Active Directory & LDAP Best Practices

- 1. Introduction
 - a. Benefits of Integration
 - b. exacqVision Server must have Enterprise license
 - c. Use groups on domain
- 2. exacqVision to AD/LDAP Data Flow
- 3. Configuration
- 4. Troubleshooting

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 that 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 the following access to a minimum of the following AD parameters:
 - * objectClass (specifically "group" & "user")
 - * userPrincipalName
 - * sAMAccountName
 - * inetOrgPerson
 - * krbPrincipalName

Created On: 11th February 2021 **KB Number:** KB-00284-284-210211



2. exacqVision to AD/LDAP Data Flow



- 1. exacqVision Client computer joined to the domain. Optionally, you can join the exacqVision Server to the domain.
- 2. The Kerberos ticket (the operating system domain login credential) is passed from the client workstation operating system to exacqVision Client.
- 3. exacqVision Client initiates communication with the exacqVision Server and passes the Kerberos ticket.
- 4. The exacqVision Server validates the ticket and extracts the user information.
- 5. The exacqVision Server passes the user to LDAP, which looks at the group and/or user associations for the passed user credential.
- 6. The exacqVision Server passes the rights and privileges based on the user and groups associated with the user credential.

3. Configuration



1. Log in to your domain controller and expand the tree.

Action View Help				
= 🔿 📶 🥇 🗀 🗶 🗊 @ 🕞 🔽 📷 😤 📚 🖆 🍸 💆 🎘				
ctive Directory Users and Comput	Name	Туре	Description	
Saved Queries	Administrator	User	Built-in account for admini	
hooch.exacq.com	Allowed RODC Password Replicatio	Security Group	Members in this group can	
E 📮 alpha	Sect Publishers	Security Group	Members of this group are	
E Buith	🕹 deloera analog	User		
E Computers	Senied RODC Password Replication	Security Group	Members in this group can	
E Coman Controllers	Sector Se	Security Group	DNS Administrators Group	
E Croups	& DnsUpdateProxy	Security Group	DNS clients who are permi	
Calcops	Somain Admins	Security Group	Designated administrators	
3 x	& Domain Computers	Security Group	All workstations and serve	
	& Domain Controllers	Security Group	All domain controllers in th	
	💐 Domain Guests 🔸 🕂	Security Group	All domain guests	
	Somain Users	Security Group	All domain users	
	& Enterprise Admins	Security Group	Designated administrators	
	& Enterprise Read-only Domain Contr	Security Group	Members of this group are	
	👗 ev admin	User		
	🐍 EV User	User		
	Scoup Policy Creator Owners	Security Group	Members in this group can	
	🛃 Guest	User	Built-in account for guest	
	🔱 Jayson SEnter	User		
	🙎 Matthew DeLoera	User		
	& RAS and IAS Servers	Security Group	Servers in this group can	
	& Read-only Domain Controllers	Security Group	Members of this group are	
	& Schema Admins	Security Group	Designated administrators	

2. Create a new group that specifies privileges in the name nested under your desired Base DN.



Portal







3. Give that Group a Name. This example creates an exacqVision Admin Group.

Active Directory Users and Computers	_ 🗆 🗙
File Action View Help	
(≠ ⇒) 2 m 10 10 0 ∞ 10 m 8 10 7 2 2	
Active Directory Users and Comput Name Tvne Description	
Saved Queries New Object - Group	
Bi hooch.exacq.com	
E 2 appa	
Computers	
Domain Controllers	
E Group name:	
Groups exacqVision Admins	
Users View Control of the Control of	
Group name (pre-Windows 2000):	
exacqVision Admins	
Group scope Group type	
C Domain local Security	
© Global C Distribution	
C Universal	
4 F	
	í

4. Add domain users to the new group.

Active Directory Users and Con	nputers			_ D ×	1	
File Action View Help						
🗢 🔿 🖄 📅 👗 🚺 🗶 🛛	1 🙆 😹 월 🖬 🕄 💐 🕅 🦷	1 🔟 🔍				
Active Directory Users and Comput Saved Queries Suboh.exacq.com Salpha	Name	Type Security Group - Global anaged By oy Domain Services Folder	?×	Select Users, Contacts, C Select Users, Contacts, C Select this object type: Users, Groups, or Other ob From this location: hooch exacq.com Enter the object names to s ex admin (evadmin@hoocl Advanced	Computers, or Groups sjects select (<u>examples</u>) h exacq com)	Object Types Dobject Types Locations Check Names Ok Cancel
	Add Remove					
	0	K Cancel App	ely .			



