HPSS DSI Installation Guide

HPSS Data Storage Interface
Release 2.1.0

March 2017

Printed in the United States of America.

DSI 2.1.0
March 2017

Table of Contents

Preface

About This Document

The HPSS Data Storage Interface (HPSS DSI) Installation Guide is for use at system installation time. It outlines the steps required to install and configure an HPSS DSI system.

Chapter 1 instructions of an HPSS DSI software installation.

Chapter 2 instructions of an HPSS DSI configuration.

Conventions Used in This Document

Example commands that should be typed as shown at a command line are preceded by a not-to-be-typed percent sign ('%') and be presented in a boldface courier font:

```
% sample command
```

Example command output and example contents of ASCII files are presented in non-bolded courier font:

```
% cat sample_file
sample file line 1
sample file line 2
```

When a file listing or command output has been shortened for display, an ellipsis will be used to indicate missing lines:

```
% sample command
some command output
   . . .
more command output
```

Example interactive command input and output is presented in a courier font, with input to be supplied at the indicated point in command execution shown in bold:

```
% sample command
command output
prompt-1> some input
more command output
prompt-2> more input
still more command output
```

User input, whether on the command line or to an interactive command prompt, that's dynamic will be shown in italics:

```
% sample command /pathname
command output
prompt-1> XYZ <calculated value>
```

In the above, "sample command" and "XYZ" would be typed exactly as shown, while

“/pathname” would be replaced by the appropriate pathname and “<calculated value>” replaced with the result of some specified calculation.

Any text preceded by a pound sign (‘#’) should be considered comment lines:

```
# This is a comment
```

1.HPSS DSI INSTALLATION

This chapter provides instructions and supporting information for installing the HPSS DSI RPMs. As of writing there are no plans to release any source code distributions of the HPSS DSI.

Instructions on how to install HPSS 7.5.1 can be found here:

http://www.hpss-collaboration.org/documents/hpss751/install_guide.pdf

Instructions on how to install Globus Toolkit 6 can be found here

http://toolkit.globus.org/toolkit/docs/latest-stable/admin/install/#gtadmin-basic-security

Both Globus Toolkit 6 and HPSS 7.5.1 should be installed and configured before you install HPSS DSI 2.1.0

NOTE: The Globus Toolkit 6 must be installed via RPMs for the DSI to function. It cannot be installed from source.

1.1. Install HPSS DSI RPMs

1. Obtain the HPSS DSI RPMs from your HPSS support representative.

2.Install the RPMs

For Redhat 6

```
% rpm -Uvh hpss-gridftp-dsi-2.1.0-0.el6.x86_64.rpm
```

For Redhat 7

```
% rpm -Uvh hpss-gridftp-dsi-2.1.0-0.el7.x86_64.rpm
```

2.HPSS DSI CONFIGURATION

The following sections describe how to configure HPSS DSI after it has been installed.

For GridFTP to function it requires a privileged user with control permission on the core server's client interface. To configure this privileged user follow the procedure in section 2.1.

The steps required to configure the HPSS DSI depend on whether you wish to xinetd or not. If configuring using xinetd, follow the procedures outlined in section 2.2. If configuring without using xinetd, follow the procedures outlined in section 2.3

There are few configuration files that must be modified for the HPSS DSI to function. These configuration files are the HPSS DSI configuration files, HPSS configuration files, and if using Kerberos, the Kerberos configuration files. Follow the procedures in section 2.4 to configure the DSI configuration files. Follow the procedures in section 2.5 to configure the HPSS configuration files. And if using Kerberos follow the procedures in section 2.6 to configure Kerberos.

2.1. Configure privileged user for HPSS

GridFTP requires a privileged user with control permission on the core server's client interface in order to log into HPSS and then it changes its credentials to that of the actual user (you). Think of it as a type of setuid process that logs in, does what it must, then changes the process owner to you.

HPSS has a special privileged user named 'hpssftp' which has the necessary permissions and special code within HPSS to not allow it to bypass the Gatekeeper callouts. Thus we recommend that you use the 'hpssftp' user in gridftp.conf.

You will, however, want the GridFTP process to run as a non-privileged user. For this reason, we run the GridFTP server as local UNIX user 'gridftp', but configure it to use hpssftp's credentials to log into HPSS.

Add the new user 'gridftp' to the system password file. Your entry should look something like the following:

gridftp:x:316:316:GridFTP Server:/home/gridftp:/bin/bash

Now you'll need to create a keytab file for the 'gridftp' user. This will be used by the DSI in order to authenticate to HPSS. For sites using UNIX authentication with HPSS (rather than Kerberos):

```
% /opt/hpss/bin/hpss_unix_keytab -f /var/hpss/etc/gridftp.keytab add
hpssftp
```

For sites using Kerberos authentication with HPSS, you'll need to create and use a Kerberos keytab file (rather than a UNIX keytab). The Kerberos utility 'ktutil' can be used for that purpose.

