

1 Introduction

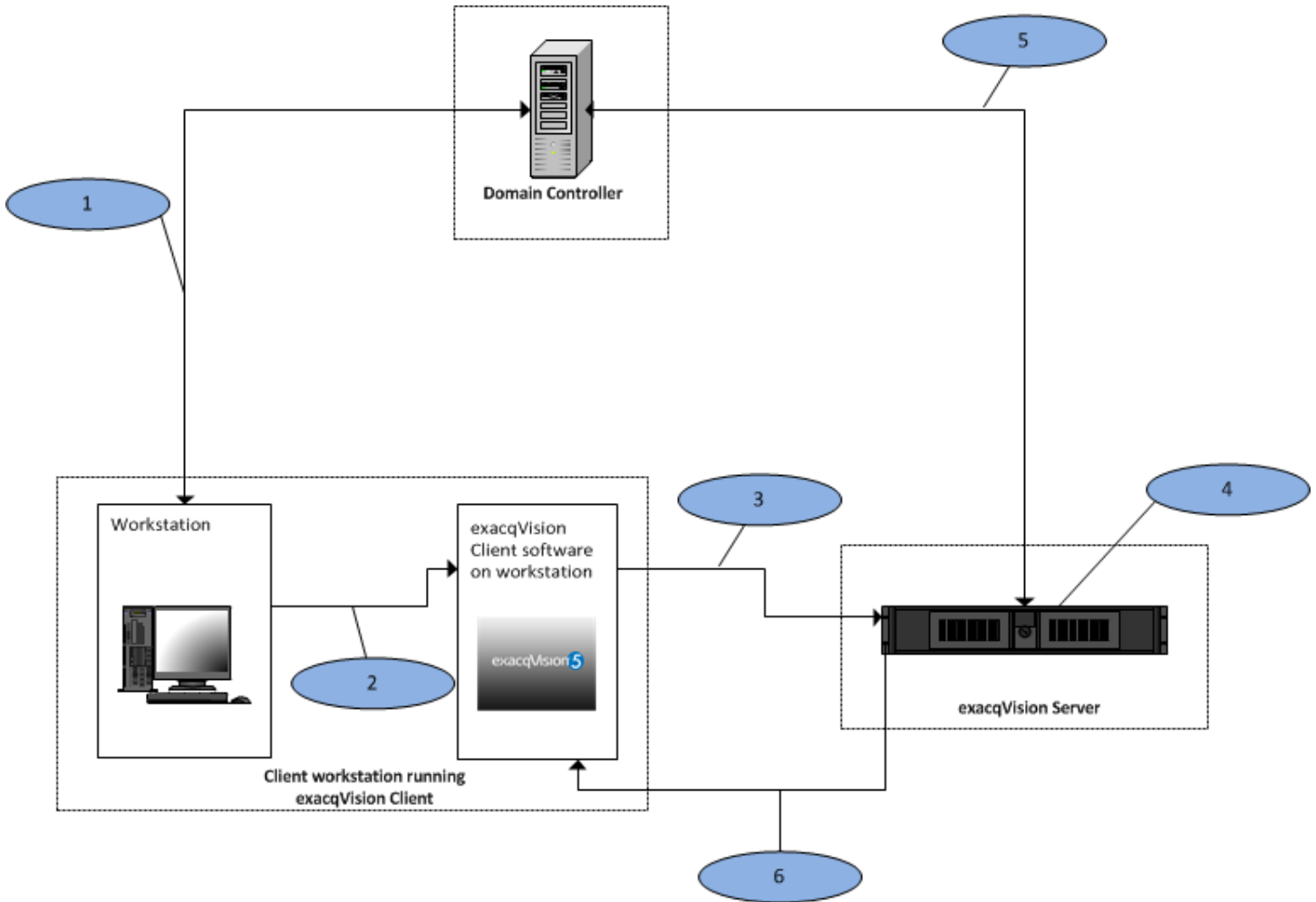
For an organization using Active Directory (AD) for user management of information technology services, integrating exacqVision into the AD infrastructure can greatly simplify continuing maintenance of user access to your video management system (VMS). On each exacqVision Server, you can assign VMS permissions to one or more AD groups and users. However AD groups is the preferred method for authentication. Then, as you add user accounts to those groups through standard IT user management practices, those users will automatically have access to log in to the exacqVision Servers with appropriate permissions. User management directly through exacqVision becomes a one-time configuration requiring that you join the server to the domain and assign permissions and privileges to groups, and all additional user management occurs through AD.

To provide the ongoing benefits of using group-based permissions with exacqVision Server, the server must do more than simply authenticate login credentials of a user requesting access; it must be able to browse AD groups to present them as configuration options and to determine whether a user requesting access is a member of any configured groups.

