adt events

ONTAP 9.12.1 EMS reference

NetApp
December 14, 2022

Table of Contents

adt events

adt.aggrcb events

adt.aggrcb.unlinkfail

Severity

ALERT

Description

This message occurs when the auditing subsystem cannot remove a stale aggregate control block entry from the Audit aggregate hash table. This could happen if the hash table rearrangement fails because of insufficient memory. In this condition, the auditing subsystem might not function or data access might be denied.

Corrective Action

Reboot the node. For high-availability (HA) configurations, perform a takeover and giveback from the partner to reduce the impact on system availability

Syslog Message

Auditing subsystem internal error: Aggregate Control Block: %s unlink failed for SVM with UUID: %s because of insufficient memory.

Parameters

AggregateUuid (STRING): UUID of the aggregate with a stale file handle.
VserverUuid (STRING): UUID of the Storage Virtual Machine(SVM, formerly Vserver).

adt.aucb events

adt.aucb.overwrite

Severity

INFORMATIONAL

Description

This message occurs in the auditing subsytem, when the subsystem overwrite an existing audit control block during audit control block creation. The overwriting of the audit control block is because of a failure in audit control block deletion.

Corrective Action

(None).

Syslog Message

Overwriting of audit control block occured.

Parameters

(None).

adt.cmdq events

adt.cmdq.init.fail

Severity

ALERT

Description

This message occurs when an internal audit command queue fails to initialize.

Corrective Action

Available system resources are required for this feature to function. The audit subsystem might not function, or might function with reduced performance. The best way to accomplish that is through a system reboot. For HA configurations, operational disruption can be minimized by initiating a partner takeover followed by a reboot of this partner. After the reboot is complete, issue a "giveback" command to return services to this partner.

Syslog Message

Audit subsystem internal error: Audit command queue failed to initialize, system reboot might be required.

Parameters

(None).

adt.cmdthrd events

adt.cmdthrd.create.fail

Severity

ALERT

Description

This message occurs when audit initialization fails because the necessary execution threads cannot be created.

Corrective Action

Available system resources are required for this feature to function. The best way to accomplish that is through a system reboot. For HA configurations, operational disruption can be minimized by initiating a partner takeover followed by a reboot of this partner. After the reboot is complete, issue a "giveback" command to return services to this partner.

Syslog Message

Audit subsystem internal error: Could not start required audit command threads, system reboot might be required.

Parameters

(None).

adt.dest events

adt.dest.access.fail

Severity

ERROR

Description

This message occurs when the audit consolidation job fails to write audit logs to the destination directory because the destination directory is not available. This event can leads to denial of service on Security Access Control List (SACL) enabled objects.

Corrective Action

Use the "volume show" command to check whether the destination volume exists, is online, and has sufficient free space. Use the "volume modify" command to bring the volume online, or increase volume size. Use the "vserver audit modify" command to modify the destination volume.

Syslog Message

Audit consolidation job failed to access destination directory "%s" of Vserver "%s"; consolidation job type is "%s".

Parameters

destination (STRING): Destination directory of the Vserver into which the consolidation job failed to write audit logs.
vserver (STRING): Vserver name whose consolidation job failed to write audit logs to the destination directory.
descriptor (STRING): Type of consolidation job - CIFS/S3.

adt.dest.directory.full

Severity

EMERGENCY

Description

This message occurs when the audit consolidation process fails to write audit logs to the destination directory because the destination directory is full. This event can lead to denial of service on Security Access Control List (SACL) enabled objects.

Corrective Action

Use the "volume show" command to check whether the destination volume exists, is online, and has sufficient free space. Use the "volume modify" command to increase volume size. Use the "vserver audit modify" command to modify the destination volume path.

Syslog Message

Audit destination directory "%s" of Vserver "%s" is full; consolidation job type is "%s".

