snmp events

ONTAP EMS reference

NetApp
November 19, 2025

Table of Contents

snmp events

snmp.authentication events

snmp.authentication.failure

Severity

ERROR

Description

This message occurs when there is an authentication failure during an SNMP query. This trap is generated for all SNMP versions.

Corrective Action

In case of SNMPv1/v2c check whether the SNMP community string is configured. In case of SNMPv3, check whether SNMPv3 authentication credentials are correctly configured. The SNMPv3 credentials include username, password, authentication protocol, authentication protocol password, privacy protocol and privacy protocol password.

Syslog Message

Authentication failure for SNMP query from port: %d.

Parameters

interface (INT): Port on which the SNMP authentication failed.

snmp.coldstart events

snmp.coldstart.trap

Severity

INFORMATIONAL

Description

This message occurs when the SNMP daemon is reinitializing itself with a coldStart. A coldStart(0) trap signifies that configuration changes are made to the agent or the protocol entity implementation during the reinitialization.

Corrective Action

(None).

Syslog Message

SNMP daemon was reinitialized with configuration changes.

Parameters

(None).

snmp.fips events

snmp.fips.objs.del.failed

Severity

ERROR

Description

This message occurs when the system fails to delete SNMP traphosts and users that are not FIPS compliant. The system tries to automatically delete them when FIPS is configured in the cluster. The SNMP traphosts and users that are left become inoperable.

Corrective Action

Delete remaining noncompliant SNMP traphosts first by using the "system snmp traphost delete" command. Then delete the remaining noncompliant SNMP users by using the "security login delete" command. The following SNMP users and traphosts are not FIPS compliant: 1. SNMPv1 users, SNMPv2c users, and SNMPv3 users having "none" or "MD5" as the authentication method or having "none" or "DES" as the encryption protocol. 2. SNMPv1 traphosts and SNMPv3 traphosts configured with a user that is not FIPS compliant.

Syslog Message

Failed to delete SNMP traphosts and users that are not FIPS compliant.

Parameters

(None).

snmp.fips.support

Severity

INFORMATIONAL

Description

This message occurs when Data ONTAP is operating in FIPS compliant mode but SNMPv3 is configured with non-compliant/weaker ciphers or hash algorithms. Hence SNMPv3 is disabled.

Corrective Action

(None).

Syslog Message

Data ONTAP is operating in FIPS compliant mode and SNMPv3 is configured with non-compliant ciphers or hash algorithms. Hence SNMPv3 is disabled.

Parameters

(None).

snmp.link events

snmp.link.down

Severity

INFORMATIONAL

Description

This message occurs when a network interface is down.

Corrective Action

If this message is not followed by a LinkUp message, the cluster administrator should manually check the link state with the "network port show" command, verifying that the port is administratively up. If the link state is still down and the port is not intentionally disabled, there might be a physical network problem: 1. Verify the switch has the corresponding port administratively and operationally up. 2. Verify that the network cable between the storage controller port and the corresponding switch is connected to the correct port and is not damaged. 3. Verify the integrity of the network cable with a cable tester, or swap in another cable known to be in good condition. 4. For further information or assistance contact NetApp technical support

Syslog Message

Interface %d is down.

Parameters

interface (INT): Number of the interface.

snmp.link.up

Severity

INFORMATIONAL

Description

This message occurs when a network interface is up.

Corrective Action

(None).

Syslog Message

Interface %d is up

Parameters

interface (INT): The number of the interface

snmp.raid events

snmp.raid.iterator.failure

Severity

ERROR

Description

This event is generated when a RAID group iterator was not able to be created.

Corrective Action

Check for other resource related issues.

Syslog Message

SNMP failed to create RAID group iterator

Parameters

(None).

snmp.server events

snmp.server.busy

Severity

ERROR

Description

This message occurs when the SNMP daemon is busy serving a high rate of incoming SNMP queries. This might be caused by multiple SNMP clients querying the cluster or a malicious client attempting a denial-of-service attack. SNMP clients might experience delays or timeouts.

Corrective Action

Run "tcpdump" on cluster to determine: If multiple SNMP clients querying the cluster, then reduce the rate of SNMP queries to the cluster or stop them entirely for a period of time (~15 minutes). If a malicious SNMP client is trying a denial-of-service attack, then update the firewall policy to block the client from querying the cluster by using the "firewall policy modify -policy mgmt -service snmp -action deny -ip-list IP_address" command.

Syslog Message

SNMP daemon is busy serving a high rate of incoming SNMP queries.

Parameters

(None).

snmp.snmpv3 events

snmp.snmpv3.enable

Severity

ERROR

Description

This message occurs when SNMPv3 is disabled due to a cluster in FIPS mode being upgraded to a version of ONTAP® software supporting the SNMPv3 FIPS feature. FIPS compliance adds more stringent limitations on SNMP users and SNMP traphosts, so SNMPv3 access has been disabled to allow the current SNMP users and SNMP traphosts to be reevaluated. If SNMPv3 functionality is required, you can reenable it; if cluster is still in FIPS mode at that time, any existing SNMP users and SNMP traphosts that are noncompliant to FIPS will be deleted. Until SNMPv3 is reenabled, SNMPv3 users cannot be created, SNMPv3 traphosts cannot be added and SNMPv3 packets will not be processed.

Corrective Action

Enable SNMPv3 in the cluster by using the 'system snmp enable-snmpv3' command.

Syslog Message

SNMPv3 is disabled due to a cluster in FIPS mode being upgraded to a version of ONTAP® software supporting the SNMPv3 FIPS feature.

Parameters

(None).

snmp.traphost events

snmp.traphost.resolve.failed

Severity

ERROR

Description

The snmp daemon could not resolve (find an IP address via DNS for) a traphost. The appliance will try again in an hour to resolve the traphost.

Corrective Action

Make sure that the network, including the domain server and traphost, are connected, running, and configured correctly. If you fix this problem, wait until the next retry or run 'snmp init 1' to force a resolve. If you don’t fix this problem, you may want to remove this traphost from the list. Attempting to resolve traphosts may take time because of network timeouts.

Syslog Message

snmp: cannot send traps to '%s' because it could not be resolved via DNS. Retries occur hourly.

Parameters

host (STRING): The host that could not be resolved via a DNS lookup.

snmp.warmstart events

snmp.warmstart.trap

Severity

INFORMATIONAL

Description

This message occurs when the SNMP daemon is reinitializing itself with a warmStart. A warmStart(1) trap signifies that no configuration changes are made to the agent or the protocol entity implementation during the reinitialization.

Corrective Action

(None).

Syslog Message

SNMP daemon was reinitialized with no configuration changes.

Parameters

(None).

Copyright information

Trademark information