DataGRID

EDG-VOMS-ADMIN USER'S GUIDE

Document identifier:	**edg-voms-admin-user-guide**
EDMS id:	
Date:	January 14, 2004
Work package:	**WP07: Security**
Partner(s):	**CERN, ELTE**
Lead Partner:	**CERN**
Document status:	**WORKING DRAFT**
Author(s):	?kos Frohner
File:	**edg-voms-admin-user-guide**

Abstract: A collection of the user documentations with an overview.

CONTENTS

1. OVERVIEW 4

2. EDG-VOMS-ADMIN-CONFIGURE 5

3. EDG-VOMS-LDAP-SYNC-CONFIGURE 8

4. EDG-VOMS-MAKE-VO-RPMS 10

5. INIT-EDG-VOMS-ADMIN 12

6. EDG-VOMS-DB-DUMP 13

7. EDG-VOMS-DB-LOAD 14

8. EDG-VOMS-DB-UPGRADE 15

9. EDG-VOMS-LDAP-SYNC 16

10. CRON-EDG-VOMS-LDAP-SYNC 17

11. EDG-VOMS-ADMIN 18

12. EDG-VOMS-ADMIN-LOCAL 22

Document Log

Issue	Date	Comment	Author
0-1	2003-08-29	First draft	?kos Frohner
0-2	2003-10-03	Included make-vo-rpsm	?kos Frohner

1. OVERVIEW

This document is a collection of individual guides of the various utilities of edg-voms-admin .

After installing the edg-voms-admin server please read the *Install Guide*, which will provide step-by-step guidance over some typical examples. For the details please refer to *edg-voms-admin-configure* (see Section 2.), *edg-voms-ldap-sync-configure* (see Section 3.) and *edg-voms-make-vo-rpms* (see Section 4.).

In the normal operation of the edg-voms-admin server one can use the following utilities:

- *edg-voms-admin* init script (see Section 5.) to start and stop the administrative services,
- *edg-voms-db-dump* (see Section 6.) to make a backup of the database,
- *edg-voms-db-dump* (see Section 7.) to load in a backup of the database,
- *edg-voms-db-dump* (see Section 8.) to upgrade to a new version of the database,
- *edg-voms-ldap-sync* (see Section 9.) to synchronize the database with an existing LDAP Authorization server and
- *edg-voms-ldap-sync* cron job (see Section 10.) to initiate the synchronization of the configured virtual organizations from cron.

For the management of a virtual organization one can either use the web interface or the *edg-voms-admin* (see Section 11.) command line utility. There is also a convenienve wrapper over this command for some regular tasks: *edg-voms-admin-local* (see Section 12.).

2. EDG-VOMS-ADMIN-CONFIGURE

SYNOPSIS

edg-voms-admin-configure (install|remove)(db|conf)? –vo=*VO_name* [–voalias=*VO_alias*] [–port=*port_number*] [–dbauser=*userid*] (–dbapwd=*password*|–dbapwdfile=*filename*) [–(no)verbose] [–password=*voms_password*] [–cert=*certificate*] [–certdir=*ca-cert-dir*] –smtp-host=*hostname* –mail-from=*email-address*

DESCRIPTION

This program will use the service configuration and database scheme templates to generate a configuration for the actual machine.

The input/templates directory is:

```
$EDG_LOCATION/etc/edg-voms-admin
```

The output/configuration directories are:

```
$EDG_LOCATION_VAR/etc/edg-voms-admin
$EDG_LOCATION/etc/voms
```

The only exception is when the edg-vomsd package is already installed and configured. In this case the necessary configuration settings are taken from the already configured VOMS instance.

COMMANDS

install

With the **install** command one can set up the service on a machine. This command is typically called from the post-install script of a package.

installdb

The **installdb** command executes the database related subset of the **install** command: it creates the database tables and roles and saves the setup in a configuration file.

It also fills up the database with some basic initial data, like the VO name itself.

The CA table is not populated, because that is automatically updated by the edg-voms-admin service.

installconf

The **installconf** executes every configuration step but the database installation: **installdb** + **installconf** = **install**

remove

With the **remove** command one can clean up the service on a machine.

removedb

The **removedb** command executes the database related subset of the **remove** command: it removes the database tables and roles.

A **removedb** and **installdb** command sequence – with the same parameters – basically cleans up the database, but keeps the same configuration.

removeconf

The **removeconf** command executes every cleanup step but the database cleanup: **removeconf** + **removedb** = **remove**

OPTIONS

–port *port_number*

The *port_number* attribute will set the listening port in the voms server. The default value is 15000.

