# SOFTWARE

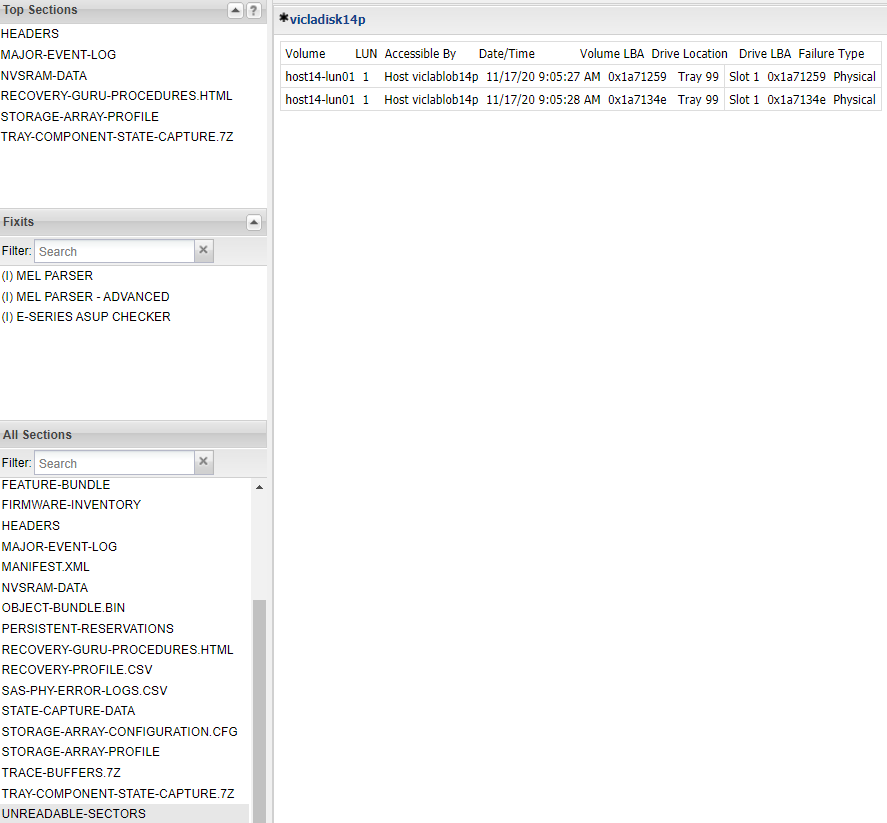
## Unresponsive Drive

* Check MEL for any event against the related drive.
* If nothing is found, then check for any FW that deals with unresponsive status.
* Reseat
* Replace Drive.

**Note:** This drive cannot be manually failed since the controllers are not able to communicate with the drive. All what need to do is to remove the drive and replace it.

## Unreadable Sector(s) Detected Data Loss Occurred

* Unreadable sectors are DA errors and will need the **trace buffers** to analyze.
* Check ASUP under Unreadable sectors section.
* If failure type is physical, go ahead and send replacement. Check under ASUPS
* Check RAID level for disk failures and data loss.
* Next steps will be to replace the drive and [clear the unreadable sectors](https://mysupport.netapp.com/NOW/public/eseries/sam/index.html#page/GUID-8538272A-B802-49D9-9EA2-96C82DAD26A2%2FGUID-12F322A5-BE73-48DF-86E9-F81F941430C6.html) table from SANtricity GUI. Then recommend a scandisk from the host side.



**Note:** Unreadable sector means is that there are sectors on the drive(s) in the **RAID 5** that have both the data and parity unreadable. Therefore, its logging unreadable sectors and data loss. the Physical Unreadable sector means that the sector is physically bad on the drive. The logical means that was reconstructed but the data or parity was not available to complete the stripe.

