ID: 1211261522992

lsiget log bundle analysis information

Solution

Yes you can analyze the logs that are generated by lsiget.

Before you begin troubleshooting, backup the data.
RAID is not a data backup solution.

If you suspect the controller is malfunctioning, you should save your RAID configuration as well with storcli, see Save RAID Configuration below.

Windows, Linux and VMware quick links (You may need an ftp client if you are unable to save the file):
Windows: lsigetwin_latest.zip / 7z lsigetwin_latest.7z
Linux: lsigetwin_latest.7z
VMware: lsigetvmware_20170228.tgz

For other OS, See the main BCMget/lsiget KB:
•Broadcom LSIget Capture Knowledge Base link:https://www.broadcom.com/support/knowledgebase/1211161499563/lsiget-data-capture-script

Once you have lsiget downloaded, copy the files from the sub directory (if applicable) and place the files in an easily accessed directory from a command prompt such as /lsi or in Windows, C:\lsi

You must run as root or sudu for linux lsigetlunix.sh and may also need chmod 777 *.*
In Windows, an elevated admin command prompt must be run for lsigetwin.bat or the storcli binary will not run. "Elevated" means that you must find cmd.exe, right click the app and choose Run as Administrator.

Before running lsiget for Linux, it is recommended that you install SmartmMon tools and have it running for at least 24 hours before running the script.

LSIget will capture SMARTCTL logs as well but only for MegaRAID.
SMARTCTL must be run manually for HBA's.

After running lsigetwin.bat or lsigetlunix.sh to completion, you should have a .tgz or .7z file with the filename of your OS, host name, and today's date.
There is a password for lsiget for Windows but not Linux: broadcom

Decompress the file and you will see the following directory structure:

Windows directory structure for lsiget:
Controller_Disk_Association
LSI_Products
lspci
script_workspace
System_Logs
System_Reg_Keys
msinfo32_report.txt
Summary.txt

Linux directory structure for lsiget:
etc
LSI_Products
lspci
lvm
proc
script_workspace
  si_host
var_log

Most often, you can find out what is wrong by going directly to the LSI_Products\MegaRAID\storcli\Controller_C0.txt file.

This is where the main portion of information is saved for your MegaRAID controller.
These are the key points that should be checked:

VD status – Make sure that you know if the array is offline, degraded, or optimal.
Parse Controller_C0.txt file for “VD LIST :”.

ROC chip temperature – A controller that is overheating can cause a variety of issues.
Parse Controller_C0.txt file for “ROC temperature”.
*Note: only SAS2208 and newer chipsets have a built in thermistor.
All MegaRAID and HBA controllers should be 55-60*C. Maintain 200 linear feet per minute airflow across the heat sink or 17.5-18 CFM direct air pressure which is the equivalent of a 40 mm fan running at 3000 RPM.
Controllers that have inadequate airflow can overheat even when idle which can cause drives to drop and fatal firmware errors which could lead to data corruption or loss of data.
If your system fans are not adjustable, consider a PCIe slot fan which are about $10.00 online.
Overtemp is one of the leading causes of controller failure and can significantly reduce the Mean Time To Failure calculation.

Firmware version – Error handling is always being improved and is recommended to update.
Parse Controller_C0.txt file for “FW Version”.
Note – Any time you make a change to your system such as a firmware update, always backup the data.
Firmware for legacy controllers can be downloaded from the Legacy products group.
See www.broadcom.com/support/knowledgebase/1211196413437/downloads-for-all-legacy-os-and-storage-controllers

SMART errors – Checking to see if any SMART errors are present often decreases troubleshooting time.
For Linux, you should make sure that SMARTMON tools are installed at least 24 hours before running the lsiget script. The SMART logs are only collected for MegaRAID controllers and are saved in the LSI_Products\MegaRAID\SMARTCTL\ directory.
HBA’s must be ran manually. See SMARTMON man page for command instructions.
For Windows, HD Sentinel should be installed which will give results on all drives attached to the MegaRAID or HBA controller in about 10 minutes.

Phy Error Counters – You can use phy error counters to find out if the controller is at fault, or the drives.
Parse Controller_C0.txt file for “phyerrorcounters”
If no SMART errors were detected, check to see if there are phy errors. Often phy errors can be caused by a loose cable or a bad connection through the hot swap backplane.
When reseating cables and drive connections, make sure that the server is shut down to avoid degrading or off lining the array.

