



ARChER Data Services Infrastructure Layer

System Administrator's Guide

VDT, CA and MyProxy SRB

- Installation
- Configuration
- Maintenance

ARChER Data Services Infrastructure Layer	1
Overview	3
Before you begin	3
Configuration	3
Installation process	5
Obtaining the deployment scripts.....	5
How to use the deployment scripts.....	5
Overview of installation	6
Installing MyProxy/VDT/CA	8
Overview:	8
CA configurations	8
MyProxy configurations	8
Before you start	9
Running the installation.....	9

Installing MyProxy with an existing CA.....	12
Troubleshooting	12
After installation	13
Configuring other machines for this CA	13
Giving other machines access to MyProxy	13
Verifying that MyProxy is running	13
Verifying that MyProxy is generating certificates	14
Verifying that MyProxy works across the network.....	14
Installing SRB	15
Prerequisites.....	15
Configuration	15
Installing SRB	15
Result	16
Verifying that the SRB server is running	17
Verifying that the SRB storage is functioning	18
Changing the srb superuser password	18
Verifying that SRB works over network.....	18
Verifying that GSI user creation is working.....	19
Verifying that MyProxy authentication is working.....	20
Maintaining VDT, MyProxy and CA.....	22
Starting and stopping.....	22
Logging.....	22
Configuration	22
Maintaining SRB	23
Starting and stopping.....	23
Logging.....	23
Configuration	23
Tool reference	24
Using cert_tool.....	24
Using dev-adduser.....	24
Creating users	25

Overview

The ARCHER Data Services (ADS) Infrastructure Layer provides storage with SRB, and authentication through MyProxy and Globus. It is installed through automated deployment scripts

The ADS Infrastructure Layer supports the ADS Service Layer and should be installed before it..

Before you begin

See the **ARCHER Overview** for an overview of ARCHER Data Services and the pre-requisites for each server.

Decrypting the SRB installer

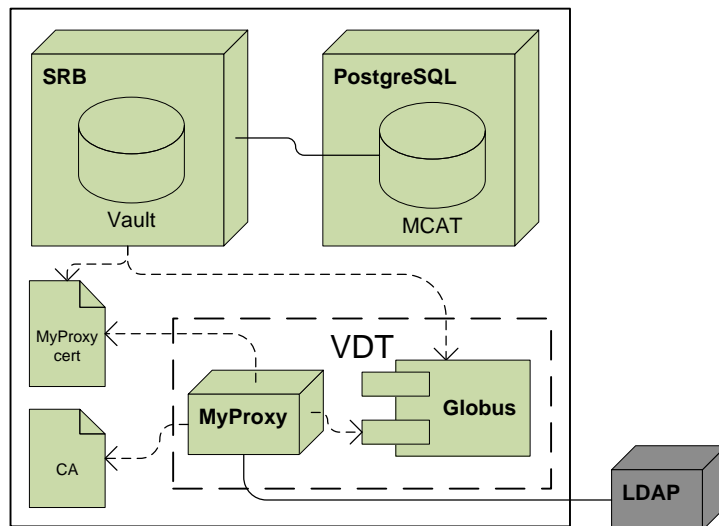


The SRB installation code is encrypted due to licensing requirements. You must obtain a decryption code before you begin. This code can be obtained from the Australian Research Collaboration Service (ARCS)¹ or the San Diego Supercomputer Centre².

See http://www.sdsc.edu/srb/index.php/Is_SRB_Open_Source for more information.

Configuration

The standard, tested ARCHER configuration places all of the ADS Infrastructure Layer on one server as follows:



It is possible to install MyProxy on a separate server from SRB. In this case:

- You will need to install VDT multiple times, once for each machine.