## Drive Reports Media Errors

* Check Drive status in Storage array profile
* Check MEL for media errors
* If you find more than two or three unrecoverable media errors on a drive in that state you can replace it.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/E-Series_reports_Drive_returned_unrecoverable_media_error>

## By-Passed drive

To re seat Drive in shelf X, drawer X, bay X

1. Unseat the by-passed drive for 2 minutes.
2. Reseat the drive.
3. If the drive remains by-passed replace the drive

**Note:** By-passed means the controllers cannot talk to the drive. You cannot manually fail it.

## Impending Drive failure

* You may need to manually fail drive before replacing.
* To manually fail a drive with hot spare available, make sure the copy content box is selected. Once failed the hot spare disk will change highlighted color to represent it is in use.
* Check operations in progress to see process details.
* If no hot spare is available, you may uncheck this box.
* If drive reconstruction will not start automatically after replacement, you may use the Manually reconstruct option.
* The Replace option may be needed if Manual reconstruction is not available.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/Diagnosing_an_impending_drive_failure>

## Check Conditions

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/Every_drive_in_E-Series_drawer_or_shelf_tray_reporting_b_4b_4_check_conditions>

<https://www.t10.org/list/2sensekey.html>

<https://www.t10.org./list/asc-num.html>

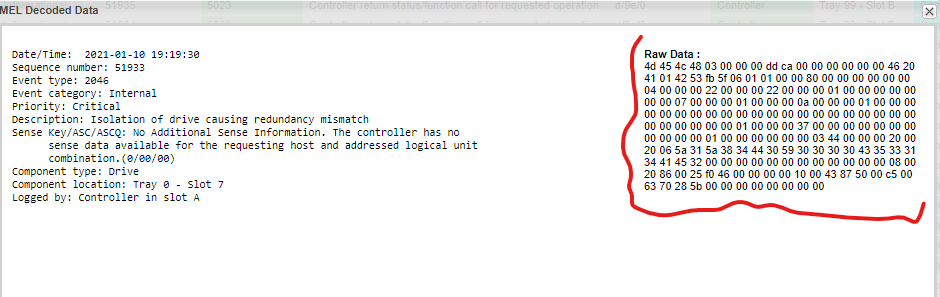
VDD repair is when a host send a write request and get no response from disk

## Isolation Of Drive Causing Redundancy Mismatch

If the following are true, a parity scan and repair on the affected volume can be performed:

* The volumes have Data Assurance turned on
* The error is only logged against one drive
* There are no other drive check conditions

Go to MEL and identify byte 33 within the raw data of the error.



Identify volume SSID within the Raw data. The byte 33. This value is in HEX and it must be converted into DEC.

Go to *evfShowVol* in State-Data-Capture with that value.

Make sure **App tag** field matches the HEX value obtained.

Check **user label** field to identify the volume.

Run the following script using the script Editor in SANtricity desktop App

*check volume ["VOLUME\_NAME"] parity mediaErrorFile="C:\MediaError.txt" parityErrorFile="C:\ParityError..txt" priority=high verbose=true;*

**Note:** You can change output location. This command may run up to 3 days. Need to wait until it completes. **DO NOT HIT CANCEL IN THE POP UP WINDOW OF THE SCRIPT.**

**Note:** This error could spread to more than a single volume.

After completion run the command bellow

repair volume ["1"] parity parityErrorFile="C:\ParityError.txt" verbose=true;

Request the parity error file after completion

This is usually faster than the checking process, however, there is not exact ETA.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/Isolation_of_drive_causes_redundancy_mismatch>

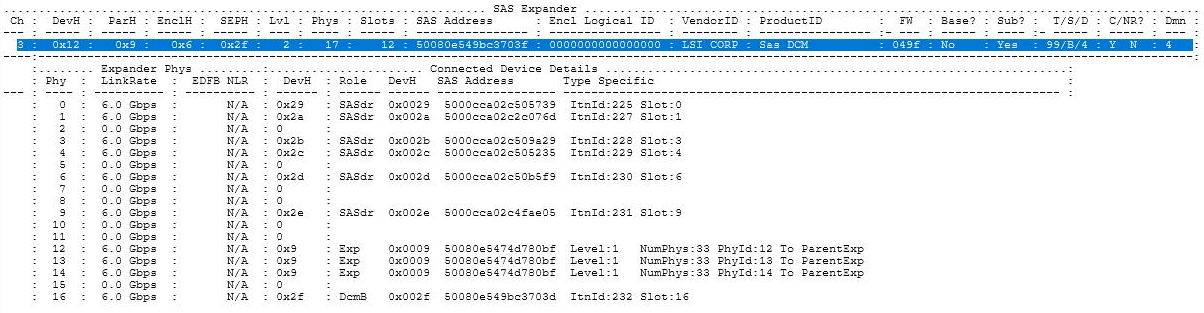
## A drawer in the tray has become degraded

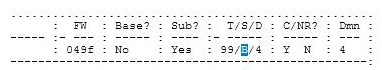
* Check the reason for degraded: Disk failures, SAS connections, loss of redundancy etc.
* Go to the Hardware section and check both front and back for any failure or warnings.
* Check **State Capture Data > sasStateCapture > sasShowAllExpanders > Error Statistics for Expander Phys**:

You may get something similar if an issue:



Now, based on above details check Channel 3 Level 2 0x12 Hex to get the exact location.