Serial number – Your controller can be checked for warranty and to verify that it is a valid channel product. If the controller was purchased online through a third party seller such as Amazon or Newegg marketplace, your controller could be used or OEM.
See Counterfeit & Gray Market Awareness Statement:
https://www.broadcom.com/support/counterfeit-statement

You may request a serial number check by filling out an online support form:
For MegaRAID controllers:
https://www.broadcom.com/support/request-tech-support?fct=Support&pf=RAID+Controller+Cards
For HBA's:
https://www.broadcom.com/support/request-tech-support?fct=Support&pf=SAS/SATA/NVMe+Host+Bus+Adapters

Event log – Build a timeline of when the failure occurred to help isolate the root cause.
lsiget sorts the errors into 4 groups; Information, Warning, Critical and Fatal.
These logs can be found in the LSI_Products\MegaRAID\Event_Logs\ directory.
Events are captured old to new ascending.
Some versions of lsiget will not capture"Event_Logs" and are also generated in the LSI_Products\MegaRAID\storcli\Cx_show_alilog_C0.txt file
You can also generate your own which is particularly helpfull if you are troubleshooting a cable, drive or backplane issue.
storcli /c0 show events > events.txt

Key drive failure events to look for are:

Unexpected sense
Unexpected sense messages means that the drive or controller firmware received a SCSI command that was unexpected and are vague unless ou have the decode table which can be found online.
See https://en.wikipedia.org/wiki/Key_Code_Qualifier.
In the following error, 3/11/00 is the SCSI sense error that is reoccurring on slot 6
Unexpected sense: PD 0e(e0x18/s6) Path 5001b4d511ec8026, CDB: 88 00 00 00 00 01 55 3f ca a0 00 00 01 60 00 00, Sense: 3/11/00

Top

Uncorrectable medium error

Uncorrectable medium errors are the effect of rebuild failures as shown below and is generally accompanied by the above SCSI sense error.
Beyond performing a risky cloning procedure, it is best to backup the data and replace the bad drives and create a new VD, then restore from backup.

Rebuild failed on PDx (xxx) due to target drive error

This error indicates that there are source drive errors on the remaining drives in the array.
Once source drive errors develop due to the lack of scheduled Consistency checks or Patrol reads, it is very difficult to fix. Sometimes the error is fixed by the drive's firmware and a consecutive rebuild will be successful.
If a second or third rebuild fails, it is unlikely that the source drive errors will be corrected and it is recommended to backup the data, replace the bad drives, create a new VD and restore the data.

POR or reset

"Power on reset" or reset events are referring to the drives, not the controller which can occur in the following conditions:
1. Not enough power is being supplied to the drives.
   - Loose power connectors or a defective power regulator on the backplane.
2. Fatal drive error that was not able to be corrected by the drive firmware.
   - Check SMART logs or HD sentinel and if there are no SMART errors, make sure that your drive and controller firmware are up to date.
3. Bad slot on the card.
   - Check for increase phy errors in "phyerrorcounters" found in Controller_C0.txt file.
4. Bad power supply.

Over time, power supplies lose efficiency and may not be able to sustain the proper current and voltages needed for the number of drives / devices in the system.
   - Hard drives generally reset at random on all slots which is a very good indicator that the power supply is failing.

Each drive takes about 35 watts at spin-up and 15 to 20 after initialization. Calculate accordingly. Power supply calculators can be found online.

Predictive failure

Review SMARTCTL logs or run HD Sentinel.
*Note: errors such as POR or resets may trigger false predictive warnings. SMARTMON or HD Sentinel are generally more reliable than MegaRAID Storage Manager.

Diagnostics failed

Every 24 hours, the controller firmware will run a generic self test for all drives connected to a MegaRAID controller (not HBA). These errors are usually accurate and a good indicator that the drive needs to be replaced.

When looking for the slot that the drive is in, you will see a similar error string:
Unexpected sense: PD 17(e0x10/s16)
Where PD is the device ID, e0x10 is the SAS expander ID and /s16 would be the slot.
These strings may or may not have a SAS expander and look slightly different but as a general rule, the trialing number is the slot on the controller (or backplane).
Your backplane may support the Start/Stop locate function in MegaRAID Storage Manager or storcli.
If not, you may need to trace the drive out by SN.
A list of serial numbers can be cross referenced in the LSI_Products\MegaRAID\storcli\ Cx_Eall_Sall_show_all-Compare-All-Parms_C0.txt file.
*Note: lot numbers are not listed but are in order starting from the first drive that is de3tected.
Slots will correspond to the "TOPOLOGY :" list in Controller_C0.txt file.
In the event where a drive does not show up, perform a reverse lookup and find the drive that is not listed.

Key controller events are:

Fatal firmware error

*Note: it is normal to see 2 or more fatal firmware errors at the top of the log file.
These were produced by manufacturing QA testing before the controller was shipped and can be ignored:
https://www.broadcom.com/support/knowledgebase/1211224285394/fatal-firmware-error

Repetitive fatal firmware errors can be an indication that the controller has an internal hardware failure. Another possibility is that a VD went offline so it is not always an indication of a bad controller.
Troubleshooting a suspected bad controller:
- Remove the BBU or CacheVault. Failing BBU or CV units may cause fatal errors making it to appear that the controller is failing
- Try all PCIe slots.
- Set the PCIe bus to gen 2 x4 if the motherboard BIOS will allow it.