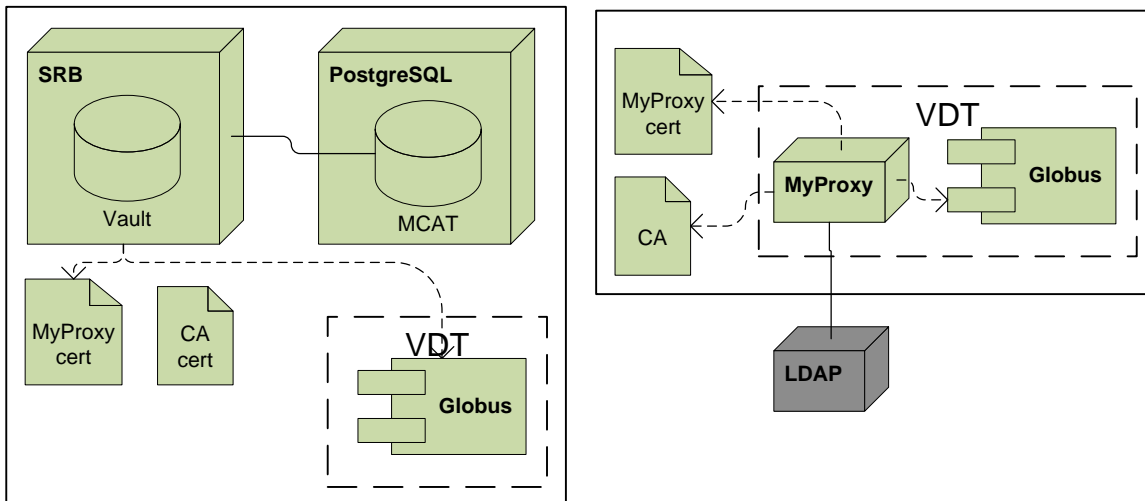
¹ <http://www.arcs.org.au/>

² <http://www.sdsc.edu/>

- You will need to copy CA certificates from the MyProxy machine to the other machines.
- You will need to manually generate host keys for each machine, on the MyProxy server.

The same applies if you later install ARCHER Collaborative Workspace on a server other than the MyProxy machine.

The configuration is as follows:



Further details are given later in this document.

Note:

This dual-server configuration is designed to work, but was not tested by the ARCHER project.

Installation process

Obtaining the deployment scripts

The Archer Data Services Infrastructure Layer is delivered through a set of deployment scripts. These scripts are run through the `setup` script, and controlled primarily through environment variables.

First, download the deployment scripts onto each machine that will be hosting any component. The ADS deployment scripts are available for download at <http://www.archer.edu.au/downloads>.

The download contains the following.

File or directory	Purpose
<code>setup</code>	Main installation script that drives all the others.
<code>*.sh</code>	Script files called by <code>setup</code> to install each component.
<code>SRBInstaller/</code>	SRB installation package, called by installation script.
<code>bin/</code>	Several useful tools that will be installed. See the "Tool Reference" section of this document.

How to use the deployment scripts

The ADS deployment scripts simplify installation of a number of components. They download and install the software for each component, and configure it according to environment variables.

The script can install any combination of the components in one run. For simplicity, these documents assume that one component is being installed at a time.

For example:

```
NO_SRB=0 NO_VDT=0 ./setup
```

This installs SRB and VDT. This is equivalent to these two lines:

```
NO_SRB=0 ./setup
NO_VDT=0 ./setup
```

Exception: Installing MyProxy and CA at the same time causes MyProxy to function as a CA. Installing them sequentially does not.

Usage:

```
setup [-h] [-i] [-p] [-f] [-v] [-c] [-o] [-d fully.qualified.domain.name]
```

Parameter	Purpose
<code>-h</code>	Shows help on all the available options.
<code>-c</code>	Uninstalls a component. You must set all the same environment variables as when the component was installed. See note below.

-d	Specify a distribution host. Equivalent to setting \$DIST_HOST.
-f	Force reinstallation of a component.
-i	Disables actual installation, instead only installing pre-requisites.
-o	Prints the scripts that would run, but does not actually install anything.
-p	Disables installation of pre-requisites.
-v	Prints all the variables that apply for a given script.

Before running each script, use the `-o` and `-v` options to display the variable values and steps that will be used.

That is, first run:

```
NO_SRB=0 ./setup -o -v
```

Verify the variables that you have set. Then run:

```
NO_SRB=0 ./setup
```

Note: The “-c” uninstallation mode is not guaranteed. In particular, it does not delete the file `/etc/sysconfig/dev-env`, which means subsequent installations can use old, possibly incorrect values. It also does not delete `/etc/yum.repos.d/jcu.hpc.repo`.

Global environment variables:

Environment variable	Purpose
GRID_SEC_DIR	Location to store keys and certificates for grid application. Default: <code>/etc/grid-security</code>
DIST_HOST	Name of the distribution host, which hosts several components required to complete installation. Default: <code>http://www.hpc.jcu.edu.au/dist/</code>
SYSCONF_LOCATION	Name of file to save persistent variable values to. Default: <code>/etc/sysconfig/dev-env</code>

Environment variables specific to each component are described in the relevant sections of this document.

Overview of installation

To install all components on one machine, proceed as follows:
1. Install MyProxy, VDT and CA using the Deployment Scripts.
2. Install SRB, using the Deployment Scripts.

