Manage LDAP

Element Software

Ann-Marie Grissino, Dave Bagwell
August 04, 2021

Table of Contents

Manage LDAP

You can set up the Lightweight Directory Access Protocol (LDAP) to enable secure, directory-based login functionality to SolidFire storage. You can configure LDAP at the cluster level and authorize LDAP users and groups.

Managing LDAP involves setting up LDAP authentication to a SolidFire cluster using an existing Microsoft Active Directory environment and testing the configuration.

You can use both IPv4 and IPv6 addresses.

Enabling LDAP involves the following high-level steps, described in detail:

1. **Complete pre-configuration steps for LDAP support**. Validate that you have all of the details required to configure LDAP authentication.
2. **Enable LDAP authentication**. Use either the Element UI or the Element API.
3. **Validate the LDAP configuration**. Optionally, check that the cluster is configured with the correct values by running the GetLdapConfiguration API method or by checking the LCAP configuration using the Element UI.
4. **Test the LDAP authentication** (with the `readonly` user). Test that the LDAP configuration is correct either by running the TestLdapAuthentication API method or by using the Element UI. For this initial test, use the username “sAMAccountName” of the `readonly` user. This will validate that your cluster is configured correctly for LDAP authentication and also validate that the `readonly` credentials and access are correct. If this step fails, repeat steps 1 through 3.
5. **Test the LDAP authentication** (with a user account that you want to add). Repeat setp 4 with a user account that you want to add as an Element cluster admin. Copy the `distinguished` name (DN) or the user (or the group). This DN will be used in step 6.
6. **Add the LDAP cluster admin** (copy and paste the DN from the Test LDAP authentication step). Using either the Element UI or the AddLdapClusterAdmin API method, create a new cluster admin user with the appropriate access level. For the username, paste in the full DN you copied in Step 5. This assures that the DN is formatted correctly.
7. **Test the cluster admin access**. Log in to the cluster using the newly created LDAP cluster admin user. If you added an LDAP group, you can log in as any user in that group.

Complete pre-configuration steps for LDAP support

Before you enable LDAP support in Element, you should set up a Windows Active Directory Server and perform other pre-configuration tasks.

Steps

1. Set up a Windows Active Directory Server.
2. **Optional:** Enable LDAPS support.
3. Create users and groups.
4. Create a read-only service account (such as “sfreadonly”) to be used for searching the LDAP directory.

Enable LDAP authentication with the Element user interface

You can configure storage system integration with an existing LDAP server. This enables LDAP administrators to centrally manage storage system access for users.

You can configure LDAP with either the Element user interface or the Element API. This procedure describes how to configure LDAP using the Element UI.