Top

Controller cache discarded due to memory/battery problems

This error can be either a bad BBU or CacheVault, or bad memory on the controller.
If the BBU / CV unit has been removed and the error is still occurring, it is not recommended to troubleshoot because bad memory can lead to data corruption. It is always recommended to replace the controller as soon as possible and ideally, shut down the server until a replacement controller arrives. Forcing the controller to operate could corrupt the array configuration data and getting the data back after the controller has been replaced is very difficult and becomes exponential as the number of drives increases.
Always save your RAID configuration to a file with storcli. See "Save RAID Configuration" below

Multi-bit or Single bit errors.

Generally this error means the memory on the board is starting to fail and as above, you should prepare for a complete failure of the controller.
But this has been known to occur due to a timing issue between the card and the PCIe bus.
Make sure that you have flashed the controller firmware to the latest. See firmware above.
You may also have the controller plugged into an x16 slot and the ECC could be failing because the card cannot clock correctly.
Try putting the controller in a gen 2 x4 slot and turn off Quick or rapid boot in te motherboard BIOS.

Controller temperature exceeded

- Shut down the server as soon as possible. This error means that the temperature is above 104* Celsius. Refer to “ROC chip temperature” above.

Precautions when working with RAID in a production server:

Migration or expansion:

Migrating to a different RAID level or expanding the capacity online is a complex operation and can take days, maybe even weeks depending on the drive size and the server IO traffic.
During Migration and or expansion, the controller cache and disk cache will be disabled.
There is no way to override disk or controller cache once migration starts.

If at all possible, it is recommended to backup the data, add new drive and recreate the array.
If you have no choice;
Never start a migration if:
- The data is not backed up.
- The server environment requires moderate to high performance with low latency.
- The drives are old and not in peak condition.
- The controller has had issues or the OS is unstable.

If there is a double fault during a migration and the firmware cannot recover the drive failure, there is little chance of recovering the array in that condition. Broadcom storage support cannot help in this scenario. Even data recovery specialists have a difficult time putting the data back together after migration/expansion failure.

Pulling a drive when the OS is running and the array is degraded:

The MegaRAID controllers can scan the drive bus and mount new drives but always take extra caution when removing a drive when the VD is degraded.
Accidentally removing the wrong drive is the number one cause of data loss.

If possible, gracefully shout down the OS and find the bad drive, then remove it.
Double check all cable connections before turning on the system to ensure that all power and data connections are connected securely. You may also want to get into the HII utility or controller BIOS to check that the array is still degraded before letting the OS boot.
Recovering from an offline array is much simpler to fix when the OS has not loaded yet especially if you are running write-back cache with no BBU or CacheVault.
If the VD becomes offline for whatever reason, return all drives to their original position and check the VD again.

Save RAID Configuration

Although MegaRAID Storage Manager can save the configuration data for your RAID controller, it is best that you use storcli because you can use rescue OS of any type to restore your config, even an EFI boot shell or a Linux live DVD such as Knoppix:

Save config instructions assumes that there is only 1 controller, /c0. If you have 2 MegaRAID controllers, run /c1 as well

Save config from storcli:
storcli64 /c0 get config file=c0.cfg

Destroy corrupt config:
storcli64 /c0 delete config force

Reload config:
storcli64 /c0 set config file=c0.cfg

You can also save the output of storcli /c0 show all>myconfig.txt and keep it with your config as reference.

Top

IMPORTANT NOTE
There is a binary difference between saving the configuration in MegaRAID Storage Manager and saving in storcli. The 2 files are not compatible.

If any drives are missing, restore will fail, but there is a workaround.
For example;
You have a RAID 1 and one drive failed in such a way that the second array member was effected. You must have 2 drives present for the saved configuration to load successfully.
In that scenario, a blank drive can be substituted as a “placeholder”, then removed right after the configuration was loaded. The save config function must see all target drives but not necessarily the originals.
NOTE Failure to remove the placeholder drive would result in pushing a blank drive into the array causing immediate data corruption thus storcli ran from an EFI boot shell is preferable.

Check the source drives in the degraded array before rebuilding:
The number two cause of offline VDs and data corruption is rebuilding in the OS while another drive fails causing the VD to go offline.
You should always backup your data before a rebuild and never assume that your drives are in perfect health. Run HD Sentinel or SMARTMON tools and make sure that other disks are not reporting errors.
If there are source drive SMART errors, the alternative is to schedule downtime and rebuild the VD in the controller’s BIOS or HII utility in the MB BIOS.

Back To Search Results

Top