Minimum Requirements

- Your exacqVision Server must have an Enterprise license to interact with AD.
- The domain controller must be running on Windows Server 2003 or later.
- To configure AD on an exacqVision Server, you must have Active Directory credentials with access to the following AD parameters:
 - objectClass (specifically "group" & "user")
 - userPrincipalName
 - sAMAccountName
 - inetOrgPerson
 - krbPrincipalName

2 exacqVision to Active Directory/LDAP Data Flow



1. The exacqVision server and exacqVision client computers are joined to the domain.
2. The Kerberos ticket (that is, the operating system login credentials) is passed from the client workstation operating system to the exacqVision Client.
3. The exacqVision Client initiates communication with the exacqVision server and passes the Kerberos ticket.
4. The exacqVision server validates the ticket passed from the client software and extracts the user information.
5. The exacqVision server passes the user to LDAP, which looks at the group and user associations for the passed user.
6. The exacqVision server passes the rights and privileges based on the user groups it is a member of.

3 Configuring exacqVision for Active Directory Integration

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 and then Advanced settings. Confirm File and Printer Sharing for Inbound and Outbound, and verify that all four rules are listed -- usually TCP port 139 (NB-Session), TCP port 445 (SMB), UDP port 137 (NB-Name), and UDP port 138 (NB-Datagram).

Name	Group	Profile
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All
File and Printer Sharing (SMB-In)	File and Printer Sharing	All
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All
File and Printer Sharing (Spooler Service - RPC-EPM...)	File and Printer Sharing	All

2. Add and confirm rules for TCP/UDP ports 389 (standard clear text LDAP) and 636 (standard SSL LDAP).

Active Directory Domain Controller - LDAP (TCP-In)	Active Directory Domain Services	All
Active Directory Domain Controller - LDAP (UDP-In)	Active Directory Domain Services	All
Active Directory Domain Controller - LDAP for Global Catalog (TCP-In)	Active Directory Domain Services	All
Active Directory Domain Controller - NetBIOS name resolution (UDP-In)	Active Directory Domain Services	All
Active Directory Domain Controller - SAM/LSA (NP-TCP-In)	Active Directory Domain Services	All
Active Directory Domain Controller - SAM/LSA (NP-UDP-In)	Active Directory Domain Services	All
Active Directory Domain Controller - Secure LDAP (TCP-In)	Active Directory Domain Services	All
Active Directory Domain Controller - Secure LDAP for Global Catalog (TCP-In)	Active Directory Domain Services	All

3. On the Active Directory server, enter 127.0.0.1 as its own DNS server address.
4. On the exacqVision server or client computer, designate the Active Directory server as the preferred DNS server. To do this, open Network Connections, right-click the connection and select Properties, select TCP/IP, click Properties, and enter the Active Directory server IP address as the Preferred DNS Server.
5. Make sure the Active Directory server's fully qualified hostname can be resolved. To do this, open a command prompt, ping the fully qualified hostname, and look for a reply.
6. Join the Windows system to the Active Directory domain. To do this, complete the following steps:
 - Open System Properties by typing `sysdm.cpl` in the Windows search, or by right-clicking Computer and choosing Properties.
 - Choose Change... .
 - Under Computer Name, type a computer name that is unique to all computers recognized by the Active Directory server.
 - Select Domain, enter the Active Directory domain name for your environment, and click OK. For example, a valid domain entry might be "exacqtest.com" (not "EXACQTEST").
 - When prompted, enter a username and password for a domain account with the right to add computers to the domain.
 - Restart the system when prompted.

- When the login screen appears after the system restarts, notice that the "Log on to:" contains the Active Directory domain. **If it does not**, type `domain\username` in the user name field.
- Open a command prompt and use `ipconfig /all` to ensure that the hostname and primary DNS suffix are correct.

```
C:\Users\bstovall>ipconfig /all

Windows IP Configuration

Host Name . . . . . : evwinserver
Primary Dns Suffix . . . . . : exacqsupport.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : exacqsupport.local
```

9. Note the fully qualified hostname (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 hostname and IP address of the Active Directory server. For example:

evserver.exacqsupport.local	192.168.1.16
Exacqsupport.local	
adserver2008.exacqsupport.local	192.168.1.7

10. If installing an exacqVision server, add a service principal name on the Active Directory server for the exacqVision server. To do this, complete the following steps:

- Open a command prompt (right-click to run as an Administrator, if necessary) on the Active Directory server and execute the following command, substituting the name and fully qualified hostname of your exacqVision Server:

setspn -A EDVR/hostname.domain.xxx hostname (example: setspn -A EDVR/evserver.exacqsupport.local evserver)

NOTE: Type the entire command above; do NOT copy and paste it. Also, all text after the forward slash should be lower case, and "EDVR" must be upper case. The SPN must replicate to, or be entered on, all Domain Controllers.

