11 Hibari Configuration Files

This chapter describes the configuration files for the Gemini Distributed Storage Server (GDSS), now called Hibari.

central.conf

Path `<GDS_HOME>/1.0.0/etc/central.conf`

Purpose Main GDSS configuration file.

Dynamic Reload You cannot dynamically reload this file. To activate changes that you make to the file, you must restart the GDSS.

The table that follows describes each parameter in the `central.conf` file. For background information about how to work with the `central.conf` file, see *page 295*.

central.conf Parameters (Part 1 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`application_home`			
GDSS top-level directory. File default = set during install (installer defaults to `/usr/local/gemini/gdss`)	STRING	see description	null

central.conf Parameters (Part 2 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`application_nodename`			
First part of the GDSS application node name. Each GDSS server is assigned a "node name". A node name identifies a specific Linux process on a specific physical machine. Different node names can be used to run multiple GDSS services on the same physical machine, if desired. An GDSS node name has three parts: 1) An application name local to the physical machine. 2) The "@" symbol. 3) The hostname of the physical machine, as shown by the output of the system command `uname -n`. If the hostname as shown by `uname -n` has one or more dots in it (for example `machine1.company.com`) then only the left-most part is used for the GDSS node name (from the example, `machine1`). A sample three-part GDSS node name is `gdss1@machine1`. The first part of the GDSS node name is determined by your `application_nodename` setting—in the sample, `gdss1`.	STRING	gdss1	null
`application_data_dir`			
Data directory for database. File default = set during install (installer defaults to `/usr/local/gemini/gdss/var/data`) IMPORTANT: Do not change the location of the data directory after installation.	STRING	see description	null

central.conf Parameters (Part 3 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`application_app_log_path`			
Path to the GDSS application log file, including file name. File default = <set during install>`/gdss-app.log` (installer defaults to `/usr/local/gemini/gdss/var/log` for the directory path portion)	STRING	see description	dev/null
`application_app_log_level`			
The lowest severity level of messages to include in the application log. Each message that the GDSS can generate has an assigned severity level appropriate to the message. You can use the `application_app_log_level` setting to filter GDSS logging so that only messages of your specified level and higher will be logged. Options are, from highest to lowest level: ◆ `ALERT` Messages indicating a condition requiring immediate correction. ◆ `WARNG` Warning messages indicating a potential problem. ◆ `INFO` Informational messages indicating normal activity. ◆ `DEBUG` Low level detail messages potentially of use when debugging the application. For example, with `application_app_log_level` set to `INFO`, the GDSS will log messages of all levels except `DEBUG`.	ATOM	INFO	INFO
`application_app_log_field_sep`			
Field separator of application log file. Enter either 124 (vertical bar in ASCII code) or 32 (space in ASCII code).	ATOM	124	124

central.conf Parameters (Part 4 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`application_stats_log_path`			
Path to the GDSS statistics log file, including file name. NOTE: The GDSS does not support statistics generation in the current release. Please ignore `application_stats_*` settings.	STRING	/dev/null	dev/null
`application_stats_log_interval`			
Not supported in current release.	TIME	60	NA
`cluster_timeout`			
Enter cluster timeout interval in seconds. WARNING: The `cluster_timeout` value must be larger than the `heartbeat_failure_interval` value, preferably by five (5) seconds or more. File default = <set during install> (installer defaults to 20 seconds for the timeout). Erlang nodes will force a disconnect from each other if this timeout value is exceeded. If there is a network partition (or other failure that will cause network traffic from a node to be dropped or delayed), client protocol operations will hang.	TIME	see description	see description
`vm_swappiness_value`			
Linux virtual memory "swappiness" correction. Should be 0 for all production environments. Red Hat EL4.4 default is 60. http://kerneltrap.org/node/3000 http://www.westnet.com/~gsmith/content/linux-pdflush.htm	see description	0	0
`cli_port`			
TCP port number for the command line interface.	INT	7597	7597

