Bestman Gateway Hands On

Highlighted items are particularly important for a correctly functioning security configuration of BeStMan.

Introduction

This documents describes the installation of BeStMan-Gateway as provided by OSG 1.2 on a host with an existing disk-based POSIX-compliant file systems, NFS in this case.

BeStMan-Gateway, developed by the Scientific Data Management Group of Lawrence Berkeley National Laboratory, is a generic SRM v2.2 load balancing frontend for transfer servers. It works on top of existing disk-based POSIX-compliant file systems, and has been reported so far to work on file systems such as NFS, GPFS, PVFS2, GFS, Ibrix, HFS+, Hadoop, XrootdFS and Lustre. It also works with any existing file transfer service, such as gsiftp, http, https, bbftp and ftp. This document is written for system administrators who are planning to use storage that is installed on top of a POSIX-compliant file system. The goal of this document is to give enough information for system administrators to do initial simple configuration of the storage as well as provide references to the documents that may help to accomplish more sophisticated configuration.

See also BeStMan Full mode for more information about BeStMan full mode installation and BeStManGateway-Xrootd for more information about BeStManGateway-Xrootd.

Requirements

It could work with ... For this exercise we will be using It will work also on a single host with a VDT supported OS and and NFS file share

For more information about recommended and possible configuration please check the reference documentation BestmanGateway

BeStMan-gateway Installation from VDT distribution

BeStMan-Gateway implements an essential subset of SRM v2.2 specifications that includes:

- srmPing()
- srmGetTransferProtocols()
- srmLs()
- srmRm()
- srmMkdir()
- srmRmdir()
- srmPrepareToPut()
- srmPrepareToGet()
- srmPutDone()
- srmReleaseFiles()
- srmGetSpaceTokens()
- srmGetSpaceMetaData()

For more information see BeStMan Gateway at SLAC

Pacman 3.28 is required. Installation is likely to fail with earlier versions. Install instructions for Pacman: PacmanInstall

Create an installation directory

Create a directory, e.g. /opt/osg-bestman. Make sure there are no non-standard versions of perl, python, tcsh, or bash in your $PATH variable. We will refer to this directory as <*VDT_LOCATION*>.

Downloading BeStMan-Gateway

The installation described here is done as root even though services does not run as root:

A few questions regarding trust of the caches from which the software is downloaded will be displayed. Please answer y (yes) so that the software can be retrieved. If you do not want to use grid-map file to set up the mappings from global identities (user certificate names) to local accounts please answer n (no) to the following question:

```
Do you want edg-mkgridmap daemon to be run via cron? [y/n] n
```

See the PacmanBestPractices guide if you encounter an 'unsupported' platform message.

```
cd <VDT_LOCATION>
```

```
export VDT_GUMS_HOST=<GUMS hostname>     # if you want to use GUMS for GridFtp and Gratia GridF
pacman -get http://software.grid.iu.edu/osg-1.2:Bestman
```

To check what services have been installed on your node you can do:

```
cd <VDT_LOCATION>
. setup.sh
 vdt-control --list

Service            | Type   | Desired State
-------------------+--------+--------------
fetch-crl          | cron   | enable
vdt-rotate-logs    | cron   | enable
vdt-update-certs   | cron   | enable
gsiftp             | inetd  | enable
gratia-gridftp-tran| cron   | do not enable
bestman            | init   | enable
edg-mkgridmap      | cron   | do not enable
gums-host-cron     | cron   | do not enable
```

Follow the instructions provided in *$VDT_LOCATION/post-install/README* to configure CA package updates.

ALSO in OSG 1.2?