To install MyProxy on a separate machine, proceed as follows:

1. Install MyProxy, VDT and CA on Machine A using the Deployment Scripts.
2. On Machine A, generate a host key for Machine B.
3. Copy certificates and keys from Machine A to Machine B.
4. Install VDT on Machine B, using the Deployment Scripts.
5. Install SRB on Machine B, using the Deployment Scripts.

Installing MyProxy/VDT/CA

Overview:

The Virtual Data Toolkit (VDT)³ is a packaging system used to install Globus, MyProxy and other grid tools. These components are used by other ARCHER components, including Plone.

MyProxy is delivered as part of VDT, and should be installed first, on the “back” server. You can make it operate as a CA at the same time. Use the “NO_VDT” and “NO_CA” environment variables on the deployment scripts to install them.

CA configurations

A CA is concretely just a set of keys, certificate and signing policy. The ARCHER CA script can be installed in two ways:

- With MyProxy: MyProxy is configured to use act as a CA, by pointing to the created CA files.
- Without MyProxy: The files are installed, along with a set of scripts that let you sign certificates.

MyProxy configurations

In the context of Archer, MyProxy serves two independent purposes:

- It allows users to authenticate against an LDAP, then generates short-lived certificates (“proxies”) which can then be passed to SRB, XDMS or other services.
- It can act as a certificate authority (CA).

The version of MyProxy installed through this process includes some ARCHER-specific patches to make this LDAP authentication possible.

Several different scenarios are possible:

MyProxy on the same machine as SRB, and acting as CA

This is the default configuration assumed in this document, most useful for testing and initial setup.
--

MyProxy on a different machine from SRB, and acting as CA.

This requires a few extra manual steps, explained in this document.

MyProxy used, but with an external CA.

This requires manual steps that depend on the CA you are using. These are covered in the relevant places.

³ <http://vdt.cs.wisc.edu/>

MyProxy used as CA, but not as proxy generator.

Proceed as per this document, but configure other tools as though it were not present. No further documentation is given on this configuration.

External MyProxy and CA used.

This is likely in a production environment. Install neither MyProxy nor CA, and configure the Archer tools to point to the existing MyProxy. Some steps are necessarily beyond the scope of this document.

Before you start

(Optional) Setting up a VDT mirror

A large part of the installation time is due to downloading the VDT components from remote servers. You can greatly improve this time and reduce bandwidth use by creating your own mirror.

To do this, obtain the VDT mirror from http://vdt.cs.wisc.edu/vdt_181_cache. Then set the VDT_CACHE environment variable:

```
export VDT_CACHE=/opt/nfs/vdtcache/vdt_181.mirror
```

Running the installation

You must install MyProxy and CA at the same time to create the standard configuration, with MyProxy acting as CA.

The following variables are used to control installation of the CA. Typically, the only variable you need to change is `$CA_DN_PREFIX`.

Variable	Purpose	Sample value
NO_CA	Set to 0 to install CA.	0
CA_GRID	If 1, sets up CA for use with grid applications. It copies CA certificate to <code>\$GRID_SEC_DIR</code> (usually <code>/etc/grid-security</code>) and creates signing policy. Don't change this. Default: 1	1
CA_DN_PREFIX	Distinguished name prefix for CA certificate.	<code>/O=ARCHER/OU=edu/OU=au</code>
CA_GRID_DN_PREFIX	Distinguished name prefix for certificates signed by CA. In most cases, do not change this. Default: <code>\$CA_DN_PREFIX</code>	(use default)
CA_HOSTCERT	If 1, a host certificate and keys are created. This is important to allow other services, such as SRB to operate. Default: 1	1
GRID_SEC_DIR	Directory for grid security	(use default)


	certificates. Default: /etc/grid-security	
CA_LOCATION	Where to store CA information. Default: /opt/CA	/usr/local/archer/CA

The following variables are used to control installation of VDT.