Parameters

destination (STRING): Destination directory of the Vserver that is full.
vserver (STRING): Vserver name whose audit consolidation process failed to write audit logs to the destination directory.
descriptor (STRING): Type of consolidation job - CIFS/S3.

adt.dest.directory.unavail

Severity

EMERGENCY

Description

This message occurs when the audit consolidation job fails to write audit logs to the destination directory because the destination directory has become unavailable or has run out of space. This event can lead to denial of service for Security Access Control List (SACL) enabled objects.

Corrective Action

Use the "volume show" command to check whether the destination volume exists, is online, and has sufficient free space. Use the "volume modify" command to bring the volume online, or increase volume size. Use the "vserver audit modify" command to modify the destination volume.

Syslog Message

Audit destination directory "%s" of Vserver "%s" is unavailable or out of space; consolidation job type is "%s".

Parameters

destination (STRING): Destination directory of the Vserver to which the consolidation job failed to write audit logs.
vserver (STRING): Name of the Vserver name whose consolidation job failed to write audit logs to the destination directory.
descriptor (STRING): Type of consolidation job - CIFS/S3.

adt.max events

adt.max.record.size.exceeded

Severity

ERROR

Description

This message occurs when a management command or file operation tries to generate an audit record, that is greater than the max_audit_record_size value. The File Services Auditing subsystem might fail the operation or truncate the record.

Corrective Action

Contact NetApp technical support.

Syslog Message

File Services Auditing subsystem failed the operation or truncated an audit record because it was greater than max_audit_record_size value. Vserver UUID=%s, event_id=%u, size=%u

Parameters

VserverUuid (STRING): UUID of then Vserver.
eventId (INT): Event ID for internal use.
size (INT): Record size.

adt.nfs events

adt.nfs.root.access.no.map

Severity

ERROR

Description

This message occurs in the auditing subsytem, when the NFS root user is accessing the file without a valid CIFS credential. Access is being allowed because the "ignore-nt-acl-for-root" NFS option is set, and hence the BUILTIN\Administrator credential is used for auditing.

Corrective Action

If NFS root user access to the file without NT ACL check should be prohibited, disable the "ignore-nt-act-for-root" option by using the "nfs modify -ignore-nt-acl-for-root" command. If a more appropriate CIFS credential should be used for auditing, configure the SVM name-mapping by using the "vserver name-mapping" command.

Syslog Message

NFS root user is accessing the file without a valid CIFS credential. Access is being allowed because the "ignore-nt-acl-for-root" NFS option is set, and hence the BUILTIN\Administrator credential is used for auditing.

Parameters

VserverUuid (STRING): UUID of the Storage Virtual Machine (SVM, formerly Vserver).

adt.service events

adt.service.block

Severity

EMERGENCY

Description

This message occurs when the volume that hosts the destination path where the final audit logs are stored is not accessible or does not have sufficient space and the audit consolidation service is not able to write to the volume. This prevents the audit service from working properly. File access and file audit logging is blocked.

Corrective Action

Use the "vserver audit show" command to get the name of the volume that hosts the destination path. Use the "volume show" command to check whether the volume exists, is online, and has sufficient free space. Use the "volume modify" command to increase volume size. Use the "vserver audit modify" command to modify the destination path.

Syslog Message

Audit destination directory "%s" of Vserver "%s" is either not accessible or full for the consolidation job type "%s". File-Operations which need to be audited will be denied. File Audit Logging will also fail.

Parameters

destinationPath (STRING): Destination path.
vserverName (STRING): Name of the Storage Virtual Machine (SVM, formerly Vserver).
descriptor (STRING): Type of consolidation job - CIFS/S3.

adt.service.ro.filesystem

Severity

EMERGENCY

Description

This message occurs when the volume that hosts the destination path where the final audit logs are stored is of type Data protection (DP) or Load sharing (LS). These volume types are read-only for the purposes of audit logging and logging will fail.

Corrective Action

Use the "vserver audit modify" command to modify the destination volume.