Install the CA Certificate Updater

As of September 2008, certificate authority certificates will no longer be installed and configured during installation. Many components of the installation will not work until these are installed. In order to finish installing the CA-Certificates package on your system you will need to do the following one-time configuration. For more information, see http://vdt.cs.wisc.edu/releases/2.0.0/certificate_authorities.html

Run the following to setup up your certificates for OSG CA distributions

```
#source VDT_LOCATION/setup.sh
#$VDT_LOCATION/vdt/bin/vdt-ca-manage setupca --location [root|local|<PATH>] --url [osg|vdt|<URL>

 Location:
    root - install into /etc/grid-security
    local - install into $VDT_LOCATION/globus/share
    PATH - install into PATH (e.g. /nfs/certificates)

A common example is to install the OSG-provided certificates into the OSG install directory:

$VDT_LOCATION/vdt/bin/vdt-ca-manage setupca --location local --url osg
```

There are 2 additional services associated with certificate authorities:

1. *vdt-update-certs* - a cron service that insures that future certificate updates are fetched automatically.
2. *fetch-crl* - a cron service that retrieves the latest certificate revocation lists (CRLs) for each CA.

On Compute Element (CE) installs, the enabling of these services is performed by the *configure_osg* script based on the following option in the *config.ini* file:

```
[Misc Services]
use_cert_updater = True
   or
use_cert_updater = %(enable)s
```

For all other installations, the following steps should be performed (you must be *root* user to use the *vdt-control* script):

1. For the *vdt-update-certs* service:
   - vdt-control --enable vdt-update-certs
   - vdt-control --on vdt-update-certs
2. For the *fetch_crl* service (this will activate the service and retrieve an initial set of CRLs)
   - vdt-control --enable fetch-crl
   - vdt-control --on fetch-crl
   - $VDT_LOCATION/vdt/bin/vdt-ca-manage fetchCRL

A complete documentation of vdt-ca-manage command can be found in the vdt-ca-manage documentation

Run `vdt-post-install` script

Configuring BeStMan-gateway

You will need to configure BeStMan to enable gateway-mode. You have to decide if you would like to use pre-defined, static space tokens. In this case, you need to provide a list of space token name, description and size of space allocated for each token. Keep in mind that in gateway-mode, BeStMan is not managing your space.

The example below shows how to configure BeStMan in gateway-mode, enable GUMS and space token usage:

```
cd <VDT_LOCATION>
. setup.sh
$VDT_LOCATION/vdt/setup/configure_bestman --server y \
 --user <user> \
 --cert <service_cert>  \
 --key  <service_key>  \
 --http-port  <public_port>  \
 --https-port  <secured_port>  \
 --gums-host  <GUMS hostname>  \
 --gums-port  <GUMS port number>  \
 --enable-gateway  \
 --with-allowed-paths="<allowed_dir_list>"  \
 --with-blocked-paths="<blocked_dir_list>"  \
 --with-tokens-list  "<TOKEN_1_NAME>[desc:<TOKEN_1_DESC>][<TOKEN_1_SIZE_GB>];<TOKEN_2_NAME>[desc
 --with-transfer-servers  <GridFTP server list>
```

Where *user* name of the non-privileged user that runs BeStMan,

service_cert path to service certificate (⚠ **the certificate file should belong to the user**)
service_key path to service certificate private key (⚠ **the certificate key file should belong to the user**).

⚠ BeStMan should be configured with host certificate in order to be able to handle requests from LCG-Utils tools. This is mandatory for at least all BeStMan servers that support ATLAS experiment. Normally the OSG BeStMan implementation uses a service certificate, not a host certificate. This causes lcg-cp to fail because the certificate name (which looks like http/hostname instead of just hostname) doesn't match the hostname.

This is a defect of LCG_Utils. The host certificate for BeStMan should be owned by the BeStMan user and be a different certificate than the host certificate owned by root (if one exists).

public_port_http public port (default : 10080;commonly used port is 8080 unless there is a co
secured_port_http private port (default: 10443;commonly used port is 8443 unless there is a
allowed_dir_list list of directories, separated by semicolon, accessible to users
blocked_dir_list list of directories separated by semicolon, non-accessible to users (default a
--with-allowed-paths / --with-bloacked-paths options should be used.
GUMS hostname the name of GUMS server,
GUMS port number the port of GUMS server,
token list example:
"ATLASDATADISK[desc:ATLASDATADISK][40000];ATLASPRODDISK[desc:ATLASPRODDISK][30000];ATLASGROUPDISK[desc:ATLASGROUPDISK][30000]"

GridFTP server list is a list FQDN of your GridFTP servers, separated by ; . e.g. “gsiftp://host1.domain.tld;gsiftp://host2.domain.tld”

IMPORTANT - GridFTP servers should be configured to use same GUMS server as BeStMan.

