HPSS Logging

Syslogging and I/O Logging

Disclaimer

- Forward looking information including schedules and future software reflect current planning that may change and should not be taken as commitments by IBM or the other members of the HPSS collaboration.

Changes with CR 375 (Syslog-based logging)

- Simplified log policy administration
  - Log policy changes are now automatically picked up
  - All servers now use a defined log policy, any changes go through that log policy
- Syslog = logging flexibility
  - Allows for things like fine-grained filtering, redirection, message deduplication, remote logging, etc.
- Improved HPSS log message format
  - We've reorganized the log format to be more human readable
  - Microsecond resolution is now possible
  - Format is still highly parseable
- SSM reads a syslog file to find Alarms and Events
  - Syslog is the single source of truth

Changes with CR 375 (Syslog-based logging)

- Movers can now easily log both to a local system and the central HPSS log
- Simpler, powerful log archiving with logrotate
  - Criteria-based log rotation (day, file size, etc)
  - Control the rotation policy
  - Scriptable interface to control log rotation and archive
  - Log compression
- New tool for archiving into HPSS
  - Command line tool
  - Control the base directory, file family, and COS of the archived log file
  - Logs success and failure via syslog

Logging – A History

- HPSS predates most standard logging protocols and libraries
- HPSS 6.2 – Binary only log files
  - hpss_delog
- HPSS 7.1 – Wrapping text log files
  - Find the beginning?
- HPSS 7.3 – Rotating text log files
  - Current Situation
- Next
  - Syslog!

Logging – A History

- What does logging in HPSS mean?
  - Log Policy Configuration (SSM)
  - Server logging (HPSS Log Client)
  - Infrastructure logging (HPSS Log Client)
  - Alarms and Events for SSM (HPSS Log Client)
  - Remote logging to central log file (HPSS Log Client)
  - Centralized log file (HPSS Log Daemon)
  - Log rotation (HPSS Log Daemon)
  - Log archiving (HPSS Log Daemon)

CR 375 – Use syslog for HPSS logging

- Switching to Syslog
- Why?
  - User driven
    - Filtering
    - Formatting
    - Configurability
    - Reduce duplication
    - → Users want more control over logging
  - Syslog provides a robust and high performance logging platform
    - Standard on systems, common admin skill
    - Proven and well supported
  - Simplify deployment
    - Two servers (log client, log daemon) were removed

