



Enable CA certificates for SnapCenter

SnapCenter Software

Soumik Das, Nirupama Sriram
June 14, 2021

This PDF was generated from https://docs.netapp.com/us-en/snapcenter/install/task_enable_ca_certificates_for_snapcenter.html on June 18, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Enable CA certificates for SnapCenter 1

Enable CA certificates for SnapCenter

You should configure the CA certificates and enable the CA certificate validation for the SnapCenter Server.

What you will need

- You can enable or disable the CA certificates using the `Set-SmCertificateSettings` cmdlet.
- You can display the certificate status for the SnapCenter Server using the `Get-SmCertificateSettings` cmdlet.





The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer the [SnapCenter Software Cmdlet Reference Guide](#).

Steps

1. In the Settings page, navigate to **Settings > Global Settings > CA Certificate Settings**.
2. Select **Enable Certificate Validation**.
3. Click **Apply**.

After you finish

The Managed Hosts tab host displays a padlock and the color of the padlock indicates the status of the connection between SnapCenter Server and the plug-in host.

-  indicates that there is no CA certificate enabled or assigned to the plug-in host.
-  indicates that the CA certificate is successfully validated.
-  indicates that the CA certificate could not be validated.
-  indicates that the connection information could not be retrieved.



When the status is yellow or green, the data protection operations completes successfully.

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.