



Import CA Certificate to the UNIX host plugins and configure root or intermediate certificates to SPL trust-store

SnapCenter Software 5.0

NetApp
July 18, 2024

Table of Contents

- Import CA Certificate to the UNIX host plug-ins and configure root or intermediate certificates to SPL trust-store 1
- Import CA Certificate to the UNIX plug-in hosts 1
- Configure root or intermediate certificates to SPL trust-store 1

Import CA Certificate to the UNIX host plug-ins and configure root or intermediate certificates to SPL trust-store

Import CA Certificate to the UNIX plug-in hosts

You should import the CA certificate to the UNIX plug-in hosts.

About this task

- You can manage the password for SPL keystore, and the alias of the CA signed key pair in use.
- The password for SPL keystore and for all the associated alias password of the private key should be same.

Steps

1. You can retrieve SPL keystore default password from SPL property file. It is the value corresponding to the key `SPL_KEYSTORE_PASS`.
2. Change the keystore password: `$ keytool -storepasswd -keystore keystore.jks`
3. Change the password for all aliases of private key entries in the keystore to the same password used for the keystore: `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Update the same for the key `SPL_KEYSTORE_PASS` in `spl.properties`` file.
5. Restart the service after changing the password.

Configure root or intermediate certificates to SPL trust-store

You should configure the root or intermediate certificates to SPL trust-store. You should add the root CA certificate and then the intermediate CA certificates.

Steps

1. Navigate to the folder containing the SPL keystore: `/var/opt/snapcenter/spl/etc`.
2. Locate the file `keystore.jks`.
3. List the added certificates in the keystore: `$ keytool -list -v -keystore keystore.jks`
4. Add a root or intermediate certificate: `$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Restart the service after configuring the root or intermediate certificates to SPL trust-store.

Configure CA signed key pair to SPL trust-store

You should configure the CA signed key pair to SPL trust-store.

Steps

1. Navigate to the folder containing the SPL's keystore `/var/opt/snapcenter/spl/etc`.
2. Locate the file `keystore.jks``.
3. List the added certificates in the keystore: `$ keytool -list -v -keystore keystore.jks`
4. Add the CA certificate having both private and public key. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. List the added certificates in the keystore. `$ keytool -list -v -keystore keystore.jks`
6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.
7. Change the added private key password for CA certificate to the keystore password.

Default SPL keystore password is the value of the key `SPL_KEYSTORE_PASS` in `spl.properties` file.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

8. If the alias name in the CA certificate is long and contains space or special characters ("*",","), change the alias name to a simple name: `$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks``
9. Configure the alias name from the keystore located in `spl.properties` file. Update this value against the key `SPL_CERTIFICATE_ALIAS`.
10. Restart the service after configuring the CA signed key pair to SPL trust-store.

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.