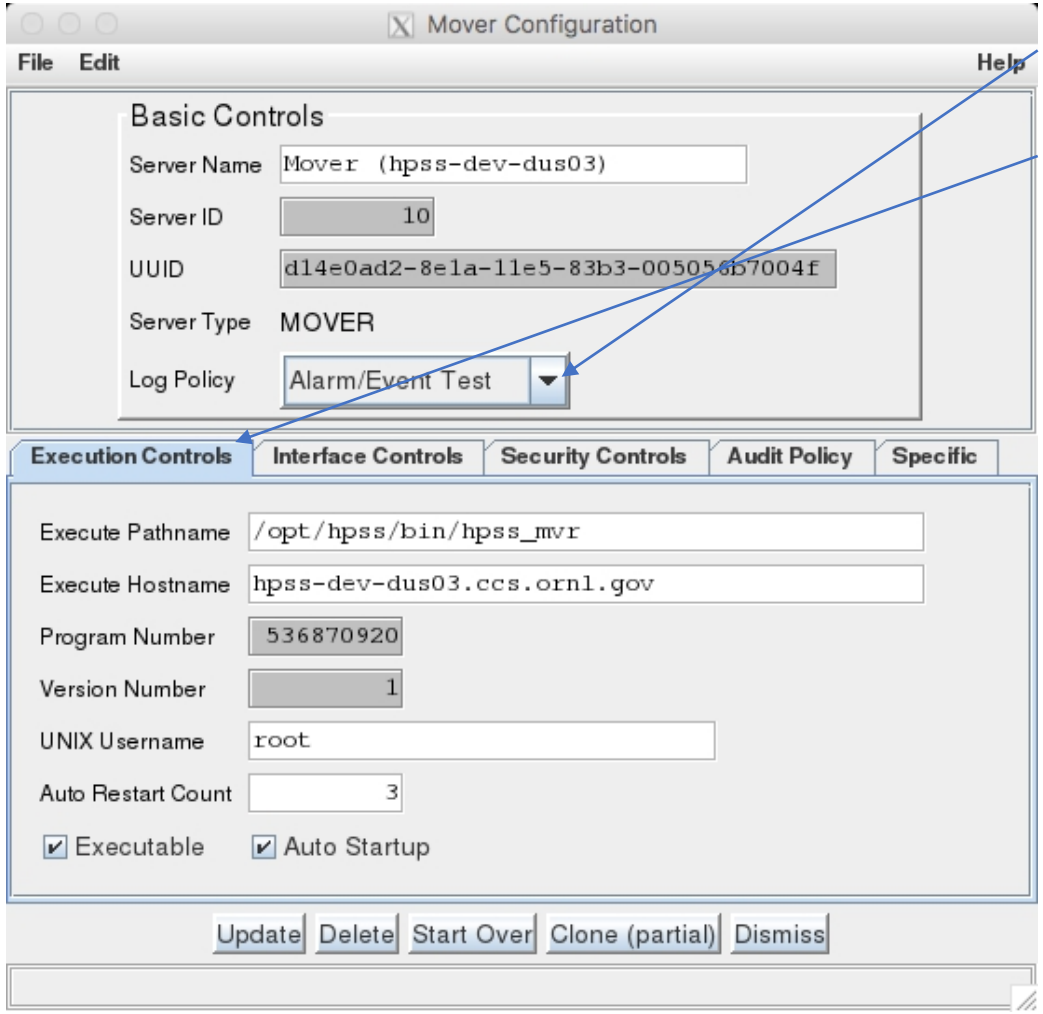
CR 375 – Use syslog for HPSS logging

- What changed?
  - Log Policy Configuration (SSM)
  - Server logging now goes directly to Syslog
  - Infrastructure logging now goes directly to Syslog
  - Alarms and Events for SSM is now read from a Syslog file
  - Remote logging is now done directly to Syslog using a remote Syslog server
  - Centralized log file – messages now all come together via Syslog
  - Log rotation is now accomplished using the logrotate system tool
  - Log archiving is now accomplished using logrotate and a new hpss_log_archive tool
- What's not changing
  - Most log message content
  - HPSS message types / severities

CR 375 – Log Policies

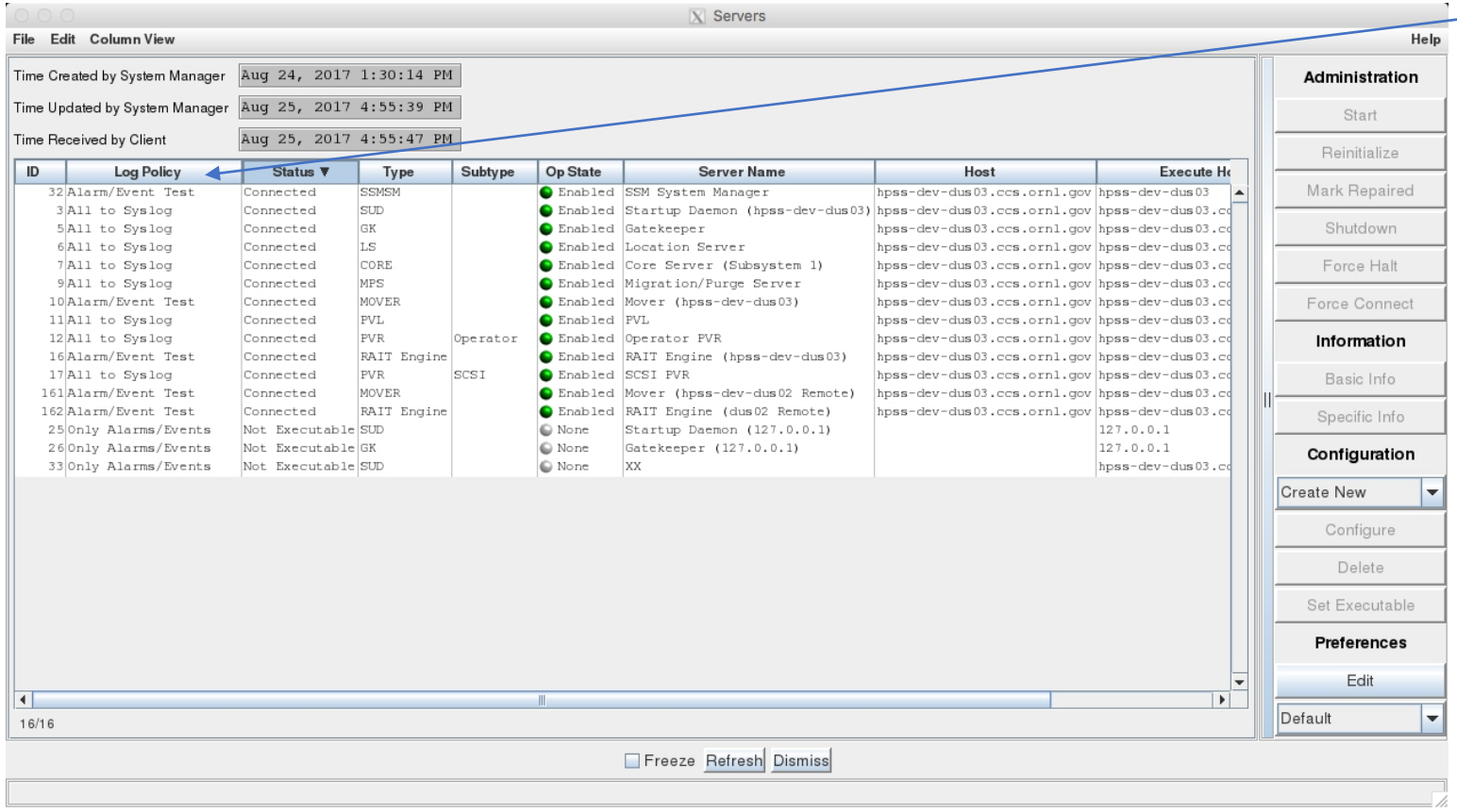
- Log types are the same (Alarm, Event, etc.)
- Servers must be assigned a log policy
  - Promotes sharing log policies among common server types
  - Default Log Policy removed from Global Config
- Removed the option to disable logging to SSM
  - Syslog should control that level of filtering
- Log policies are now re-read *automatically*
  - Server reinitialization is not required
- Question – Why not drop log policies and rely solely on syslog for filtering message types?
  - You could, but…
  - Sending all of the messages to syslog for filtering puts an additional load on the system to generate the actual message text