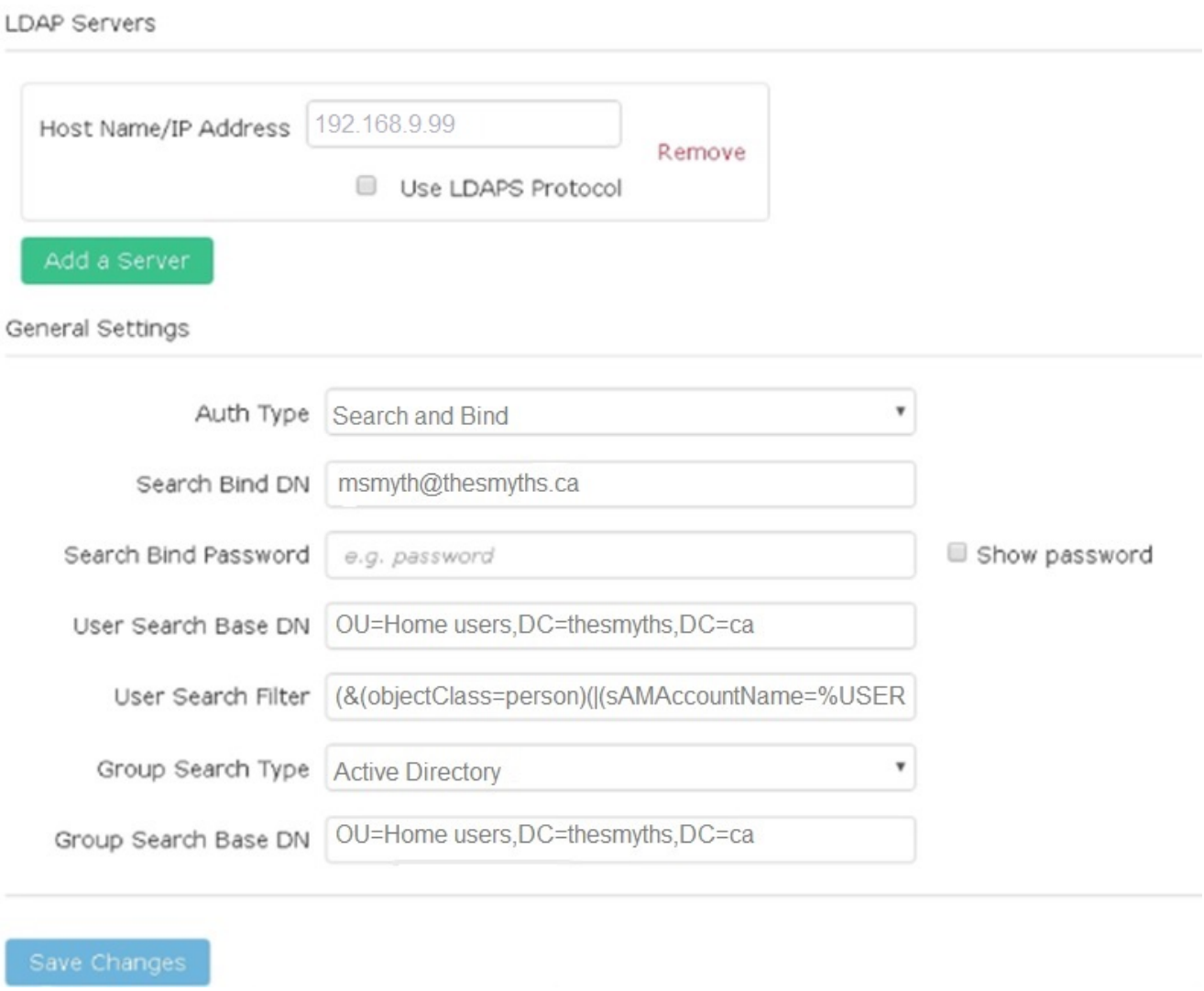
This example shows how to configure LDAP authentication on SolidFire and it uses `SearchAndBind` as the authentication type. The example uses a single Windows Server 2012 R2 Active Directory Server.

