



crypto events

ONTAP EMS reference

NetApp
November 22, 2024

Table of Contents

- crypto events 1
- crypto.debug events 1
- crypto.export events 1
- crypto.import events 1
- crypto.key events 2
- crypto.okmrecovery events 3
- crypto.ssal events 3

crypto events

crypto.debug events

crypto.debug

Severity

INFORMATIONAL

Description

The Crypto module debug event.

Corrective Action

(None).

Syslog Message

%s.

Parameters

debug_string (STRING): Description of the event being logged.

crypto.export events

crypto.export.failed

Severity

ALERT

Description

This message occurs when the export of a cryptographic key fails.

Corrective Action

This message might be seen when attempting to create an encrypted volume. Contact NetApp technical support if further attempts to create the encrypted volume fail.

Syslog Message

ERROR: Export of key with key ID %s failed. Additional information: %s.

Parameters

key_id (STRING): Key ID for the cryptographic key.

msg (STRING): Associated failure message.

crypto.import events

crypto.import.failed

Severity

ALERT

Description

This message occurs when the import of a cryptographic key fails.

Corrective Action

This message might be seen when attempting to bring an encrypted volume online. Contact NetApp technical support if manual attempts to bring the encrypted volume online fail.

Syslog Message

ERROR: Import of key with key ID %s failed. Additional information: %s.

Parameters

key_id (STRING): Key ID for the cryptographic key.

msg (STRING): Associated failure message.

crypto.key events

crypto.key.deleted

Severity

NOTICE

Description

This message occurs when a cryptographic key is deleted.

Corrective Action

(None).

Syslog Message

Deleted key with key ID %s. Reason %s.

Parameters

key_id (STRING): Key ID for the cryptographic key.

reason (STRING): Reason for deletion.

crypto.key.stored

Severity

NOTICE

Description

This message occurs when a cryptographic key is stored.

Corrective Action

(None).

Syslog Message

Stored key with key ID %s. Key digest: %s.

Parameters

key_id (STRING): Key ID for the cryptographic key.

key_digest (STRING): Key digest for the cryptographic key.

crypto.okmrecovery events

crypto.okmrecovery.failed

Severity

ALERT

Description

This message occurs when the Onboard Key Manager (OKM) recovery command in the boot menu fails to recover the OKM hierarchy. Without the the OKM hierarchy, volumes encrypted using OKM will not come online, and you will not be able to use OKM to encrypt volumes.

Corrective Action

This message is usually seen when an incorrect cluster passphrase was entered during a previous boot menu recovery command. Often, using the "security key-manager onboard sync" command will resolve the situation. If that does not fix the problem, the OKM hierarchy can be recovered during the boot process. To recover the OKM hierarchy during the boot process, enter option 10 ("Set Onboard Key Manager recovery secrets.") at the boot menu prompt. You will need to have the cluster passphrase and a copy of the output from the "security key-manager backup show" command. If the boot menu recovery process fails again, contact NetApp technical support.

Syslog Message

Import of the Onboard Key Manager (OKM) hierarchy has failed: %s. Additional information: %s.

Parameters

failure_msg (STRING): Message describing which operation failed.

additional_msg (STRING): Additional information regarding the failure.

crypto.ssal events

crypto.ssal.failed

Severity

ALERT

Description

This message occurs when a Secure Storage Access Layer(SSAL) operation fails. This might cause import of the onboard key hierarchy to fail and might result in a temporary loss of access to any data secured using the SSAL.

Corrective Action

(Call support).

Syslog Message

SSAL operation failed: %s. %s

Parameters

failure_msg (STRING): Message describing which operation failed.

additional_msg (STRING): Additional information regarding the failure.

crypto.ssal.tpm.clear

Severity

NOTICE

Description

This message occurs when a Trusted Platform Module(TPM) clear operation is performed successfully. A TPM clear operation can happen while reverting to a previous release or when the "security tpm clear" command was executed. A TPM clear operation clears out the TPM and resets it with a new seed for the TPM's storage hierarchy.

Corrective Action

(None).

Syslog Message

A TPM clear operation has been completed successfully.

Parameters

(None).

crypto.ssal.tpm.reset

Severity

NOTICE

Description

This message occurs when a Trusted Platform Module(TPM) reset operation is performed successfully. A TPM reset operation can happen when the node boots up for the first time or when the "security tpm reset" command was executed. A TPM reset operation clears out the TPM and resets it with a new seed for the TPM's storage hierarchy. The TPM then generates a new primary key under the same hierarchy and makes it persistent.

Corrective Action

(None).

Syslog Message

A TPM reset operation has been completed successfully.

Parameters

(None).

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.