1 Configuration

The following process allows you to configure exacqVision permissions and privileges for accounts that exist on an OpenLDAP/Kerberos server:

1. On the OpenLDAP/Kerberos server, ensure that your installed schema includes the following object types:

    - **inetOrgPerson** (RFC 2798)
    - **organization** (RFC 2256)
    - **krbPrincipalAux** (provided by the Ubuntu krb5-kdc-ldap package)

2. On the OpenLDAP/Kerberos server, ensure that your user accounts exist as inetOrgPerson objects, and that each account is also marked with the krbPrincipalAux auxiliary object type. Ensure that each user account has the following attribute values:

    - **cn** -- the user account's display name (for example, "John Smith").
    - **krbPrincipalName** -- the user account's Kerberos principal name (for example, "john.smith@REALM").
    - **entryUUID** -- the unique identifier for the user account, managed by the slapd daemon

3. On the OpenLDAP/Kerberos server, ensure that your user groups exist as organization objects and that each group has the following attribute values:

    - **o** -- the group's display name (for example, "Marketing")
    - **entryUUID** -- the unique identifier for the group, managed by the slapd daemon

4. On the OpenLDAP/Kerberos server, ensure that your user accounts are associated with groups via an "o" attribute for each group. Each inetOrgPerson object can have as many associated "o" attribute values as desired. The attribute value should resemble "o=Engineers", for example, instead of "o=Engineers,dc=exacq,dc=test,dc=com."

If installing an exacqVision server, complete steps 5 through 10. Otherwise, skip to step 11.

5. On the exacqVision server or client computer, configure your DNS domain name. Configure the hostname file with your fully qualified host name, as in the following example:

    ```
    /etc/hostname
    evserver.exacq.test.com.
    ```

6. Edit your hosts file with your fully qualified host name preceding localhost, as in the following example:

    ```
    /etc/hosts
    127.0.0.1 evserver.exacq.test.com localhost
    ```

7. Restart the system.

8. Open a terminal window and confirm the fully qualified host name using the following command:

    ```
    dnsdomainname --fqdn
    ```

9. If installing an exacqVision server, add a service principal name on the OpenLDAP/Kerberos server for the exacqVision server. To do this, open a terminal window on the OpenLDAP/Kerberos server and execute the following command (using your information where appropriate):

```
sudo kadmin.local
ank –e rc4-hmac:normal EDVR/evserver.exacq.test.com
ktadd –k ./ev.keytab EDVR/evserver.exacq.test.com
quit
```

   NOTE: All text after the forward slash should be lower case, and "EDVR" must be upper case.

10. Copy the keytab file to a location from where it can be installed on the Linux exacqVision Server later in this procedure.

The following steps apply to all situations.

11. Note the fully qualified host name (*hostname.primary-dns-suffix*) and IP address of the exacqVision server computer that you will connect to, the OpenLDAP/Kerberos domain, and the fully qualified host name and IP address of the OpenLDAP/Kerberos server. For example:

```
evserver.exacq.test.com       192.168.1.16
EXACQ.TEST.COM
kdc.exacq.test.com            192.168.1.70
```

12. If necessary, install Kerberos. It is recommended that you use MIT Kerberos V5, also known as KRB5. Installing krb5-user also installs krb5-config, which is valid for all Ubuntu variations. To install KRB5 (or to verify that it is already installed), go to the Start menu and select System, Administrator, and Symptic Package Manager. Click Reload. Search for krb5-user; if it is not already checked, install it.

   NOTE: If you purchased the system from Exacq after 2009, MIT Kerberos V5 is likely already installed.

13. Make sure the fully qualified host names of the OpenLDAP/Kerberos server and exacqVision server can be resolved. To do this, open a terminal window, ping the fully qualified host names, and look for a reply. Make sure the IP addresses match the IP addresses of the servers as noted in the previous step.

   NOTE: If the fully qualified host names cannot be resolved for either server, configure your hosts file with the fully qualified host names, as in the following example:

```
/etc/hosts
192.168.1.16      evserver.exacq.test.com
192.168.1.70      kdc.exacq.test.com
```

   Alternatively, you can add the OpenLDAP/Kerberos server to the DNS Server list. To do this, go to the Start menu and select System, Administrators, and Network.

14. Configure the /etc/krb5.conf file. To do this, add a stanza for your OpenLDAP/Kerberos domain and make the OpenLDAP/Kerberos domain the default realm. For example:

    ```
    [libdefaults]

          default_realm = EXACQ.TEST.COM
    ...

    [realms]
          EXACQ.TEST.COM = {
                kdc = kdc.exacq.test.com
                admin_server = kdc.exacq.test.com
                }
    ```

    NOTE: Using fully qualified host names instead of IP addresses is recommended because IP addresses can be subject to change. Also, be sure you enter the OpenLDAP/Kerberos domain name in upper case, as shown in the example.

15. Make sure the Kerberos configuration works correctly. Use the *kinit* command to obtain a ticket for your Kerberos login, and then verify it using *klist*. To release the ticket, use *kdestroy*.