central.conf Parameters (Part 5 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`cli_hello`			
CLI hello message. Default = GDSS CLI Server	TEXT	see description	see description
`cli_prompt`			
CLI prompt.	TEXT	CLI>	CLI>
`brick_max_log_size_mb`			
In MB, the maximum size of any individual file in the transaction write-ahead log.	INT	100	100
`brick_check_checkpoint_max_mb`			
The number of MBs written since the last checkpoint. This is the threshold at which the new checkpoint operation will start. The value should be larger than a single checkpoint dump, which is directly related to the number of keys in the table and the length of each key (to avoid checkpointing every 30 seconds) and smaller than the maximum amount of time to wait for a brick to start, given that the hardware's disks are capable of N MBytes per second and the GDSS can only read some number of MBytes per second.	INT	3072	3072
`brick_check_checkpoint_throttle_bytes`			
It is possible to overwhelm disks with too much I/O checkpoint operations that will interfere with regular operations. This is the number of bytes per second that multiple software bricks executing checkpoints simultaneously will restrict themselves to.	INT	1048576	1000000

central.conf Parameters (Part 6 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`brick_sync_interval_msec` A loose upper bound on the interval between brick fsync requests for its main transaction log. WARNING: Do not set this value to be too small.	TIME	200	500
`brick_scavenger_start_time` The scavenger daily start time in hh:mm where hh is in hours greater than, or equal to zero and less than 23.	TIME	03:00	03:00
`brick_skip_live_percentage_greater_than` For the daily scavenger run, specify threshold for which data files with "live" data greater than this percentage will be ignored. A value of 0 will skip all files, 100 will skip no files.	0 to100	90	90
`brick_scavenger_throttle_bytes` Scavenger disk bandwidth throttle in bytes per seconds. File default = 600000000 Internal default = 600000000	INT	see description	see description
`brick_scavenger_temp_dir` The temporary directory used by the scavenger for data sorting. It is used by scavenger for temporary swapping. The work directory will be unconditionally removed by `rm -rf` at the start of the scavenger and then created. Any parent directories are not automatically created and therefore must exist. Up to tens of gigabytes of scratch space may be required. File default = `/tmp/gdss_scavenger`	STRING	see description	/tmp

central.conf Parameters (Part 7 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`brick_repair_max_bytes`			
The maximum number of value blob bytes per repair round. File default = 65000000 Internal default = 65000000	INT to INT_MAX	see description	see description
`brick_repair_max_primers`			
Maximum number of parallel repair primer processes.	INT > 0	7	7
`brick_mbox_high_water`			
High water mark for the number of messages queued for a brick's processing. To disable congestion control set this number to zero (0).	INT (0 to INT_MAX)	500	500
`brick_mbox_low_water`			
Low water mark for the number of messages queued for a brick's processing. To disable congestion control set this number to zero (0).	INT (0 to INT_MAX)	100	100
`brick_mbox_repair_high_water`			
High water mark for the number of messages queued for a brick's processing while under repair. Repair will be halted if this high water mark is reached. To disable congestion control set this number to zero (0).	INT (0 to INT_MAX)	1500	1500
`brick_mbox_repair_overload_resume_interval`			
After overload condition, the number (in seconds) to wait before attempting to resume a brick repair.	TIME	300	300

central.conf Parameters (Part 8 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`brick_dirty_buffer_wait`			
The maximum time an OS virtual memory dirty memory page will remain dirty (in seconds). Changes to this attribute or to `/proc/sys/vm/dirty_writeback_centisecs` or to `/proc/sys/vm/dirty_expire_centisecs` or to the XFS-specific VM settings must be coordinated. The default is 60 seconds which is two times the defaults for RedHat EL 4.x and 5.x kernels.	TIME	60	60
`brick_do_op_too_old_timeout`			
The timeout in milliseconds for a brick to consider a client's request "too old". Requests that are too old will be silently ignored.	TIME	3000	3000
`brick_preprocess_method`			
This parameter is commented out (disabled). Specifies the brick key preprocessing method. If this attribute is not present all bricks use the default table properties list that is recommended by Gemini Technical Support only. If `none`, all bricks use no preprocessors. If `ssf_only`, all bricks use SSF preprocessor only	ATOM	none	none
`brick_expiration_processor`			
This parameter is commented out (disabled). Specifies the brick key expiration method. If an attribute is not present, the default expiration method is the table properties list that is recommended by Gemini Technical Support only.	ATOM	[].	[].

