Configure Remote Authentication (remoteauth)

The remoteauth overlay to slapd provides pass-through authentication to remote directory servers, e.g. Active Directory, for LDAP simple bind operations. The local LDAP entry referenced in the bind operation is mapped to its counterpart in the remote directory. An LDAP bind operation is performed against the remote directory, and results are returned based on those of the remote operation.

A slapd server configured with the remoteauth overlay handles an authentication request based on whether the authenticating entry contains the userPassword attribute. If the authenticating entry does not contain the userPassword attribute, the slapd server performs the authentication request to the remote directory server. On the other hand, authentication is performed locally, if the authenticating entry contains the userPassword attribute.

The remoteauth overlay requires the remoteauth.schema be included and the remoteauth module to be loaded in `/opt/symas/etc/openldap/slapd.conf`.

```
include       /opt/symas/etc/openldap/schema/remoteauth.schema

moduleload    remoteauth.la
```

Configuration Options

The following options can be applied to the remoteauth overlay within the slapd.conf file. All options should follow the overlay remoteauth directive.

overlay remoteauth

This directive adds the remoteauth overlay to the current database, see slapd.conf(5) for details.

remoteauth_dn_attribute <dnattr>

Attribute in entry that is used to store the bind DN to a remote directory server. For Active Directory, this should map to the userPrincipalName attribute.

remoteauth_mapping <domain> <hostname|file://path/to/list_of_hostnames>

For a non-Windows deployment, a domain can be considered as a collection of one or more hosts to which slapd server authenticates against on behalf of authenticating users. For a given domain name, the mapping specifies the target server(s), e.g., Active Directory domain controller(s), to connect to via LDAP.

The second argument can be given either as a hostname, or a file containing a list of hostnames, one per line. The hostnames are tried in sequence until the connection succeeds.

This option can be provided more than once to provide mapping information for different domains. For example,

```
remoteauth_mapping  example       file:///path/to/example.hosts
```

Example `example.hosts` content

```
dc1.example.com
dc2.example.com
dc3.example.com
dc4.example.com
```

remoteauth_domain_attribute <attr>

Attribute in entry that specifies the domain name. For Windows, the ntUserDomainID attribute can be used, because any text after "\" or ":" is ignored.

remoteauth_default_domain <default domain>

Default domain (Can be used in place of the remoteauth_domain_attribute)

remoteauth_default_realm <server>

Fallback server to connect to for domains not specified in remoteauth_mapping

remoteauth_cacert_dir <directory>

Hashed trusted CA directory. Defaults to OpenLDAP configuration.

remoteauth_cacert_file <CA cert>

Trusted CAs in PEM format. Defaults to OpenLDAP configuration.

remoteauth_starttls <on|off>

Issue StartTLS request at beginning of session. Default is on.

remoteauth_validate_certs <on|off>

Enable/disable validation of remote server certificate. Default is on.