Variable	Purpose	Sample value
NO_VDT	Set to 0 to install VDT.	
VDT_CACHE	URL or file path of mirror to obtain VDT software from. See "Setting up a VDT mirror".	http://archer.edu.au/vdt_181.mirror /opt/nfs/vdtcache/vdt_181.mirror
VDT_MYPROXY_LDAP_BASE	The search base to use when authenticating with LDAP.	ou=users,dc=testing,dc=archer,dc=edu,dc=au
VDT_MYPROXY_LDAP_HOST	The LDAP server name.	ldap.archer.edu.au
VDT_MYPROXY_LDAP	1 (not the default) to install MyProxy, the MyProxy LDAP patch and connect MyProxy to LDAP. Default: 0	1
VDT_JCU_CACHE	Location of JCU specific pacman packages. See "Network access" section of ARCHER Overview. Default: \$DIST_HOST/pacman/jcu	http://www.hpc.jcu.edu.au/dist/pacman/jcu/
VDT_LOCATION	Directory to install all VDT software. Default: /opt/vdt	/opt/nfs/vdt
VDT_PACKAGES	Comma separated list of specific VDT packages to install. Leave it as the default unless you have specific needs. Default: Globus-SRB-DSI	OpenLDAP,Globus-Base-SDK,MyProxy
VDT_PLATFORM	Only needs to be set if installing on non-standard distributions: not Centos, RHEL or Scientific Linux. Default: linux-rhel-5	linux-rhel-5
VDT_SDK	If 1, the Globus SDK is installed, rather than just the runtime libraries. Required for the SRBContent Plone plugin. Default: 1	1

Variable	Purpose	Sample value
VDT_VERSION	Which version of VDT to install. This must match the version in the VDT cache you are using. Default: 181	181

Note: When running `./setup -o -v`, sometimes other variables can be spuriously reported. Modifying these variables will not affect the installation in a useful way.

Note	
	Don't forget to also set general environment variables, such as <code>\$DIST_HOST</code> , as described in "How to use the deployment scripts" above.

For example, consider a typical installation with MyProxy being used as CA, and connected to an LDAP at `ldap.uni.edu.au`, with a search base of `"ou=users,dc=testing,dc=uni,dc=edu,dc=au"`. VDT is being installed on an NFS.

The final command lines might look as follows:

Command	Comment
<code>export VDT_MYPROXY_LDAP=1</code>	Cause MyProxy-LDAP integration to be installed.
<code>export VDT_MYPROXY_LDAP_HOST=ldap.uni.edu.au</code>	Define LDAP host.
<code>export VDT_MYPROXY_LDAP_BASE="ou=users,dc=testing,dc=ARCHER,dc=edu,dc=au"</code>	Define LDAP search base.
<code>export VDT_LOCATION=/opt/nfs/vdt</code>	Define location to install VDT.
<code>export VDT_CACHE=/opt/nfs/vdtcache/vdt_181.mirror</code>	Define source of VDT components.
<code>export CA_DN_PREFIX="/O=uni/OU=edu/OU=au"</code>	Define DN for CA certificate.
<code>export DIST_HOST=www.hpc.jcu.edu.au/dist</code>	Define location of "distribution host".
<code>NO_CA=0 NO_VDT=0 ./setup -o -v</code>	Verify variables, don't install yet.
<code>NO_CA=0 NO_VDT=0 ./setup -v</code>	Install.

This does the following:

- Installs VDT, including MyProxy and Globus to `$VDT_LOCATION`.
- Configures MyProxy to authenticate to the provided LDAP.
- Generates a host key and certificate in `/etc/grid-security`
- Generates a CA key and certificate in `/opt/CA` (the default directory).
- Copies CA certificate to `/etc/grid-security/certificates`
- Creates a symlink from Globus (`$VDT_LOCATION/globus/TRUSTED_CA`) to `/etc/grid-security/certificates`.

Installing MyProxy with an existing CA

To use MyProxy to serve proxies for a CA you do not control:

1. Leave `NO_CA` undefined or set to 1.
2. Copy the CA certificate (`xxx.0`) and signing policy (`xxx.signing_policy`) files into `/etc/grid-security/certificates`. Obtaining these files will depend on your CA.
3. Install MyProxy as described above.
4. Place a server certificate signed by the CA in `/etc/grid-security/certificates`.
5. Obtain certificates for users, signed by the CA. Upload these into MyProxy.

To use MyProxy to sign certificates using a CA you control:

1. Leave `NO_CA` undefined or set to 1.
2. Copy the CA certificate (`xxx.0`) and signing policy (`xxx.signing_policy`) files into `/etc/grid-security/certificates`.
3. Copy the CA certificate to `/etc/grid-security/certificates`.
4. Copy the CA key to `/etc/grid-security`.
5. Install MyProxy as described above.

Installing without MyProxy

If you have an existing MyProxy installation that you wish to use, or do not wish to use MyProxy at all:

1. Leave `VDT_MYPROXY_LDAP` undefined, or set to 0.
2. Install VDT as described above.

Troubleshooting

Common sources of problems installing these components include:

- An unspecified, or not working, VDT cache location. Ensure that the installer can access the cache, and that it contains the correct version.
- Attempting to install over previous, incomplete installations. Ensure that target directories (such as `$VDT_LOCATION`) do not exist. Use the `-c` clean option as appropriate.
- Errors can result from a badly generated `/etc/yum.repos.d/jcuahpc.repo` file. Delete this file when rolling back an installation.

