
```

Alcuni bug:

1. La password dell'amministratore di database `--dbapwd` non può contenere caratteri speciali per la shell, p.es. non può essere `pippo; 2` oppure `gino" 3`
2. Se la password dell'utente usato dal server VOMS per accedere alle tabelle non è specificata sulla riga di comando, dovrebbe essere auto-generata, secondo la documentazione; invece, lo script fallisce e non riesce ad accedere al database.
3. Se non sono indicate password sulla riga di comando, lo script riporta di aver generato alcuni file SQL da inserire a cura dell'amministratore del DB; non si capisce in quale directory vengano creati questi file SQL.
4. **PROBLEMA DI SICUREZZA:** tutti gli utenti MySQL creati dallo script usano la stessa password!
5. Se si usano "-" nel nome della VO, lo script `/etc/init.d/edg-voms-admin` prende il VO *alias* invece del nome di VO corretto e quindi non riesce a trovare i file necessari. (I nomi delle VO sono presi da: `/opt/edg/var/etc/edg-voms-admin`)
6. Sembra che lo script di configurazione non popoli il database delle CA di VOMS con il contenuto di `/etc/grid-security/certificates`; si possono inserire a mano le CA presenti in `/etc/grid-security/certificates` con il seguente script:

```
for x in /etc/grid-security/certificates/*.0; do \  
    y="openssl x509 -noout -subject -in $x | cut -c10-"; \  
    z="echo $y | sed -e 's/. *CN=//'"; \  
    mysql -D voms_stormdev \  
        -e "INSERT INTO voms_stormdev.ca VALUES (NULL, '$y', '$z');" \  
        -p'*****';  
done
```

7. Lo script `edg-voms-make-vo-rpms` non funziona:

```
# edg-voms-make-vo-rpms  
Generating edg-voms-vo-stormdev.noarch.0.1-1.rpm  
Written /tmp/edg-voms-make-vo-rpms-25413/SPECS/edg-voms-vo-stormdev.spec  
rpm -bb /tmp/edg-voms-make-vo-rpms-25413/SPECS/edg-voms-vo-stormdev.spec  
error: no description in %changelog
```

Il modo di procedere è questo: per prima cosa si esegue:

```
# edg-voms-make-vo-rpms --dryrun  
Generating edg-voms-vo-stormdev.noarch.0.1-1.rpm  
Written /tmp/edg-voms-make-vo-rpms-25437/SPECS/edg-voms-vo-stormdev.spec  
rpm -bb /tmp/edg-voms-make-vo-rpms-25437/SPECS/edg-voms-vo-stormdev.spec
```

Poi si aggiunge una riga qualunque nella parte `%changelog` del file `.spec` generato dal script:

```
%changelog  
* Thu Sep 18 2003 ?kos Frohner <Akos.Frohner@cern.ch>  
RIGA AGGIUNTA PER CALMARE RPM
```

E infine si esegue `rpm -bb` a mano:

```
rpm -bb /tmp/edg-voms-make-vo-rpms-25437/SPECS/edg-voms-vo-stormdev.spec
```

1. **[BUG]** Creazione di `voms.database.properties`

Lo script `edg-voms-admin` non crea il file `/opt/edg/etc/voms/stormdev/voms.database.properties`, necessario al server `edg-voms` per accedere al database; occorre provvedere a mano:

```
ln /opt/edg/var/etc/edg-voms-admin/stormdev/voms.database.properties \  
/opt/edg/etc/voms/stormdev/
```

## 2. Abilitazione degli script di partenza

Gli script di avvio vengono messi in `/opt/edg/etc/init.d`; per renderli disponibili al sistema, si usa:

```
ln -s /opt/edg/etc/init.d/* /etc/init.d/  
chkconfig --del tomcat4  
chkconfig --add edg-tomcat4  
chkconfig --add edg-voms-admin
```

Nonostante il nome, `init.d/edg-voms-admin` è lo script che fa partire il server VOMS.

## 3. Controllo di funzionamento

L'interfaccia web di VOMS server risponderà agli URL:

`https://localhost:8443/edg-voms-admin/stormdev` `http://localhost:8080/edg-voms-admin/stormdev`

*Attenzione!* Collegandosi agli URL su `localhost` si è automaticamente autorizzati come amministratori! Per modificare questo comportamento, si alteri il file `/opt/edg/var/etc/edg-voms-admin/stormdev/voms.service.properties`

*Nota:* Collegandosi ad un URL locale fuori dalla gerarchia `/edg-voms-admin/stormdev`, Tomcat risponderà con un errore "No Context configured to process this request"

A questo punto, si può creare il primo utente ed assegnargli il ruolo amministrativo con:

```
edg-voms-admin --vo=stormdev create-user /tmp/usercert.pem \  
assign-role VO VO-Admin /tmp/usercert.pem
```

## 4. Ulteriori passi di installazione

In [VOMS+LCMAPS], sezione 2.1 sono elencati due ulteriori passi da seguire per abilitare la corretta registrazione degli utenti.

## Modifiche

\$Log: installazione.txt,v \$ Revision 1.6 2004/12/03 09:22:16 rmurri

- configurazione di `VO.databases.properties`

Revision 1.5 2004/11/30 14:30:25 rmurri

- Usare la versione corretta del server

Revision 1.4 2004/11/25 19:42:41 rmurri

- corretti i permessi per `hostcert.pem`

Revision 1.3 2004/11/25 18:27:34 rmurri

- come disabilitare accesso amministrativo da `localhost`
- ulteriori passi di installazione dal documento di Enrico Ferro

Revision 1.2 2004/11/25 18:06:59 rmurri

- note sulla sicurezza di MySQL

Revision 1.1 2004/11/25 17:58:08 rmurri

- prima stesura