If you want to use grid-map-file for user authentication and authorization do not specify the following options:

--gums-host

--gums-port

If you do not want to use pre-defined, static space tokens, do not specify the following options:

--with-tokens-list

⚠ Please, make the appropriate modification to */etc/sudoers* described in the BeStMan documentation, namely add the following lines to this file:

```
# Comment out this line, if it is in your /etc/sudoers file (RHEL5+)
#Defaults    requiretty

Cmnd_Alias SRM_CMD = /bin/rm, /bin/mkdir, /bin/rmdir, /bin/mv, /bin/ls
Runas_Alias SRM_USR = ALL, !root
<user_name> ALL=(SRM_USR) NOPASSWD: SRM_CMD
```

Please keep in mind that this is just an example, you can choose more be more restrictive policy for your site. BeStMan server will not be able to run if this step is missed.

If you are running your BeStMan-Gateway on the node that doesn’t have an access to your file system, you will have to modify the following attributes in *$VDT_LOCATION/bestman/conf/bestman.rc* configuration file:

```
checkSizeWithFS=false
```

```
checkSizeWithGsiftp=true
```

Configuring GridFTP

GridFTP server comes with BeStMan installation. If you want to use the grid-map-file for user authentication and authorization ignore the rest of this section. Copy two files from *$VDT_LOCATION/post-install* to in */etc/grid-security*:

```
cp $VDT_LOCATION/post-install/prima-authz.conf /etc/grid-security
cp $VDT_LOCATION/post-install/gsi-authz.conf /etc/grid-security
```

If you are dealing with firewall the gridftp port range should be properly set. In order to do so you will have to modify *vdt-local-setup.sh*.

```
#edit $VDT_LOCATION/vdt/etc/vdt-local-setup.sh
GLOBUS_TCP_SOURCE_RANGE=<low_port,high_port>
GLOBUS_TCP_PORT_RANGE=<low_port,high_port>
export GLOBUS_TCP_SOURCE_RANGE
export GLOBUS_TCP_PORT_RANGE
```

Where *low_port,high_port* - controls all outbound globus connections for gridftp (e.g GLOBUS_TCP_SOURCE_RANGE=40000,49150)

You can have multiple installation of GridFTP servers located on the nodes you have specified in BeStMan-gateway configuration (see section about standalone GridFTP installation if you want to install it as a standalone server).

You will need to make sure that users have write permission in to the storage area.

Gratia Gridftp Transfer Probe

If you are using GridFTP server that is installed during the BeStMan installation you will need to enable,configure Gratia GrdFTP transfer probe and perform the actions described in Preparing, Installing and Validating Gratia transfer probe

Installation of standalone GridFTP from VDT distribution

If you want to use several GridFTP servers (e.g for load balancing) you will need to install GridFTP on each dedicated node. In order to that Create a directory, e.g. /opt/http://software.grid.iu.edu/osg-1.2-gridftp. Make sure there are no non-standard versions of perl, python, tcsh, or bash in your $PATH variable. We will refer to this directory as <*VDT_LOCATION*>.

The installation described here is done as root:

* A few questions regarding trust of the caches from which the software is downloaded will be displayed. Please answer y (yes) so that the software can be retrieved. If you do not want to use grid-map file to set up the mappings from global identities (user certificate names) to local accounts please answer n (no) to the following question:

```
Do you want edg-mkgridmap daemon to be run via cron? [y/n] n
```

```
cd <VDT_LOCATION>
```

```
. setup.sh
export VDT_GUMS_HOST=<GUMS hostname>  # if you want to use GUMS for GridFTP authorization
pacman -get http://software.grid.iu.edu/osg-1.2:GridFTP
. setup.sh                          #DON'T forget to do that otherwise PRIMA will not work
pacman -get http://software.grid.iu.edu/osg-1.2:Gratia-GridFTP
. setup.sh
```

Where *GUMS hostname* is a GUMS server and <*VDT_LOCATION*> is a root directory of http://software.grid.iu.edu/osg-1.2 installation.

