AMX Tutorial Managing Unix Accounts

This tutorial is for IT staff who are experienced in identity management, it requires insight into Unix and Windows. AMX uses ssh to communicate with the Unix system. An ssh client is recommended to verify that ssh is working and working on port 22.

This exercise will demonstrate some of the more advanced features of AMX, specifically:

- Managing Unix accounts on Linux. Solaris works similarly.
- Using identityReport to extract Unix accounts for use as an Identity source
- Synchronising accounts with the Identity source
- Extracting, Transforming and Loading the Comment or GECOS field
- Sending status reports using email

1. Setup

AMX runs on Windows and must be setup as shown in the AMX Tutorial Setup document. In this tutorial identityReport and identitySync are run from the Command Line using AMXRun which sets the environment variables, in production it is expected to be run by the Task Scheduler.

2. Create an Identity Source

For the tutorial a CSV file will be created as an Identity Source from the Unix system. In production a spreadsheet might be used or the Active Directory used with a filter to extract only those persons who are a member of a special group entitling them to Unix privileges, for example LinuxAdmins. This group might have no meaning and is never used to give privileges or access to resources in Windows.

Review Unix1.properties Properties

Open the identityReport Properties file Unix1.properties, it is in the <installDirectory>\Tutorial1 directory. Note:

- Other Account resources such as the ActiveDirectory are commented out.

  ```
  // Systems
  //ActiveDirectoryResource1 = dc1.example.com
  ```

  The Unix resource parameters that will need updating are:

  ```
  // Systems
  UnixResource1 =
  UnixName1 = AMX5
  UnixSchema1 = UnixSchema1.txt
  UnixUser1 =
  UnixPasswd1 = UnixPasswd1.txt
  UnixType1 = Linux
  UnixFilterValue1 = 1000
  ```

  - UnixResource1 is the DNS name or ip address of the system.
  - UnixUser1 is the account name on the Unix system.
  - Create a UnixPasswd1.txt file and add the password in the first line, it will be encrypted when identityReport first runs.
  - UnixFilterValue1 selects accounts with uids greater than or equal to the value. It can be changed to suit. Run identityReport with the value 0 to see all the accounts and then select the ones you need.

    A value of 1000-1999 will only extract accounts with uids between 1000 and 1999.

    A value of 50:51:55 will extract 3 accounts with those uids. See the AMX reference guide for more details.
  - UnixType, Linux or Solaris

Review Unix Schema File

The schema file UnixSchema1.txt does not need any modification unless the comment field in /etc/passwd is non-standard. The schema file matches an entry such as:

```
   albonw:x:1000:1000:Alban Wilson,Edinburgh,0845 085 5555,0781 409 5555,00075151:/home/albonw:/bin/bash
```

If the comment or gecos field does not use ‘,’ the schema file must be modified. The comment field is f4

```
f4,fullName;left0,
f4,firstName;left0,;left0 ;nosync
f4,lastName;left0,;right0 ;nosync
f4,location;left1,
f4,telephone;left2,
f4,mobile;left3,
f4,employeeID;left4,;unique;join
```

