Configure network security using federal information processing standards (FIPS)

ONTAP System Manager

NetApp
December 14, 2020

This PDF was generated from https://docs.netapp.com/us-en/ontap/networking-app/configure_network_security_using_federal_information_processing_standards_@fips@.html on December 17, 2020. Always check docs.netapp.com for the latest.

Table of Contents

Configure network security using federal information processing standards (FIPS) 1

Configure network security using federal information processing standards (FIPS)

ONTAP is compliant in the Federal Information Processing Standards (FIPS) 140-2 for all SSL connections. You can turn on and off SSL FIPS mode, set SSL protocols globally, and turn off any weak ciphers such as RC4 within ONTAP.

By default, SSL on ONTAP is set with FIPS compliance disabled and SSL protocol enabled with the following:

- TLSv1.2
- TLSv1.1
- TLSv1

When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

Enable FIPS

It is recommended that all secure users adjust their security configuration immediately after system installation or upgrade. When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

About this task

The following settings are recommended to enable FIPS:

- `FIPS: on`
- `SSL protocol = {TLSv1.2}`
- `SSL ciphers = {ALL:!LOW:!aNULL:!EXP:!eNULL:!RC4}`

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Enable FIPS:

   ```
   security config modify -interface SSL -is-fips-enabled true
   ```

3. When prompted to continue, enter `y`
4. One by one, manually reboot each node in the cluster.

Example

```
security config modify -interface SSL -is-fips-enabled true
Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y
Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Disable FIPS

If you are still running an older system configuration and want to configure ONTAP with backward compatibility, you can turn on SSLv3 only when FIPS is disabled.

About this task

The following settings are recommended to disable FIPS:

- `FIPS = false`
- `SSL protocol = {SSLv3}`
- `SSL ciphers = {ALL:!LOW:!aNULL:!EXP:!eNULL}`

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

2. Disable FIPS by typing:

   `security config modify -interface SSL -supported-protocols SSLv3`

3. When prompted to continue, enter `y`.
4. Manually reboot each node in the cluster.

Example

```
security config modify -interface SSL -supported-protocols SSLv3
Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y
Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
security config show
ClusterCluster Security
Interface FIPS Mode Supported ProtocolsSupported Ciphers Config Ready
--------- ---------- ---------------------- -----------------
----------------
SSLfalseSSLv3ALL:!LOW:!aNULL: yes
!EXP:!eNULL
```

View FIPS compliance status

You can see whether the entire cluster is running the current security configuration settings.

Steps

1. One by one, reboot each node in the cluster.

   Do not reboot all cluster nodes simultaneously. A reboot is required to make sure that all applications in the cluster are running the new security configuration, and for all changes to FIPS on/off mode, Protocols, and Ciphers.

2. View the current compliance status:

   ```
   security config show
   ```

Example

```
security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ---------------------- -----------------
----------------
SSL       false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL:  yes
                                             !EXP:!eNULL
```

Copyright Information

Copyright © 2020 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.