LDAP authentication

As of version 6.0.20, Redis Enterprise Software integrates Lightweight Directory Access Protocol (LDAP) authentication and authorization into its role-based access controls (RBAC). You can now use LDAP to authorize access to the admin console and to authorize database access.

Furthermore, you can configure LDAP roles using the admin console or the Redis Software REST API.

Previously, you could enable LDAP authentication for admin console users by configuring a cluster either through the command-line or the REST API.

The cluster-based LDAP mechanism is supported in v6.0.20; however, the mechanism is deprecated and will be removed in a future update.

Note that the cluster-based mechanism is not compatible with the new role-based approach. You can use either for now, but not both at the same time.

If you are using the earlier LDAP mechanism, you will need to migrate to role-based LDAP at some point in the near future. For help, see Migrate to role-based LDAP.

How it works

Here's how role-based LDAP integration works:

1. User signs in using their LDAP credentials.
   
   Based on the LDAP configuration details, the username is mapped to an LDAP Distinguished Name.

2. A simple LDAP bind request is attempted using the Distinguished Name and the password. The sign-in fails if the bind fails.

3. Obtain user's LDAP group memberships.
   
   Using configured LDAP details, obtain a list of the user's group memberships.

4. Compare the user's LDAP group memberships to those mapped to local roles.

5. Determine if one of the user's groups is authorized to access the target resource. If so, the user is granted the level of access authorized to the role.

To access the admin console, the user needs to belong to an LDAP group mapped to an Administrative role.

For database access, the user needs to belong to an LDAP group mapped to a role listed in database's access control list (ACL). The rights granted to the group determine the user's level of access.

Prerequisites

Before enabling LDAP in Redis Software, you should verify a few things:

1. You'll need to know the LDAP groups that correspond to the levels of access you wish to authorize. Each LDAP group will be mapped to a Redis Software access control role.

2. You'll also need a Redis Software access control role for each LDAP group. If you haven't already set up role-based access controls (RBAC), you should do so before enabling LDAP.
3. Finally, you need the following LDAP info:

- Server URI, including host, port, and protocol details.
- Certificate details for secure protocols.
- Bind credentials, including Distinguished Name, password, and (optionally) client public and private keys for certificate authentication.
- Authentication query details, whether template or query.
- Authorization query details, whether attribute or query.
- The Distinguished Names of LDAP groups you’ll use to authorize access to Redis Software resources.

**How to enable LDAP**

Once everything’s in place, you should:

1. Use Settings | LDAP to enable LDAP access.
2. Map LDAP groups to access control roles.
3. Update database access control lists (ACLs) to authorize role access.

If you already have appropriate roles, you can update them to include LDAP groups.

**Related info**

- Enable and configure role-based LDAP
- Map LDAP groups to access control roles
- Update database ACLs to authorize LDAP access
- Learn more about Redis Software security & practices

**Updated:** April 13, 2021