Consider redirecting the output of the log to a file and checking line by line for subtle error or warning messages.

After installation

Configuring other machines for this CA

If your ADS Infrastructure Layer is spread across more than one machine, you must copy the CA certificates to each other machine using this CA, such as your SRB machine. This is required in the “dual-server configuration” described above.

1. Copy all files from `$CA_ROOT/grid` on the CA machine to `/etc/grid-security/certificates` on the other machine. `$CA_ROOT` defaults to `/opt/CA`.
2. On the CA machine, generate a host key and certificate for the second machine as follows:

```
cert_tool -s -c machineb.uni.edu.au -e admin@machineb.uni.edu.au
```

See the “Tool Reference” section for more information `cert_tool`.

3. Copy the generated files (`hostcert.pem`, `hostkey.pem`, `openssl.cnf`, `req.pem`) from the `/tmp` directory on the CA machine where they are generated, to `/etc/grid-security` on the other machine. The correct subdirectory under `/tmp` is given as output from the `cert_tool` command.

Giving other machines access to MyProxy

Most likely, TCPWrappers on your server does not allow external access to MyProxy. You should now open this up by editing `/etc/hosts.allow`.

For example, to open up MyProxy access to a specific machine, you can use a line like:

```
myproxy-server: servername
```

See the “`hosts.allow`” man page for more information.

Verifying that MyProxy is running

After starting MyProxy (see “Maintaining VDT”), telnet to `localhost` on port 7512, then send two carriage returns. The output should look roughly as follows:

```
# source /etc/profile
# vdt-control --on

# telnet localhost 7512
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.

VERSION=MYPROXYv2
RESPONSE=1
ERROR=authentication failed
Connection closed by foreign host.
```

If this step fails:

- Check that the installation completed successfully by looking in the VDT log (`$VDT_LOCATION/vdt-install.log`)

- Ensure that the “myproxy-server” file exists in `/etc/xinet.d/`. If it doesn’t, the installation was incomplete.
- Make sure that LDAP is running and is accepting connections from your machine:
`ldapsearch -x -h <ldapservername>`
- Check for network issues by seeing if `xinetd` is in fact listening on port 7512:

```
# netstat -tlnp | grep 7512
tcp        0      0 0.0.0.0:7512  0.0.0.0:* LISTEN      31805/xinetd
```

Verifying that MyProxy is generating certificates

If necessary, first create an LDAP user. The mechanism will depend on your LDAP server, but for example:

```
# smbldap-adduser ldapuser
```

Then run the following command:

```
$ $VDT_LOCATION/globus/bin/myproxy-logon -s localhost -l ldapuser -v
Enter MyProxy pass phrase:
A credential has been received for user ldapuser in /tmp/x509up_u0.
```

Verify that the certificate is valid with a command like the following:

```
$ openssl verify -CAfile /etc/grid-security/certificates/bc6f5a0e.0 /tmp/x509up_u0
/tmp/x509up_u0: OK
```

If this step fails:

- Double check the contents of the file `$VDT_LOCATION/globus/etc/myproxy-server.config`.
- Check the logs (see “Maintenance” section).
- Try increasing the logging level (see “Maintenance” section).

Verifying that MyProxy works across the network

For this test, choose a desktop machine that has access to the MyProxy server.

1. Transfer `bc6f5a0e.0` from `$CA_LOCATION/grid` to `~/.globus/certificates` on the desktop machine. On Windows XP, this is `Documents and Settings\username\.globus\certificates`
2. Download the MyProxy Logon desktop tool there from <http://grid.ncsa.uiuc.edu/myproxy/MyProxyLogon/>.
3. Run MyProxy Logon, and test receiving a certificate from the MyProxy server.

Troubleshooting:

- If this step fails (but the previous step succeeded), the problem is network related. Double check the configuration of your `/etc/hosts.allow` file.
- If you receive the message “Path does not chain with any of the trust anchors”, you probably have not correctly carried out step 1.

Installing SRB

Prerequisites

See the **ARCHER Overview** for the standard requirements for operating system, network access etc. In addition:

- ARCHER deployment scripts must be present.
- The server must have a DNS name that can be resolved externally. That is:
 - "host <fully qualified server name>" returns a valid IP address.
 - "host <ip address>" returns a fully qualified domain name.
- VDT must already be installed on this machine.
- `$GLOBUS_LOCATION` must be set with the location of the Globus libraries.