–vo *VO_name*

The *VO_name* will be used as the name of the Virtual Organization.

–voalias *VO_alias*

If the <VO_name> contains non-word characters, which prevent its usage in normal filenames, then this option can be used to secify an alternate alias to be used in the config filenames. The alias may contain only alphanumeric characters and it can be only six characters long.

The *default* value is the first six characters of the VO name.

–dbauser=*userid*

The *userid* of the database administrator on the localhost. This is database userid, which has nothing to do with the Unix userids!.

The *default* value is *root*.

–dbapwd=*password*

The *password* of the database administrator on the localhost.

–dbapwdfile=*filename*

The *file*, which contains the *password* of the database administrator on the localhost. (To avoid exposure of the password in the process list.)

If neither *–dbapwd* and *–dbapwdfile* is specified, then the necessary SQL commands are saved in the configuration directory. The system administrator can take them and feed them to MySQL.

–password=*voms_password*

The *password* of the voms database users in MySQL.

The *default* value is an automatically generated random string, which is stored in the service's configuration file (voms.database.properties).

–(no)verbose

Print detailed information at each step.

–cert=*certificate*

Location of the service's certificate. The *default* value is

```
/etc/grid-security/hostcert.pem
```

This is needed to create the UI config for *voms-proxy-init* (see the vomses file in the configuration directory).

–certdir=*ca-cert-dir*

Location of the CA certificates. The *default* value is

```
/etc/grid-security/certificates
```

This directory is used by the server to update the database's CA table (see voms.service.properties in the configuration directory).

–smtp-host=*hostname*

Hostname of the SMTP delivery service at the site of this VOMS server. The host **must** accept emails for delivery.

There is **no default value** for this parameter!

–mail-from=*email-address*

The sender email address for the notification messages, sent by this service. This is adised to be a real address, otherwise the failure notifications will end up in devnull...

However the administrative interface will try to set the from address to the email address of the user, who initiated the action of the notification, if it is appropriate.

There is **no default value** for this parameter!

AUTHOR

SEE ALSO

edg-voms-admin

3. EDG-VOMS-LDAP-SYNC-CONFIGURE

SYNOPSIS

edg-voms-ldap-sync-configure (–voalias=*VO_alias*|–all) ... [–help] [–(no)verbose] [–version] [–dryrun]

DESCRIPTION

This program will call **edg-voms-admin-configure** to configure a VOMS server. The only convenience option is that the actual VO name and VOMS port number is derived by this script from the LDAP Authorization server configuration file:

```
$EDG_LOCATION/etc/edg-voms-admin/ldap-servers.conf
```

If the **–voalias** option is used, then only one VO will be configured. If the **–all** option is used, then all the VOs in the above mentioned configuration file will be installed.

This program searches for the VO with the alias in the configuration file and passes the **VO name** to the configure script.

The other additional derived parameter is the port number of the core VOMS server: it it the (non-comment) line number of the VO in the config file + 15000. For example the config file has the following lines:

```
# server name | group base | base | VO name | VO alias
marianne.in2p3.fr|ou=ITeam|o=testbed,dc=eu-datagrid,dc=org|ITeam|iteam
marianne.in2p3.fr|ou=EDGtutorial|o=testbed,dc=eu-datagrid,dc=org|EDG Tutorial|tutorial
```

In case the program is called with the *–voalias=tutorial* parameter, it calls the **edg-voms-admin-configure** program with the following parameters:

```
--voalias=tutotrial
--vo=EDG_Tutorial
--port=15002
```

All the additional parameters are passed on to **edg-voms-admin-configure**. It means that installing all the VOs, which already have LDAP authorization server is

```
edg-voms-ldap-sync-configure --all install
```

and removing all of them is

```
edg-voms-ldap-sync-configure --all install
```

OPTIONS

Additional options:

–help

Prints a help message with the available virtual organisations.

–(no)verbose

Prints the commands before they are executed (default is on).

–version

Prints the version number.

–dryrun

Does not execute the commands (for testing).

AUTHOR

SEE ALSO

edg-voms-admin-configure, edg-voms-ldap-sync

4. EDG-VOMS-MAKE-VO-RPMS

SYNOPSIS

edg-voms-make-vo-rpms [VO-alias-1 [VO-alias-2 ...]] [–help] [–version] [–dryrun] [–verbose] [–rpmversion=VERSION] [–rpmrelease=RELEASE] [–hostcert=path-to-certificate]

DESCRIPTION

This program generates the configuration RPMs for the UI and CE machines from the running host's VOMS configuration.