2.2. Configuration using xinetd

The globus GridFTP server does not need to run as a privileged user. You should create a system account for this purpose. It is important to make sure that both the keytab files generated above and the GSI (Grid Security Infrastructure) host key are both owned by this system account. In the following example, I will use the system account 'gridftp'. Since our HPSS installation currently uses the system password file (instead of the HPSS specific password file) this is the same account created earlier for authentication to HPSS. However, if your site uses the HPSS specific password file, you will need to create a separate system account for the GridFTP server process (they may both have the same name).

Add an entry to /etc/services for the default gsiftp port:

gsiftp 2811/tcp # GSI FTP

Here's an example xinetd entry (/etc/xinetd.d/gridftp). Note that the HPSS DSI requires that the server run with threads so you must use -threads with a value of 2 or greater.

Some fine-tuning will be required to find the optimal number of threads at a specific site.

```
service gsiftp
{
        flags      = IPv4
        wait       = no
        user       = gridftp
        # You may need to set group depending upon the account chosen
        group       = gridftp
        server      = /usr/local/globus/sbin/globus-gridftp-server
        # auth-level 6 = 2 for frontend default + 4 for no-change-uid/gid
        #  0 - Disables all authorization checks
        #  1 - Authorize identity
        #  2 - Authorize all file/resource accesses (Default for fronend)
        #  4 - Disable changing process uid to authenticated user
        server_args = -inetd -threads 2 -auth-level 7 -dsi hpss_local -disable-command-list
SCKS,APPE,REST
        env        = GRIDMAP=/etc/grid-security/grid-mapfile
        env        = LD_LIBRARY_PATH=/opt/hpss/lib:/usr/local/gridftp_hpss_dsi-2.1.0
        socket_type = stream
        per_source  = 100
}
```

2.3. Configuration without using xinetd

If you are launching GridFTP without xinetd (for example, a Globus Connect Server install), you can configure the server as follows.

Add these lines to /etc/gridftp.d/extra:

```
auth_level 7
load_dsi_module hpss_local
disable_command_list SCKS,APPE,REST
```

Add the following line to /etc/init.d/globus-gridftp-server:

export LD_LIBRARY_PATH=/usr/local/gridftp_hpss_dsi-2.1.0

2.4. Setup the HPSS DSI configuration file

Create the file /var/hpss/etc/gridftp.conf
Enter the following into gridftp.conf:

```
Authenticator <The location of your HPSS keytab>
AuthenticationMech <unix or Kerberos>
LoginName hpssftp
ChecksumSupport <on or off>
UDAChecksumSupport <on or off>
```

The ChecksumSupport option will store a checksum calculated during a file transfer on the file when set to “on”. The UDAChecksumSupport option will store a checksum during a file transfer on a file's User Defined Attributes (UDA's) when set to “on”.

The UDA's that are stored are:

/hpss/user/cksum/algorithm
/hpss/user/cksum/checksum
/hpss/user/cksum/lastupdate
/hpss/user/cksum/errors
/hpss/user/cksum/state
/hpss/user/cksum/app
/hpss/user/cksum/filesize

When using the Globus Webapp, checksums are calculated for transfers using the following options:

1. verify file integrity after transfer option
2. sync "checksum is different" option.

When using globus-url-copy, checksums are calculated for transfers using the following options:

1. -checksum
2. -sync -sync-level 3.

2.5. HPSS configuration files

The HPSS DSI needs to run on a system that has sufficient HPSS configuration files installed to permit it to talk to the appropriate HPSS servers (such as an HPSS mover node), as well as to perform authentication of users. These files typically are kept under /var/hpss/etc. It is recommended to install the HPSS DSI on an HPSS Client node since this will have the required configuration files

The HPSS user authentication files may be separate from the system's authentication files (i.e. in /var/hpss/etc/{group,passwd}), but can be set in /var/hpss/etc/env.conf to point to any suitable files. The DSI will also need to store credential files in the /var/hpss/cred directory.

2.6. Kerberos configuration

Kerberos must be configured for access to the proper Kerberos realm that contains HPSS. This file is usually kept in /etc/krb5.conf. You may need to enable the allow_weak_crypto option in the [libdefaults] section if the DSI module cannot talk to the HPSS servers.

Please note this will allow for weaker encryption types to be used, which may pose a security risk.

For details about the krb5.conf file visit:
https://web.mit.edu/Kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html

For the encryption types that are allowed visit:
https://web.mit.edu/Kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#encryption-types

Encryption types marked as "weak" will only be allowed when allow_weak_crypto is set to true.