CR 375 – Log Policies



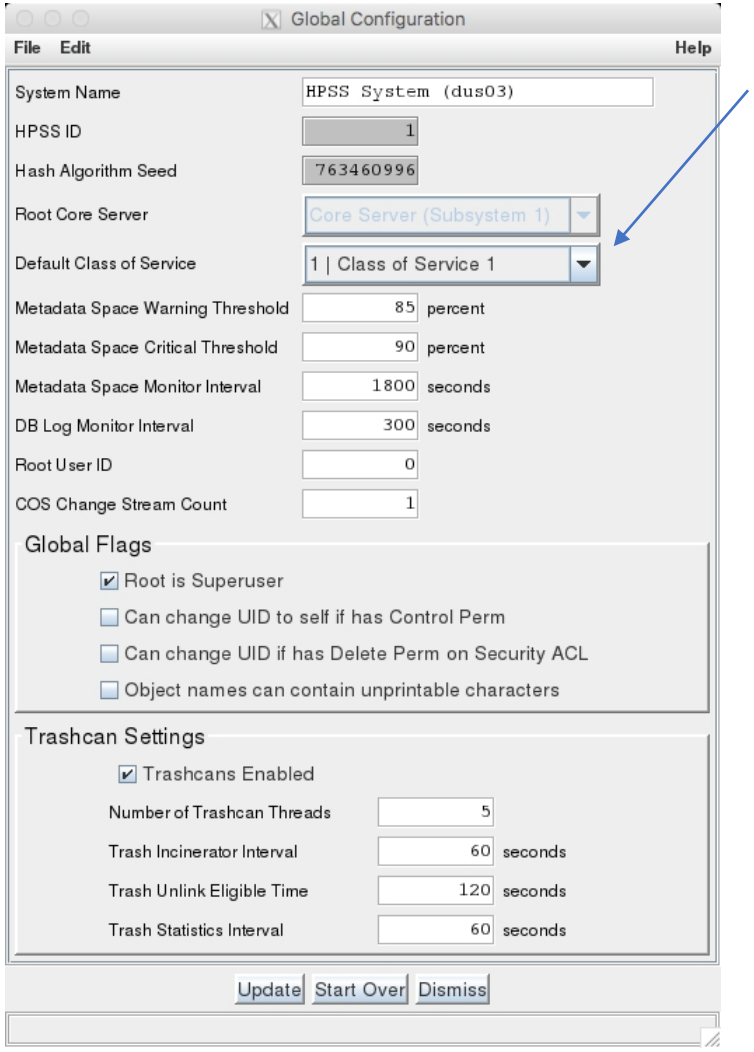
- Log policy for the server is selected from the server configuration window
- Log tab has been removed

