LDAP API methods

Element Software

NetApp
October 01, 2024

Table of Contents

LDAP API methods

You can use the Lightweight Directory Access Protocol (LDAP) to authenticate access to Element storage. The LDAP API methods described in this section enable you to configure LDAP access to the storage cluster.

- AddLdapClusterAdmin
- EnableLdapAuthentication
- DisableLdapAuthentication
- GetLdapConfiguration
- TestLdapAuthentication

Find more information

- SolidFire and Element Software Documentation
- Documentation for earlier versions of NetApp SolidFire and Element products

AddLdapClusterAdmin

You can use the `AddLdapClusterAdmin` to add a new LDAP cluster administrator user. An LDAP cluster administrator can manage the cluster using the API and management tools. LDAP cluster admin accounts are completely separate and unrelated to standard tenant accounts.

Parameters

You can also use this method to add an LDAP group that has been defined in Active Directory®. The access level that is given to the group is passed to the individual users in the LDAP group.

This method has the following input parameters:

Name	Description	Type	Default value	Required
access	Controls which methods this cluster admin can use.	string array	None	Yes
acceptEula	Accept the End User License Agreement. Set to true to add a cluster administrator account to the system. If omitted or set to false, the method call fails.	boolean	None	Yes

Name	Description	Type	Default value	Required
attributes	List of name-value pairs in JSON object format.	JSON object	None	No
username	The distinguished user name for the new LDAP cluster admin.	string	None	Yes

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "AddLdapClusterAdmin",
  "params": {"username":"cn=mike
jones,ou=ptusers,dc=prodtest,dc=solidfire,dc=net",
    "access": ["administrator", "read"
    ]
  },
"id": 1
}
```

Response example

This method returns a response similar to the following example:

```
{
 "id": 1,
 "result": {}
}
```

New since version

9.6

Find more information

Access control

EnableLdapAuthentication

You can use the `EnableLdapAuthentication` method to configure an LDAP directory connection for LDAP authentication to a cluster. Users that are members of the LDAP directory can then log in to the storage system using their LDAP credentials.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
authType	Identifies which user authentication method to use. Possible values: • `DirectBind` • `SearchAndBind`	string	SearchAndBind	No
groupSearchBaseDN	The base DN of the tree to start the group subtree search.	string	None	No
groupSearchType	Controls the default group search filter used. Possible values: • NoGroups: No group support. • ActiveDirectory: Nested membership of all of a user's active directory groups. • MemberDN: MemberDN style groups (single level).	string	ActiveDirectory	No

Name	Description	Type	Default value	Required
serverURIs	A comma-separated list of LDAP or LDAPS server URIs. You can add a custom port to the end of an LDAP or LDAPS URI by using a colon followed by the port number. For example, the URI "ldap://1.2.3.4" uses the default port and the URI "ldaps://1.2.3.4:123" uses the custom port 123.	string array	None	Yes
userSearchBaseDN	The base DN of the tree to start the subtree search. This parameter is required when using an authType of SearchAndBind.	string	None	No
searchBindDN	A fully qualified DN to log in with to perform an LDAP search for the user. The DN requires read access to the LDAP directory. This parameter is required when using an authType of SearchAndBind.	string	None	Yes
searchBindPassword	The password for the searchBindDN account used for searching. This parameter is required when using an authType of SearchAndBind.	string	None	Yes

Name	Description	Type	Default value	Required
userSearchFilter	The LDAP search filter to use when querying the LDAP server. The string should have the placeholder text "%USERNAME%" which is replaced with the username of the authenticating user. For example, (&(objectClass=person)(sAMAccountName=%USERNAME%)) will use the sAMAccountName field in Active Directory to match the username entered at cluster login. This parameter is required when using an authType of SearchAndBind.	string	None	Yes
userDNTemplate	A string template used to define a pattern for constructing a full user distinguished name (DN). The string should have the placeholder text "%USERNAME%" which is replaced with the username of the authenticating user. This parameter is required when using an authType of DirectBind.	string	None	Yes

Name	Description	Type	Default value	Required
groupSearchCustomFilter	For use with the CustomFilter search type, an LDAP filter to use to return the DNs of a user's groups. The string can have placeholder text of %USERNAME% and %USERDN% to be replaced with their username and full userDN as needed.	string	None	Yes

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "EnableLdapAuthentication",
  "params": {
     "authType": "SearchAndBind",
     "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
     "groupSearchType": "ActiveDirectory",
     "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
     "searchBindPassword": "zsw@#edcASD12",
     "sslCert": "",
     "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
     "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))",
     "serverURIs":[
           "ldaps://111.22.333.444",
           "ldap://555.66.777.888"
           ]
       },
  "id": 1
}
```

Response example

This method returns a response similar to the following example:

```
{
"id": 1,
"result": {
  }
}
```

New since version

9.6

DisableLdapAuthentication

You can use the `DisableLdapAuthentication` method to disable LDAP authentication and remove all LDAP configuration settings. This method does not remove any configured cluster admin accounts for users or groups. After LDAP authentication has been disabled, cluster admins that are configured to use LDAP authentication can no longer access the cluster.

Parameters

This method has no input parameters.

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "DisableLdapAuthentication",
  "params": {},
"id": 1
}
```

Response example

This method returns a response similar to the following example:

```
{
"id": 1,
"result": {}
}
```

New since version

9.6

GetLdapConfiguration

You can use the `GetLdapConfiguration` method to get the currently active LDAP configuration on the cluster.

Parameters

This method has no input parameters.

Return value

This method has the following return value.

Name	Description	Type
ldapConfiguration	List of the current LDAP configuration settings. This API call does not return the plain text of the search account password. **Note:** If LDAP authentication is currently disabled, all the returned settings are empty with the exception of "authType", and "groupSearchType" which are set to "SearchAndBind" and "ActiveDirectory" respectively.	ldapConfiguration

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetLdapConfiguration",
  "params": {},
  "id": 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id": 1,
  "result": {
    "ldapConfiguration": {
        "authType": "SearchAndBind",
        "enabled": true,
        "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
        "groupSearchCustomFilter": "",
        "groupSearchType": "ActiveDirectory",
        "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
        "serverURIs": [
           "ldaps://111.22.333.444",
           "ldap://555.66.777.888"
            ],
        "userDNTemplate": "",
        "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
        "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
     }
   }
}
```

New since version

9.6

TestLdapAuthentication

You can use the `TestLdapAuthentication` method to validate the currently enabled LDAP authentication settings. If the configuration is correct, the API call returns the group membership of the tested user.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
username	The username to be tested.	string	None	Yes

Name	Description	Type	Default value	Required
password	The password for the username to be tested.	string	None	Yes
ldapConfiguration	An ldapConfiguration object to be tested. If you provide this parameter, the system tests the provided configuration even if LDAP authentication is currently disabled.	ldapConfiguration	None	No

Return values

This method has the following return values:

Name	Description	Type
groups	List of LDAP groups that include the tested user as a member.	array
userDN	The tested user's full LDAP distinguished name.	string

Request example

Requests for this method are similar to the following example:

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

Response example

This method returns a response similar to the following example:

```
{
 "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"
  }
}
```

New since version

9.6

Copyright information

Trademark information