



Troubleshooting security issues

Snap Creator Framework

NetApp
August 30, 2024

This PDF was generated from https://docs.netapp.com/us-en/snap-creator-framework/administration/reference_transport_layer_security_tls.html on August 30, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Troubleshooting security issues 1
 - Cryptographic flaws in Transport Layer Security 1
 - Self-signed SSL certificate not matching the URL 1
 - CA-signed SSL certificate is required for Snap Creator Framework 2

Troubleshooting security issues

You must be aware of certain security issues in Snap Creator and know how to troubleshoot them.

Cryptographic flaws in Transport Layer Security

- **Issue**

TLS 1.0 has several cryptographic flaws. An attacker might exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

- **Cause**

The remote service accepts connections encrypted by using TLS 1.0.

- **Corrective action**

Snap Creator has an option to enable or disable TLS 1.0 protocol .

- To support backward compatibility, set the `ENABLE_SECURITY_PROTOCOL_TLS_V1` parameter as Y in the `snapcreator.properties` and `agent.properties` files. The `ENABLE_SECURITY_PROTOCOL_TLS_V1` parameter is set as N by default.



The `ENABLE_SECURITY_PROTOCOL_TLS_V1` parameter can only be used in releases earlier than Snap Creator Framework 4.3.3. Because the Snap Creator Framework 4.3.3. release only supports Oracle Java and OpenJDK 1.8 and later, the support for TLS 1.0 was removed from Snap Creator Framework.

Self-signed SSL certificate not matching the URL

- **Issue**

The self-signed SSL certificate provided with Snap Creator Framework does not match the URL.

- **Cause**

The common name (CN) of the SSL certificate presented on the Snap Creator service is for a different machine, and so it does not match the host name.

- **Corrective action**

System IP parameter has been introduced during the installation of Snap Creator Server and Snap Creator Agent to resolve host name.

- Enter the system IP address on which Snap Creator Framework is being installed in the System IP option.
 - The common name of the SSL certificate can be created using the same IP address.

CA-signed SSL certificate is required for Snap Creator Framework

- **Issue**

The Certificate Authority (CA)-signed SSL certificate is required for Snap Creator Framework.

- **Cause**

The server's X.509 certificate does not have a signature from a known public certificate authority.

- **Corrective action**

Snap Creator Framework supports installation of a third-party certificate.

- a. Update the following parameter values in the snapcreator.properties and agent.properties files:

 snapcreator.properties file:

 SNAPCREATOR_KEYSTORE_PASS

 SNAPCREATOR_KEYSTORE_PATH

 agent.properties file:

 KEYSTORE_FILE

 KEYSTORE_PASS

- b. Restart the server and the agent services.

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.