B Side

Replace or Reseat any faulty SAS parts, Disk or SAS cables

Reset SAS Statistics

* *reset storagearray SASPHYBaseline;*
* *clear allDriveChannels stats;*

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/E-Series_drawer_degraded_or_multiple_disk_errors_on_one_drawer>

**Note:** Drawer replacements can be done either Offline or Online. Check Drawer loss protection status.

## E-Series tray/drawer loss of redundancy

Check the recoveryGURU to see which components and trays are reporting the loss of redundancy.

* Controller / Controller Tray
* ESM / IOM (Environmental Services Module / Input Output Module) / Expansion Tray.
* Drive Drawer (60-Bay Enclosure)

Investigate any components specified in the recoveryGURU to ensure those components are seated properly and powered on.

Controllers and ESMs/IOMs can be unseated and reseated if needed to ensure proper seating and power.

Investigate the backend cabling to ensure that all cables are securely connected and the ports display link lights.

Cables connected to controllers and ESMs/IOMs can be unseated and reseated if needed.

**Note**: Be sure not to unseat or disconnect cables on the working side. Doing so will result in a complete loss of access to that tray and any tray below it in the chain.

The difficulty in troubleshooting a loss of redundancy on drive trays ranges from simple to very complex and may require active knowledge of how to read and interpret the State Capture data located within a standard support bundle.

### Additional Information

* <https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/How_to_troubleshoot_E-Series_tray%2F%2Fdrawer_loss_redundancy>
* <https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/E-series_all_disk_drivers_are_Loss_of_redundancy_status_in_one_Drawer>

## Degraded SAS port

Check State Capture Data > ionShow(99,0,0,0) > chall 0 for errors, luall 0 to identify degraded channels.

Check *ogmShowRecoveryFailureList*  and make sure the failure reports equal on both controller to discard stale data.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/How_to_identify_a_degraded_SAS_port_on_an_ESM_within_E-Series>

## Nominal/Maximun Temperature Exceeded

* Environmental conditions caused over temperature reading on component sensor.
* Diagnose to confirm root cause
* Recovery guru message or alert with component location continues
* Ensure hardware module is not removed for extended times from the chassis
* Ensure disk populate the front row of draws in a 60 drive enclosure
* Ensure Hardware installation guide is followed
* Reduce environmental temperature
* Request datacenter operator reduce the temperature in front of the array chassis
* Improve airflow
* Ensure minimum 15 cm free of obstructions front and back of the array chassis.

## Power Supply Failed

* Ensure that the power supply is fully seated.
* Is the power switch toggled to the ON position?
  + On = |
  + Off = O
* Ensure the power cable is making a secure connection at both ends.
* Unseat and reseat the power supply.
* Try another outlet on the PDU (Power Distribution Unit)
* Try a new power cable.

## Fibre channel link errors

These are most commonly an issue with an SFP or cable.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/Fibre_channel_link_errors_detected_on_E-Series_controller_host_port>

## Write-Back Caching Forcibly Disabled

Cache memory is an area of temporary volatile storage (RAM) on the controller that has a faster access time than the drive media. If you use cache memory, you can increase overall I/O performance because of these reasons:

* Data requested from the host for a read might already be in the cache from a previous operation, thus eliminating the need for drive access.
* Write data is written initially to the cache, which frees the application to continue instead of waiting for the data to be written to the drive.

Write-back caching was disabled on one or more volumes. This problem can occur for the following reasons:

* Battery Failure
* **Battery below minimum capacity(Most common)**
* The cache size memory of the controllers are different
* Cache Reconfiguration
* A Cache Data-Restore operation is in progress, which interrupted the normal write-back caching process
* The space in the cache backup device is insufficient for storing the cache.
* Memory parity error
* Simplex configuration - cache cannot be mirrored.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/E-Series%3A_Write_back_caching_forcibly_disabled_alert>

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/Write-back_caching_forcibly_disabled_due_to_low_battery_capacity>

## Amber light with no Apparent Reason

If customer is complaining about amber light however storage array looks in optimal conditions do the following:

* Check State Capture Data > ssmShowSubTree
* Look for *Fault LED State* condition and match it with a controller.
* Check for any amber light at the rear side of the controller.
* A staggered reboot might be needed if no apparent reason.

