dfu events

ONTAP EMS reference

NetApp
November 20, 2025

This PDF was generated from https://docs.netapp.com/us-en/ontap-ems-9151/dfu-badbridgeshelfconfig-events.html on November 20, 2025. Always check docs.netapp.com for the latest.

Table of Contents

dfu events . . . 1
- dfu.badbridgeshelfconfig events . . . 1
  - dfu.badBridgeShelfConfig . . . 1
- dfu.clusterdisknotready events . . . 1
  - dfu.clusterDiskNotReady . . . 1
- dfu.clustericdown events . . . 2
  - dfu.clusterIcDown . . . 2
- dfu.clustericerror events . . . 2
  - dfu.clusterIcError . . . 2
- dfu.clusterpartner events . . . 3
  - dfu.clusterPartner . . . 3
- dfu.clustertakeover events . . . 3
  - dfu.clusterTakeover . . . 3
- dfu.disksizechanged events . . . 4
  - dfu.diskSizeChanged . . . 4
- dfu.firmwaredownloading events . . . 4
  - dfu.firmwareDownloading . . . 4
- dfu.firmwaredownrev events . . . 5
  - dfu.firmwareDownrev . . . 5
- dfu.firmwareuptodate events . . . 5
  - dfu.firmwareUpToDate . . . 5
- dfu.fwdownloadfailedmultfiles events . . . 6
  - dfu.fwDownloadFailedMultFiles . . . 6
- dfu.fwdownloadfailedstatus events . . . 6
  - dfu.fwDownloadFailedStatus . . . 6
- dfu.fwdownloadfailedwbuf events . . . 7
  - dfu.fwDownloadFailedWbuf . . . 7
- dfu.init events . . . 7
  - dfu.init.noMemory . . . 7
- dfu.mallocfailed events . . . 8
  - dfu.mallocFailed . . . 8
- dfu.nomemory events . . . 8
  - dfu.noMemory . . . 8
- dfu.readtestfailed events . . . 9
  - dfu.readTestFailed . . . 9
  - dfu.readTestFailed.fatal . . . 9
- dfu.readtestfailedstatus events . . . 9
  - dfu.readTestFailedStatus . . . 10
- dfu.refreshinquiryfailed events . . . 10
  - dfu.refreshInquiryFailed . . . 10
- dfu.suspended_disasterrecovery events . . . 10
  - dfu.suspended_DisasterRecovery . . . 11

dfu events

dfu.badbridgeshelfconfig events

dfu.badBridgeShelfConfig

Severity

ERROR

Description

This message occurs when the disk firmware update aborts because it cannot contact the two peer FC-to-SAS bridges.

Corrective Action

Make sure that the storage controller is correctly cabled to the two peer FC-to-SAS bridges and that the bridges are correctly cabled to the SAS disk shelves. Then retry the 'disk_fw_update' command.

Syslog Message

Error contacting two peer FC-to-SAS bridges. Unable to download firmware to disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.
productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.clusterdisknotready events

dfu.clusterDiskNotReady

Severity

ERROR

Description

This message occurs when the controller failover partner reports that a disk selected for download is in the NOT READY state.

Corrective Action

Only disks in the READY state can be downloaded to. If a disk is in the NOT READY state, it indicates that the disk has probably failed for some reason and should be returned for RMA.

Syslog Message

Controller failover partner reports disk as NOT READY. Unable to download firmware to disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.

productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.clustericdown events

dfu.clusterIcDown

Severity

ERROR

Description

This message occurs when the high-availability (HA) interconnect is not available.

Corrective Action

The HA interconnect was not functional. Make sure that controller failover is enabled. Check that the HA interconnect cables are connected properly, and if applicable (based on the HA interconnect type), that the SFPs (Small Form-Factor Pluggables) are seated properly on both controllers.

Syslog Message

HA interconnect not available (cf disabled?). Unable to download firmware to disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.
productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.clustericerror events

dfu.clusterIcError

Severity

ERROR

Description

This message occurs when communication with the controller failover partner cannot be established.

Corrective Action

Typically, these errors are related to cable or transmission errors from the HA interconnect. Check that the HA interconnect cables are connected properly, and if applicable (based on the HA interconnect type), that the SFPs (Small Form-Factor Pluggables) are seated properly on both controllers.

Syslog Message

HA interconnect error %d encountered. Unable to download firmware to disk %s [%s %s %s] S/N [%s].

Parameters

clusterError (INT): High-availability (HA) interconnect error number.
diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.

productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.clusterpartner events

dfu.clusterPartner

Severity

ERROR

Description

This message occurs when automatic firmware download is performed as part of system boot and partner disks are downrev.

Corrective Action

Firmware download is not allowed to update partner disks automatically. Manual invocation of the "storage disk firmware update" command is required. See the "storage disk firmware update" man page for details.

