The VOMS Software Suite: An Installation and User's Guide

Vincenzo Ciaschini

December 20, 2005

Contents

Chapter 1

Generalities

1.1 Getting the software

Voms can be downloaded from the authoritative infnforge CVS at http://infnforge.cnaf.infn.it, or the EGEE copy at http://jra1mw.cvs.cern.ch:8180/cgi-bin/jra1mw.cgi/org.glite.security.voms You can get the nightly rpms at http://glite.web.cern.ch/glite/packages/. You may skip the next chapter if you downloaded the RPM version.

1.2 Compiling the source

After having downloaded and installed the source, go to the `voms/` subdirectory and run `./configure`. Apart from the usual standard options, there are four extra ones you may be interested into:

–**enable-docs=[yes/no]** — This option, enabled by default, specifies whether the documentation should or should not be generated.

–**with-debug** — This option, disabled by default, specifies that the source should be compiled with debug options, e.g. without optimizations and with the symbol table included. It is not advised to use a version compiled with this switch for production.

–**with-globus-flavor=<flavor>** — This option compiles the code against the specified flavor of Globus. Please note that this means that the specified flavor should be installed on the compiling machine. The default is `gcc32dbg`.

–**with-globus=<dir>** — This option specifies the path under which the Globus toolkit has been installed. The default value is `/opt/globus`.

After that, a simple `make` is more than enough to compile the sources.

1.3 Installation

To install the software you may execute the commands `make install` will install all the components of the software.

1.4 Compatibility

With version 1.6.0 and onwards, compatibility with VOMS version 1.1.x and previous version is now dropped. This means that servers that are not capable of generating ACs are now unsupported.

Chapter 2

edg-voms

2.1 Configuration

To complete configuration of `edg-voms`, you are supposed to execute the `/opt/edg/libexec/voms_install_db` command. It takes the following options:

–**mysql-home**	This option lets you specify the home directory of mysql. This information is usually included in the $MYSQL_HOME environment variable, and if that is the case on your machine then you do not need to specify this option.
–**db**	This is the name of the database that will contain the information about the VO. Its default name is "voms", and you need to specify this information if and only if you are installing multiple servers on the same machine. Otherwise the default is perfectly fine.
–**port**	This is the port number where the VOMS server will be listening. There is no default value for this option, although 15000 is the recommended choice for the first server installed on a host, and additional servers may use 15001, 15002, etc...
–**voms-vo**	This is the name of the VO to which the VOMS server belongs. Its default value is "unspecified" which is *not* a valid value for a VO name. For this reason, this option should be *always* specified.
–**mysql-admin**	This is the name of the MySQL root user. It is needed because the script needs to create a new DB and a new user. Its default value is "root", which is the standard on the default MySQL installation.

–mysql-pwd	This is the password of the MySQL account specified by the previous option. Its default value is “”, meaning that there is no password. This is *not* advisable. The root account of a MySQL server hosting a VOMS DB *must* be protected by a password.
–voms-name	This is the username of the voms MySQL account that will be setup to access the newly created DB. Its default value is “voms”, and it is perfectly fine if you are installing a single server. If you are installing further servers on the same machine, you *MUST* change this name to some other value.
–voms-pwd	This is the password associated with the *voms-name* account. It does have a default value, but this should never be used. You should always specify a new value.
–code	This is a unique code for each server installed on the same host. It is a value between 0 and 65535, and its default is the value of **–port**.
–db-type	This specifies the type of db that will be used by the server. Currently accepted values are *mysql* and *oracle*. There is no default for this option.
–sqlloc	This specifies the full path to the DB interface library. Again, there is no default for this option.
–compat	This option must be specified if you plan to use voms 1.5.x on a MySQL backend with an old version of voms-admin. It requires –db-type to be *mysql*.
–newformat	This forces the server to generate ACs in the new (correct) format. This is meant as a compatibility feature to ease migration while the servers upgrade to the new version.

A couple example invocations follows:

for the first VO.

voms-install-db –port 15000 –vo-name my-vo –mysql-pwd 'some' –voms-pwd 'thing'

for a second VO on the same host.

voms-install-db –db new-vo –port 15001 –vo-name new-vo –mysql-pwd 'some' –voms-name 'voms2' –voms-pwd 'thing' –code 1

The server also needs to have an host certificate installed. Obtain it from your CA using the CA-specific procedures, and then copy the certificate in `/etc/grid-security/hostcert.pem` and the private key to `/etx/grid-security/hostkey.pem`. The owners should be set to root.root for both files, and permission should be, respectively, 644 and 600 or, better, 444 and 400.

