1 Configuration

The following process allows you to configure exacqVision permissions and privileges for accounts that exist on an Active Directory server:

NOTE: The domain controller must run on Windows Server 2003 operating system or later.

1. On the Active Directory server, open the Windows Firewall control panel. In File and Printer Sharing, verify that all four rules are listed (usually TCP port 139, TCP port 445, UDP port 137, and UDP port 138). If you want to connect from a different subnet, click Change Scope and specify a custom list, as in the following example:

   ```
   192.168.1.0/255.255.255.0,192.168.100.0/255.255.255.0
   ```

2. Add a rule for the DNS server (c:\windows\system32\dns.exe), observing the same scope setting if appropriate.

3. Add a rule for the Local Security Authentication Server (c:\windows\system32\lsass.exe), observing the same scope setting if appropriate.

4. Add rules for TCP ports 389 (standard cleartext LDAP) and 636 (standard SSL LDAP), observing the same scope setting if appropriate.

5. On the Active Directory server, enter 127.0.0.1 as its own DNS server address.

If installing an exacqVision server, complete steps 6 through 12. Otherwise, skip to step 13.

6. 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
   evserver1.exacq.test.com.
   ```

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

   ```
   /etc/hosts
   127.0.0.1 evserver1.exacq.test.com localhost
   ```

8. Restart the system.

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

   ```
   dnsdomainname --fqdn
   ```

10. On the Active Directory server, create one individual user account for each Linux exacqVision server. A Domain User account is sufficient for each server, but make sure you remember the password for each one. It can be helpful for future system maintenance to use a name for each user account that matches the corresponding system.

    NOTE: The rest of this document assumes that the system is named *evserver1*, the user account is also *evserver1*, and the password is *Exacq123*. Substitute your specific information in the examples where applicable.

11. In Active Directory, create a keytab file for the Linux exacqVision server. At a command prompt on the Active Directory server, determine your Active Directory version and then type the following:

If using Active Directory 2003:
```
ktpass  –princ EDVR/evserver1.exacq.test.com@EXACQ.TEST.COM
        -mapuser "evserver1"
        -pass Exacq123
        -out evserver1.keytab
        -crypto DES-CBC-MD5
        +desonly
        -ptype KRB5_NT_PRINCIPAL
```

If using Active Directory 2008:
NOTE: With Active Directory 2008, right-click and run the command prompt as Administrator.

```
ktpass  –princ EDVR/evserver1.exacq.test.com@EXACQ.TEST.COM
        -mapuser "evserver1@EXACQ.TEST.COM"
        -pass Exacq123
        -out evserver1.keytab
        -crypto all
        -ptype KRB5_NT_PRINCIPAL
```

NOTES: All the text in the command is case sensitive. The quotation marks are required in the –mapuser line only if the account name contains spaces; otherwise, they are optional.

12. Copy the keytab file created in the previous step to a location that can be used later in this procedure to install it on the Linux exacqVision Server.

The following steps apply to all situations.

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

```
evserver1.exacq.test.com       192.168.1.16
EXACQ.TEST.COM
adserver2008.exacq.test.com    192.168.1.70
```

14. 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.

15. Make sure the fully qualified host names of the Active Directory 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, you can configure your hosts file with the fully qualified host names, as in the following example:

```
/etc/hosts
192.168.1.16     evserver1.exacq.test.com
192.168.1.70     adserver2008.exacq.test.com
```

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

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

```
[libdefaults]

     default_realm = EXACQ.TEST.COM
...

[realms]
     EXACQ.TEST.COM = {
          kdc = adserver2008.exacq.test.com
          admin_server = adserver2008.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 Active Directory domain name in upper case, as shown in the example.

17. 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*.

18. 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".

19. 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 evserver1.keytab
wkt /etc/krb5.keytab
quit
```

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

```
EDVR/evserver1.exacq.test.com@EXACQ.TEST.COM
```

21. 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.

exacq ®
Technologies

www.exacq.com

+1.317.845.5710   USA (Corporate Headquarters)
+44.1438.310163   Europe/Middle East/Asia

Page 3 of 5
12/1/2011

22. 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.

23. 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 Active Directory in the LDAP Schema drop-down list.
    D.   Enter the Active Directory 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 Active Directory server's connection port. Unless you have reconfigured your Active Directory 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 Active Directory Database

When the exacqVision server is appropriately configured and connected to your Active Directory 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 Active Directory. 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 Active Directory users along with their Active Directory origin (whether each user was mapped as an individual or part of a user group) in parentheses.