16. If desired, download and install the exacqVision Client software on the exacqVision client computer from www.exacq.com. You must be logged in with root privileges to do this.

If installing an exacqVision server, complete the following steps. Otherwise, skip to “Connecting to exacqVision Servers”.

17. Copy the keytab file that you created earlier to the Linux exacqVision server and install it to */etc/krb5.keytab*.

    - **If you do not already have a keytab file on the exacqVision server**, which could happen if you do not use any other Kerberos-related software on the server, copy the file to */etc/krb5.keytab*.

    - **If you already have a keytab file on the exacqVision server**, you can merge the new keytab into the existing keytab as follows:

      ```
      sudo ktutil
      rkt /etc/krb5.keytab
      rkt ev.keytab
      wkt /etc/krb5.keytab
      quit
      ```

18. Open a terminal window and run sudo klist –k to verify the service principal name, which should look similar to the following example:

    ```
    EDVR/evserver.exacq.test.com@EXACQ.TEST.COM
    ```

19. On the exacqVision server computer, download and install the exacqVision software from www.exacq.com. You must be logged in with root privileges to do this. The software automatically starts after the installation is complete.

20. If installing an exacqVision server, license the exacqVision server as an Enterprise system. To do this, complete the following steps:

    A. Install the exacqVision Client software on the server if it is not already installed.
    B. Run the exacqVision Client and connect to the local server (127.0.0.1) using the default “admin” account.
    C. Open the System Setup page for the exacqVision server you want to license and select the System tab.
    D. Enter the valid Enterprise license as generated by exacq Technologies and click Apply in the License section.

21. If installing an exacqVision server, configure the directory settings. To do this, complete the following steps:

    A. In the exacqVision Client software, select the ActiveDirectory/LDAP tab on the System Setup page.
    B. Select the Enable Directory Service checkbox
    C. Select OpenLDAP/Kerberos in the LDAP Schema drop-down list.
    D. Enter the OpenLDAP/Kerberos server’s IP address in the Hostname/IP Address field.
    E. Select the SSL checkbox if you want LDAP operations to use secure SSL. If so, see the *Configuring SSL on an exacqVision Server* document.

    NOTE: On Ubuntu Linux systems purchased from Exacq before April 2010, you must use Synaptic Package Manager to download packages that are required for SSL support. To do this, the exacqVision Server must be able to connect to the Internet.

    F. Verify the OpenLDAP/Kerberos server’s connection port. Unless you have reconfigured your OpenLDAP/Kerberos server, the port should be 636 when using SSL, or 389 without SSL.
    G. Enter the LDAP Base DN, the container of all directory user accounts or groups that you want to map in the exacqVision software. For example, if the domain were *exacq.test.com*, the LDAP Base DN might be:

        CN=Users, DC=exacq, DC=test, DC=com

    NOTE: Check with the system administrator for the correct LDAP Base DN for your situation.

    H. Enter the LDAP Binding DN, the fully qualified distinguished name (DN) of a directory user who has access to view the records of the directory user accounts. It is recommended that you enter the Administrator user account as the LDAP Binding DN. For example, if the domain were *exacq.test.com*, the LDAP Binding DN of the Administrator account would be:

        CN=Administrator, CN=Users, DC=exacq, DC=test, DC=com

    I. Enter the password for the account entered in the previous step.
    J. To prevent any non-directory users that have previously been created from connecting to the exacqVision server (optional), deselect Enable Local User Accounts.
    K. Click Apply to connect. An indicator on the ActiveDirectory/LDAP tab displays the success or failure of the connection attempt.

2 Connecting to exacqVision Servers

You can connect to your Enterprise exacqVision servers from the Linux exacqVision Client software in any of the following ways:

- You can use a local exacqVision username and password.
- If you have already executed the kinit command to log in to the domain, you can use your system login without entering a username or password. In this case, leave the username and password fields empty on the Add Systems page, select Use Single Sign-On, and click Apply.
- If using the Linux version of the exacqVision Client, you can use any domain user account. Use the kinit command to log in to the domain. Enter the account name in user@REALM format as the username (for example, "test.user@EXACQ.TEST.COM"). You do not need to enter a password in the exacqVision Client. The realm must be in upper case, as shown in the example. Do NOT select Use Single Sign-On with this login method.

NOTE: If you attempt to connect to an exacqVision server using your system login without first executing *kinit*, the connection will fail.

3 Adding exacqVision Users from the OpenLDAP/Kerberos Database

When the exacqVision server is appropriately configured and connected to your OpenLDAP/Kerberos server, the Users page and the Enterprise User Setup page each contain a Query LDAP button that allows you to search for users or user groups configured in OpenLDAP/Kerberos. You can manage their exacqVision server permissions and privileges using the exacqVision Client the same way you would for a local user. On the System Information page, the Username column lists any connected OpenLDAP/Kerberos users along with their OpenLDAP/Kerberos origin (whether each user was mapped as an individual or part of a user group) in parentheses.