It scancs the `$EDG_LOCATION_VAR/etc/edg-voms-admin` directory for VO names and generates the RPMs for all, unless the VO names are specified as arguments.

The generated RPMs are placed into the current directory.

OPTIONS

Additional options:

–help

Prints a help message.

–verbose

Prints the commands before they are executed (default is on).

–version

Prints the version number.

–dryrun

Does not execute the commands (for testing).

–rpmversion

The version of the generated RPM.

The default value is "0.1".

–rpmrelease

The release number of the generated RPM.

The default value is "1", but it is automatically incremented, if there is already an RPM with the same filename.

–hostcert=path

The location of the host certificate.

The default value is `/etc/grid-security/hostcert.pem`.

AUTHOR

SEE ALSO

edg-voms-admin-configure

5. INIT-EDG-VOMS-ADMIN

SYNOPSIS

$EDG_LOCATION/etc/init.d/**edg-voms-admin** (status|start|stop|restart) [VO_name...]

DESCRIPTION

The **edg-voms-admin** init.d script is used to start and stop the administrative services for VOMS databases.

Without any further arguments the commands are applied on all VOs. If there are VO names specified, then the commands only apply to them.

COMMANDS

status

Prints status information on the services. It is only static information, the script only checks if the appropriate config files are in place, but does not makes a call to the service to see if it is actually running.

start

Starts the service by copying its context file from `${EDG_LOCATION_VAR}/etc/edg-voms-admin/VO-name/` to `${CATALINA_BASE}/webapps` and `${CATALINA_BASE}/webapps-secure` respectively.

It also restarts Tomcat, if it is running by using the `edg-tomcat4` program.

stop

Stops the service by removing the context file from `${CATALINA_BASE}/webapps` and `${CATALINA_BASE}/webapp` respectively.

It also restarts Tomcat, if it is running by using the `edg-tomcat4` program.

restart

Stops then starts the service.

AUTHORS

Ákos Frohner <Akos.Frohner@cern.ch>

SEE ALSO

edg-voms-admin-configure

6. EDG-VOMS-DB-DUMP

SYNOPSIS

edg-voms-db-dump [*VO_alias*]

DESCRIPTION

The **edg-voms-db-dump** command is a simple wrapper around the *mysqldump* program. Its main purpose is to simplify the dump process by extracting the DB configuration from the service's config files and calling mysqldump with the appropriate parameters.

OPTIONS

VO_alias

The name of the virtual organization, which you want to dump.

If no VO is specified then this script will iterate through all the configured VOs.

The name of the database dump for each VO is:

```
edg-voms-VO_alias-YYYY-MM-DD.sql
```

AUTHOR

Akos Frohner, Karoly Lorentey

SEE ALSO

edg-voms-db-load, edg-voms-db-upgrade

7. EDG-VOMS-DB-LOAD

SYNOPSIS

edg-voms-db-load *VO_alias db_dump_file*

DESCRIPTION

The **edg-voms-db-load** command is a simple wrapper around the *mysql* program. Its main purpose is to simplify the load process by extracting the DB configuration from the service's config files and calling mysql with the appropriate parameters.

OPTIONS

VO_alias

Mandatory attribute, there is no default value.

db_dump_file

The filename, where the dump will was saved. If no value is given, then the default value is the last filename, which is like:

```
edg-voms-VO_alias-????-??-??.sql
```

AUTHOR

Akos Frohner, Karoly Lorentey

SEE ALSO

edg-voms-db-dump, edg-voms-db-upgrade

8. EDG-VOMS-DB-UPGRADE

SYNOPSIS

edg-voms-db-upgrade [*VO_alias*]

DESCRIPTION

The **edg-voms-db-upgrade** command is a simple wrapper around the *mysql* program. Its main purpose is to simplify the load process by extracting the DB configuration from the service's config files and calling mysql with the appropriate parameters to load in the database upgrade scripts.

OPTIONS

VO_alias

The name of the virtual organization, which you want to upgrade.

If no VO is specified then this script will iterate through all the configured VOs.

AUTHOR

Akos Frohner, Karoly Lorentey

SEE ALSO

edg-voms-db-dump, edg-voms-db-load

9. EDG-VOMS-LDAP-SYNC

SYNOPSIS

edg-voms-ldap-sync –voalias=*alias* **–url**=*url* [–help] [–verbose] [–dryrun] [–delete] [–version]

DESCRIPTION

This program synchronizes an LDAP Authorization server to a VOMS server.

It connects to the LDAP server (option **-s**) and to the VOMS administration server and executes the appropriate commands on the later one to synchronize their states.

