csm events

ONTAP 9.11.1 EMS reference

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-ems-9111/csm-badauthaccess-events.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents

csm events . . . 1
- csm.badauthaccess events . . . 1
- csm.badconnection events . . . 1
- csm.badplainaccess events . . . 2
- csm.ctfallbackactiveopen events . . . 2
- csm.ctfallbackswitchless events . . . 3
- csm.homeportinfounexpected events . . . 3
- csm.mismatchremotedevice events . . . 4
- csm.rdmarecoveractiveopen events . . . 4
- csm.rdmarecoverswitchless events . . . 5
- csm.unmarshallerror events . . . 5

csm events

csm.badauthaccess events

csm.badAuthAccess

Severity

NOTICE

Description

This message occurs when a blade fails an attempt to authenticate as a given peer cluster, and Cluster Session Manager (CSM), which establishes and manages SpinNP sessions between blades in the cluster, denies access of the unauthenticated blade. This could indicate that an interloper is attempting to gain access to the cluster.

Corrective Action

(None).

Syslog Message

Access as peer cluster %s was claimed from network address %s, but has not been granted because %s.

Parameters

clusterUuid (STRING): UUID of the cluster to which the blade claimed to belong.
addrstr (STRING): Remote network address of the blade.
msg (STRING): Reason that access could not be authenticated.

csm.badconnection events

csm.badConnection

Severity

ALERT

Description

This message occurs when ONTAP® software receives a Cluster Session Manager (CSM) connection with unrecognizable content. This might indicate that the system is under attack. As a precaution, the connection used to receive that data has been closed.

Corrective Action

Carefully inspect the networking configuration, event messages, and logs of both the local and remote nodes. If any evidence exists of an intrusion attempt, configure site networking equipment to avoid forwarding data to the local address and port, and if necessary, from forwarding data from the remote address and port. Check external site security tools for unauthorized access attempts. Audit site security logs.

Syslog Message

ONTAP received a CSM connection with unrecognizable content at local address %s local port %d, from remote address %s remote port %d, via IPspace %d.

Parameters

localAddr (STRING): Full internet address of the local end of the connection.
localPort (INT): Local port number.
remoteAddr (STRING): Full internet address of the remote end of the connection.
remotePort (INT): Remote port number.
IPspace (INT): Identifier of the IPspace within which the remote address was reached.

csm.badplainaccess events

csm.badPlainAccess

Severity

NOTICE

Description

This message occurs when a blade attempts to access the local cluster without encrypting its communication channel, and Cluster Session Manager (CSM), which establishes and manages SpinNP sessions between blades in the cluster, denies access of the unencrypted communication channel. This could indicate that an interloper is attempting to gain access to the cluster.

Corrective Action

(None).

Syslog Message

Access as peer cluster %s was claimed from network address %s, but has not been granted because it was not using TLS.

Parameters

clusterUuid (STRING): UUID of the cluster to which the blade claimed to belong.
addrstr (STRING): Remote network address of the blade.

csm.ctfallbackactiveopen events

csm.ctFallbackActiveOpen

Severity

NOTICE

Description

This message occurs when the Cluster Session Manager (CSM) uses CT (TCP transport) as the default when creating LIF pairs because connections running CSM over remote direct memory access (RDMA) repeatedly fail during successive retry attempts.

Corrective Action

(None).

Syslog Message

Cluster Session Manager (CSM) could not successfully create the RDMA connections for session "%s" even after several retry attempts. CSM will use TCP connections as defaults.

Parameters

uniquifier (STRING): Unique identifier for this session.

csm.ctfallbackswitchless events

csm.ctFallbackSwitchless

Severity

NOTICE

Description

This message occurs when the Cluster Session Manager (CSM) defaults to use CT (TCP transport) when creating LIF pairs because remote device ID information is not available on switchless clusters running CSM over remote direct memory access (RDMA).

Corrective Action

(None).

Syslog Message

Cluster Session Manager (CSM) could not determine the cluster ports that are directly connected between the switchless cluster nodes to create the RDMA connections for session "%s". CSM will use TCP connections as defaults.

Parameters

uniquifier (STRING): Unique identifier for this session.

csm.homeportinfounexpected events

csm.homePortInfoUnexpected

Severity

NOTICE

Description

This message occurs when the Cluster Session Manager (CSM) establishes a connection between nodes over the cluster network interface of a switchless cluster and detects that the logical interface’s (LIF’s) home port and the corresponding remote device information are not the expected values.

Corrective Action

This message can occasionally happen during normal operations on a system startup or a LIF migration event. If the message repeats every few minutes, it might indicate a problem in the cluster interface configuration or the physical cabling of the switchless cluster.

Syslog Message

CSM reports unexpected information for cluster LIF ID "%d" (home port: "%s", remote device ID: "%s").

Parameters

vifId (INT): ID of the local cluster LIF over which the connection gets established.
homePort (STRING): Home port hosting the LIF.
remoteDeviceId (STRING): Remote device associated with the home port.

csm.mismatchremotedevice events

csm.mismatchRemoteDevice

Severity

ERROR

Description

The message occurs when the Cluster Session Manager (CSM) establishes a connection between nodes over the cluster network interface, but the node's remote device IDs do not match.

Corrective Action

Ensure that the Cisco Discover Protocol (CDP) is running on the nodes and switches. In addition, ensure that the cluster ports are up and the cluster LIFs are configured and hosted according to the suggested cluster configuration.

Syslog Message

CSM connection between source LIF %d and destination address %s might not be optimal for session %s. The source is currently connected to %s remote device and the destination is currently connected to %s remote device.

Parameters

sourceLIF (INT): Source logical interface.
destAddr (STRING): Destination IP address.
uniquifier (STRING): Unique identifier for this session.
sourceRemoteDevice (STRING): Remote device associated with the source logical interface.
destRemoteDevice (STRING): Remote device associated with the destination IP address.

csm.rdmarecoveractiveopen events

csm.rdmaRecoverActiveOpen

Severity

NOTICE

Description

This message occurs when the Cluster Session Manager (CSM) attempts to restore the use of the preferred remote direct memory access (RDMA) transport for the eligible sessions because the condition which triggered the CSM to use CT (TCP transport) as default might have resolved.

Corrective Action

(None).

Syslog Message

Cluster Session Manager (CSM) is attempting to restore the use of the preferred RDMA connections for eligible sessions, which had previously defaulted to use TCP connections due to repeated active open failures.

Parameters

(None).

csm.rdmarecoverswitchless events

csm.rdmaRecoverSwitchless

Severity

NOTICE

Description

This message occurs when the Cluster Session Manager (CSM) attempts to restore the use of the preferred remote direct memory access (RDMA) transport for the eligible sessions because the condition which triggered the CSM to use CT (TCP transport) as default might have been resolved in the switchless cluster.

Corrective Action

(None).

Syslog Message

Cluster Session Manager (CSM) is attempting to restore the use of the preferred RDMA connections for eligible sessions, which had previously defaulted to use TCP connections in the switchless cluster.

Parameters

(None).

csm.unmarshallerror events

csm.unmarshallError

Severity

ERROR

Description

The message occurs when the Cluster Session Manager (CSM) fails to unmarshal a packet.

Corrective Action

Unmarshal errors reported in CSM indicate corrupted packet(s) were delivered to CSM. Often this can be attributed to network layer problems. TCP checksum errors should be checked for if unmarshal errors continue to increment.

Syslog Message

Cluster Session Manager (CSM) failed to unmarshall packet for session %s.

Parameters

sessionId (STRING): Full session ID of this session.

Copyright information

Copyright © 2024 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.