2.2 Server options

Installing the server using the above described procedure should correctly create a set of configuration files that will execute it with the proper options. However, there are many other options that are not used by the default configuration script. The following lines will so describe the totality of the options.

–port	The port number on which the server should be listening. The default value is 50000
–vo	The name of the VO to which this server will belong. The default value is "unspecified".
–logfile	The location of the log file. The default location is "/opt/edg/var/log/<voname>"
–globusid	The value of the GLOBUSID environment variable. There is no default value.
–globuspwd	The value of the GLOBUSPWD environment variable. There is no default value
–x509_cert_dir	The location where the CA certificates are kept. The default value is /etc/grid-security/certificates
–x509_cert_file	A file containing all the CA certificates. There is no default value.
–x509_user_proxy	The location of the server's proxy. There is no default value.
–x509_user_cert	The location of the server's certificate. The default value is "/etc/grid-security/hostcert.pem"
–x509_user_key	The location of the server's private key. The default value is "/etc/grid-security/hostkey.pem"
–desired_name	OBSOLETE. This option will be removed in the future. Do *not* use it.
–foreground	OBSOLETE. This option will be removed in the future. Do *not* use it.
–username	The name of the user with which VOMS will access the DB. The default value is "voms"
–dbname	The name of the DB that VOMS will use. The default value is "voms".
–contactstring	The contactstring for DB connection, default to localhost.
–mysql-port	Sets the connection port when using MySQL backend. The default is MySQL default port.
–mysql-socket	Sets the connection socket when using MySQL backend. The default is MySQL default socket.
–timeout	The maximum length of validity of the ACs that VOMS will grant. (in seconds) The default value is 24 hours

–passfile The location of the file containing the password needed to access the DB. This file should be owned by root and have permissions set to 400. There is no default value. If this option is not specified, than the password will be asked to the user during server startup.

–uri The URI that the server will publish for himself. The default value is <hostname>:<port>.

–globus The version of Globus installed on the server's host. Use 20 for Globus 2.0 or Globus 2.1, and 22 for Globus 2.2 and Globus 2.4. The default value is 22.

–version Prints the version number and compilation date and then exits.

–backlog Sets the backlog on the socket. The default value is 50.

–conf Lets you specify a file from which options will be loaded. This file should have exactly one option per line, and option that do have values should be specified in the format "option=value".

–code This is a unique numeric code, between 0 and 65535, used to identify different servers installed on the same machine. Its default value is the value of **–port**.

–logtype Chooses the type of messages that will be logged. Possible values for this option are:

1 *STARTUP* — Messages during the startup phase.

2 *REQUEST* — Messages during the request processing phase.

4 *RESULT* — Messages during the result processing and sending phase.

The different possible values may be ORed together. The default value is 255.

–loglevel Sets the level of verbosity on log messages. Its possible values are:

1 *LEV_NONE* — Does not log anything.

2 *LEV_ERROR* — Only log error messages.

3 *LEV_WARN* — Also logs warning messages.

4 *LEV_INFO* — Also logs informational messages.

5 *LEV_DEBUG* — Also logs debug messages. This also sets the *-logtype* options to 255.

Higher levels of verbosity include all messages from the lower levels. The default value for this option is 2 (*LEV_ERROR*), also any value higher than 5 is treated as 5 (*LEV_DEBUG*)

–logformat This option sets the format for the log messages. Its default value is "%d:%h:%s(%p):%V:%T:%F (%f:%l):%m". Details on the syntax will be given in the *LOG Format* section below.

–logdateformat This option sets the format in which the date will be printed. It is the same format used by the *strftime(3)* option, and its default value is "%c".

–debug Slightly modifies the internal workings of the server to ease debug. *Never* use it on production servers. Use of this option is guaranteed to severely hurt scalability. This option also implies a *–loglevel=5*.

–sqlloc This is the fully qualified path of the DB access library. Please note that there is no default to this option.

–socktimeout The maximum number of seconds that a server will wait on an inactive connection before dropping it.

–maxlog The maximum size of a single lock file. Please note that this size is approximate and may be exceeded by a few thousand bytes. Whenever this amount is exceeded, log files are rotated. The default value is 10M.

–newformat This forces the server to generate ACs in the new (correct) format. This is meant as a compatibility feature to ease migration while the servers upgrade to the new version.

2.3 LOG Format

The format used for logging can be specified by the user via a format string passed to the *–logformat* option. This string has a format similar to that used by the printf-family function.