Steps

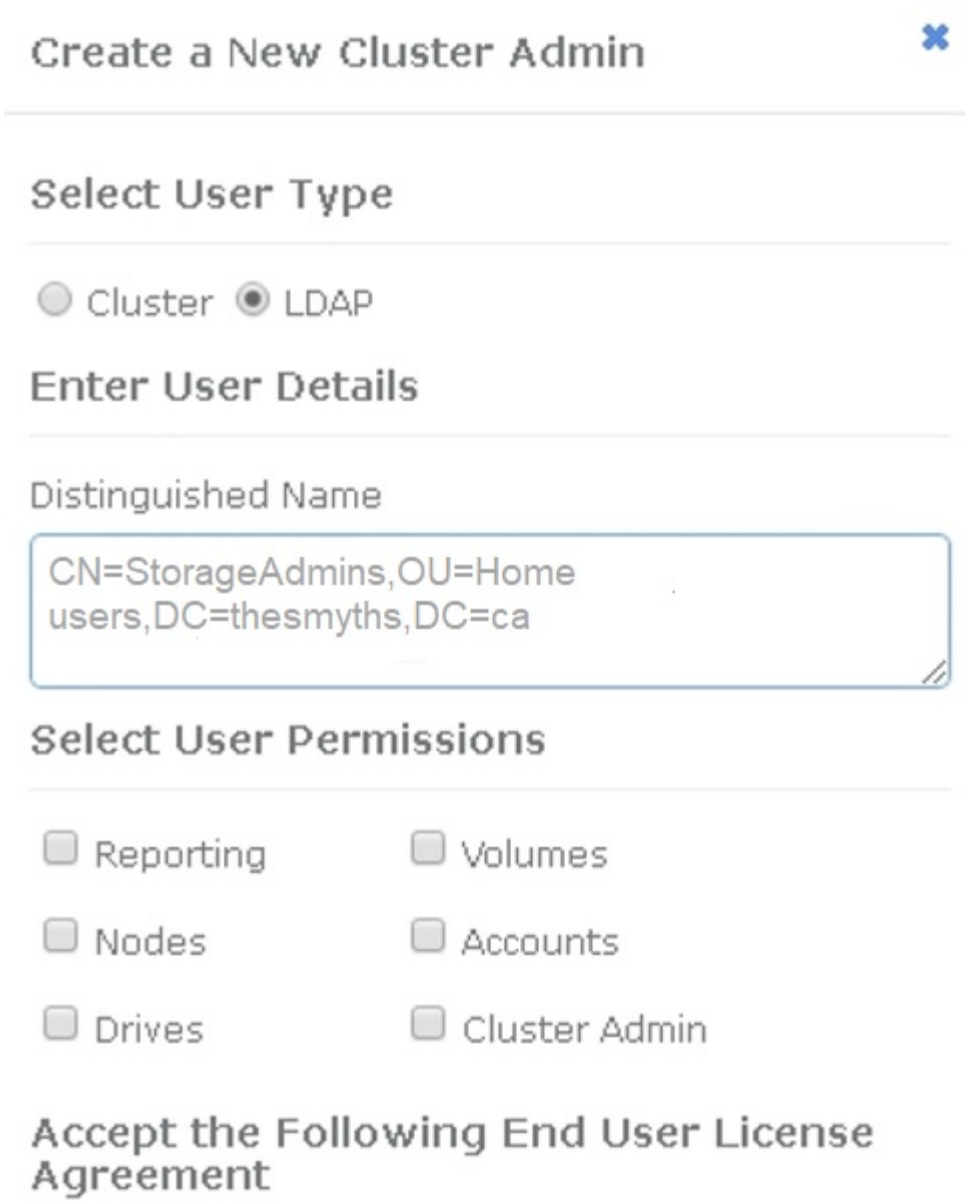
1. Click **Cluster** > **LDAP**.
2. Click **Yes** to enable LDAP authentication.
3. Click **Add a Server**.
4. Enter the **Host Name/IP Address**.

   An optional custom port number can also be entered.

   For example, to add a custom port number, enter <host name or ip address>:<port number>
5. **Optional:** Select **Use LDAPS Protocol**.
6. Enter the required information in **General Settings**.



7. Click **Enable LDAP**.
8. Click **Test User Authentication** if you want to test the server access for a user.
9. Copy the distinguished name and user group information that appears for use later when creating cluster administrators.
10. Click **Save Changes** to save any new settings.
11. To create a user in this group so that anyone can log in, complete the following:
    a. Click **User** > **View**.



b. For the new user, click **LDAP** for the User Type, and paste the group you copied to the Distinguished Name field.
c. Select the permissions, typically all permissions.
d. Scroll down to the End User License Agreement and click **I accept**.
e. Click **Create Cluster Admin**.

   Now you have a user with the value of an Active Directory group.

To test this, log out of the Element UI and log back in as a user in that group.

Enable LDAP authentication with the Element API

You can configure storage system integration with an existing LDAP server. This enables LDAP administrators to centrally manage storage system access for users.

You can configure LDAP with either the Element user interface or the Element API. This procedure describes

how to configure LDAP using the Element API.

To leverage LDAP authentication on a SolidFire cluster, you enable LDAP authentication first on the cluster using the `EnableLdapAuthentication` API method.

Steps

1. Enable LDAP authentication first on the cluster using the `EnableLdapAuthentication` API method.
2. Enter the required information.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Change the values of the following parameters:

Parameters used	Description
authType: SearchAndBind	Dictates that the cluster will use the readonly service account to first search for the user being authenticated and subsequently bind that user if found and authenticated.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Specifies the location in the LDAP tree to begin searching for groups. For this example, we've used the root of our tree. If your LDAP tree is very large, you might want to set this to a more granular sub-tree to decrease search times.
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Specifies the location in the LDAP tree to begin searching for users. For this example, we've used the root of our tree. If your LDAP tree is very large, you might want to set this to a more granular sub-tree to decrease search times.