SRB and MyProxy



In order for SRB to use MyProxy or GSI authentication, Globus must be installed before installing SRB – you can't add it later. Globus is installed through the VDT scripts.

Configuration

MCAT

SRB stores metadata about the files in its storage in a PostgreSQL database called MCAT. This database is created automatically on the SRB machine, installing PostgreSQL automatically in the process, if required.

Although SRB supports placing MCAT on a separate machine, this is not supported by the ARCHER deployment scripts.

Vault

You must also choose a location for the "vault" – the directory root where the contents of the SRB will be stored.

For more information, see:

- http://www.sdsc.edu/srb/index.php/FAQ#What_is_a_SRB_Vault.3F

Domain and zone

Finally, you must choose a domain and zone for the SRB.

For more information, see:

- <http://www.sdsc.edu/srb/index.php/Zones>
- http://www.sdsc.edu/srb/index.php/FAQ#What_is_a_domain.3F

Installing SRB

Refer to the "Using the deployment scripts" section above for an overview of how to obtain and run these scripts.

The following variables control the installation of SRB. The SRB software is then downloaded and installed from the internet.

Environment variable	Specifies	Example
NO_SRB	0 to cause SRB to be installed.	0
SRB_INSTALL_BASE	Location to install SRB software.	/opt/srb
SRB_INSTALL_VAULT	Location of actual storage.	/opt/srb/vault
SRB_DOMAIN	Domain the SRB is set up to serve.	testDomain
SRB_ZONE	Zone the SRB is set up in.	testZone
SRB_DECRYPT	Decryption string required to install SRB. Ensure that you are using the appropriate string for the SRB version being installed.	nstha2o4nh9t2Q6 (not the real key)
<i>You should generally not change the following variables.</i>		
SRB_DATABASE_NAME	PostgreSQL database name.	MCAT
SRB_DATABASE_USER	User in PostgreSQL.	srb
SRB_INSTALL_USER	Local user name to create, and run SRB server as.	srb
SRB_VERSION	Version of SRB to install. It must be available on \$DIST_HOST.	3.5.0

At a minimum, set NO_SRB, SRB_INSTALL_BASE and SRB_INSTALL_VAULT.

A typical installation is thus as follows:

```
export SRB_INSTALL_BASE="/opt/nfs/srb"
export SRB_INSTALL_VAULT="/opt/nfs/srb/vault"
export SRB_DECRYPT="xxxxxxxx"
NO_SRB=0 ./setup -o -v
```

Verify all the install parameters, before proceeding.

```
NO_SRB=0 ./setup
```

Result

The installation causes the following actions to take place. It is worth verifying that each has installed correctly.

Action	Verification
A user called "srb" is created and configured with an SRB environment (.MdasEnv, .MdasAuth)	Ensure that ~srb/.srb/.MdasEnv and ~srb/.srb/.MdasAuth exist and contain meaningful content. See: http://www.sdsc.edu/srb/index.php/MdasEnv_Template http://gridinfo.niees.ac.uk/index.php/Scommands

Action	Verification
The SRB software is installed in \$SRB_INSTALL_BASE – /opt/nfs/srb in this case.	Look for approximately 500mb of installed software in this directory.
Variable values are written to /etc/sysconfig/dev-env.	Verify these values.
PostgreSQL is installed if necessary, with a new database called MCAT. This database runs as the specified user.	psql MCAT srb \dt Expect 102 rows.
An empty vault is created in \$SRB_INSTALL_VAULT.	Verify this directory exists.
Scripts, commands etc installed in \$SRB_INSTALL_BASE/srb/installer/SRB3_5_0/utilities/bin.	Check for approximately 68 “S commands”.
ARCHER’s commands, like cert_tool and dev-adduser are installed in /usr/local/sbin.	Verify that they exist. See the “Tool Reference” section for details on these tools.
An SRB host certificate is generated in /etc/grid-security/srbcert.pem and srbkey.pem.	Verify that these exist. You can use the “openssl” command to confirm they have been generated correctly.
Auto-user creation is enabled.	See the rest of this section for verification of these features.
Authentication via GSI (and hence MyProxy) is enabled.	
The SRB server is started up.	
The “metadata security flag” is turned on, which means by default users have no access to other directories.	

Verifying that the SRB server is running

You can verify that the SRB server is operational by running scripts in the SRB home directory, as follows.

