Configure Active Directory, LDAP, and LDAPS

SnapCenter Software 4.9

NetApp
March 20, 2024

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-49/install/task_register_untrusted_active_directory_domains.html on March 20, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Configure Active Directory, LDAP, and LDAPS 1
Register untrusted Active Directory domains 1
Configure CA client certificate for LDAPS 2

Configure Active Directory, LDAP, and LDAPS

Register untrusted Active Directory domains

You should register the Active Directory with SnapCenter Server to manage hosts, users, and groups from multiple untrusted Active Directory domains.

Before you begin

LDAP and LDAPS protocols

- You can register the untrusted active directory domains using either LDAP or LDAPS protocol.
- You should have enabled bidirectional communication between the plug-in hosts and the SnapCenter Server.
- DNS resolution should be set up from the SnapCenter Server to the plug-in hosts and vice-versa.

LDAP protocol

- The fully qualified domain name (FQDN) should be resolvable from SnapCenter Server.

  You can register an untrusted domain with the FQDN. If the FQDN is not resolvable from the SnapCenter Server, you can register with a domain controller IP address and this should be resolvable from SnapCenter Server.

LDAPS protocol

- CA certificates are required for LDAPS to provide end-to-end encryption during the active directory communication.

  Configure CA client certificate for LDAPS

- Domain controller host names (DCHostName) should be reachable from SnapCenter Server.

About this task

- You can use either the SnapCenter user interface, PowerShell cmdlets, or REST API to register an untrusted domain.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Global Settings**..
3. In the Global Settings page, click **Domain Settings**.
4. Click to register a new domain.
5. In the Register New Domain page, select either **LDAP** or **LDAPS**.
   a. If you select **LDAP**, specify the information that is required for registering the untrusted domain for LDAP:

For this field…	Do this…
Domain Name	Specify the NetBIOS name for the domain.
Domain FQDN	Specify the FQDN and click **Resolve**.
Domain controller IP addresses	If the domain FQDN is not resolvable from the SnapCenter Server, specify one or more domain controller IP addresses. For more information, see Add domain controller IP for untrusted domain from GUI.

b. If you select **LDAPS**, specify the information that is required for registering the untrusted domain for LDAPS:

For this field…	Do this…
Domain Name	Specify the NetBIOS name for the domain.
Domain FQDN	Specify the FQDN.
Domain controller Names	Specify one or more domain controller names and click **Resolve**.
Domain controller IP addresses	If the domain controller names is not resolvable from SnapCenter Server, you should rectify the DNS resolutions.

6. Click **OK**.

Configure CA client certificate for LDAPS

You should configure the CA client certificate for LDAPS on the SnapCenter Server when the Windows Active Directory LDAPS is configured with the CA certificates.

Steps

1. Go to the Microsoft management console (MMC), and then click **File** > **Add/Remove Snapin**.
2. In the Add or Remove Snap-ins window, select **Certificates** and then click **Add**.
3. In the Certificates snap-in window, select the **Computer account** option, and then click **Finish**.
4. Click **Console Root** > **Certificates – Local Computer** > **Trusted Root Certification Authorities** > **Certificates**.
5. Right-click on the folder “Trusted Root Certification Authorities”, and then select **All Tasks** > **Import** to start the import wizard.
6. Complete the wizard, as follows:

In this wizard window…	Do the following…
In the second page of the wizard	Click **Browse**, select the *Root Certificate* and click **Next**.
Completing the Certificate Import Wizard	Review the summary, and then click **Finish** to start the import.

7. Repeat Steps 5 and 6 for the intermediate certificates.

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.