Syslog Message

Operator must issue disk_fw_update command to download firmware to partner Disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.
productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.clustertakeover events

dfu.clusterTakeover

Severity

ERROR

Description

This message occurs when firmware download is attempted while in takeover mode.

Corrective Action

Firmware download is not allowed while in takeover mode. Exit takeover mode and attempt the "storage disk firmware update" command again. See the "storage disk firmware update" man page for details.

Syslog Message

Unable to download firmware while in takeover mode to Disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.
productId (STRING): Product id of the disk.

fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.disksizechanged events

dfu.diskSizeChanged

Severity

NOTICE

Description

This message occurs when a size change is detected after a firmware update. This can be either an increase or decrease in physical size of the disk.

Corrective Action

The disk might not be usable any longer by the RAID subsystem because of the size change that occurred. If RAID cannot access the disk any longer, it will be failed and should be returned for RMA. If the disk is still accessible, leaving it in the system is perfectly fine.

Syslog Message

Disk %s [%s %s %s] S/N [%s] size changed (%x:%x %llx:%llx %llx:%llx %llx:%llx %llx:%llx)

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.
productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.
oldSectorSize (INTHEX): Old sector size of the disk.
newSectorSize (INTHEX): New sector size of the disk.
oldLastSector (LONGINTHEX): Old right-size of the disk.
newLastSector (LONGINTHEX): New right-size of the disk.
oldDiskBlocks (LONGINTHEX): Old right-sized blocks on the disk.
newDiskBlocks (LONGINTHEX): New right-sized blocks on the disk.
oldRealLastSector (LONGINTHEX): Old raw size of the disk.
newRealLastSector (LONGINTHEX): New raw size of the disk.
oldRealDiskBlocks (LONGINTHEX): Old raw blocks on the disk.
newRealDiskBlocks (LONGINTHEX): New raw blocks on the disk.

dfu.firmwaredownloading events

dfu.firmwareDownloading

Severity

INFORMATIONAL

Description

This message occurs when firmware is being downloaded for a specific product ID of disks on the system.

Corrective Action

(None).

Syslog Message

Now downloading firmware file %s on %d disk(s) of plex [%s]…

Parameters

file (STRING): Firmware file which is being downloaded.
diskcount (INT): Number of disks being downloaded to.
plex (STRING): Plex name being downloaded to.

dfu.firmwaredownrev events

dfu.firmwareDownrev

Severity

ERROR

Description

This message occurs when the system finds disks with a downrev version of firmware, as defined by the installed version of Data ONTAP®.

Corrective Action

Use the "storage disk firmware update" command to update the downrev firmware on the disks. Check your support provider for more information about obtaining the latest disk firmware. If the problem persists, contact NetApp technical support.

Syslog Message

Downrev firmware on %d disks.

Parameters

downrev (INT): Number of disks with downrev firmware.

dfu.firmwareuptodate events

dfu.firmwareUpToDate

Severity

NOTICE

Description

This message occurs when all eligible disks are determined to be updated to the latest version of firmware available on the system.

Corrective Action

(None).

Syslog Message

Firmware is up-to-date on all eligible disks.

Parameters

(None).

dfu.fwdownloadfailedmultfiles events

dfu.fwDownloadFailedMultFiles

Severity

ERROR

Description

This message occurs when more than one file is found for downloading to an ATA drive. Because there is no version string control, only one file at a time is allowed on the system.

Corrective Action

Two or more firmware files were found for download. Delete all except the one that should be downloaded to the drive. Background firmware update should download on the next check cycle.

Syslog Message

Download failed due to multiple firmware files found for Disk type [%s %s].

Parameters

vendorName (STRING): Vendor name of the disk.
productId (STRING): Product ID of the disk.

dfu.fwdownloadfailedstatus events

dfu.fwDownloadFailedStatus

Severity

ERROR

Description

This message occurs when a firmware download failure occurs.

Corrective Action

Decode sense codes based on drive supplier to determine the reason for the failure. Most situations can be recovered by attempting to download firmware again using the "disk_fw_update" command. See the disk_fw_update man page for complete details.

Syslog Message

Status: (0x%x/0x%x/0x%x) (SCSI sense 0x%x/0x%x/0x%x/0x%x)

Parameters

OpStatus (INTHEX): Status of the passthru I/O.
HostStatus (INTHEX): Host Status of the passthru I/O.
TargetStatus (INTHEX): Target Status of the passthru I/O.
sense_key (INTHEX): SCSI Sense key.
sense_code (INTHEX): SCSI Sense Code.
sense_code_qualifier (INTHEX): SCSI Sense Code Qualifier.

fru (INTHEX): SCSI Sense Code FRU identifier.

dfu.fwdownloadfailedwbuf events

dfu.fwDownloadFailedWbuf

Severity

ERROR

Description

This message occurs when retries are exhausted on the write buffer command that is used to download firmware to a disk.

Corrective Action

Disk firmware might still need to be updated. See the disk_fw_update man page for complete details on performing this.