## No Access to SANtricity Web UI

You may need to restart the web services. You can do this from:

### Linux Host

### curl -k -X POST -u USERNAME:PASSWORD https://<Controller\_Management\_Address>/devmgr/v2/restart

### Windows Host

#### PowerShell

$Header = @{"Authorization" = "Basic "+[System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes("USERNAME:PASSWORD "))}  
Invoke-RestMethod -Method POST -Headers $Header -ContentType "application/json" -SkipCertificateCheck -Uri "<https://controller_ip/devmgr/v2/restart>"

### Controller shell

1. SSH to the controller shell using the "diag" user.
   * [Enable remote access using SSH](https://mysupport.netapp.com/NOW/public/eseries/sam/index.html#page/GUID-8538272A-B802-49D9-9EA2-96C82DAD26A2/GUID-71D62476-4E05-4578-A594-8BC2330FD60C.html)
   * The diag user password depends on the controller firmware level
     + 11.30.x: eos/wy3oo&w4 (for eos shell) and diag/wy3oo&w4 (for dom0/linux shell)
     + 11.40.x: eos/<UI admin password> (for eos shell) and diag/<UI admin password> (for dom0/linux shell)
2. Run the command "sudo systemctl restart msw"

Keep in mind that after restarting the web services, SANtricity System Manager web interface will take approx. 5-10 minutes to become available again.

## Reset SANtricity Password

Shell access mandatory. Not SSH

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/How_to_reset_SANtricity_System_Manager_local_admin_password_starting_with_11.40.2_code>

**Note:** Make sure to request approval from the customer before jumping into password reset.

## An ASUP message could not be Delivered from the Array Management

* Check ASUP configuration
* If Ok, Restart Web Services (Staggered reboot, controller shell, or host side)
* Check if this applies.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/E-Series_DBM_Backup_AutoSupport_could_not_be_delivered_starting_on_9%2F%2F30%2F%2F20>

**Note:** ASUP transmission logs in the Autosupport are only available in manual support bundles, AODs, or critical ASUPs

## Volume Failure

Find the reason for volume(s) to fail. Most common scenarios are:

* Power outage
* Tray or drawer loss of communication
* Multiple drive failures

In 08.25.14.00 CFW *vdmRecoverAllRAIDVols* will only revive drives that failed due to a power outage or connectivity issue. Any drives that remain failed will need to be recovered using the manual disk pool volume recovery covered in the following KB.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/E-Series_failed_disk_pool_volumes_on_SANtricity_OS_pre-8.30.40.00_or_pre-8.40.10_due_to_hardware_failures>

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/E-Series_Failed_Volume_recovery_for_traditional_Volume_Groups_pre-11.40.4%2F%2F11.50.2_releases>

## Persistent Cache Backup Device At End Of Life

* Check Storage Array Profile > Controllers
* Under *Cache Backup Device* review *Wear life used (100% means end of life)*
* *Endurance remaining should be 0* (After replacement)
* If the above is met then controller must be replaced.
* Controller has reached end\_of\_life cycle naturally.

<https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/E-Series_Storage_Array/E-series_persistent_cache_backup_device_at_end_of_life>

## Cache Backup Failed

* Check Storage Array Profile > Controllers.
* Check Cache backup status.
* If failed, controller replacement must be done.

## ALB\_Host\_Redundancy\_Lost

### iSCSI

* Check **ISCSI-SESSION-CONNECTION** in ASUPs to check connections
* The iscsi iniator displays a single session
* Identify host initiator and controller connection
* MEL may report IO shipping
* Make sure if controller host ports are pingable from host command line
* MPIO at host level
  + Add an additional session in the iSCSI initiator to connect to the three remaining target ports on the storage.
  + Perform the following steps to resolve the issue:
  + Open the Microsoft iSCSI initiator; on the Targets tab, click Properties
  + In the Properties window, under the Sessions tab, click Add Session
  + Add a check mark to enable multi-path and click Advanced
  + Set Local Adapter to Microsoft iSCSI Initiator
  + Set Initiator IP to Local hosts IP
  + Set the Target Portal IP to the IP of the remaining host ports that are not
  + currently connected, and click OK.