central.conf Parameters (Part 9 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`brick_s3_conf_path` If brick_s3_conf_path option is not present, S3 listener will not run. NOTE: The definitive value of brick_s3_tcp_port is really in s3.conf brick_s3_tcp_port: pS3_TCP_PORT File default = <set during install>`/root/conf/s3.conf` (installer defaults to `/root/conf/s3.conf` for the directory path portion).	TEXT	see description	see description
`gdss_ebf_tcp_port` TCP port for the GDSS EBF protocol server. File default = <set during install> The installer defaults to `7580`.	TEXT	see description	see description
`gdss_ubf_server_tcp_port` TCP port for the GDSS UBF protocol server. File default = <set during install> The installer defaults to `7581`.	TEXT	see description	see description
`gdss_jsf_server_tcp_port` TCP port for the GDSS JSF protocol server. File default = <set during install> The installer defaults to `7582`.	TEXT	see description	see description
`gdss_json_rpc_tcp_port` TCP port for the GDSS JSON-RPC protocol server. File default = <set during install> The installer defaults to `7588`.	TEXT	see description	see description

central.conf Parameters (Part 10 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`brick_admin_http_tcp_port`			
NOTE: The definitive value of brick_admin_http_tcp_port is really in the admin.conf file. File default = <set during install> (installer defaults to `23080`.)	TEXT	see description	see description
`brick_admin_conf_path`			
If brick_admin_conf_path option is not present, admin HTTP listener will not run. File default = <set during install> (installer defaults to `etc/root/conf/admin.conf`	TEXT	see description	see description
`admin_server_distributed_nodes`			
Comma separated list of nodes eligible to run the Admin Server used by main application startup Tcl script. File default = <set during install> (installer defaults to `'gdss1@machineA', 'gdss1@machine-B-with-hyphens'`	TEXT	see description	see description

central.conf Parameters (Part 11 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`network_monitor_enable`			
Enable network partition monitoring. Options are: ◆ `true` Enable network partition monitoring. You can enable network monitoring only if you have set up two networks, A and B, that connect your GDSS nodes. Gemini recommends that A and B be physically separate networks. Network monitoring works by comparing heartbeats from network A and network B. ◆ `false` Disable network partition monitoring. IMPORTANT: For network partition monitoring to function properly, these `central.conf` settings must be assigned identical values on each GDSS node: ◆ `network_monitor_enable` ◆ `network_a_*` ◆ `network_b_*` ◆ `heartbeat_*`	ATOM	set during install (installer defaults to 'false')	false
`network_monitor_monitored_nodes`			
List of all GDSS nodes (without single quotes) that will be monitored. File default = <set during install> (installer defaults to `gdss1@node-a, gdss1@node-b`	TEXT	see description	see description
`network_a_address`			
IP address for the A network. This network *must* be the same network used by the Erlang network distribution protocol (i.e. the network used for Mnesia replication traffic). File default = set during install (installer defaults to `10.1.1.12`)	STRING	see description	null