Syslog Message

Write buffer command failed to Disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.
productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.init events

dfu.init.noMemory

Severity

ERROR

Description

This message occurs when the disk firmware update initialization routine cannot allocate memory.

Corrective Action

Memory allocation relies on the availability of memory resources in the system. If possible, reduce the workload so that fewer resources are needed. If the failure persists after reducing the workload, contact NetApp technical support.

Syslog Message

Could not allocate memory for disk firmware update. Requested size=%d bytes.

Parameters

size (INT): Size (in bytes) of the memory allocation request.

dfu.mallocfailed events

dfu.mallocFailed

Severity

ALERT

Description

This message occurs when Data ONTAP® cannot allocate memory to read the disk firmware file and aborts the disk firmware update.

Corrective Action

Inability to allocate memory for this action indicates a failure within Data ONTAP. Take a core for reference, and then open a support case to address the underlying issue. The reboot process when you take the core resolves the immediate problem.

Syslog Message

Cannot allocate memory to read disk firmware file %s; disk firmware update aborted.

Parameters

filename (STRING): Name of the disk firmware file.

dfu.nomemory events

dfu.noMemory

Severity

ERROR

Description

This message occurs when the disk firmware update routine cannot allocate memory to update the disk firmware.

Corrective Action

Memory allocation relies on the availability of memory resources in the system. If possible, reduce the workload so that fewer resources are needed. Rebooting the system can recover memory resources that might have been lost. If the failure persists after reducing the workload and rebooting, contact NetApp technical support for assistance in determining whether additional system memory is indicated.

Syslog Message

Could not allocate memory for disk firmware update. Unable to download firmware to disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Name of the vendor of the disk.
productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.readtestfailed events

dfu.readTestFailed

Severity

ERROR

Description

This message occurs when a read of the disk fails after downloading firmware to a disk.

Corrective Action

Disk was unable to be read from after a firmware update occurred. I/O will be retried. If the retries are not successful, you should fail the disk and return it for RMA.

Syslog Message

Media Access test failed on Disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.
productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.readTestFailed.fatal

Severity

ERROR

Description

This message occurs when a read of the disk fails after downloading firmware to a disk and all retries have been exhausted.

Corrective Action

Disk was unable to be read from after a firmware update occurred. I/O will be retried. If the retries are not successful, you should fail the dise and return it for RMA.

Syslog Message

Unable to access media after firmware update on Disk %s [%s %s %s] S/N [%s].

Parameters

diskName (STRING): Name of the disk.
vendorName (STRING): Vendor name of the disk.
productId (STRING): Product ID of the disk.
fwVersion (STRING): Firmware version of the disk.
serialno (STRING): Serial number of the disk.

dfu.readtestfailedstatus events

dfu.readTestFailedStatus

Severity

ERROR

Description

This message occurs when a read test failure occurs after a firmware download.

Corrective Action

Decode sense codes based on drive supplier to determine the reason for the failure. Most situations can be recovered by the system automatically retrying the I/O operation.

Syslog Message

Status: (0x%x/0x%x/0x%x) (SCSI sense 0x%x/0x%x/0x%x/0x%x)

Parameters

OpStatus (INTHEX): Status of the read I/O.
HostStatus (INTHEX): Host Status of the read I/O.
TargetStatus (INTHEX): Target Status of the read I/O.
sense_key (INTHEX): SCSI Sense key.
sense_code (INTHEX): SCSI Sense Code.
sense_code_qualifier (INTHEX): SCSI Sense Code Qualifier.
fru (INTHEX): SCSI Sense Code FRU identifier.

dfu.refreshinquiryfailed events

dfu.refreshInquiryFailed

Severity

ERROR

Description

This message occurs after a successful disk firmware update, when the 'SCSI inquiry' command, which is issued to all disks as part of the disk firmware download process, fails to finish. It is also possible to get messages indicating that disks have downrev firmware.

Corrective Action

When this error happens, check the connection to the partner node and manually retry the firmware download process. If the problem still persists, open a support case to investigate the underlying cause.

Syslog Message

(None).

Parameters

retryCount (INT): Number of times the command was retried and failed.

dfu.suspended_disasterrecovery events

dfu.suspended_DisasterRecovery

Severity

ERROR

Description

This message occurs in a MetroCluster™ environment when firmware download to remote disks is suspended during disaster recovery. This event is signaled at most once during disaster recovery, the first time firmware download to a remote disk is suspended.

Corrective Action

Firmware download to remote disks is suspended during MetroCluster disaster recovery. Wait until switchback has completed, and either allow the firmware to be downloaded automatically, or run the "storage disk firmware update" command. See the "storage disk firmware update" man page for details.

Syslog Message

Suspend firmware download to remote disks while in MetroCluster Disaster Recovery state %s

Parameters

dr_state (STRING): Current MetroCluster disaster recovery state.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.