Command	Purpose
su - srb	Switch to srb user, running SRB initialisation script (setup.sh) in the process.
Sinit	Initialises the SRB client environment
Sls	Lists files in the srb user’s home collection.

The name of the current collection is printed if the server is running correctly.

Note: to use the “S commands”, a user must have a .MdasEnv file defined in its home directory. See the “Creating users” section. The “srb” user is guaranteed to already exist in the SRB, and to have a corresponding .MdasEnv file.

For more information on "S commands", see <http://www.sdsc.edu/srb/index.php/Scommands>.

Verifying that the SRB storage is functioning

In the same session as the previous test, now try adding a file to SRB as follows:

Command	Purpose
<code>echo TEST > /tmp/testFile</code>	Create a test file
<code>Sput /tmp/testFile</code>	Import it into the current SRB collection
<code>Scat testFile</code>	Display it from the current SRB collection

If SRB storage (ie, the vault) is configured correctly, you will see the contents of the file.

Changing the srb superuser password

By default, a super user called "srb" with password "password" is created within SRB. Now that the SRB is running, you should change this.

```
# su - srb
$ Sinit
$ Spasswd
  Type New Password:
  ReType New Password:
Successfully updated /net/srb/.srb/.MdasAuth
Password successfully updated in Catalog
```

This updates a record in MCAT, and modifies `~srb/.srb/.MdasAuth` to match.

Verifying that SRB works over network

The next few tests require Hermes, a tool in the ARCHER suite. Hermes is a desktop tool used for transferring files to and from SRBs. You can install it on any machine that has access to the SRB server, including Windows machines. See the Hermes System Administrator's Guide for pre-requisites, installation and use.

First, ensure that you can connect to SRB using username/password authentication. In most cases, the only user that will be set up this way is the "srb" superuser itself.

1. Install and run Hermes.
2. Create a new connection with the following parameters:

Field	Value
Protocol	srb://
Display name	Anything
Host	Address of the SRB server
Port	5544
Zone	(Leave blank)

Domain	The domain you specified as \$SRB_DOMAIN
Home	(Leave blank)
Resource	Generally, "<servername>Disk".
Authentication	Username/Password
Username	srb
Password	The password you created in the previous step.

If a new connection is created with a green light, the SRB server is accessible. Try copying a file to it.

Troubleshooting:

- If the previous steps worked, but this one fails, your problem is likely network related. Also check the logs indicated in the Maintenance section.

Verifying that GSI user creation is working

SRB is configured with "auto user creation", meaning SRB users are created automatically when authorised users connect via GSI authentication, including via MyProxy.

To test that the server is accepting GSI connections, use

1. Assuming you are using the CA installed with ADS, first generate a certificate for the user, using the `cert-tool` script. You will use a command like the following.

```
cert_tool -u username -l ldap.uni.edu.au -b dc=search,dc=base
```

Refer to the "Tool Reference" section for details.

2. Transfer the certificate to the Hermes machine, in `~/.globus`. On Windows, this is `\Documents and Settings\username\.globus4`.

3. Run Hermes.

4. Create a new connection with the following properties.

⁴ On Windows XP, you must use the Windows command shell ("cmd.exe") to create the `.globus` directory due to a bug/misfeature in the Windows Explorer shell.

Field	Value
Protocol	srb://
Display name	Anything
Host	Address of the SRB server
Port	5544
User Path / Mode	Leave as default
Authentication	GSI

5. Connect to the SRB server.
6. Copy any file to the SRB server.

If this succeeds, then the SRB server has been correctly set up, and is accepting GSI authentication.

Troubleshooting:

- Check the Hermes console window for information on the error.
- Check the SRB log. See "Maintenance" for more information.

For information on `cert_tool`, see "Tool Reference".

Verifying that MyProxy authentication is working

Testing MyProxy authentication is, of course, simpler than GSI.

1. Ensure the CA certificates are present in `~/.globus/certificates`.
2. Run Hermes.
3. Create a new connection as follows:

Field	Value
Protocol	srb://
Display name	Anything
Host	Address of the SRB server
Port	5544
Zone	(Leave blank)
Domain	(Leave blank)
Home	(Leave blank)
Resource	Generally, " <code><servername>Disk</code> ".
Authentication	MyProxy
Server	Host name of MyProxy server – the same as the SRB server in the standard ARCHER configuration.
Username	Name of a user that MyProxy accepts – typically a user in the associated LDAP.

Password	Password for that user.
----------	-------------------------

If previous tests succeed but this fails, possible causes include:

- Incorrectly sourced or located certificates on the desktop machine.
- The SRB server not having access to the correct CA certificate.
- Misconfiguration of SRB or MyProxy.