CR 375 – Log Policies



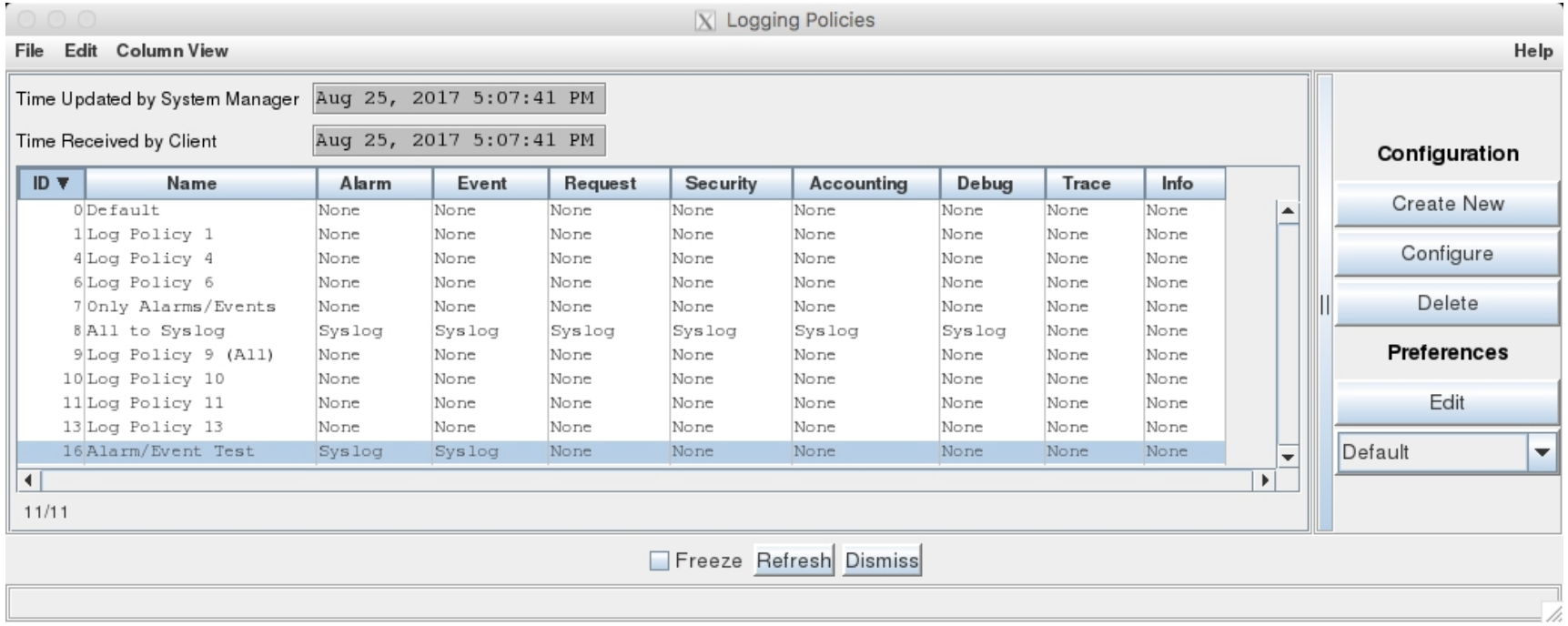
- Log policy is visible on the Server screen
- No more Log Client / Log Daemon

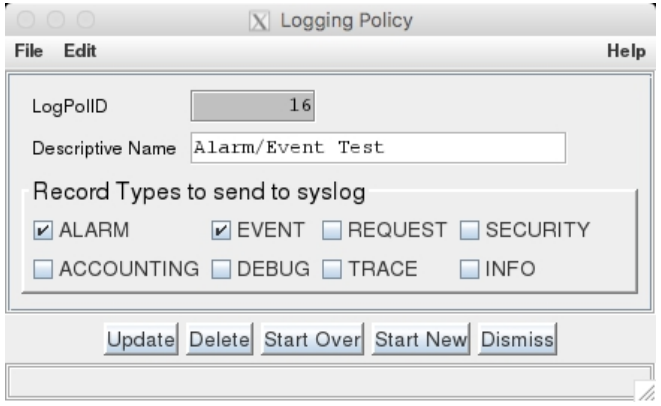
CR 375 – Log Policies



- Default Log Policy has been removed

CR 375 – Log Policies





- Log Policy summary window shows a summary of each policy
- Configuration window allows the name and record types to be modified