5. Create additional groups. This example will create a Live and Search Only group.





6. Add domain users to the group.



7. Now you have multiple groups to query in the exacqVision Client. This allows you to assign permissions to users based on their Directory Group.



Portal

Action View Help	Type	Description
el 2 1 4 1 × 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Type	Description
Active Directory Users and Comput Name	Type Security Group - Global	Description
	Security Group - Global	e-cost ipoloiti
Saved Queries Saved Queries	pocarity aroup - aroour	
RexacqVision Live and Search only	Security Group - Global	
alpha		
± buitn		
Computers		
Ecraigo Security Originals		
Groups		
Lisers		
F S x		

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:

Active Directory Users and Comput	Name	Туре	Description
 Saved Queries Saved Queries exacqsupport.local Base DN Builtin Computers Domain Admins Domain Controllers ForeignSecurityPrincipals Groups Managed Service Accounts T3 Computers 	Builtin Computers Computers Domain Admins Domain Cont ForeignSecur Groups Managed Ser T3 Computers T3 Computers T3 Users	builtinDomain Container Organizational Organizational Container Organizational Organizational Organizational	Default container for upgr Default container for dom Default container for secu Default container for man
I 3 Users I Set Users I Set Users	Users	Container	Default container for upgr
		Users and group	S

Better:



Portal



Bad:



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

Users and groups

8. Log in to the client workstation with an exacqVision user account.

	Windows ^{xp}	
Copyright © 1985 Recosoft Corpora	2001 Professional Micr	050
Liser name:	evadmin	
East manual		
Password:		



9. Open the exacqVision Client and select the System tab on the Config (Setup) page. Enter the Base DN and Binding DN for the directory.

NOTE: Make sure the Base DN is at least one level above the Group container you will be querying.

V exacqVision Client	
里 🔍 🗞	
Configuration Systems Systems G Add Systems G Clent	System
Event Monitoring Maps Wews Tours Enterprise Excerption Storage Storage Storage Storage Event Unitications Auto Export Event Linking Schedule Users	System Date/Time Network ActiveDirectory/LDAP Directory Service Status: Cannetted Pate/Time /IP Address: IDAP Server Address Hostname/IP Address: IDAP Server Address: Port: 399 Use SSL FQDN: newbelgium.hooch.exacq.com LDAP Schema: Active Directory LDAP Schema: Active Directory UDAP Base DN: DC=hooch,DC=exacq,DC=com LDAP Base DN: DC=hooch,DC=exacq,DC=com LDAP Binding DN: (N=ev admin,CN=Users,DC=hooch,DC=exacq,DC=com LDAP Base DN: Confirm: IDAP Base DN: Cancel

The status should now be Connected.

10. To map each group created on the domain to an exacqVision user, select Users from the configuration tree and click Query LDAP. This will allow us to assign exacqVision permissions to all domain users in each group.



Portal

VexacqVision Client			
🕎 🔍 🎭			🔛 🔄 🛞 exacqVision
Configuration Systems Add Systems		Users	
Cont	Choose Item	Username: Password: Password Confirm: User Group: User Group Name:	October Control October Control U A Group Type Admin Full Admin Local
- Storage - Serial Profiles - Serial Profiles - Notifications - Notifications - Auto Export		PTZ Priority:	Select Users or Groups Select Base DN: DC=hooch,DC=exacq,DC=com (192.168.100.250)
Custon User Permissions Custon User Permission	Apply Cancel Query LDAP	Connected Enter Name to Search (Include wildcards):	

11. Select the group returned by the query and assign permissions to that group. This example gives full admin rights to the exacqVision Admins group.

