# Access Management – Gluu Server

This tutorial is for IT staff who are experienced in identity management, it requires insight into how the ActiveDirectory and LDAP work, and a working knowledge of Windows.

This tutorial will demonstrate some of the features of AMX, specifically:

- Connecting to the Gluu OpenDj Ldap server
- Using IdentityReport to Extract accounts from the Ldap server
- Synchronising OpenDj with the Identity Report CSV File
- Synchronising OpenDj with the Active Directory

AMX runs on Windows and must be setup as shown in the AMX Tutorial Setup document.

In this tutorial AMX is run from the Command Line, in production it is expected to be run by the Task Scheduler.

#### 1. Connect to Gluu OpenDJ

The OpenDj exposes port 1636 as an Ldaps connection. Using a Ldap directory manager such as Apache Studio setup a connection to the directory

Properties for "AMX10"				_		×
type filter text	Connection			¢	• 🔿	• •
> Connection	Network Parameter	Authentication Browser Options	Edit Options			
	Network Parameter					
	Hostname:	amx10.corp.example.com				$\sim$
	Port:	1636				$\sim$
	Encryption method:	Use SSL encryption (Idaps://)				$\sim$
		Server certificates for LDAP connect Certificate Validation' preference p	ctions can be r age.	nanage	d in the	
	Provider:	Apache Directory LDAP Client AP	I			$\sim$
			Check N	Vetwork	Parame	ter
	Read-Only (preven	ts any add, delete, modify or renam	ne operation)			
0	1		ОК		Cance	ł

The user name is CN=Directory Manager and the password was set in the ./setup.py script when Gluu was installed. Details can be seen in the Gluu Configuration / Manage Authentication page.

# IDAP - o=@!C527.98AC.187E.020B!0001!7099.D2F6,o=gluu - AMX10 - Apache Directory Studio

File Edit Navigate LDAP Window Help

[] - 🗄 🏟 💉 🖢 - 🖓 - 🏷 - ↔ -			
😫 LDAP Browser 🛛 🙀 🗇 📄 🔄 🏹 🖓		■ o=@!C527.98AC.187E.020B!000	11!7099.D2F6,o=gluu 🛛
	9	DN: o=@!C527.98AC.187E.020B!00	01!7099.D2F6,o=gluu
✓ 🖉 Root DSE (10)	^	Attribute Description	Value
✓ & o=gluu (2)		objectClass	gluuOrganization (structural)
• • • • • • • • • • • • • • • • • • •		objectClass	top (abstract)
옯 ou=hosts		description	Welcome to oxTrust!
👗 ou=sector_identifiers		displayName	axnt
👗 ou=session		gluuAddPersonCapability	enabled
> 🖧 ou=attributes		gluuManagerGroup	inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0003!60
> 🖧 ou=clients		gluuOrgShortName	axnt
> 🖧 ou=federation		gluuThemeColor	166309
> 🖧 ou=groups		0	@!C527.98AC.187E.020B!0001!7099.D2F6
> 🖧 ou=metric		scimAuthMode	basic
> 🧰 ou=oxasimba		scimStatus	disabled
> 🖧 ou=oxProx			
✓ ♣ ou=people (103)			
> 🥟 [1100]			
> 🥟 [101103]			
> 🖧 ou=push			
> 🖧 ou=scopes			
> 🖧 ou=scripts			
> 🖧 ou=u2f			
> 🖧 ou=uma			
> 🏯 ou=appliances			
✓ ♣ o=site (1)	۷.		

Connect to the Gluu directory and copy the DN of the ou=people organisational unit.

## 2. identityReport

identityReport will read the Gluu directory and produce a report of accounts and their attributes. identityReport can be run with a non-privileged account.

#### Update Gluu1 Properties

Edit the Properties file Gluu1.properties, it is in the <installDirectory>\Tutorial1 directory. identityReport properties are consistent with identitySync and the same properties file is used for both applications.

The parameters that need to be updated are:

LdapResource1 = ldaps://amx10.corp.example.com:1636 LdapAccountContainer1 = ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6,o=gluu

- LdapResource1 is the resolvable DNS name of the target Gluu server.
- LdapAccountContainer1 is the ou identified in the ldap browser in the previous step.

#### Update the Idap password

Create a GluuPasswd.txt file, add the password to the first line, it will be encrypted the first time that identityReport runs.