Syslog Message

Auditing and file-ops failing on SVM %s, the volume containing %s for consolidation job of type %s is read only filesystem.

Parameters

vserverName (STRING): Name of the Storage Virtual Machine (SVM, formerly Vserver).
destinationPath (STRING): Destination path.
descriptor (STRING): Type of consolidation job - CIFS/S3.

adt.service.unblock

Severity

INFORMATIONAL

Description

This message occurs when the volume that hosts the destination path where the final audit logs are stored was resized or cleaned up and the audit consolidation service is able to write to the volume thereby unblocking the audit service. File access and file audit logging is unblocked.

Corrective Action

(None).

Syslog Message

Audit destination directory "%s" of Vserver "%s" for consolidation job of type "%s" is now accessible and File-Operations which need to be audited will be unblocked. File Audit Logging will also be unblocked.

Parameters

destinationPath (STRING): Destination path.
vserverName (STRING): Name of the Storage Virtual Machine (SVM, formerly Vserver).
descriptor (STRING): Type of consolidation job - CIFS/S3.

adt.stgvol events

adt.stgvol.info.notavailable

Severity

ERROR

Description

This message occurs when retreiving staging volume information fails. This might be due to an internal system problem or the staging volume creation failed.

Corrective Action

Contact Cserver admin to check if staging volume has been created.

Syslog Message

Audit subsystem internal error: Either staging volume %s is not created or unable to retrieve staging volume information.

Parameters

volName (STRING): The Name of the staging volume.

adt.stgvol.missing

Severity

ALERT

Description

This message occurs when retrieving staging volume information fails. Either the staging volume was not created or information cannot be retrieved due to some internal error. As a result, auditing is not performed for operations on the corresponding volume.

Corrective Action

Use the command "vserver audit repair" in diagnostic mode to correct the problem.

Syslog Message

Audit subsystem internal error: Staging volume "%s" is either not created or not available.

Parameters

volName (STRING): Name of the volume that is missing.

adt.stgvol.nospace

Severity

EMERGENCY

Description

This message occurs when a staging volume does not have enough space and the audit service tries to create a new staging file or directory for writing audit logs.

Corrective Action

Check the volume for older staging files that are no longer required and remove those files. Then retry the operation.

Syslog Message

Audit subsystem internal error: Staging volume %s is full.

Parameters

volName (STRING): Name of the volume that is full.

adt.stgvol.offline

Severity

EMERGENCY

Description

This message occurs when a staging volume is offline and the audit service tries to write an audit log into the staging volume.

Corrective Action

Contact the Cserver administrator to set the staging volume status to online.

Syslog Message

Audit subsystem internal error: Staging volume %s is offline.

Parameters

volName (STRING): The Name of the volume which is offline.

adt.wrkrq events

adt.wrkrq.init.fail

Severity

ALERT

Description

This message occurs when an internal audit worker queue fails to initialize.

Corrective Action

Available system resources are required for this feature to function. The Audit subsystem might not function, or might function with reduced performance. The best way to accomplish that is through a system reboot. For HA configurations, operational disruption can be minimized by initiating a partner takeover followed by a reboot of this partner. After the reboot is complete,issue a "giveback" command to return services to this partner.

Syslog Message

Audit subsystem internal error: Audit worker queue failed to initialize; system reboot might be required.

Parameters

(None).

adt.wrkrthrd events

adt.wrkrthrd.create.fail

Severity

ALERT

Description

This message occurs when audit initialization fails because the necessary execution threads cannot be created.

Corrective Action

Available system resources are required for this feature to function. The best way to accomplish that is through a system reboot. For HA configurations, operational disruption can be minimized by initiating a partner takeover followed by a reboot of this partner. After the reboot is complete,issue a "giveback" command to return services to this partner.

Syslog Message

Audit subsystem internal error: Could not start required audit worker threads; system reboot might be required.

Parameters

(None).

Copyright information

Trademark information