CR 375 – Log Format

- Goals:
  - Balance readability and parseability
  - Remove unused information
  - Organize information logically
- In the syslog files, the message format looks like:

  Aug 7 16:24:13.895249 hpss_rait_engine_tcp(HPSS)[21596]::ALARM/MINOR # RAIT Engine (mystic)@mystic.clearlake.ibm.com # RemoteInterfaceSync # -5000 # RAIT1009 # 12345 -- Failed to sync with remote process

CR 375 – Log Format Dissected

Aug 7 16:24:13.895249 hpss_rait_engine_tcp(HPSS)[21596]::ALARM/MINOR # RAIT Engine (mystic)@mystic.clearlake.ibm.com # RemoteInterfaceSync # -5000 # RAIT1009 # 12345 -- Failed to sync with remote process

- High resolution timestamp: Aug 7 16:24:13.895249
- Process name: hpss_rait_engine_tcp
  - Processes that use the HPSS logging library will append (HPSS) to facilitate filtering
- Process ID: [21596]
- Log type and severity: ALARM/MINOR
- Server descriptive name and node name:
  RAIT Engine (mystic)@mystic.clearlake.ibm.com

CR 375 – Log Format Dissected (Continued)

Aug 7 16:24:13.895249 hpss_rait_engine_tcp(HPSS)[21596]::ALARM/MINOR # RAIT Engine (mystic)@mystic.clearlake.ibm.com # RemoteInterfaceSync # -5000 # RAIT1009 # 12345 -- Failed to sync with remote process

- Function logging the error: RemoteInterfaceSync
- Error Code: -5000
- Message type and number: RAIT1009
- Request ID: 12345
- Formatted message text: Failed to sync with remote process

CR 375 – Server and Infra Logging

- Server and Infrastructure logging first apply the Log Policy
- They are then sent to Syslog
  - Syslog then formats the header and directs the output to the correct log file
  - Header must stay consistent
  - Sites can configure syslog behavior for HPSS logs (rsyslog, syslog-ng)
- Our default/recommended configuration:
  - HPSS Alarms and Events go to /var/log/messages
  - All HPSS log messages go to /var/hpss/log/HPSS.log on the core server system
  - We will provide templates for the recommended configuration
- Admins may tweak their syslog configuration to reflect logs to other sources and do some filtering
- There **must** be a log file where HPSS logs are collected without filtering

CR 375 – Syslog Example

Aug 28 11:34:02.540997 hpss_core(HPSS)[28521]:: DEBUG # Core Server (Subsystem 1)@hpss-dev-dus03.ccs.ornl.gov # ss_WriteDisk:Client IOD (line 266) # 0 # CORE0000 # 2069430284 -- Request ID = 2069430284#012 Function = WRITE#012 Flags = NONE#012 SrcDescLength = 1#012 SinkDescLength = 1#012#011SRC:[0] Flags = XFER_OPT_IP #012#011SRC:[0] Offset = 0#012#011SRC:[0] Length = 478211#012#011SRC:[0] Shared Device Info = 0x0#012#011SRC:[0] Addr type = NET:#012#011SRC:[0] NET: Transfer ID = 0x000000007b59000c#012#011SRC:[0] NET: SockAddr.addr = 172.30.60.22#012#011SRC:[0] NET: SockAddr.port = 44287#012#011SRC:[0] NET: Offset = 0#012#011SRC:[0] Server defined = 0x0000000000000000#012#011SINK:[0] Flags = NONE#012#011SINK:[0] Offset = 0#012#011SINK:[0] Length = 478211#012#011SINK:[0] Shared Device Info = 0x0#012#011SINK:[0] Addr type = SSEG:#012#011SINK:[0] SSEG: SOID = 00000001-05-00000007-01e78c0651a216d4-1056#012#011SINK:[0] SSEG: Hash = 1856#012#011SINK:[0] SSEG: Offset = 0#012#011SINK:[0] Server defined = 0x00007f729009ebe0

Aug 28 11:35:44.405420 hpss_mps(HPSS)[28522]:: EVENT # Migration/Purge Server@hpss-dev-dus03.ccs.ornl.gov # mps_TapeFileMigr (line 3925) # 0 # MPSR0148 # 0 -- Tape file migration start (SClassID 2, SubSysID 1).