All characters are copied into the output string unchanged, except for substitution sequences, which have the following format: %[<engthg>]<char>, where <length> is optional and, if specified, express the maximum length of the text that will be substituted. Characters in excess will be silently truncated.

<char>, on the other hand, selects the type of substitution desired, according to the following table:

- **%** Substitutes a plain % character.
- **d** Substitutes the date. The date format is specified by the *-logdateformat* option.
- **f** Substitutes the name of the file that logged the message.
- **F** Substitutes the name of the function that logged the message.
- **h** Substitutes the hostname of the machine hosting the service.
- **l** Substitutes the line number of the code that logged the message.
- **m** Substitutes the message proper.
- **t** Substitutes the number of the message type. (see *-logtype*)
- **T** Substitutes the name of the message type. (see *-logtype*)
- **v** Substitutes the number of the message level. (see *-logtype*)
- **V** Substitutes the name of the message level. (see *-logtype*)

Chapter 3

edg-voms-proxy-init

3.1 Introduction

This command is used to contact the VOMS server and retrieve an AC containing user attributes that will be included in the proxy certificates.

3.2 Configuration

First of all, in "/etc/grid-security/vomsdir" you should include a copy of the host certificates of all the VOMS servers that could be contacted by the users.

Second, in "/opt/edg/etc/vomses" You should put a copy of the *vomses* file distributed by all the VOMS servers you wish to contact. This subtree will be recursed into to examine all pertinent files.

The easier way to comply to both previous points is to install the VO config RPM that should be distributed by the VOMS servers themselves.

This is all the configuration that should be done for the use of this command.

3.3 Invocation

The edg-voms-proxy-init command can be invoked with the following options:

−voms Specifies which server to contact. The parameter has the following syntax: <alias>[:<command>] where <alias> is the alias of the server as specified in the vomses files. If the same alias is associated to more than a single server, than those servers are considered replicas of each other, and are contacted in random order until one succeeds or all fail.
The [:<command>] part is optional. If not specified then the information returned will include only group membership, while if you specify :/Role=<rolename> then you will also get the role you asked for, provided that the server is already prepared to grant it to you.
Finally, if you specify :/group/Role=<rolename> as command, then you will get the role *rolename* in the group */group* only, again granted that the server is prepared to grant you that role.
This option can be specified multiple times, and the operations will be carried out in the exact order in which these options are specified in the command line.

−version Prints version information and exits.

−quiet Prints only minimal informations. *WARNING*: some vital warnings may get overlooked by this option.

−verify Verifies the certificate from which to create the proxy. This is not normally done, since in any case, an invalid user certificate will be detected when the proxy is actually used.

−pwstdin Specifies that the private key's passphrase should be received from stdin instead than directly from the console.

−limited Creates a limited certificate.

−hours Specifies the length of the validity of the generated proxy, measure in hours. The default value is 12 hours.

−bits Specifies the length in bits of the private key of the newly generated proxy certificate. The default value is 512.

−cert Specifies a non-standard location of the user's certificate. The default value is "$X509_USER_CERT" or, if this value is unset, "/$HOME/.globus/usercert.pem".

−key Specifies a non-standard location of the user's private key. The default value is "$X509_USER_KEY" or, if this value is unset, "$HOME/.globus/userkey.pem".

–certdir	Specifies a non-standard location of the trusted cert (CA) directory. The default value is "/etc/grid-security/certificates".
–out	Specifies a non-standard location of the generated proxy certificate. The default value is "$X509_USER_PROXY" or, if this is empty, "/tmp/x509up_u<id>" where <id> is the user's UID.
–order	This option specifies the order in which the attributes granted by the VOMS servers should be returned. The format of the parameter for this option is: <group[:role]>, where "group" is a group name and "role" is an (optional) role name. This option may be specified multiple times, to create an ordered list of attributes. Each server will receive this list, and will strive to return the attributes he will grant in the exact order specified by this list. All attributes not on this list will be returned in an unspecified order, but after the recognized attributes. Also, should this list include an attribute unknown to a specific server, such an attribute will be simply ignored. Finally, should a server be unable to grant the first attribute of the list, it will return a warning to the user. However, this warning will only be significant for the first server contacted.
–target	This option take advantage of the capability ACs have to target themselves to a specific set of receivers, so that only those receivers should, in conforming implementation, act on the data they get, while all others should reject it. This options lets you specify a set of FQHNs, each on a separate option, that will constitute the set of targets for the generated AC.
–vomslife	This option lets you specify the validity, in seconds, that you wish for the generated ACs. Remember that this value has only an advisory role. VOMS servers may lower this duration if the requested value exceeds the maximum they have been configured to grant. The default value of this option is "the value of the –hours option."
–proxyver	The version of proxy certificate that will be generated. May be 3 for new proxy certificate with critical Proxy Certificate Extension or 2 for old. When not specified the version is decided upon underlying globus version.
–policy	Specify the file containing the policy expression to put in the PCI extension. The default is an empty policy expression.

