



Get an IP address of an external key management server for storage encryption

ONTAP Systems

Barb Einarsen, Aksel Davis, Amanda Stroman, Paula Carrigan
May 10, 2021

This PDF was generated from https://docs.netapp.com/us-en/ontap-systems/upgrade-arl-auto-app/getting_an_ip_address_of_an_external_key_management_server_for_storage_encryption.html on May 12, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Get an IP address of an external key management server for storage encryption 1

Get an IP address of an external key management server for storage encryption

After upgrading, you must immediately configure Storage Encryption and establish a cluster-wide authentication key to replace the previous node-level authentication keys.

Steps

1. Install the necessary client and server secure sockets layer (SSL) certificates required to communicate with key management servers by using the following command:

```
security certificate install
```

2. Configure Storage Encryption on all nodes by using the following command on each node:

```
security key-manager setup
```

3. Add the IP address for each key management server by using the following command:

```
security key-manager add
```

4. Verify that the same key management servers are configured and available on all nodes in the cluster by using the following command:

```
security key-manager show -status
```

5. Create a new cluster-wide authentication key by using the following command:

```
security key-manager create-key
```

6. Make a note of the new authentication key ID.

7. Rekey all self-encrypting drives with the new authentication key by using the following command:

```
storage encryption disk modify -disk * -data-key-id <authentication_key_id>
```

Manage authentication using KMIP servers

With ONTAP 9.8, you can use Key Management Interoperability Protocol (KMIP) servers to manage authentication keys.

Steps

1. Add a new controller by using the following command:

```
security key-manager setup -node <new_controller_name>
```

2. Add the key manager by using the following command:

```
security key-manager -add <key_management_server_ip_address>
```

3. Verify that the key management servers are configured and available to all nodes in the cluster by using the following command:

```
security key-manager show -status
```

4. Restore the authentication keys from all linked key management servers to the new node by using the following command:

```
security key-manager restore -node <new_controller_name>
```

5. Rekey all self-encrypting disks with the new authentication key by using the following command:

```
storage encryption disk modify -disk * [-data-key-id nonMSID AK]
```

6. If you use the Federal Information Processing Standard (FIPS), rekey all self-encrypting disks with the new authentication key by using the following command:

```
storage encryption disk* modify -disk * [-fips-key-id nonMSID AK]
```

Manage storage encryption using Onboard Key Manager

You can use the OKM to manage encryption keys. If you plan to use OKM, you must record the passphrase and backup material before beginning the upgrade.

Steps

1. Save the passphrase to a secure location.
2. Create a backup for recovery purposes. Run the following command and save the output:

```
key-manager onboard show-backup
```

Quiesce the SnapMirror relationships (optional)

Before you proceed with the replacement steps, you must confirm that all the SnapMirror relationships are quiesced. When a SnapMirror relationship is quiesced, it remains quiesced across reboots and failovers.

Steps

1. Verify the SnapMirror relationship status on the destination cluster by using the following command:

```
snapmirror show
```



If the status is **Transferring**, you must abort those transfers by using the following command: `snapmirror abort -destination-vserver <vserver name>`

The abort fails if the SnapMirror relationship is not in the **Transferring** state.

2. Quiesce all relationships between the cluster by using the following command:

```
snapmirror quiesce -destination-vserver <vserver name>
```

Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.