Aug 28 11:34:02.545293 hpss_core(HPSS)[28521]:: DEBUG # Core Server (Subsystem 1)@hpss-dev-dus03.ccs.ornl.gov # ss_WriteDisk:Client IOR (line 628) # 0 # CORE0000 # 2069430284 -- Request ID = 2069430284#012 Flags = COMPLETE #012 Status = 0#012 SrcReplyLength = 1#012 SinkReplyLength = 1#012#011SRC:[0] Flags = COMPLETE #012#011SRC:[0] Status = 0#012#011SRC:[0] Bytes moved = 478211#012#011SRC:[0] Shared Device Info = 0x0#012#011SRC:[0] POSITION: Flags = 0#012#011SRC:[0] POSITION: Granularity = 0#012#011SRC:[0] POSITION: RELATIVE: Section = 0#012#011SRC:[0] POSITION: RELATIVE: Offset = 0#012#011SRC:[0] POSITION: Absolute = 0x00000000 (INVALID)#012#011SRC:[0] POSITION: SSEG: RELATIVE: Section = 0#012#011SRC:[0] POSITION: SSEG: RELATIVE: Offset = 0#012#011SRC:[0] POSITION: SSEG: Absolute = 0x00000000 (INVALID)#012#011SINK:[0] Flags = COMPLETE #012#011SINK:[0] Status = 0#012#011SINK:[0] Bytes moved = 478211#012#011SINK:[0] Shared Device Info = 0x0#012#011SINK:[0] POSITION: Flags = 0#012#011SINK:[0] POSITION: Granularity = 0#012#011SINK:[0] POSITION: RELATIVE: Section = 0#012#011SINK:[0] POSITION: RELATIVE: Offset = 0#012#011SINK:[0] POSITION: Absolute = 0x00000000 (INVALID)#012#011SINK:[0] POSITION: SSEG: RELATIVE: Section = 0#012#011SINK:[0] POSITION: SSEG: RELATIVE: Offset = 0#012#011SINK:[0] POSITION: SSEG: Absolute = 0x00000000 (INVALID)

Aug 28 11:35:44.419018 hpss_mps(HPSS)[28522]:: EVENT # Migration/Purge Server@hpss-dev-dus03.ccs.ornl.gov # mps_TapeFileMigr (line 4660) # 0 # MPSR0149 # 0 -- Tape file migration end (SClassID 2, SubSysID 1, Files 0, Bytes 0, Volumes 0, Active 1, Down 0, Errors 0).

Aug 28 11:38:53.366523 hpssd(HPSS)[28181]:: ALARM/CRITICAL # Startup Daemon (hpss-dev-dus03)@hpss-dev-dus03.ccs.ornl.gov # vigilRoutine # 0 # SUDD0006 # 0 -- Server Gatekeeper died on host hpss-dev-dus03.ccs.ornl.gov, pid = 28519, exit status = 0

Aug 28 11:40:06.213710 hpss_pvl(HPSS)[28524]:: ALARM/MAJOR # PVL@hpss-dev-dus03.ccs.ornl.gov # openSocket (file pvl_mvr.c, line 901) # 111 # PVLS0004 # 0 -- Returned, function = "hpss_net_connect", arg = "hpss-dev-dus03.ccs.ornl.gov" (Connection refused)

Aug 28 11:44:11.720172 hpss_pvr_scsi(HPSS)[28527]:: ALARM/CLEARED # SCSI PVR@hpss-dev-dus03.ccs.ornl.gov # sendNotification (file pvr_notify.c, line 970) # 0 # PVRS0274 # 0 -- PVR reestablished connection to SSM

Aug 28 11:44:45.835344 hpss_pvl(HPSS)[28524]:: ACCOUNTING # PVL@hpss-dev-dus03.ccs.ornl.gov # dismount_drive (file pvl_pvr.c, line 1587) # 0 # PVLS0094 # 0 -- Dismounting Deferred Volume, jobid = "165", drive = "34", arg = "A0001600”

Aug 28 11:44:46.674348 hpss_pvl(HPSS)[28524]:: ACCOUNTING # PVL@hpss-dev-dus03.ccs.ornl.gov # dismount_drive (file pvl_pvr.c, line 1631) # 0 # PVLS0003 # 0 -- Calling, function = "pvr_DismountCart", jobid = "165", drive = "34", arg = "A00016“