V/ exacqVision Client			
里 🔍 🎭			exacqVision
Configuration Systems Add Systems Configuration	Custon User Permissions	Users Detais Username: exactivition Advins Password: Password: Password: Password: Password: User Group: add Admin User Group Name: PTZ Priorky: Delete Apply Cancel Query LDAP Custom User Privleges Custom User Privleges Custom User Privleges Custom User Privleges Custom Searching Custom Searching Custom Searching Custom Searching Custom Custo	User Accounts Q Search Q U Group Type Admin Full Admin Local
	At Audio Inputs	Avalable in Search Hease Avalable in Search Hease	0.0048/c Edday March 01.2013 12:01-41.6

12. Click Apply. The group and all its domain users now have permissions, and the type is specified as LDAP.

Created On: 11th February 2021 **KB Number:** KB-00284-284-210211



Portal

V exacqVision Client			
💻 Q %			🔛 💿 🛞 exacqVision
Configuration		Users Cotals Username: exacq/fision Admins Password:	User Accounts Q Search Username A Group Type
Vrens Crous Crous Crous Crous Crous Crous Crous System Crous Sorape Sorape Sorape Sorape Soral Profiles Notifications Notifications Notifications	Choose Item	Password Confirm: User Group: Full Admin User Group Name: PTZ Priority: 1 Delete Delete	Adnin Full Admin (DAP)
- Schedule Users	Custom User Permissions exactifision Server Point Al Soft Tropers Al Soft Tropers Al A Soft Tropers Al Audo Inputs	Apply Cancel Query LDAP	

13. On the Users page, click Query LDAP and search for the next group that was created.

Vexac qVision Client			
🕎 🔍 🗞			🔛 💿 🛞 exacqVision
Configuration	Choose Item	Users Detais Username: exacplifation Admins Password: Password Confirm: User Group: Full Admin	Uter Accounts Q. Search (3) Utername A Group Type Admin Full Admin Loal exact/fision Admins Full Admin LDAP
Custon User Permissions Custo	User Group Name: PTZ Priority: 1 0 Set New Delote Apply Cancel Query LDAP	Inct Users or Groups Inct Base DN: C=hoodh_DC=exacq_DC=com (192.168.100.250)	
	- Custon User Pernissions	Custon User Privileges	Econe test ter Name to Search (include wildcards): only Search Select a Group Below: Select Select
	Ľ		a maleir Buley March of 2012 12-05-595

14. Add permissions for this specific group. This example selects the Live + Search permission for the Live and Search Only group.

Portal

			exacqVisio
Systems Configuration Systems Configuration Con	Cuton User Permissions	Users Username: Index/Macri Line and Search Uder Password: Password Confere: User Group: Line + Search User Group: Name: PT2 Priority: PT2 Pr	User Accounts Q Search Advin Full Admin Lood encoghistion Admins Full Admin LDaP
		- Configuration	

15. Now both groups are mapped on the exacqVision Server with the appropriate permission levels.

Details	n r	User Accounts			
Username:		Q Search			8
Password:		Username A	Group	Type	
Password Confirm		Admin	Full Admin	Local	_
		exacqVision Admins	Full Admin	LDAP	
User Group:		exacqVision Live and Search only	Live + Search	LDAP	
User Group Name:					
PTZ Prioriky: 1					
New Delete					
Apply Cancel Query LDAP					
Custom User Privileges					
OF Allow Live Viewing Generating Configuration Configuration					
Ver Admin Ver Admin					
View Admin					

16. On the Add System page, select Use Single Sign-On so that exacqVision Client will pass the client computer's login credentials to the server for validation when it starts.



Portal

System Information				
Hostname/IP Address:	127.0.0.1			
Port:	22609			
۲	ise Single Sign-On			
0	Nways prompt for credentials			
0	Use credentials entered below:			
Username:				
Password:				
	Connection Speed			
	Obialup ODSL OLAN OLocal			
	Apply Cancel			

17. Because you are logged in to the Client workstation with an exacqVision Admin user account, the system will automatically log in to the server with these credentials.