–policy-language	Specify the language in which the policy is expressed. Two generic language are defined: id-ppl-inheritAll (default choice with an empty policy expression, else invocated with IMPERSONATION_PROXY or own OID), which indicates an unrestricted proxy that inherits all rights from the issuing PI, and id-ppl-independent (invocated with INDEPENDENT_PROXY) which indicates an independent proxy that inherits no rights from the issuing PI.
–path-length	Specify the maximum depth of the path of proxy certificates that can be signed by this proxy certificate. A value of 0 means that this certificate must not be used to sign a proxy certificate. If not present means that unlimited proxy can be signed.
–globus	The version of Globus installed on the server's host. Use 20 for Globus 2.0 or Globus 2.1, and 22 for Globus 2.2 and Globus 2.4. The default value is 22.
–noregen	For its normal workings, edg-voms-proxy-init first creates a proxy with which to contact the VOMS servers, and then creates a new proxy to hold all of the returned ACs. This option skips the creation of the first proxy, and assumes that such a proxy already exists.
–separate	This option save the ACs in a separate file, instead than including them into a proxy certificate.
–ignorewarn	Specify this if you do not want to allow warnings to be printed.
–failonwarn	Specify this if you want warnings to be upgraded into errors.
–confile, **–userconf**, **–vomses**	These options specify the location of the vomses files or directories. They should be either owned by the user, or by root. "$PREFIX/etc/vomses" and "$HOME/.edg/vomses" are added by default. The three options are synonyms, with one exception: –vomses may be specified any number of times.. COMPATIBILITY NOTE: This behaviour differs from the behaviour of previous versions, where –confile was reserved for root-owned files, and –userconf was reserved for user-owned files. This modification is backwards compatible and should solve all the confusion problems. –userconf and –confile are now deprecated
–conf	Lets you specify a file from which options will be loaded. This file should have exactly one option per line, and option that do have values should be specified in the format "option=value".

–debug	This option prints a series of additional debug informations on stdout. The additional output returned by this option should *always* be included into bug reports for the edg-voms-proxy-init command. User should not, however, ever rely on informations printed by this options. Both content and format are guaranteed to change between software releases.
–list	Instead of producing an AC, this option prints on screen a list of all attributes available to the user.

Chapter 4

edg-voms-proxy-info

4.1 Introduction

This command is used to print to the screen the informations included in an already generated VOMS proxy.

4.2 Configuration

The same as edg-voms-proxy-init.

4.3 Invocation

–debug	This option prints a series of additional debug informations on stdout. The additional output returned by this option should *always* be included into bug reports for the edg-voms-proxy-info command. User should not, however, ever rely on informations printed by this options. Both content and format are guaranteed to change between software releases.
–version	Prints version information and exits.
–conf	Lets you specify a file from which options will be loaded. This file should have exactly one option per line, and option that do have values should be specified in the format "option=value".
–file	This option lets you specify a non-standard location of the user proxy. The default value is "$X509_USER_PROXY" or, if this is empty, "/tmp/x509up_u<id>", where <id> is the user's UID.
–subject	Prints the subject information.
–issuer	Prints the issuer information.
–type	Prints the proxy's type.
–strength	Prints the length (in bits) of the private key.

–valid	Prints the start and end validity times.
–time	Prints the end validity as a number of seconds for which the object will still be valid.
–info	Lets "–subject", "–issuer", "–valid" and "–time" also apply to ACs, and prints attributes values.
–extra	Prints extra informations that were included in the proxy.
–all	Prints everything. (Implies all other options.)
–fqan	Specifies that attributes should be printed in the FQAN format. (default)
–extended	Specifies that attributes should be printed in the extended format.
–exists	Activates the "–hours" and "–bits" options.
–hours	Verifies that the proxy, and the ACs if "–info" was specified, will be valid for at least <H> hours.
–bits	Verifies that the proxy key has at least <B> bits.

Chapter 5

edg-voms-proxy-destroy

5.1 Introduction

This command destroys an already existing VOMS proxy.

5.2 Configuration

No configuration needed.