It will create and delete the users and groups in VOMS according to the state in the LDAP server. Deletion of non-LDAP groups has to be explicitly requested, since there might be updates made only on the VOMS server, which should not be lost.

The script will **not** modify the LDAP database and it can also be requested to skip modifications on the VOMS server as well. In this case (**-n**) the required modifications are printed to the standard output, so a sysadmin can execute them separately.

OPTIONS

The options for **edg-voms-ldap-sync**

–help

Prints a help message with the available list of virtual organisations.

–verbose

verbose output (default is off)

–delete

Delete non-LDAP groups from VOMS (default is no delete to allow additional groups in VOMS).

–voalias=VOalias

The *VOalias* selecting the LDAP directory server.

–url=https://...

URL of the VOMS server.

–dryrun

No modifications, just print the commands.

–version

Prints the program version.

AUTHORS

10. CRON-EDG-VOMS-LDAP-SYNC

SYNOPSIS

$EDG_LOCATION/etc/cron/**edg-voms-ldap-sync**

DESCRIPTION

The **edg-voms-ldap-sync** cron job scans the configured virtual organizations and calls the *edg-voms-ldap-sync* program to synchronize them with the VOMS server.

It will skip those VOs, which are not in the ldap-servers.conf file (i.e. locally configured virtual organizations).

The output of the *edg-voms-ldap-sync* runs are appended to

```
$EDG_LOCATION_VAR/log/edg-voms-ldap-sync
```

AUTHORS

Ákos Frohner <Akos.Frohner@cern.ch>

SEE ALSO

edg-voms-ldap-sync, edg-voms-ldap-sync-configure

11. EDG-VOMS-ADMIN

SYNOPSIS

edg-voms-admin [–url=*service-url*] [–[no]verbose] [–[no]quiet] [–[no]usercert] [–separator=':'] [–nullstring=''] [–version] [–help] (*command1 parameter1 ...*| -)

DESCRIPTION

The **edg-voms-admin** command provides a simple command line interface for VOMS adminstartors. It basically connects to the *edg-voms-admin* service and calls the appropriate functionality over SOAP.

OPTIONS

–url=*service_url*

The URL of the service, for example

```
http://localhost:8080/edg-voms-admin/fred
```

You may also specify the "https" in which case user's proxy certificate will be used for authentication.

–[no verbose]

The commands print verbose messages during operation.

The default is *verbose*.

–[no quiet]

Errors and warnings are supressed.

The default is *noquiet*.

–[no header]

The complex commands print a header line describing the fields of the following data lines. One may disable this header with this option.

The default is *header*.

–separator=':'

Use the specified separator character (or string) as a separator, when printing complex data structures.

The default is | (vertical bar).

–nullstring='NULL'

Use the specified string, when a NULL value is returned from the server.

The default is an empty strings.

–[no usercert]

The user is specified by a certificate (filename, which contains the user's certificate) not by a *DN CA* pair. All operations (e.g. add-member), which take a user as a parameter will behave differently.

As a special case you may use the word **myself**, instead of a filename, when the routine will load your default certificate from `$HOME/.globus/usercert.pem`.

With the *–nousercert* option you must specify two strings at every *user* parameter: DN and CA!

The default is *usercert*.

–help

Prints the short usage instructions.

–version

Prints the version and release numbers.

ALIASES

You may specify `/` or `VO` instead of the VO name for any groupname or container input parameter. The program will look up the VO's real name and replace it in the parameters.

You may specify `myself` instead of a user certificate file name. The program will replace if by `$HOME/.globus/usercert`

COMMANDS

The following commands are calling the corresponding methods of the *VOMSAdmin* interface. The commands are available in lower case versions as well, with '-' on the word boundaries (e.g. `get-vo-name` for `getVOName`).

One may specify `-` in the command line arguments, which means that the rest of the commands and parameters are read from the standard input.

The lines from the standard input may contain comments (`#` to the end of line is stripped) and quoted strings (among `"` characters). Quotation marks (`"`) can be escaped by backslash: `\"`.

getVOName

Returns the name of the Virtual Organization.

listUsers

Lists the registered users of this VO.

create-user *user_attributes*

Registers a new user in VOMS using the attributes from the user's certificate (*usercert_file*), if –usercert is specified or the attributes after the command (*DN CA CN mail*).

deleteUser *user*

Deletes a user from VOMS (all attributes are deleted also!).

listCAs

Lists the Certificate Authorities in this VO.

listRoles

Lists the roles in this VO.

createRole *rolename*

Creates a new role.

deleteRole *rolename*

Deletes a role.

