



Configure and enable two-way SSL communication on Linux host

SnapCenter Software 6.0

NetApp
July 23, 2024

Table of Contents

- Configure and enable two-way SSL communication on Linux host 1
- Configure two-way SSL communication on Linux host 1
- Enable SSL communication on Linux host 2

Configure and enable two-way SSL communication on Linux host

Configure two-way SSL communication on Linux host

You should configure the two-way SSL communication to secure the mutual communication between SnapCenter Server on Linux host and the plug-ins.

Before you begin

- You should have configured the CA certificate for Linux host.
- You must have enabled two-way SSL communication on all the plug-in hosts and the SnapCenter Server.

Steps


1. Copy **certificate.pem** to `/etc/pki/ca-trust/source/anchors/`.
2. Add the certificates in the trust list of your Linux host.
 - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
 - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
 - `update-ca-trust extract`
3. Verify if the certificates were added to the trust list. `trust list | grep "<CN of your certificate>"`
4. Update **ssl_certificate** and **ssl_certificate_key** in the SnapCenter **nginx** file and restart.
 - `vim /etc/nginx/conf.d/snapcenter.conf`
 - `systemctl restart nginx`
5. Refresh the SnapCenter Server GUI link.
6. Update the values of the following keys in **SnapManager.Web.UI.dll.config** located at `_/<installation path>/NetApp/snapcenter/SnapManagerWeb_` and **SMCoreServiceHost.dll.config** located at `/<installation path>/NetApp/snapcenter/SMCore`.
 - `<add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />`
 - `<add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>`
7. Restart the following services.
 - `systemctl restart smcore.service`
 - `systemctl restart snapmanagerweb.service`
8. Verify that the certificate is attached to the SnapManager web port. `openssl s_client -connect localhost:8146 -brief`
9. Verify that the certificate is attached to the smcore port. `openssl s_client -connect localhost:8145 -brief`
10. Manage password for SPL keystore and alias.
 - a. Retrieve SPL keystore default password assigned to the **SPL_KEYSTORE_PASS** key in SPL property file.
 - b. Change the keystore password. `keytool -storepasswd -keystore keystore.jks`

- c. Change the password for all the aliases of private key entries. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
 - d. Update the same password for the key **SPL_KEYSTORE_PASS** in *spl.properties*.
 - e. Restart the service.
11. On plug-in Linux host, add the root and intermediate certificates in SPL plug-in's keystore.
- `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
 - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
 - a. Check the entries in keystore.jks. `keytool -list -v -keystore <path to keystore.jks>`
 - b. Rename any alias if required. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepass`
12. Update the value of **SPL_CERTIFICATE_ALIAS** in *spl.properties* file with the alias of **certificate.pfx** stored in *keystore.jks* and restart the SPL service: `systemctl restart spl`
13. Verify that the certificate is attached to the smcore port. `openssl s_client -connect localhost:8145 -brief`

Enable SSL communication on Linux host

You can enable two-way SSL communication to secure the mutual communication between SnapCenter Server on Linux host and the plug-ins using PowerShell commands.

Step

1. Perform the following to enable one-way SSL communication.
 - a. Log into SnapCenter GUI.
 - b. Click **Settings > Global Settings** and select **Enable certificate validation on SnapCenter Server**.
 - c. Click **Hosts > Managed Hosts** and select the plug-in host for which you want to enable one-way SSL.
 - d. Click , and then click **Enable certificate validation**.
2. Enable two-way SSL communication from the SnapCenter Server Linux host.
 - `Open-SmConnection`
 - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
 - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
 - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

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.