Windows Server & Client and OpenLDAP/Kerberos

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)

    And at least 1 of the following opject types:

    groupOfNames (rfc 2256)
    groupOfUniqueNames (rfc 2256) - supported with exacqVision 6.8+
    organizationRole (rfc 2256) - supported with exacqVision 6.8+
    posixGroup (rfc 2256) - supported with exacqVision 6.8+

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

And that each group uses the corresponding attribute to map users.

    member (for groupOfNames)
    uniqueMember (for groupOfUniqueNames)
    roleOccupant (for organizationalRole)
    memberUid (for posixGroup)

Created On: 5th February 2021
KB Number: KB-00173-173-210205

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."

5. Make sure the OpenLDAP/Kerberos server's fully qualified host name can be resolved. To do this, open a command prompt, ping the fully qualified host name, and look for a reply.

6. Make sure you have access to the ksetup command by completing the following steps:

A. For Windows XP, install the Windows XP Service Pack 2 Support Tools, available from Microsoft; for Windows Vista, find and install the equivalent package. When installing Support Tools, select a "complete" install. After installation, log out of Windows and then log in again.

NOTE: *Other recent Windows versions, such as Windows 7 and Windows Server 2003, already include the ksetup command.*

B. Open a command prompt and verify that you can execute the ksetup command.

C. Execute ksetup commands to add your Windows machine to the OpenLDAP/Kerberos domain, as shown in the following examples (all are case-sensitive):

ksetup /addkdc EXACQ.TEST.COM kdc.exacq.test.com
ksetup /addkpasswd EXACQ.TEST.COM kdc.exacq.test.com
ksetup /setrealm EXACQ.TEST.COM
ksetup /setcomputerpassword YOURCOMPUTERPASSWORD

NOTE: *Be sure to note your chosen computer password for steps later in this process.*

7. Restart the server. When the login screen appears after the system restarts, notice that the drop-down list contains the OpenLDAP/Kerberos domain. Select the domain and log in.

8. Open a command prompt and use ipconfig to ensure that the hostname and primary DNS suffix are correct.

9. 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

10. 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
quit

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

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

12. 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.

13. 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.

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.

Connecting to exacqVision servers

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

A. You can use a local exacqVision username and password.

B. If you are already logged into Windows as a domain user, 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.

C. You can use any domain user account. Enter the account name in user@REALM format as the username (for example, 'test.user@EXACQ.TEST.COM'), and use the password associated with that account. 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 logging in to Windows through the domain, the connection will fail.*

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.