Then copy two files from *$VDT_LOCATION/post-install* to in */etc/grid-security*:

```
cp $VDT_LOCATION/post-install/prima-authz.conf /etc/grid-security
cp $VDT_LOCATION/post-install/gsi-authz.conf /etc/grid-security
```

Follow the instructions provided in *$VDT_LOCATION/post-install/README* to configure CA package updates.

If you are dealing with firewall the gridftp port range should be properly set. In order to do so you will have to modify *vdt-local-setup.sh*.

```
#edit $VDT_LOCATION/vdt/etc/vdt-local-setup.sh
GLOBUS_TCP_SOURCE_RANGE=<low_port,high_port>
GLOBUS_TCP_PORT_RANGE=<low_port,high_port>
export GLOBUS_TCP_SOURCE_RANGE
export GLOBUS_TCP_PORT_RANGE
```

Where *low_port,high_port* - controls all outbound globus connections for gridftp (e.g GLOBUS_TCP_SOURCE_RANGE=40000,49150) You will need to make sure that users have write permission in to the storage area.

Gratia GridFTP Transfer Probe

If you are using standalone GridFTP server you will need to enable, configure Gratia GridFTP transfer probe and perform the actions described in Preparing, Installing and Validating Gratia transfer probe

Running the system

Start the system

You have to be root to start each service. You have to start all the components in the following order (this is order is optional but seems logical):

1. Start BeStMan (GridFtp and Gratia transfer probe). Login on BeStMan node, then:

   ```
   cd  <VDT_LOCATION>
   . setup.sh
   vdt-control –on
   ```

2. Start standalone GridFTP and Gratia transfer probe. Login on each GridFTP node, then:

```
cd  <VDT_LOCATION>
. setup.sh
vdt-control –on
```

Stop the system

You have to be root to stop each service. You have to stop all the components in the following order (this is order is optional but seems logical):

1. Stop BeStMan (GridFtp and Gratia transfer probe). Login on BeStMan node, then:

```
cd  <VDT_LOCATION>
. setup.sh
vdt-control –off
```

2. Stop standalone GridFtp and Gratia transfer probe. Login on each GridFTP node, then:

```
cd  <VDT_LOCATION>
. setup.sh
vdt-control –off
```

System Validation

In order to verify that the system is functional you may use LBNL srm client that is installed with BeStMan. In order to do so you will need to add the path to all the srm client scripts to your *PATH* environment variable:

```
cd <VDT_LOCATION>
. setup.sh
export PATH=$PATH:$VDT_LOCATION/bestman/bin
```

or if you want to install srm-client on different node you will need to download it from http://software.grid.iu.edu/osg-1.2:

```
mkdir /opt/http://software.grid.iu.edu/osg-1.2_wn_client
cd  /opt/http://software.grid.iu.edu/osg-1.2_wn_client
pacman -get http://software.grid.iu.edu/osg-1.2:wn-client
. setup.sh
```

Follow the instructions provided in *$VDT_LOCATION/post-install/README* to configure CA package updates.

You will need to get your voms-proxy certificate:

```
voms-proxy-init –voms <voname>:/<voname>
```

Execute srm-ping:

```
 srm-ping srm://<BeStMan_host>:<secured_port_http>/srm/v2/server
```

Expected results:

```
##########################################
SRM_HOME is /usr/local/osg-client/srm-client-lbnl
JAVA_HOME is /usr/local/osg-client/jdk1.5 X509_CERT_DIR =
/usr/local/osg-client/globus/TRUSTED_CA
GSI_DAEMON_TRUSTED_CA_DIR = /usr/local/osg-client/globus/TRUSTED_CA
##########################################

SRM-CLIENT: got remote srm object

SRM-PING: Thu Sep 18 11:55:50 CDT 2008 Calling SrmPing Request...
Ping versionInfo=v2.2

Extra information
        Key=backend_type
        Value=BeStMan
        Key=backend_version
        Value=2.2.1.1
        Key=GatewayMode
        Value=Enabled
        Key=gsiftpTxfServers
        Value=gsiftp://osg-ress-2.fnal.gov
        Key=clientDN
        Value=/DC=org/DC=doegrids/OU=People/CN=Tanya Levshina 508821
        Key=localIDMapped
        Value=fnalgrid
        Key=staticToken(0)
        Value=DISK1 desc=DATA1 size=1073741824
        Key=staticToken(1)
        Value=DISK2 desc=DATA2 size=2147483648
```

