

1 Introduction

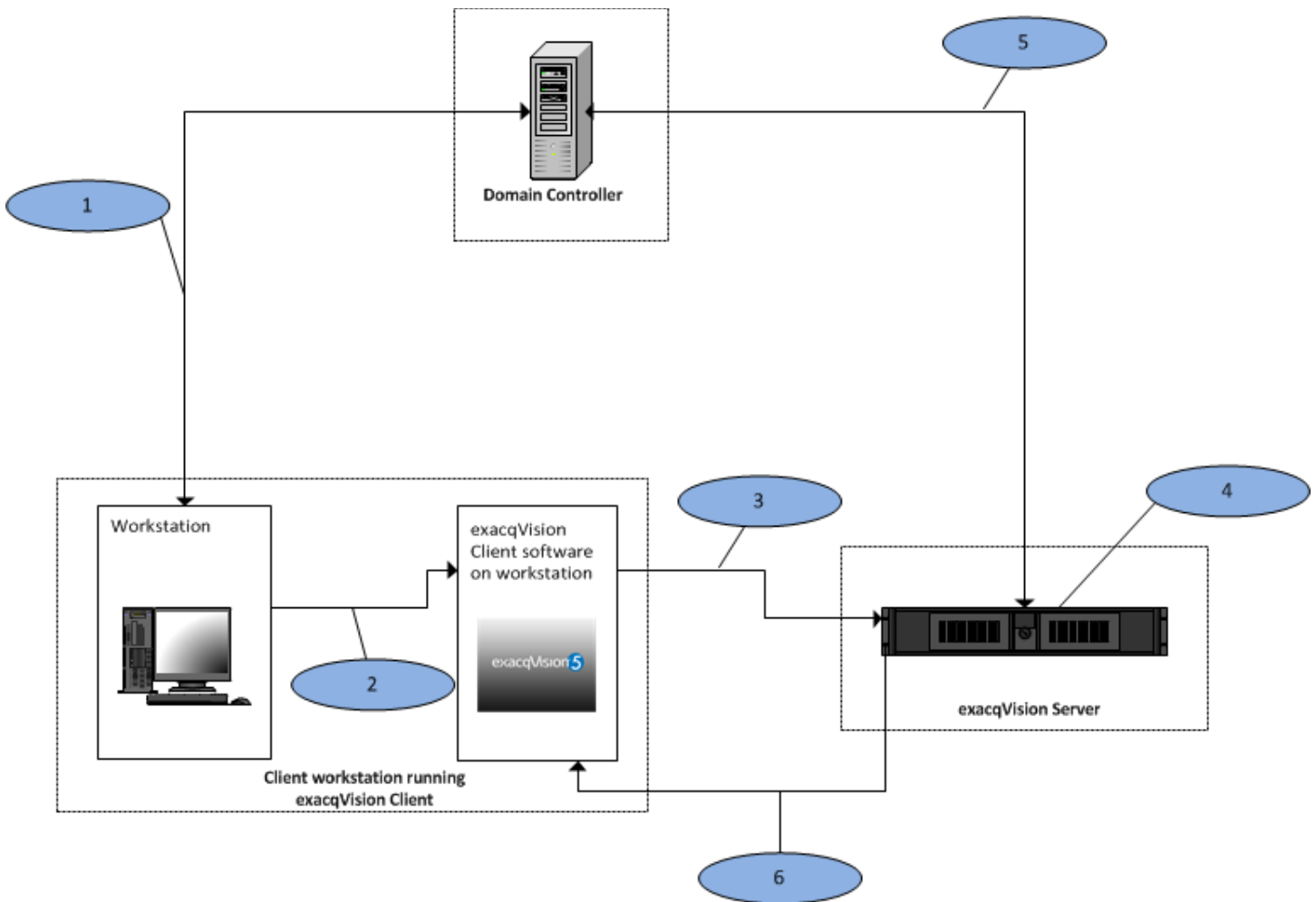
For an organization using Active Directory (AD) for user management of information technology services, integrating exacqVision into the AD infrastructure can greatly simplify continuing maintenance of user access to your video management system (VMS). On each exacqVision Server, you can assign VMS permissions to one or more AD groups. 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 AD credentials with access to a minimum of the following AD parameters:
 - objectClass (specifically "group" & "user")
 - userPrincipalName
 - sAMAccountName
 - inetOrgPerson
 - krbPrincipalName

2 exacqVision-to-Active Directory Data Flow



- 1 Exacq Server and Client machine are joined to the Domain
- 2 The Kerberos Ticket (i.e. the OS Login Credentials) is now passed from the client workstation OS to the Exacq Client
- 3 The Exacq Client initiates communication with the Exacq Server and passes the Kerberos ticket
- 4 The Exacq Server will now validate the ticket passed from the client software and extract the user information
- 5 The Exacq Server passes the user to LDAP. LDAP will now look at the Group and User associations for the passed User
- 6 The Exacq server passes the Rights and Privileges based on the User and Groups it is a member of