Aug 28 11:44:47.089125 hpss_pvl(HPSS)[28524]:: ACCOUNTING # PVL@hpss-dev-dus03.ccs.ornl.gov # dismount_drive (file pvl_pvr.c, line 1642) # 0 # PVLS0004 # 0 -- Returned, function = "pvr_DismountCart", jobid = "165", drive = "34", arg = "A00016“

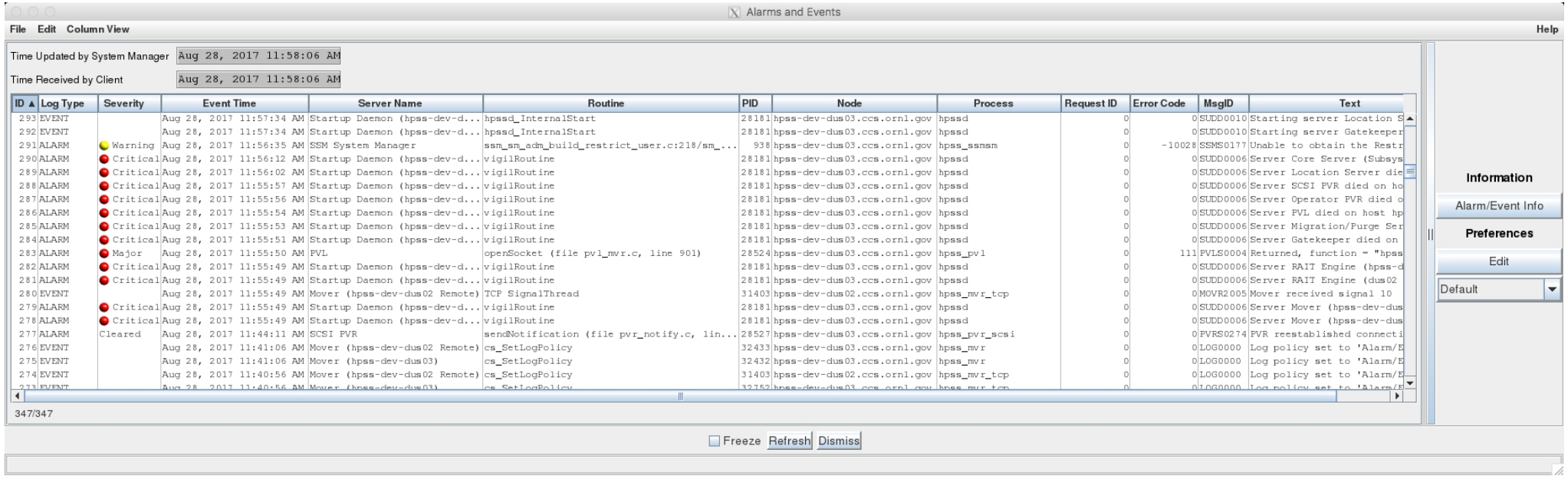
Aug 28 11:44:47.157332 hpss_pvl(HPSS)[28524]:: TRACE # PVL@hpss-dev-dus03.ccs.ornl.gov # reallocate_drive (file pvl_mount.c, line 2821) # 0 # PVLS0132 # 0 -- PVL DEBUG: (++) DriveType= Titanium 10000B, PoolID= 0, Num= 16,Avail = 16, PVR SCSI PVR