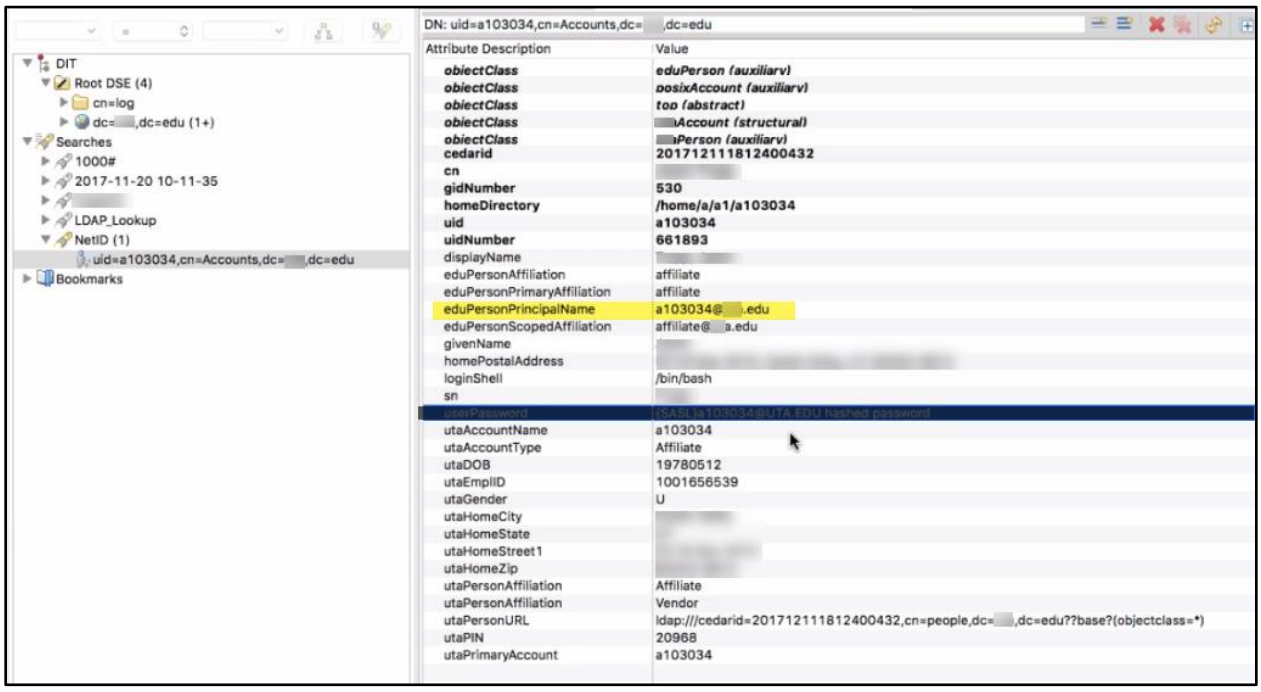
remoteauth_retry_count <num>

Number of connection retries attempted. Default is 3.

Example Configuration

```
overlay remoteauth
remoteauth_mapping  EXAMPLE      file:///opt/symas/etc/openldap/hosts
remoteauth_dn_attribute          eduPersonPrincipalName
remoteauth_domain_attribute      dc
remoteauth_default_domain        EXAMPLE
remoteauth_validate_certs        no
remoteauth_starttls              TRUE
remoteauth_cacert_file           /opt/symas/ssl/CA-cert.pem
```

LDAP Database User Entry

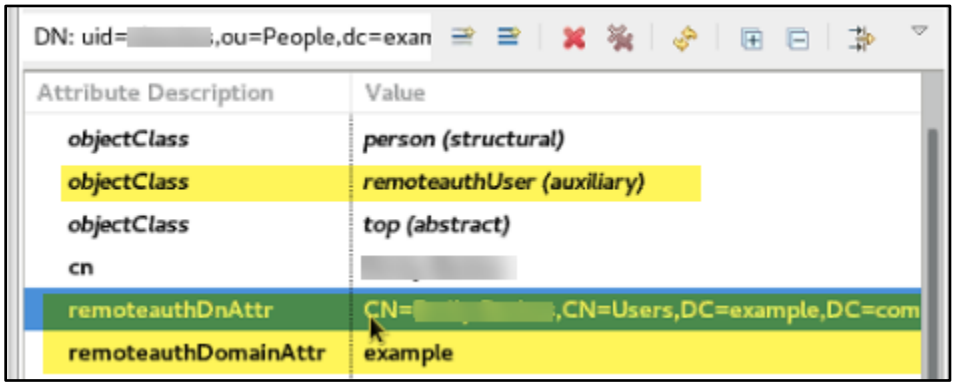


The `remoteauth_dn_attribute` setting needs to point to an attribute in the LDAP database that contains the expected backed (i.e. Active Directory) username.

Note: LDAP Database entries configured to pass through authentication should **NOT** contain a userPassword attribute. If the userPassword attribute is present, LDAP will attempt to authenticate using that value instead of passing the authentication task and password to the specified backend.

Adding Remoteauth Attributes to LDAP Database

In the event no attribute exists in that OpenLDAP database that contains the expected username or domain, simply add the `remoteauthUser` object class to the entry. This will create two new attributes which can then be populated with the requisite data, `remoteauthDnAttr` and `remoteauthDomainAttr`.



Then direct `remoteauth_dn_attribute` and `remoteauth_domain_attribute` options in the remoteauth overlay configuration to these new attributes.