



Use directory services

SANtricity 11.8

NetApp
July 26, 2024

Table of Contents

- Use directory services 1
 - Add directory server 1
 - Edit directory server settings and role mappings 3
 - Remove directory server 6

Use directory services

Add directory server

To configure authentication for Access Management, you establish communications between an LDAP server and the host running the Web Services Proxy for Unified Manager. You then map the LDAP user groups to the local user roles.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.
- User groups must be defined in your directory service.
- LDAP server credentials must be available, including the domain name, server URL, and optionally the bind account user name and password.
- For LDAPS servers using a secure protocol, the LDAP server's certificate chain must be installed on your local machine.

About this task

Adding a directory server is a two-step process. First you enter the domain name and URL. If your server uses a secure protocol, you also must upload a CA certificate for authentication if it is signed by a non-standard signing authority. If you have credentials for a bind account, you also can enter your user account name and password. Next, you map the LDAP server's user groups to local user roles.



Steps

1. Select **Access Management**.
2. From the **Directory Services** tab, select **Add Directory Server**.

The Add Directory Server dialog box opens.

3. In the **Server Settings** tab, enter the credentials for the LDAP server.

Field details

Setting	Description
Configuration settings	
Domain(s)	Enter the domain name of the LDAP server. For multiple domains, enter the domains in a comma separated list. The domain name is used in the login (<i>username@domain</i>) to specify which directory server to authenticate against.
Server URL	Enter the URL for accessing the LDAP server in the form of <code>ldap[s]://host:*port*</code> .
Upload certificate (optional)	<div>  <p>This field appears only if an LDAPS protocol is specified in the Server URL field above.</p> </div> <p>Click Browse and select a CA certificate to upload. This is the trusted certificate or certificate chain used for authenticating the LDAP server.</p>
Bind account (optional)	Enter a read-only user account for search queries against the LDAP server and for searching within the groups. Enter the account name in an LDAP-type format. For example, if the bind user is called "bindacct", then you might enter a value such as <code>CN=bindacct,CN=Users,DC=cpoc,DC=local</code> .
Bind password (optional)	<div>  <p>This field appears when you enter a bind account.</p> </div> <p>Enter the password for the bind account.</p>
Test server connection before adding	<p>Select this checkbox if you want to make sure the system can communicate with the LDAP server configuration you entered. The test occurs after you click Add at the bottom of the dialog box.</p> <p>If this checkbox is selected and the test fails, the configuration is not added. You must resolve the error or de-select the checkbox to skip the testing and add the configuration.</p>
Privilege settings	
Search base DN	Enter the LDAP context to search for users, typically in the form of <code>CN=Users, DC=cpoc, DC=local</code> .
Username attribute	Enter the attribute that is bound to the user ID for authentication. For example: <code>sAMAccountName</code> .
Group attribute(s)	Enter a list of group attributes on the user, which is used for group-to-role mapping. For example: <code>memberOf, managedObjects</code> .

- Click the **Role Mapping** tab.
- Assign LDAP groups to the predefined roles. A group can have multiple assigned roles.

Field details

Setting	Description
Mappings	
Group DN	Specify the group distinguished name (DN) for the LDAP user group to be mapped. Regular expressions are supported. These special regular expression characters must be escaped with a backslash (\) if they are not part of a regular expression pattern: \.[]{}()<>*+.=!/?^\$
Roles	<p>Click in the field and select one of the local user roles to be mapped to the Group DN. You must individually select each role you want to include for this group. The Monitor role is required in combination with the other roles to log in to SANtricity Unified Manager. The mapped roles include the following permissions:</p> <ul style="list-style-type: none"> • Storage admin — Full read/write access to storage objects on the arrays, but no access to the security configuration. • Security admin — Access to the security configuration in Access Management and Certificate Management. • Support admin — Access to all hardware resources on storage arrays, failure data, and MEL events. No access to storage objects or the security configuration. • Monitor — Read-only access to all storage objects, but no access to the security configuration.



The Monitor role is required for all users, including the administrator.

- If desired, click **Add another mapping** to enter more group-to-role mappings.
- When you are finished with the mappings, click **Add**.

The system performs a validation, making sure that the storage array and LDAP server can communicate. If an error message appears, check the credentials entered in the dialog box and re-enter the information if necessary.

Edit directory server settings and role mappings

If you previously configured a directory server in Access Management, you can change its settings at any time. Settings include the server connection information and the group-to-role mappings.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access

Management functions do not appear.

- A directory server must be defined.

Steps

1. Select **Access Management**.
2. Select the **Directory Services** tab.
3. If more than one server is defined, select the server you want to edit from the table.
4. Select **View/Edit Settings**.

The Directory Server Settings dialog box opens.

5. In the **Server Settings** tab, change the desired settings.

Field details

Setting	Description
Configuration settings	
Domain(s)	The domain name(s) of the LDAP server(s). For multiple domains, enter the domains in a comma-separated list. The domain name is used in the login (<i>username@domain</i>) to specify which directory server to authenticate against.
Server URL	The URL for accessing the LDAP server in the form of <code>ldap[s]://host:port</code> .
Bind account (optional)	The read-only user account for search queries against the LDAP server and for searching within the groups.
Bind password (optional)	The password for the bind account. (This field appears when a bind account is entered.)
Test server connection before saving	Checks that the system can communicate with the LDAP server configuration. The test occurs after you click Save . If this checkbox is selected and the test fails, the configuration is not changed. You must resolve the error or clear the checkbox to skip the testing and re-edit the configuration.
Privilege settings	
Search base DN	The LDAP context to search for users, typically in the form of <code>CN=Users, DC=cpoc, DC=local</code> .
Username attribute	The attribute that is bound to the user ID for authentication. For example: <code>sAMAccountName</code> .
Group attribute(s)	A list of group attributes on the user, which is used for group-to-role mapping. For example: <code>memberOf, managedObjects</code> .

6. In the **Role Mapping** tab, change the desired mapping.

Field details

Setting	Description
Mappings	
Group DN	The domain name for the LDAP user group to be mapped. Regular expressions are supported. These special regular expression characters must be escaped with a backslash (\) if they are not part of a regular expression pattern: <code>\.[]{}()<>*+~!/?^\$ </code>
Roles	The roles to be mapped to the Group DN. You must individually select each role you want to include for this group. The Monitor role is required in combination with the other roles to log in to SANtricity Unified Manager. The roles include the following: <ul style="list-style-type: none">• Storage admin — Full read/write access to storage objects on the arrays, but no access to the security configuration.• Security admin — Access to the security configuration in Access Management and Certificate Management.• Support admin — Access to all hardware resources on storage arrays, failure data, and MEL events. No access to storage objects or the security configuration.• Monitor — Read-only access to all storage objects, but no access to the security configuration.



The Monitor role is required for all users, including the administrator.

7. If desired, click **Add another mapping** to enter more group-to-role mappings.
8. Click **Save**.

Results

After you complete this task, any active user sessions are terminated. Only your current user session is retained.

Remove directory server

To break the connection between a directory server and the Web Services Proxy, you can remove the server information from the Access Management page. You might want to perform this task if you configured a new server, and then want to remove the old one.

Before you begin

You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

About this task

After you complete this task, any active user sessions are terminated. Only your current user session is retained.

Steps

1. Select **Access Management**.
2. Select the **Directory Services** tab.
3. From the list, select the directory server you want to delete.
4. Click **Remove**.

The Remove Directory Server dialog box opens.

5. Type `remove` in the field, and then click **Remove**.

The directory server configuration settings, privilege settings, and role mappings are removed. Users can no longer log in with credentials from this server.

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.