CR 375 – SSM reads a syslog file to find Alarms and Events

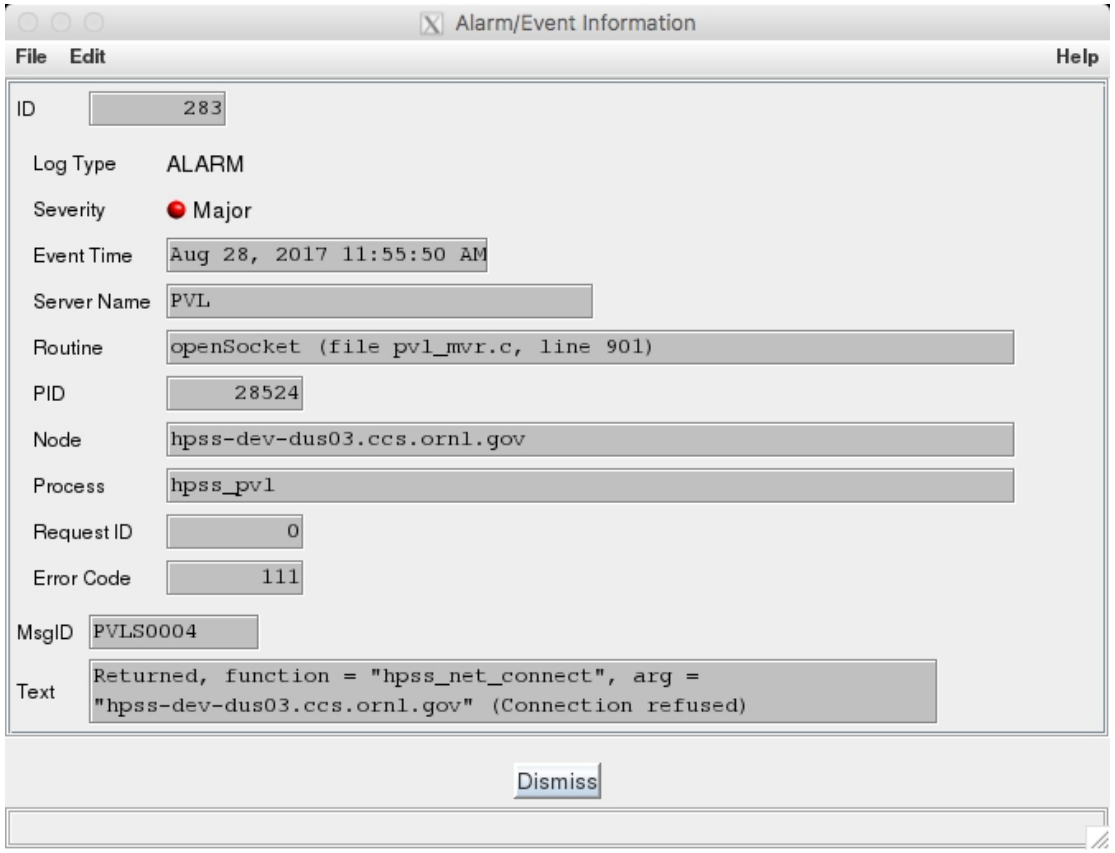
- Previously, the Log Client would send log messages to SSM
  - No more Log Client
- SSM will now read a syslog file for HPSS-formatted log messages, and display those in A&E
  - Rather than servers pushing messages to SSM, SSM is pulling from syslog
  - This means that syslog filters will affect SSM
- The file to be read can be controlled via the HPSS_SSM_ALARMS environment variable
  - Default: /var/hpss/log/HPSS.log
  - This is important because if this is not properly configured, A&E will be empty

CR 375 – SSM Alarms and Events

- Available information is generally the same as before
- Process name is now included
- Object Class field has been removed



CR 375 – SSM Alarms and Events



- Information is generally the same
- Dropped Object Class
- Client ID is now the process name

CR 375 – Remote Logging

- Previously, remote processes like Mover and RAIT Engine would send logs back to the core machine Log Client
  - Running other servers remotely required a Log Client
- Remote processes can log directly to syslog
  - The Core Server syslog will need to be configured to accept incoming syslog connections
  - The remote system syslog will need to be configured to forward the messages
  - Remote processes can also apply local filtering and log locally if desired
  - We will provide a template for remote logging

CR 375 – Logrotate

- Logrotate is a standard Linux tool for rotating, compressing, and archiving log files
  - man logrotate(8)
- When run, logrotate checks the configured log files for meeting some criteria
  - Can be automatically run at a specific time interval using cron(8)
  - May have a specific configuration per log file
  - Multiple log files may be configured
- Options include
  - How many log files to keep before deleting
  - How often to run / what file size to trigger
  - Compression
  - Custom tasks during rotation (archiving)

CR 375 – Log Archive Tool

- Previously done by the Log Daemon
- Assumes logrotate is being used and archives the most recently rotated file
  - e.g. logfile.1
- Options
  - Change the base log path (default /log)
  - Specify the COS
  - Specify the File Family
  - Log status via syslog

CR 320 – I/O Logging

- Provide more information about how data is moving through the system
  - Reads, writes, stages, migrations
- Identify files written to a particular volume (disk and tape)
- Identify drives used for file I/O
- Additional information for mount/dismount/deferred dismount
- Identify when file I/O operations began and completed
- Logging to new INFO type