#### Run identityReport

#### Open a Command prompt and cd to the AMX Tutorial1 directory

C:\AMX\Tutorial1>..\identityReport.exe Gluu1.properties Begins Fri, 01 Jul 2016 16:06:35 GMT identityReport Total of 0 Identities

LDAP1 Gluu Extracted 103 Accounts LDAP Finished Fri, 01 Jul 2016 16:06:35 GMT Finished Fri, 01 Jul 2016 16:06:35 GMT

C:\AMX\Tutorial1>

Check that the expected number of accounts were returned. In situations where the number of accounts is incorrect, open the debug file and check for errors.

After a successful run this will create identityReportGluu1.csv, open it and check the data. Notice that the first line is:

displayName, firstName, lastName, accountName, mail, status, distinguishedName

Default Admin User,Admin,User,admin,,active, inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!A8F2.DE1E.D7FB,ou=people,o=@!C527.98AC.187E.020B!0001!7099 .D2F6,o=gluu This account should not be managed, it does not exist in any identity source. Edit Gluu1 and Gluu2 properties and add a filter to remove it

```
LdapFilterAttribute1 = displayName
LdapFilterValue1 = !Default Admin User
```

The filter is fully described in the reference manual, this will use the displayName to filter all records and filter out any one that has the value Default Admin User. You may need to filter out other records, in which case use the ActionFileDelimList string to delimit them. The default is ":".

LdapFilterValue1 = !Default Admin User:Other Admin User

Run identityReport again and check that the Admin user has been filtered out of the IdentityReportGluu1.csv report.

#### Errors

Error: LDAP Extract Create Connection The LDAP server is unavailable. For <host>:<port>

This can be caused by many issues, such as unresolvable hostname, firewalls, incorrect port etc. Troubleshoot using an LDAP client such as Apache LDAP Studio <a href="http://directory.apache.org/studio/">http://directory.apache.org/studio/</a> this will give better diagnostics concerning certificates and protocols.

Try using Idap:// on port 389 for attribute LdapServer1. This is not always available, but if this works:

- The server's certificate may not be trusted by the system running identitySync. Try running with the ldap property CertificateTrust = Yes. If this resolves the problem it is a certificate issue, try:
  - Export the certificate from Apache Directory Studio and install the certificate in the Trusted Root CA store.
  - Hostname must match the certificate and be resolvable with dns. Use nslookup to check.

Error: LDAP Extract. The object does not exist. For <adapterInstance>

Can be caused by a bad AccountContainer property value referring to a non-existent container.

Error: LDAP Extract. The server does not support the control. The control is critical. For <adapterInstance> The AdapterInstance does not support PagedRead. Set the PageSize property to 0.

#### 3. IdentitySync with the IdentityReport CSV File

#### Syncronising the identity report extracted before will show no changes

C:\AMX\Tutoriall>..\identitySync.exe Gluu2.properties Warning: Not run as administrator Begins Tue, 19 Jul 2016 11:18:07 GMT analyze CSVIdentity1 C:\AMX\Tutoriall\IdentityReportGluu1.csv Last updated 19/07/2016 11:18:01 Extracted 102 Identities CSVIdentity Finished Tue, 19 Jul 2016 11:18:07 GMT Total of 102 Identities

LDAP1 Gluu

Extracted 102 Accounts Account joins 102 Account creates 0 Account updates 0 Account disables 0 Account deletes 0 LDAP Manual Update LDIF do File manual.ldf LDAP Finished Tue, 19 Jul 2016 11:18:07 GMT Finished Tue, 19 Jul 2016 11:18:07 GMT

C:\AMX\Tutorial1>

#### Update the Identity Report

Add some extra records and change some existing ones in the IdentityReport1.csv. For example add a new record:

```
,Y,Ailsa Sutherland,Ailsa,Sutherland,,
```

#### Run identitySync

Run identitySync again and the transaction file ActionFile.txt will contain the changes. To make the changes to the LDAP directory run identitySync in the do mode. To undo the changes run it again in undo mode.

```
C:\AMX\Tutoriall>..\identitySync.exe Gluu2.properties do
Warning: Not run as administrator
Begins Tue, 19 Jul 2016 11:29:41 GMT do
CSVIdentity 1 C:\AMX\Tutorial1\IdentityReportGluu1.csv
Last updated 19/07/2016 11:28:04
Extracted 103 Identities
CSVIdentityFinished Tue, 19 Jul 2016 11:29:41 GMT
Total of 103 Identities
```