Maintaining VDT, MyProxy and CA

Starting and stopping

To start MyProxy, CA, Globus and other packages:

```
source /etc/profile
$VDT_LOCATION/vdt/sbin/vdt-control --on
```

To stop them all:

```
$VDT_LOCATION/vdt/sbin/vdt-control --off
```

You control MyProxy individually like this:

```
$VDT_LOCATION/vdt/sbin/vdt-control --on myproxy-server
```

For more information:

<http://vdt.cs.wisc.edu/releases/1.10.1/man/vdt-control.html>

To stop MyProxy permanently, set the "disable" property to "yes" in `/etc/xinetd.d/myproxy-server`. Then restart xinetd:

```
service xinetd reload
```

Logging

MyProxy uses Syslog to write to `/var/log/messages`.

You can get debug output from MyProxy as follows:

1. Shut down MyProxy.
2. Run `$VDT_LOCATION/globus/sbin/myproxy-server -d`

Configuration

MyProxy is configured through `$GLOBUS_LOCATION/etc/myproxy-server.config`.

For more information:

<http://grid.ncsa.uiuc.edu/myproxy/man/myproxy-server.config.5.html>

As an xinetd service, it also configured through `/etc/xinetd.d/myproxy-server`.

Maintaining SRB

Starting and stopping

To stop SRB:

```
# ~srb/install/bin/killsrb
```

To start SRB:

```
# su - srb  
$ install/bin/runsrb
```

Logging

SRB writes logs within `~srb/install/data/log/`.

Configuration

Certain configuration variables are stored in `/etc/sysconf/dev-env`.

Tool reference

Using cert_tool

The `cert_tool` script is installed as part of the VDT deployment script.

```
usage: /usr/local/sbin/cert_tool [-h] [-s] [-u user_id] [-c common_name] [-e
email_address] [-r] [-l ldap_uri] [-b ldap_base]

-h this message
-s make a server (host) certificate
-u the user_id from which to extract the email address and common_name for a user
certificate
-c the common_name for the user (overrides LDAP entry)
-e the email_address for the user (overrides LDAP entry)
-r revoke the certificate (requires either -s or -u)
-l the location of the ldap server
-b the base of the ldap tree
```

This script generates user or host certificates, and their corresponding private keys. It is only useful if you installed a CA.

To create a host key for a server, use a command like:

```
cert_tool -s -c icat@server.uni.edu.au -e admin@uni.edu.au
```

To create a user key, use a command like:

```
cert_tool -u user@uni.edu.au -l ldap.uni.edu.au
```

In most cases it is preferable to use `dev-adduser` when creating user certificates. `Dev-adduser` calls `cert_tool` to actually generate the certificates.

Using dev-adduser

The bundled script `dev-adduser` simplifies creating users and setting up their environment. It is only useful if using MyProxy or grid tools.

```
usage: /usr/local/sbin/dev-adduser [-h] [-c] [-e] [-g] [-s] username

-h      this help message
-c      skip certificate creation (implies -g)
-e      skip user creation (user must already exist)
-g      skip gridmap-file modification
-s      skip srb setup
```


Step	What it does	Disable with
Local user	Creates a local (PAM) user account.	-e
Certificate	Generates a user certificate and stores it in <code>~username/.globus</code> Note: This is required to use GSI authentication. However, if the user is connecting from another location, such as from Windows, you need to copy their generated certificate to that desktop.	-c
Gridmap-file modification	Adds an entry to <code>/etc/grid-security/grid-mapfile</code> .	-c or -g
SRB setup	Writes a <code>~username/.MdasEnv</code> file, allowing them to use "S commands".	-s

Creating users

To allow users to use ARCHER tools, they need to be enabled in various ways.

To use	You need	Which is created with
SRB "S commands"	<code>.MdasEnv/.MdasAuth</code> in <code>~/srb</code>	<code>dev-adduser</code>
MyProxy authentication for XDMS, Hermes	An LDAP account	* <code>smbldap-adduser</code>
GSI/GridFTP	User certificate, entry in <code>/etc/grid-security/grid-mapfile</code>	<code>dev-adduser</code> (without <code>-c -g</code>)
SRB, if not using auto-logon with MyProxy	User account in SRB.	** <code>mcatadmin</code>

* No LDAP client tools are included in Archer. LDAP user creation depends on the LDAP software you are using.

** http://www.sdsc.edu/srb/index.php/Admin_Tool