Portal



18. Now you can log out of the Client Workstation with admin credentials and log in as a Live and Search Only user. Notice that the account does not have any of the server configuration options available when logged in to the Admin group account.



Portal

VexacqVision Client						
🖳 🔍 🎭						
Configuration Systems	System List	Suter lit				
Clent Anno Server	Systemeter		11			
C. everytown server	Ena	Address	System Name	Usern	Status	
	New]				
	Syst	 Address 	Model	Serial		
EV User						
Internet Internet Explorer	My Documer	nts				
Cutlook Express	My Recent D	ocuments >				
MSN	My Music					
Windows Media Player	My Compute	r				
Windows Messenger	Set Program A	ccess and				
Tour Windows XP	Printers and Fe	axes				
Files and Settings Transfer Wizard	Help and Supp	ort				
VexacqVision	Search					
All Programs 👂	👸 Windows Secu	rity				



Portal

4. Troubleshooting

LDAP Not Connecting

On the Domain Controller, 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 I DAD for Clobal Catalon (TCD-In)	Activa Directory Domain Services	All I

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. Import the exacqVision configuration file to restore settings and preferences.

Client-Side Kerberos Errors

Either the binding DN account does not have permission to set the SPN or you did not manually run the setspn command on all DCs, or it has not replicated to all DCs. If you entered the SPN manually, you can check on each DC by opening a command prompt on the DC and typing setspn -I *hostname* (the hostname of the exacqVision server). If your machine was on the domain, use setspn -I *fqdn*. If your machine was not on th domain, use setspn -I *serial* (where serial is the exacqVision Serial number, or mac_address for a 3rd party server).

You should have something like this:

👞 Administrator: Command Prompt					
Microsoft Windows [Version 6.1.7601] Copyright <c> 2009 Microsoft Corporation. All rights reserve</c>					
C:\Users\Administrator>setspn -1 evwinserver Registered ServicePrincipalNames for CN=EUWINSERUER,OU=T3 Con ort,DC=local: EDUR/evwinserver.exacqsupport.local TERMSRU/evwinserver.exacqsupport.local RestrictedKrbHost/evwinserver.exacqsupport.local HOST/evwinserver.exacqsupport.local TERMSRU/EUWINSERUER RestrictedKrbHost/EUWINSERUER HOST/EUWINSERUER					

Name Resolution Issues Created On: 11th February 2021 KB Number: KB-00284-284-210211



Portal

You should be able to ping and resolve the exacqVision server from the client computer. If connecting using a hostname, DNS must be resolvable. 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\bstovall>ping evwinserver
Pinging evwinserver.exacqsupport.local [2002:198c:a9bc::198c:a9] 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:a9hc::198c:a9hc:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Mininum = 0ms, Maximum = 0ms, Average = 0ms

If it is still not resolving:

1.

- 1. Check DNS PTR records. Make sure the hostname and IP address are correct.
- 2. Delete and add back the DNS record for the exacqVision server, if needed.
- 3. Verify that you can resolve any FQDNs.
- 4. 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.
- 5. Verify that ports are open for 636 (secure LDAP) or 389 (LDAP).
- 6. In Linux, 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.

GNU nano 2	.2.2	File: /etc/hosts
127.0.0.1 127.0.1.1	exacqsh exacqsh	ostname.domain.xxx localhost ostname.domain.xxx exacqshostname
xxx.xxx.xxx.	XXX YOURKDC	server.domain.xxx yourKDCserver

Server-Side Kerberos Errors

1. The exacqVision server log could contain the following error:

StreamPI_____SSPIerror: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.

- 2. Make sure the User and Group OU/Container are nested under the Base DN (see discussion earlier in this document).
- 3. Can you ping all your DC FQDNs and resolve them from the client and server?
- 4. You may have entered your Service Principle Name (SPN) incorrectly. You can verify the SPN from a command prompt on the DC, enter setspn -I *hostname* (the hostname or the exacqVision server). If your machine was on the domain, use setspn -I *fqdn*. If your machine was not on the domain, use setspn -I *serial* (where serial is the exacqVision Serial number, or mac_address for a 3rd party server).