Parameters used	Description
groupSearchType: ActiveDirectory	Uses the Windows Active Directory server as the LDAP server.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
To use the userPrincipalName (email address for login) you could change the userSearchFilter to:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Or, to search both userPrincipalName and sAMAccountName, you can use the following userSearchFilter:
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

Leverages the sAMAccountName as our username for logging in to the SolidFire cluster. These settings tell LDAP to search for the username specified during login in the sAMAccountName attribute and also limit the search to entries that have “person” as a value in the objectClass attribute.	searchBindDN
This is the distinguished name of readonly user that will be used to search the LDAP directory. For active directory it’s usually easiest to use the userPrincipalName (email address format) for the user.	searchBindPassword

To test this, log out of the Element UI and log back in as a user in that group.

View LDAP details

View LDAP information on the LDAP page on the Cluster tab.

> You must enable LDAP to view these LDAP configuration settings.

1. To view LDAP details with the Element UI, click **Cluster** > **LDAP**.
   - **Host Name/IP Address**: Address of an LDAP or LDAPS directory server.

- **Auth Type**: The user authentication method. Possible values:
  - Direct Bind
  - Search And Bind
- **Search Bind DN**: A fully qualified DN to log in with to perform an LDAP search for the user (needs bind-level access to the LDAP directory).
- **Search Bind Password**: Password used to authenticate access to the LDAP server.
- **User Search Base DN**: The base DN of the tree used to start the user search. The system searches the subtree from the specified location.
- **User Search Filter**: Enter the following using your domain name:

  ```
  (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
  ```

- **Group Search Type**: Type of search that controls the default group search filter used. Possible values:
  - Active Directory: Nested membership of all of a user's LDAP groups.
  - No Groups: No group support.
  - Member DN: Member DN-style groups (single-level).
- **Group Search Base DN**: The base DN of the tree used to start the group search. The system searches the subtree from the specified location.
- **Test User Authentication**: After LDAP is configured, use this to test the user name and password authentication for the LDAP server. Enter an account that already exists to test this. The distinguished name and user group information appears, which you can copy for later use when creating cluster administrators.

Test the LDAP configuration

After configuring LDAP, you should test it by using either the Element UI or the Element API `TestLdapAuthentication` method.

Steps

1. To test the LDAP configuration with the Element UI, do the following:
   a. Click **Cluster** > **LDAP**.
   b. Click **Test LDAP Authentication**.
   c. Resolve any issues by using the information in the table below:

Error message	Description
`xLDAPUserNotFound`	• The user being tested was not found in the configured `userSearchBaseDN` subtree. • The `userSearchFilter` is configured incorrectly.

Error message	Description
`xLDAPBindFailed (Error: Invalid credentials)`	• The username being tested is a valid LDAP user, but the password provided is incorrect. • The username being tested is a valid LDAP user, but the account is currently disabled.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	The LDAP server URI is incorrect.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	The read-only username or password is configured incorrectly.
`xLDAPSearchFailed (Error: No such object)`	The `userSearchBaseDN` is not a valid location within the LDAP tree.
`xLDAPSearchFailed (Error: Referral)`	• The `userSearchBaseDN` is not a valid location within the LDAP tree. • The `userSearchBaseDN` and `groupSearchBaseDN` are in a nested OU. This can cause permission issues. The workaround is to include the OU in the user and group base DN entries, (for example: `ou=storage, cn=company, cn=com`)

2. To test the LDAP configuration with the Element API, do the following:
   a. Call the TestLdapAuthentication method.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

   b. Review the results. If the API call is successful, the results include the specified user's distinguished name and a list of groups in which the user is a member.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Disable LDAP

You can disable LDAP integration using the Element UI.

Before you begin, you should note all the configuration settings, because disabling LDAP erases all settings.

Steps

1. Click **Cluster** > **LDAP**.
2. Click **No**.
3. Click **Disable LDAP**.

Find more information

- SolidFire and Element Resources page
- NetApp Element Plug-in for vCenter Server