LDAP1 Gluu

Extracted 102 Accounts Account joins 102 Account creates 1 Account updates 0 Account disables 0 Account deletes 0 LDAP Manual Update LDIF do File manual.ldf LDAP Finished Tue, 19 Jul 2016 11:29:42 GMT

LDAP1 Gluu Number of Mandatory 1 LDAP Load Gluu Create do inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!GBP3.Z7U7,ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6 ,o=gluu Finished Tue, 19 Jul 2016 11:29:42 GMT

Check the LDAP Directory Manager, this will need a refresh. Compare the new entry with an adjacent one to check all the attributes are present and correct.

Check the Gluu server, search for Sutherland

# ⊗gluu

≡

GL	UU Identity Appliance	Users •Update User			ñ
F	Configuration d	gluuPerson eduPerson inetOrgPerson	Display Name	Ailsa Sutherland	×
8 : 6 (	SAML <	Add attributes to person entry	Email	Ailsa.Sutherland@example.com	×
В	UMA 🤇	Birthdate Country	First Name	Ailsa	×
*	Users	Gender, male or female	iname	*person*SutherIA	×
> I > I	Manage Groups Manage People	Locale memberOf	Inum	@!C527.98AC.187E.020B!0001!7099.D2F6!0000!BNQE.WB3N	×
> / > 1	Add person Import People	Middle Name Nickname	Last Name	Sutherland	×
	Personal	OpenID Connect JSON formatted address Organization i-number PersistentId	Name search keywords	Ailsa Sutherland Sutherland	×
		Phone Number Verified Picture URL	User Status	active	×
		Preferred Language Preferred Username Profile URL	Username	SutherIA	×

Run identitySync in the undo mode. This is the only situation where a resource account is deleted.

## 4. IdentitySync with the Active Directory

If you have been using Gluu's Cache Refresh facility and the Gluu accounts are well synchronised with the Active Directory, identitySync can be used to check it. It will be run in info mode so that the changes that it intends to make can be seen before actually making them.

### Update Gluu2 Properties

Edit the Properties file Gluu2.properties, it is in the <installDirectory>\Tutorial1 directory. identityReport properties are consistent with identitySync and the same properties file is used for both applications.

#### Comment out the CSV identity file

// CSV File of Identities
// Tutorial AM3.3
//CSVIdentityResource1 = IdentityReportGluu1.csv

#### The parameters that need to be copied from Glu1.properties are:

```
LdapResource1 = ldaps://amx10.corp.example.com:1636
LdapAccountContainer1 = ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6,o=gluu
LdapDNTemplate1 =
inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!%random%.%random%,ou=people,o=@!C527.98AC.187E.020B!0001!7
099.D2F6,o=gluu
LdapObjectClasses1 = gluuPerson,ox-C52798AC187E020B00017099D2F6,top
```

- LdapResource1 is the resolvable DNS name of the target Gluu server.
- LdapAccountContainer1 is the ou identified in the Idap browser in the previous step. The same ou must be added to the DNTemplate
- IdapDNTemplate1, copy the preamble of the inum from an existing record, leaving the last two fields as random. A unique inum will be generated in the transaction file from this template.
- Check a record in the ou= people to see the objectClasses and add them to LdapObjectClasses1.

Update the ActiveDirectoryIdentity resource to suit your environment. Uncomment the ActiveDirectoryIdentityResource. other parameters that need to be updated are:

ActiveDirectoryIdentityResource1 = DC.corp.example.com ActiveDirectoryIdentityAccountContainer1 = ou=accounts,DC=corp,DC=example,DC=com ActiveDirectoryIdentityName1 = corp ActiveDirectoryIdentityUser1 = corp\philn

The User does not need to be an administrative account, the Active Directory is being read which is a very low level privilege.

#### Update the Active Directory password

If the computer running identitySync is not in the same domain as the Active Directory, create an ActiveDirectoryPasswd1.txt file, add the password to the first line. It will be encrypted when identitySync first runs.

#### Run identitySync

The results should be no creates, updates, disables or deletes.