If you have reasonable result you may try to srm copy. In order to do so create a file *"test1"* in */tmp* directory and execute:

```
srm-copy   file:////tmp/test1
srm://<BeStMan_host>.gov:<secured_port_http >/srm/v2/server\?SFN=<FS_ROOT_DIR>/test1 -spacetoken
```

You should get back something like that:

```
srm-copy   file:////tmp/test1_1 srm://fapl118.fnal.gov:8443/srm/v2/server\?SFN=/home/tlevshin/ca
##########################################
SRM_HOME is /usr/local/vdt_client/srm-client-lbnl
JAVA_HOME is /usr/local/vdt_client/jdk1.5
X509_CERT_DIR = /etc/grid-security/certificates
```

```
GSI_DAEMON_TRUSTED_CA_DIR = /etc/grid-security/certificates
############################################
SRM-CLIENT: Mon Nov 03 11:32:03 CST 2008 Connecting to
httpg://fapl118.fnal.gov:8443/srm/v2/server
SRM-CLIENT: Mon Nov 03 11:32:04 CST 2008 Calling SrmPrepareToPutRequest
now ...
request.token=put:5
status=SRM_SUCCESS
explanation=null

SRM-CLIENT: RequestFileStatus for SURL=file:////tmp/test1_1 is Ready.
SRM-CLIENT: received
TURL=gsiftp://fg0x5.fnal.gov//home/tlevshin/cache/test_4
>>>Total Memory=17932288
>>>Free Memory=6875256
>>>Memory in use=11057032

SRM-CLIENT: Mon Nov 03 11:32:08 CST 2008 start file transfer.
SRM-CLIENT:Source=file:////tmp/test1_1
SRM-CLIENT:Target=gsiftp://fg0x5.fnal.gov//home/tlevshin/cache/test_4

SRM-CLIENT: Mon Nov 03 11:32:10 CST 2008 end file transfer.

SRM-CLIENT: Mon Nov 03 11:32:10 CST 2008 Calling putDone for
srm://fapl118.fnal.gov:8443/srm/v2/server?SFN=/home/tlevshin/cache/test_4

SRM-CLIENT: Mon Nov 03 11:32:18 CST 2008 end file transfer.

SRM-CLIENT: Mon Nov 03 11:32:18 CST 2008 end file transfer.

SRM-CLIENT: Request completed with success

SRM-CLIENT: Printing text report now ...

SRM-CLIENT*REQUESTTYPE=put
SRM-CLIENT*TOTALFILES=1
SRM-CLIENT*TOTAL_SUCCESS=1
SRM-CLIENT*TOTAL_FAILED=0
SRM-CLIENT*REQUEST_TOKEN=put:5
SRM-CLIENT*REQUEST_STATUS=SRM_SUCCESS
SRM-CLIENT*SOURCEURL[0]=file:////tmp/test1_1
SRM- CLIENT*TARGETURL[0]=srm://fapl118.fnal.gov:8443/srm/v2/server?SFN=/home/tlevshin/cache/test
SRM-CLIENT*TRANSFERURL[0]=gsiftp://fg0x5.fnal.gov//home/tlevshin/cache/test_4
SRM-CLIENT*ACTUALSIZE[0]=16
SRM-CLIENT*FILE_STATUS[0]=SRM_SUCCESS
SRM-CLIENT*EXPLANATION[0]=SRM-CLIENT: PutDone is called successfully
ExitCode=0
```

If you turn on Gratia GridFTP transfer probes you should be able to see the accounting information by accessing your Gratia collector. See details in Preparing, Installing and Validating Gratia transfer probe.