3 Configuration

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

1. On the AD 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)
 - UDP port 138 (NB-Datagram)).

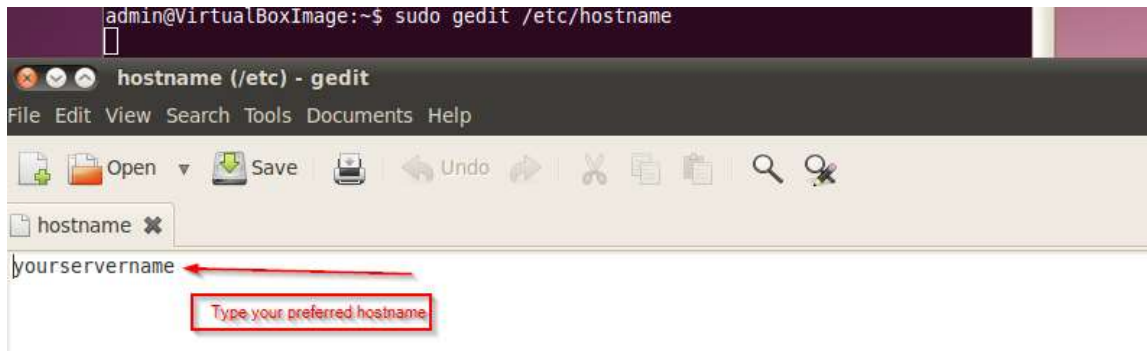
Name	Group	Profile
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All
File and Printer Sharing (NB-Datagram-In)	File and 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 AD server, enter 127.0.0.1 as its own DNS server address.
4. On the exacqVision server, download and install the exacqVision server and client software from www.exacq.com. You must be logged in with Local Administrator privileges to do this.
5. License the exacqVision server as an Enterprise system using following steps:
 - Run 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 then select the System tab.
 - Enter the valid Enterprise license as generated by Exacq Technologies, and then click Apply in the License section.
6. In exacqVision Client, configure the IP address and designate the AD server as the preferred DNS server, or use a preferred internal DNS server.

7. On the exacqVision server, modify `/etc/hostname` to reflect your desired hostname. To do this, open Terminal and then type **sudo gedit /etc/hostname**, enter your preferred hostname, save, and close the file.



8. On the exacqVision server, modify `/etc/hosts` to reflect your fully qualified domain name (FQDN). To do this, open Terminal and then type **sudo gedit /etc/hosts**, modify as needed, save, and close the file. The result should look something like the following (replacing `exacqshostname` with your actual hostname and `domain.xxx` with your domain):



9. Make sure the AD server's FQDN can be resolved. To do this, open Terminal, ping the FQDN, and look for a reply.

4 Join the exacqVision Server to the Domain

To join an exacqVision Linux server to the domain and apply a proper SPN, complete the following steps on the exacqVision Server using Centrify.

NOTE: After installing Centrify, edit the `/etc/centrifydc/user.ignore` file and add the user admin (if you have an AD user named admin)

Instructions WITH Internet Access on the Server

1. Download the `centrifyserver.sh` script from:

<http://cdnpublic.exacq.com/support/downloads/files/CentrifyServer.sh>

2. Copy `centrifyserver.sh` to your exacqVision server.
3. In Terminal, change to the directory where you installed `centrifyserver.sh` (for example, type `cd /home/admin/Desktop` the script is on the Desktop).
4. Type `sudo chmod +x CentrifysServer.sh` to make it executable.
5. Type `sudo ./CentrifysServer.sh -w yourdomain.xxx -u domainuser@domain.xxx` to download and install `centrifydc` and join to the domain.
6. You will be prompted for the domain user credential, and it will not display the password as you type it.
7. When finished without errors, restart the server.

NOTE: to run this script successfully, the server needs to have internet access

Instructions WITHOUT Internet Access on the Server

1. On a computer with Internet access, download the Centrify package from:

<http://www.centrify.com/express/download.asp?asset=centrify-suite-2014-deb5-i386.tgz>

2. Copy the downloaded .tgz file to the exacqVision server. Extract centrifydc*.deb by right-clicking on the .tgz file and choosing Extract Here.
3. In Terminal, change to the directory containing the centrifydc*.deb file.
4. Run **sudo dpkg -i centrifydc*.deb**.
5. Change your directory to /etc/centrifydc.
6. Type **sudo gedit centrifydc.conf**.
7. Search for the following line:

```
# adclient.krb5.service.principals: http ftp cifs nfs
```

8. Uncomment this line (remove the #) and add the text **EDVR** to the end (EDVR must be in caps). The line should now appear like this:

```
# adclient.krb5.service.principals: http ftp cifs nfs EDVR
```

9. Run **sudo adjoin -w DOMAINNAME.EXT -u domainuser@domainname**.
10. When finished without errors, restart the server.

5 Verify the Kerberos Configuration

To 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`.