C:\AMX\Tutoriall>..\identitySync.exe Gluu2.properties Warning: Not run as administrator Begins Fri, 01 Jul 2016 16:16:15 GMT analyze ActiveDirectoryIdentity1 DC.corp.example.com Extracted 103 Identities ActiveDirectoryIdentity Finished Fri, 01 Jul 2016 16:16:15 GMT Total of 103 Identities

LDAP1 Gluu

Extracted 102 Accounts Account joins 102 Account creates 1 Account updates 1 Account disables 1 Account deletes 0 LDAP Finished Fri, 01 Jul 2016 16:16:15 GMT Finished Sat, Fri, 01 Jul 2016 16:16:15 GMT

C:\AMX\Tutorial1>

The result is there is a create, an update and it's a disable. To find the account that is being updated, open the ActionFile.txt file. In this case it contained:

01/07/2016|Gluu;inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!IVWA.EX4N,ou=people,o=@!C527.98AC.187E.020 B!0001!7099.D2F6,o=gluu|Create|firstName=Ailsa;accountName=SutherlA;lastName=Sutherland;passwdTemplate=Cv cnCvcn

01/07/2016|Gluu;inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!2414.FA88,ou=people,o=@!C527.98AC.187E.020 B!0001!7099.D2F6,o=gluu|Update|active=Y|active=N

The meaning of this is that the directory entry will be updated, the old value is active=Y, the new value is N. Both the old and the new values are written to the transaction log so that the update can be undone if required. The difficulty with the Gluu distinguishedName is it cannot be found in the Gluu GUI. It cannot even be pasted into the search field. Using Apache Directory Studio the entry can be found by pasting the distinguished name into the Search Base.

Search Quick Se	earch $\Leftrightarrow \bullet \bullet \bullet$		
Search Name:	Quick Search		
Connection:	AMX10 Browse		
Search Base:	20B!0001!7099.D2F6,o=gluu ∨ 🕼 Br <u>o</u> wse		
Filter:	(objectClass=*) $\checkmark$ Filter Editor		
Returning Attributes:	givenName, sn		
Controls ManageDsalT Subentries Paged Search	Page Size: 100 Scroll Mode		
Scope <u>O</u> bject One <u>L</u> evel S <u>u</u> btree	Limits <u>C</u> ount Limit: 1000 <u>T</u> ime Limit (s): 0		
Aliases Dereferencin Finding Base DN Search	ing Referrals Handling N <ul> <li>Follow Referrals manually</li> <li>Follow Referrals automatically</li> <li>Ignore Referrals</li> </ul>		
	Search Quick Se Search Name: Connection: Search Base: Filter: Returning Attributes: ManageDsalT Subentries Paged Search Scope Object One Level Subtree Aliases Dereferenci Finding Base DN Search		

The alternative is to look in the IdentityReportGluu1.csv created in the first step.

As an example, this is the result of running identitySync in the update mode

```
C:\AMX\Tutoriall>..\identitySync.exe Gluu2.properties do
Warning: Not run as administrator
Begins Fri, 01 Jul 2016 16:17:10 GMT do
ActiveDirectoryIdentity1 DC.corp.example.com
Extracted 102 Identities
ActiveDirectoryIdentity Finished Fri, 01 Jul 2016 16:17:10 GMT
Total of 102 Identities
```

LDAP1 Gluu

Extracted 102 Accounts Account joins 102 Account creates 0 Account updates 1 Account disables 1 Account deletes 0 LDAP Finished Fri, 01 Jul 2016 16:17:10 GMT

LDAP1 Gluu LDAP Load Gluu Update do inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!2414.FA88,ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6 ,o=gluu => active=N Finished Fri, 01 Jul 2016 16:17:10 GMT

C:\AMX\Tutorial1>..\identitySync.exe Gluu2.properties undo Warning: Not run as administrator Begins Fri, 01 Jul 2016 16:17:25 GMT undo

LDAP1 Gluu LDAP Load Gluu Update undo inum=@!C527.98AC.187E.020B!0001!7099.D2F6!0000!2414.FA88,ou=people,o=@!C527.98AC.187E.020B!0001!7099.D2F6 ,o=gluu => active=Y Finished Fri, 01 Jul 2016 16:17:25 GMT

C:\AMX\Tutorial1>