listCapabilities

Lists the capabilities in this VO.

createCapability *capability*

Creates a new capability.

deleteCapability *capability*

Deletes the *capability* capability.

listSubGroups *groupname*

List sub-groups of *groupname*.

createGroup *parent groupname*

Creates the new *groupname* group under *parent*.

deleteGroup *groupname*

Deletes the *groupname* group.

addMember *groupname user*

Adds the *user* to the *groupname* group.

removeMember *groupname user*

Removes the *user* from the *groupname* group.

listMembers *groupname*

Lists all members of the given group.

assignRole *groupname rolename user*

Adds the *user* to the *groupname*/*rolename* role.

dismissRole *groupname rolename user*

Removes the *user* from the *groupname*/*rolename* role.

listUsersWithRole *groupname rolename*

Lists all members of the given group/role.

assignCapability *capability user*

Adds the *user* to the *capability*.

dismissCapability *capability user*

Removes the *user* from the *capability*.

listUsersWithCapability *capability*

Lists all members of the given capability.

getACL *container*

Lists the ACL of a given container.

You must use explicit types in the container name ("VO_name/group", "Role=role1" or "Capability=capability2") otherwise the system will not be able to figure out which one is selected.

getDefaultACL ***groupname***

Lists the default ACL of group *groupname*.

add-acl-entry ***container allow operation user***

Adds an ACL entry to the *container*'s access control list.

You must use explicit types in the container name ("VO_name/group", "Role=role1" or "Capability=capability2") otherwise the system will not be able to figure out which one is selected.

The entry can "allow" or "deny" (*allow*) any of the following operations: "all", "create", "delete", "add", "remove", "set-acl", "get-acl", "set-default-acl", "get-default-acl" and "list".

addDefaultACLEntry ***groupname allow operation user***

Adds an ACL entry to the group *groupname* default access control list.

The entry can "allow" or "deny" (*allow*) any of the following operations: "all", "create", "delete", "add", "remove", "set-acl", "get-acl", "set-default-acl", "get-default-acl" and "list".

removeACLEntry ***container allow operation user***

Removes an ACL entry from the *container*'s access control list.

You must use explicit types in the container name ("VO_name/group", "Role=role1" or "Capability=capability2") otherwise the system will not be able to figure out which one is selected.

The entry can "allow" or "deny" (*allow*) any of the following operations: "all", "create", "delete", "add", "remove", "set-acl", "get-acl", "set-default-acl", "get-default-acl" and "list".

removeDefaultACLEntry ***groupname allow operation user***

Removes an ACL entry from the group *groupname* default access control list.

The entry can "allow" or "deny" (*allow*) any of the following operations: "all", "create", "delete", "add", "remove", "set-acl", "get-acl", "set-default-acl", "get-default-acl" and "list".

listUserGroups ***user***

Lists the groups of a *user*.

listUserRoles ***user***

Lists the roles of a *user*.

listUserCapabilities ***user***

Lists the capabilities of a *user*.

Unimplemented methods of the VOMSAdmin interface: setACL, setDefaultACL, getUser, setUser, getGroupPath.

AUTHORS

Ákos Frohner <Akos.Frohner@cern.ch>, Károly Lőrentey <Lorentey.Karoly@elte.hu>

SEE ALSO

edg-voms-ldap-sync, EDG::HTTPS

12. EDG-VOMS-ADMIN-LOCAL

SYNOPSIS

edg-voms-admin-local *VO_alias* (*–add-admin usercert*|*–add-host hostcert*)

DESCRIPTION

The **edg-voms-admin-local** command is a simple wrapper around the *edg-voms-admin* script. Its main purpose is to simplify the initial steps of a VO administrator by specifying as few parameters as possible.

OPERATIONS

–ADD-ADMIN

Adds the administrator to the database and assigns her/him to the *VO-Admin* role. By default every ACL contains this role with full permissions, so the administator will be able to do anything in this VO.

–ADD-HOST

Adds the host with list permission to the VO group, so the host will be able to query the user list and generate a gridmap-file.

The host will not be able to do anything else, no other operations and no other groups/roles are affected.

OPTIONS

VO_alias

Mandatory attribute, there is no default value.

cert

The certificate file of the administrator or host.

The default value is *myself*, which is an alias for `$HOME/.globus/usercert.pem` or `/etc/grid-security/hostc` respectively.

AUTHORS

Ákos Frohner <Akos.Frohner@cern.ch>, Károly Lőrentey <Lorentey.Karoly@elte.hu>

SEE ALSO

edg-voms-admin, edg-voms-admin-configure