READ-ONLY ACTIVE DIRECTORY WITH WEBADM

Read-Only Active Directory with WebADM

Active Directory

How To Configure WebADM with a Read-Only Active Directory

Important Note

An entreprise license is mandatory for that setup since WebADM 1.6.6

In some circumstances, we can not write in the LDAP backend. In that case, we need to store some configurations in a local LDAP database and users extra information in a SQL database.

In this example, we will start with a WebADM server running with a local MariaDB and RCDevs Directory Server. It could be the VMWare Appliance or a new installation WebADM Installation Guide. We will configure it to use a read-only Active Directory server.

1. WebADM Configuration

We edit `/opt/webadm/conf/webadm.conf` and change `webadm_account_oclasses` and `webadm_group_oclasses` parameters. It should contain the following class:

```
webadm_account_oclasses "person"
webadm_group_oclasses "group", "groupOfNames", "groupOfUniqueNames", "groupOfURLs",
"posixGroup"
```

We change also the data store to SQL:

```
data_store SQL
```

We restart WebADM:

```
/opt/webadm/bin/webadm restart
```

2. Container Creation

In WebADM, we create a container for the mount point. We click on `Create`, we select `Domain` and we click on `Proceed`:

We enter a name for the domain, for example, *test*, and we click on `Proceed`:

We click on `Create Object`:

3. Mount Point Creation

To create a Mount Point, click on `Admin` tab and click on `LDAP Mount Points` box:

We click on `Add MountPoint`:

We add a name and click on `Proceed`:

We click on `Create Object`:

We click on `Select` and choose the container previously created for *Mount DN*. Now, we add the IP address of the Active Directory server in *Host Name(s)* field, the port number, the tree base of the AD and AD user and password to connect to the LDAP.

> **Note**
>
> The AD user should have read access on the Active Directory.

We click on `Apply`:

4. Local Domain Creation

Now, we create a local domain for the mount point. A local domain works only with one LDAP backend, so the default local domain works only with OpenLDAP.

We click on `Admin` tab and on `Local Domains` box:

Click on `Add Domain`:

We enter the name of the domain and click on `Proceed`.

Click on `Create Object`:

We select the mount point as *User Search Base*. We can add domain name aliases, like *test.local* if needed, and we click on `Apply`:

It's done:

Now, we can try an authentication by following this documentation Authentication. We need to select the right local domain during the authentication. Otherwise, OpenOTP won't be able to find the user.