NOTES:

- When you run `kinit domainuser@DOMAIN.XXX`, there will be no output; it just returns to the Terminal prompt). `DOMAIN.XXX` must be in all capital letters.
- If `kinit` returns an error such as “cannot find KDC” see the Troubleshooting section.
- The `klist` command displays information about your Kerberos ticket if `kinit` was successful.

6 Configuring the Directory Settings

To configure the directory settings. To do this, complete the following steps:

1. In the exacqVision Client software, select the ActiveDirectory/LDAP tab on the System page.
2. Select the Enable Directory Service checkbox.
3. Select Active Directory in the LDAP Schema drop-down list.
4. Enter the AD server's IP address in the Hostname/IP Address field.
5. 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=39474>.
6. Verify the AD server's connection port. Unless you have reconfigured your AD server, the port should be 636 when using SSL, or 389 without SSL.

NOTE: It is best practice to make sure you have AD connectivity without SSL (port 389) before trying SSL (port 636).

7. 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:

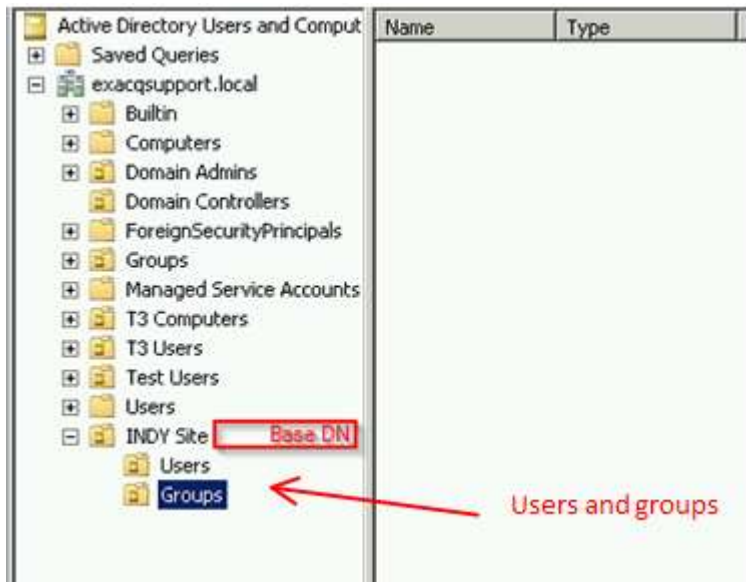
CN=Users, DC=exacq, DC=test, DC=com

NOTE: Check with the system administrator for the correct LDAP Base DN for your situation. User and Group OUs/containers must be below (nested under) the Base DN, not equal to or above the Base DN. Binding will succeed, but users will not be able to log in.

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:



Bad:



8. 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:
9. CN=Administrator, CN=Users, DC=exacq, DC=test, DC=com
10. Enter the password for the account entered in the previous step.
11. To prevent any non-directory users that have previously been created from connecting to the exacqVision server (optional), deselect Enable Local User Accounts.
12. Click Apply to connect. An indicator on the ActiveDirectory/LDAP tab displays the success or failure of the connection attempt.

7 Adding exacqVision Users from the Active Directory Database

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

8 Connecting to exacqVision Servers

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

- Use a local exacqVision username and password.
- If you are already logged into Windows as a domain user, 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.
- Use any domain user account. Enter the account name in *user@realm* format as the username (such as *test.user@exacq.com*). Use the password associated with that account. 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.

To connect with your exacqVision Linux client software:

- Open a terminal and type the **kinit** command discussed earlier before using Single Sign-On.
- You cannot sign in by typing your UPN name at the **Use credentials entered below:** prompt.