central.conf Parameters (Part 12 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`network_a_broadcast_address` IP broadcast address for the A network. This network *must* be the same network used by the Erlang network distribution protocol (i.e. the network used for Mnesia replication traffic). File default = set during install (installer defaults to `10.1.1.255`)	STRING	see description	null
`network_a_tiebreaker` IP address for the A network to act as a tiebreaker. If the network monitoring application determines that the A network is partitioned and the B network is not partitioned, then if `network_a_tiebreaker` responds to an ICMP echo (a ping), then the local GDSS node is on the "correct" side of the partition. If the local GDSS node is not on the correct side of the partition (if the attempt to ping the tiebreaker address fails), then it shuts down immediately. The `network_a_tiebreaker` address must be extremely reliable and must be as close to the local GDSS node as possible (from a network Layer 1 and 2 point of view) as well as close to all other GDSS nodes. Ideally the tiebreaker should be the address of the Layer 2 switch or Layer 3 router that all Mnesia communications flow through. File default = set during install (installer defaults to `10.1.1.254`)	STRING	see description	null
`network_b_address` IP address for the B network. This network should be physically separate from the A network. File default = set during install (installer defaults to `10.10.10.12`)	STRING	see description	null

central.conf Parameters (Part 13 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`network_b_broadcast_address`			
IP broadcast address for the B network. This network should be physically separate from the A network. File default = set during install (installer defaults to `10.10.10.255`)	STRING	see description	null
`heartbeat_beacon_interval`			
Heartbeat beacon interval in milliseconds. At this interval, UDP heartbeart signals are transmitted from the local GDSS node to each other GDSS node in the cluster. The heartbeats are sent out both through network A and through network B. Gemini recommends that this interval be between 250 and 1000 (milliseconds).	INT	1000	1000
`heartbeat_warning_interval`			
Heartbeat alarm interval in seconds. If this interval passes without the local GDSS node receiving a heartbeat signal from a peer GDSS node, an alert is written to the local application log.	INT	set during install (installer defaults to 5)	5

central.conf Parameters (Part 14 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`heartbeat_failure_interval` Heartbeat failure interval in seconds. A serious error has occurred if during this interval a heartbeat from a peer GDSS node has been detected on network B but no heartbeat from that node has been detected on network A. The `network_a_tiebreaker` (*page 391*) address will be pinged to determine whether or not the local GDSS node should be shut down to avoid database damage. NOTE: The value of `heartbeat_failure_interval` should be larger than the value of `heartbeat_warning_interval` by a factor of at least 1.5x but preferably 2x or more. Cluster timeout interval. Erlang nodes will force a disconnect from each other if this timeout value is exceeded. If there is a network partition (or other failure that will cause network traffic from a node to be dropped or delayed). Operations will hang. WARNING: The `cluster_timeout` value must be larger than the `heartbeat_failure_interval` value, preferably by 5 seconds or more.	INT	set during install (installer defaults to 15)	15
`heartbeat_status_udp_port` UDP port for heartbeat listener	INT	63099	63099
`heartbeat_status_xmit_udp_port` UDP port for heartbeat transmitter (base port, actual port may be higher)	INT	63100	63100
`ticket_server_tcp_port` Port on which the GDSS listens for requests to its internal ticket broker. In the current release, this listener is not used.	INT	set during install (installer defaults to 2298)	2299

central.conf Parameters (Part 15 of 15)

Parameter Description	Valid Range	File Default	Internal Default
`ticket_server_distributed_nodes`			
List of all GDSS nodes running the distributed ticket server. This node list is required for GDSS start-up. The node list must be identically configured on each of your GDSS nodes. If you are using only one GDSS node, specify just the one node's name for this setting. NOTE: If a node name includes a hyphen, then you must surround the node name with single quotes. For example: `'GDSS1@tc-gt22-6'`	STRING	set during install	null
`ticket_maker_reset_timeout`			
This setting works together with the congestion monitoring controls that you establish in the `congestion_watcher.conf` file (*page 313*). When you start or restart the GDSS, or when you dynamically reload the `congestion_watcher.conf` file, the ticket broker will wait for `ticket_maker_reset_timeout` seconds before issuing any messaging tickets. This pause allows time for the congestion monitor to send restriction requests to the ticket broker, if congestion has been detected.	INT	6	6
`gms_imapd_conf`			
For internal use—do not modify.	STRING	/dev/null	/dev/null