- 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 using following steps:

- Install the exacqVision Client software on the server if it is not already installed.
- Run the exacqVision Client and connect to the local server (127.0.0.1) using the default admin account.
- Open the System Setup page for the exacqVision server you want to license and select the System tab.
- 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:

- In the exacqVision Client software, select the Active Directory/LDAP tab on the System Setup page.
- Select the Enable Directory Service checkbox.
- Select Active Directory in the LDAP Schema drop-down list.
- Enter the Active Directory server's hostname (preferred) or IP address in the Hostname/IP Address field. Select the SSL checkbox if you want LDAP operations to use secure SSL. If so, see the Configuring SSL on an exacqVision server document at <https://www.exacq.com/kb/?crc=37223>

NOTE: It is best practice to confirm LDAP connectivity over port 389 (non-SSL) before configuring SSL.

- 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.
- 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 exacqsupport.local, the LDAP Base DN might be:

DC=exacqsupport, DC=local (the root of the AD structure)

NOTE: Check with the system administrator for the correct LDAP Base and Binding DN for your situation. User and Group OU's/Containers must be below (nested) the Base DN, not equal to or above the Base DN. Binding will occur, but users will not be able to login.

For faster connection and searches, it is best to have the Base DN close to your user and group containers/OU's.

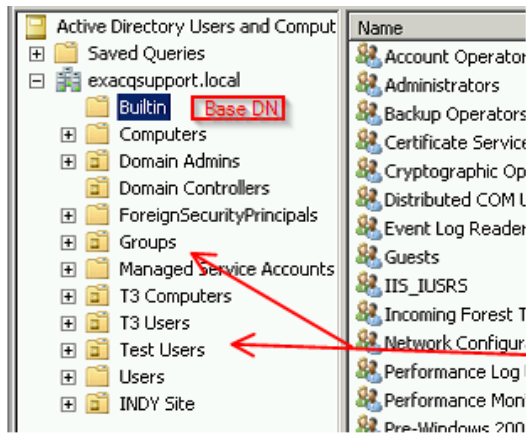
Good:

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgr...
Domain Admins	Organizational ...	
Domain Cont...	Organizational ...	Default container for dom...
ForeignSecur...	Container	Default container for secu...
Groups	Organizational ...	
Managed Ser...	Container	Default container for man...
T3 Computers	Organizational ...	
T3 Users	Organizational ...	
Test Users	Organizational ...	
Users	Container	Default container for upgr...

Better:

Name	Type
Users	
Groups	

Bad:



The Groups and Users OU's are not nested under the "Builtin" Container.

Users and groups

- 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.com, the LDAP Binding DN of the Administrator account would be:

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

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

NOTE: The binding DN user's password should be set to never expire. The Binding DN user must be a member of Domain Users.

4 Connecting to exacqVision Servers

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

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

5 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.

6 Troubleshooting

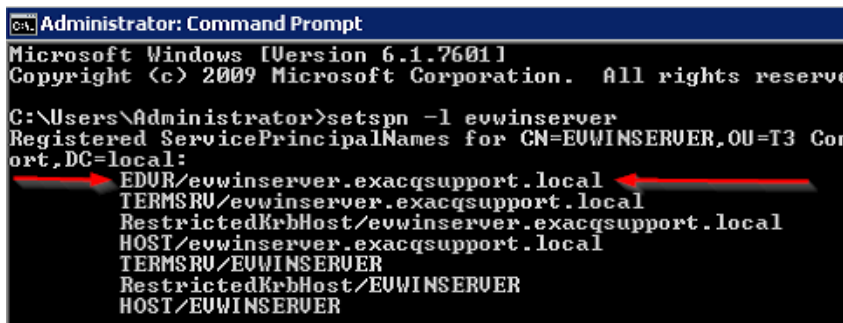
1. Re-imaging system or replacing system (including virtual machines)

- Use a different hostname and IP (recommended)
- If using same hostname and IP, make sure all instances and references of this hostname, IP, and SPN have been removed from the DC.
- Rejoin to the domain using the steps outlined earlier in this document.
- Import the exacqVision configuration file to restore settings and preferences.

2. Client Side Kerberos errors

- You did not run the setspn command on all DCs, or it has not replicated to all DCs. You can check on each DC by opening a command prompt on the DC and typing **setspn -l *hostname*** (the hostname of the exacqVision server).