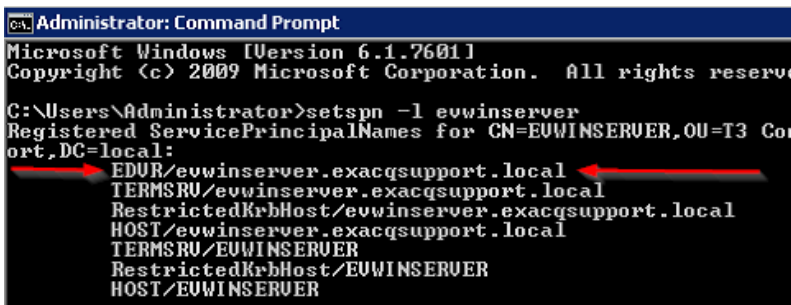
9 Troubleshooting

Re-imaging or Replacing System (Including Virtual Machines)

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

Client-Side Kerberos Errors

Mostly likely, you did not run the **setspn** command (done by Centrify), 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*** (using the hostname of your 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=EUWINSERUER,OU=T3 Co...ort,DC=local:
EDUR/ewinserver.exacqsupport.local
TERMSRU/ewinserver.exacqsupport.local
RestrictedKrbHost/ewinserver.exacqsupport.local
HOST/ewinserver.exacqsupport.local
TERMSRU/EUWINSERUER
RestrictedKrbHost/EUWINSERUER
HOST/EUWINSERUER
```

Name Resolution Issues

You should be able to ping and resolve the exacqVision server from the client computer. In Command Prompt on the client computer, type **ping *exacqhostname.domain.xxx***.

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

C:\Users\bstoval>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

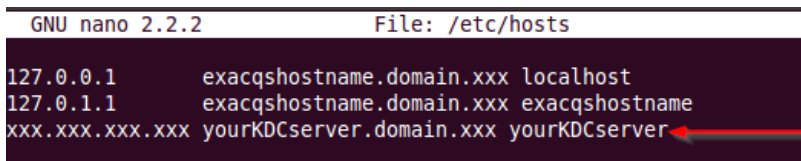
Ping statistics for 2002:198c:a9bc::198c:a9bc:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If it is still not resolving:

- Check DNS PTR records. Make sure the hostname and IP address are correct.
- Delete and add back the DNS record for the exacqVision server, if needed.
- Verify that you can resolve any FQDNs.
- Try logging in using your UPN name instead of Single Sign-On (Windows clients only). UPN=user@domain.xxx. If successful with the UPN name, restart the client computer and try Single Sign-On again.
- Verify that ports are open for 636 (secure LDAP) or 389 (LDAP).
- Check the `/etc/hosts` file on the exacqVision Linux server by typing **sudo gedit /etc/hosts** in Terminal. It should look something like the following, replacing *exacqshostname* with your actual hostname and *domain.xxx* with your domain:



- Check whether **kinit** returns an error stating it cannot find or connect to the KDC server. Ping your KDC server's FQDN (usually your DC). If you cannot ping the KDC, this is a DNS issue. You can resolve by making sure you have set a valid internal DNS server via exacqVision Client, or by adding your KDC server to your HOSTS file.



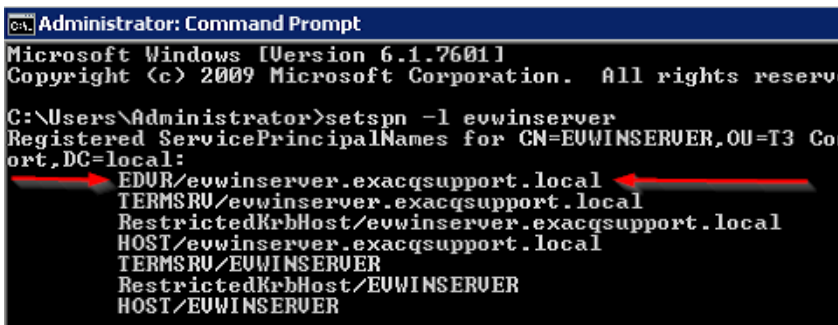
Server-Side Kerberos Errors

- The exacqVision server log could contain the following error:

```
StreamPI Error SSPI error: SEC_E_TIME_SKEW
```

This means the clocks on the client and server computers do not match. The exacqVision server time can be no more than five minutes off the DC's time.

- Make sure the User and Group OU/Container are nested under the Base DN (see discussion earlier in this document).
- Can you ping all your DC FQDNs and resolve them from the client and server?
- You have entered your Service Principle Name (SPN) incorrectly. In a Command Prompt on the DC, enter **setspn -l hostname** (hostname should be the hostname of your 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=EUWINSERVER,OU=T3 Corport,DC=local:
EDUR/ewinserver.exacqsupport.local
TERMSRU/ewinserver.exacqsupport.local
RestrictedKrbHost/ewinserver.exacqsupport.local
HOST/ewinserver.exacqsupport.local
TERMSRU/EUWINSERVER
RestrictedKrbHost/EUWINSERVER
HOST/EUWINSERVER
```

Cannot Log In to the admin Account After Joining the Domain

You have an AD account named admin but did not add it to the /etc/centrifydc/user.ignore file. To recover:

- Rename the AD user from admin to another name.
- Log in to Ubuntu using your local admin account.
- Add admin to /etc/centrifydc/user.ignore.
- Rename the AD account to admin.