5.3 Invocation

The following options may be used:

–**debug**	This option prints a series of additional debug informations on stdout. The additional output returned by this option should *always* be included into bug reports for the edg-voms-proxy-info command. User should not, however, ever rely on informations printed by this options. Both content and format are guaranteed to change between software releases.
–**version**	Prints version information and exits.
–**conf**	Lets you specify a file from which options will be loaded. This file should have exactly one option per line, and option that do have values should be specified in the format "option=value".
–**quiet**	Prints only minimal informations. *WARNING*: some vital warnings may get overlooked by this option.
–**file**	This option lets you specify a non-standard location of the user proxy. The default value is "$X509_USER_PROXY" or, if this is empty, "/tmp/x509up_u<id>", where <id> is the user's UID.
–**dryrun**	Only prints messages, but do not take any actions.

Chapter 6

edg-voms-proxy-fake

6.1 Introduction

This command creates proxy certificates with fake ACs. This is useful for test purposes.

6.2 Configuration

No configuration is needed.

6.3 Invocation

–help	Displays usage.
–version	Displays version.
–debug	Enables extra debug output. Note that the exact format of this output is version-dependent, and should not be relied upon.
-q	Quiet mode, minimal output.
–verify	Verifies certificate used to make proxy.
–pwstdin	Allows passphrase from stdin.
–limited	Creates a limited proxy.
–hours	The proxy is valid for the specified number of hours. The default values is 12 hours.
–vomslife	Makes an AC with information valid for the specified number of hours. The default value of 0 means "as long as the proxy certificate."
–bits	Number of bits in the key 512—1024—2048—4096
–cert	Non-standard location of the user certificate.
–key	Non-standard location of the user key.
–certdir	Non-standard location of the trusted certificates directory.
–out	Non-standard location of the new proxy cert.

–voms	Specifies the fake VOMS server that will appear in the attribute certificate. The command part (the same as that of the voms-proxy-init command) is ignored and is present for compatibility with voms-proxy-init.
–include	Includes the specified file in the certificate (in a non critical extension).
–conf	Read options from the specified file.
–policy	The file containing the policy expression.
–policy-language	The language in which the policy is expressed. Default is IMPERSONATION_PROXY.
–path-length	Maximum depth of proxy certificate that can be signed from this.
–globus	Underlying Globus version.
–proxyver	Version of the proxy certificate to create. May be 2 or 3. The default value is dependent on the underlying globus version.
–separate	Saves the voms credential on the specified file.
–hostcert	The cert that will be used to sign the AC.
–hostkey	The key that will be used to sign the AC.
–fqan	The string that will be included in the AC as the granted FQAN. No check is done on the formal correctness of this string.
–oldformat	This allows AC generation in the old (incorrect) format.

Chapter 7

voms-install-replica

7.1 Introduction

This script allows a VOMS server to be setup as a slave of a master host, so that it will automatically pickup all DB updates from the master. It only works for MySQL-based servers.

7.2 Configuration

Prior to using this script, the VOMS who has to become the master must be configured. The instructions to do so follow.

From the shell (just once):

```
cat >>/etc/my.cnf <<EOF
log-bin
server-id=1
EOF
```

and then, every time a new replica must be created:

```
mysql -p -e "grant super, reload , replication slave, replication
client on voms_myvo.* to replica@'grid-se.pr.infn.it' identified by
'replicapass'"

mysql -p -e "grant select, lock tables on voms_myvo.* to
replica@'grid-se.pr.infn.it'"
```

The last two commands are meant to be specified on one line only, and have been broken into multiple lines here for legibility.

You should obviously replace `replica@grid-se.pr.infn.it` and `replicapass` with the hostname of your new replica server and the username that it will be using. The username and the associated password should then be communicated to the administrator of the replica server.

7.3 Invocation

After having configure the slave via the *voms-install-db* script, the *voms-install-replica* script should be run. It takes the following options:

–db	This is the name of the DB that will be replicated. It must be the same name used in the master.
–mysql-admin	This is the root account on the *slave* DB.
–mysql-pwd	This is the password associated to the **–mysql-admin** account.
–master-host	This is the fully qualified hostname of the machine on which the server is running.
–master-mysql-user	This is the username that the master administrator created for the replica to use.
–master-mysql-pwd	This is the username that is associated to the **–master-mysql-pwd** account.
–master-db	This is name of the DB that should be replicated. It must be the same as the argument of the **–db** option.
–master-log-file	This is the name of the copy of the master log file that will be created on the slave machine.
–master-log-pos	This is the location in which the file specified by the **–master-log-file** will be placed.