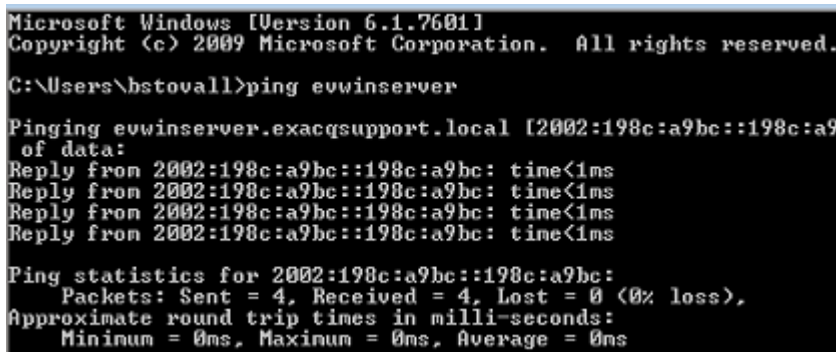
You should have something like this:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -l ewinserver
Registered ServicePrincipalNames for CN=EUWINSERVER,OU=T3 Cor
ort,DC=local:
EDUR/ewinserver.exacqsupport.local
TERMSRU/ewinserver.exacqsupport.local
RestrictedKrbHost/ewinserver.exacqsupport.local
HOST/ewinserver.exacqsupport.local
TERMSRU/EUWINSERVER
RestrictedKrbHost/EUWINSERVER
HOST/EUWINSERVER
```

- You have name resolution issues. You should be able to ping and resolve the exacqVision server from the client computer. In command prompt on the client machine type **ping *exacqhostname.domain.xxx***.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\bstovall>ping ewinserver

Pinging ewinserver.exacqsupport.local [2002:198c:a9bc::198c:a9bc]
with 32 bytes of data:
Reply from 2002:198c:a9bc::198c:a9bc: time<1ms
Reply from 2002:198c:a9bc::198c:a9bc: time<1ms
Reply from 2002:198c:a9bc::198c:a9bc: time<1ms
Reply from 2002:198c:a9bc::198c:a9bc: time<1ms

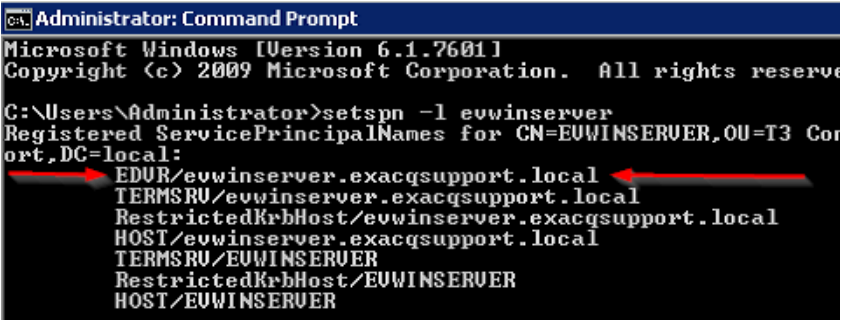
Ping statistics for 2002:198c:a9bc::198c:a9bc:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Not resolving:

- Check DNS (A) records to ensure the hostname and IP are correct.
- Delete and re-add the DNS record for the exacqVision server, if needed.
- Check whether you can resolve any FQDNs from the client.
- Try logging in using your UPN name instead of Single Sign-On. UPN= user@domain.xxx. If successful with the UPN name, restart the client computer and try the Single Sign-On again.
- Ports are not open for 636 (secure LDAP) or 389 (LDAP).

4. Server Side Kerberos errors

- The exacqVision Server log contains **StreamPI Error SSPI error: SEC_E_TIME_SKEW** (the clocks on the client and server computers are skewed). The exacqVision Server time can be no more than five minutes off from the DC's time.
- Make sure the Base DN is above the User or group OU/Container, not below or equal to it, as described in Section 3 of this document. Make sure all the DC's FQDNs can be pinged and resolved from both the client and server
- You have entered your Service Principle Name (SPN) incorrectly.
- From a command prompt on the DC, enter **setspn -l hostname** (the hostname or the exacqVision server) .



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved

C:\Users\Administrator>setspn -l ewinserver
Registered ServicePrincipalNames for CN=EWINSERVER,OU=T3 Container,DC=local:
EDUR/ewinserver.exacqsupport.local
TERMSRV/ewinserver.exacqsupport.local
RestrictedKrbHost/ewinserver.exacqsupport.local
HOST/ewinserver.exacqsupport.local
TERMSRV/EWINSERVER
RestrictedKrbHost/EWINSERVER
HOST/EWINSERVER
```