Troubleshooting

If system validation failed, you would probably need to check the each component in order to verify your installation. In order to do so you should check all of them in the following order:

- GUMS (if in use)
- GridFTP
- BeStMan

Verifying GUMS

Make sure that the service certificate you are specified for BeStMan configuration with --cert <service_cert> , --key <service_key> options and GridFTP service certificate are accepted by GUMS (see GUMS Installation Documentation)

Get mapping *uid* for your certificate and verify that this *uid* exists on BeStMan and GridFTP node.

Verifying GridFTP

Login on the node where you have installed have your certificate installed and access to http://software.grid.iu.edu/osg-1.2:wn_client.

You will need to get your voms-proxy certificate:

```
voms-proxy-init –voms <voname>:/<voname>
```

Then test GridFtp:

```
cd $VDT_LOCATION
. setup.sh
echo “This is a test” >/tmp/test
globus-url-copy -dbg file:///tmp/test gsiftp://<GridFtp_host>/tmp/test
```

Verifying BeStMan

Make sure that BeStMan is running and there is no error in the log file (*$VDT_LOCATION/vdt-app-data/bestman/logs/event.srm.log*)

```
[root@cmswn085 itb_bestman]# ps auxww|grep $VDT_LOCATION/bestman|grep -v grep
daemon   27648  0.0  0.0  4944 1168 pts/2    S    07:46   0:00 /bin/sh /usr/local/itb_bestman/be
daemon   27676  3.3  7.4 715240 155208 pts/2 Sl   07:46   1:59 /usr/local/itb_bestman/jdk1.6/bin
```

List of utilized ports

Module Name	Port Number	Protocol
BeStMan	8080 (default 10080)	tcp

Module Name	Port Number	Protocol
	8443 (default 10443)	tcp
GridFTP	2811	tcp
	lowPort,maxPort if needed to control outbound globus connections	tcp

Log file and configuration locations

If any of the tests described above have failed or you are just curious to see what's going on you could find log and configuration files for each of the module in the following location on a relevant node:

Module Name	Configuration files	Log files
BeStMan	$VDT_LOCATION/bestman/conf/bestman.rc	$VDT_LOCATION/vdt-app-data/bestman /logs/event.srm.log
GridFTP	$VDT_LOCATION/vdt/services/vdt-run-gsiftp.sh.env	$VDT_LOCATION/globus/var/log/gridftp.log $VDT_LOCATION/globus/var/log/gridftp-auth.log

Reference

- OSG BeStMan Full Mode page
- OSG BeStMan Gateway and Xrootd page
- OSG BeStMan Gateway on CE page
- OSG Gratia Transfer Probe page
- BeStMan Home Page at LBNL - BeStMan User guides, BeStMan FAQ and latest downloadable tar files available here. Latest downloadables should be the same version as in VDT.
- SRM v2.2 LBNL client command line examples
- SRM-Tester
- UNL BeStMan Instruction
- SLAC BeStMan Gateway mode Instruction - SLAC guide on BeStMan gateway mode
- US ATLAS BeStMan instruction page
- UMD BeStMan Admin Instruction - UMD experience on how to admin BeStMan
- OSG SRM Daily Testing Results - OSG provides SRM v2.2 daily testing. Site registration is needed HERE
- SRM specifications and collaboration - from SRM collaboration working group
- GridFTP Documentation
- VDT Home Page - The information related to current VDT cache, installation and configuration
- OSG documentation Home - Numerous documents about storage solutions supported by OSG as well as other useful links

Support

- Frequently Asked Questions answered here
- If you cannot find answers, please send all your questions to osg-storage@opensciencegrid.org

Presentation

Can include attached PDF presentation. Until you attach the presentation you'll see a Not Found error.

Comments

Complete:
Responsible: MarcoMambelli - 31 Jul 2009
Reviewer - date:

This topic: ReleaseDocumentation > Integration > WebHome > TutorialsFromThisRelease > SiteAdminsWorkshopTutorialsAug09 > BestmanGatewayHandsOn
Topic revision: r1 - 31 Jul 2009 - 19:45:47 - MarcoMambelli