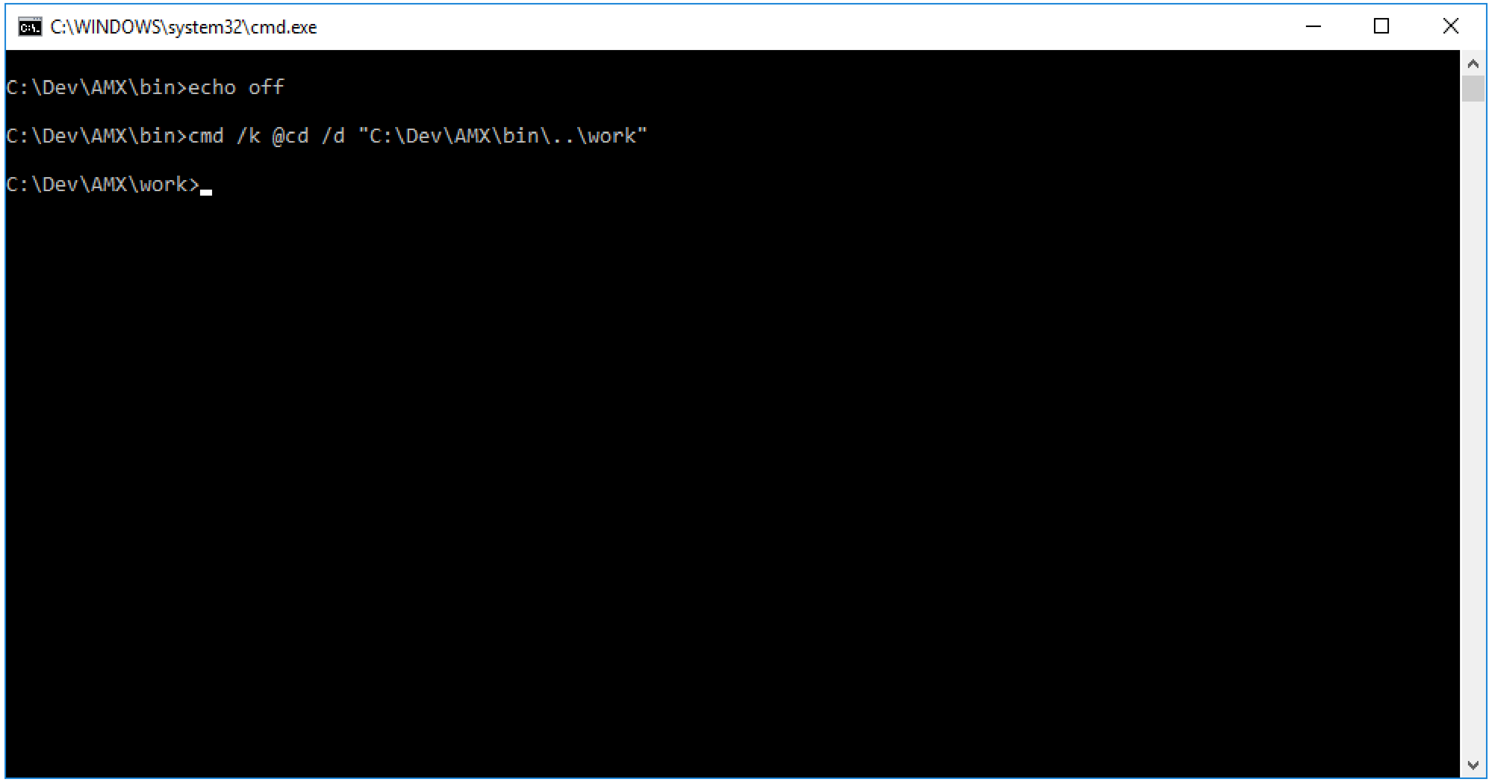
The schema makes extensive use of the substring Attribute Modifiers left and right. If the comment delimiter is something other than “,” change the left attribute modifier to suit. For example if the comment uses”;” change the modifier to left;;

Update Unix Passwd

When UnixUser1 is defined, enter the password in the first line of the UnixPasswd.txt file. The password will be encrypted when identityReport runs and the clear text password removed.

Run identityReport

AMX runs on Windows and must be setup as shown in the AMX Tutorial Setup document. In this tutorial identityReport and identitySync are run from the Command Line using AMXRun which sets the environment variables.



```
C:\Dev\AMX\bin>echo off

C:\Dev\AMX\bin>cmd /k @cd /d "C:\Dev\AMX\bin\..\work"

C:\Dev\AMX\work>
```

This will open a Command Prompt.

Change directory to Tutorial1 and run identityReport.exe which is in the parent directory.

Change directory to Tutorial1 and run identityReport.exe

```
C:\AMX\Tutorial1>identityReport.exe Unix1.properties
Begins Mon, 31 Oct 2016 13:22:00 GMT
```

```
Total of 0 Identities

Unix System1 AMX5.corp.example.com
OK
Extracted 6 Accounts
Finished Mon, 31 Oct 2016 13:22:04 GMT

C:\AMX\Tutorial1
```

This has created IdentityReportUnix1.csv. 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.

Error: Unix Extract Auth fail
    Bad username or password

Error: Unix Extract cannot find Linux Header of lastlogon
    Error typically caused by running against a non Linux Unix system, for example SunOS

Error: Unix Extract ssh connection to < strServer> failed.
    Connection was OK but ssh is aborting. Check with ssh client.

3. Synchronize Accounts

Review Unix2 Properties

Edit the identitySync Properties file Unix2.properties, it is in the <installDirectory>\ Tutorial1 directory. Note the schema used by the CSV identity file

```
// Tutorial UX1
//CSVIdentityschema1 = IdCSVschemaUnix1.txt
```

Additional properties are:

- DefaultGroup, optional property. The name or gid of the user’s default group on create. If omitted the Unix O/S default group is used as shown by useradd -D.

- DeletedGroup, optional property. The name of a group which is used to identify users that have left the organisation and no longer have an identity record. When using v leave this blank or don’t define it to see all the accounts. When using identitySync leave this blank and accounts belonging to persons that have left the organisation and have no identity record will be identified as ghosts. These will not be deleted, but they will appear in the transaction file Action.txt unless the UnixLoadMode = CRUD and not CRUDD.

Run identitySync

Run identitySync with no changes to IdentityReportUnix1.csv and identitySync will report no updates

```
    C:\AMX\Tutorial1 >identitySync.exe Unix2.properties
    Error: must be run as an admin
    Begins Tue, 10 Feb 2015 20:21:15 GMT  analyze
    CSVIdentity 1 C:\AMX\Tutorial1\IdentityReportUnix1.csv
    Last updated 10/02/2015 20:20:28
```

```
Extracted 3 Identities
CSVIdentity Finished Tue, 10 Feb 2015 20:21:15 GMT
Total of 3 Identities

Unix1 AMX5.corp.example.com
OK
Extracted 3 Accounts
Account joins    3
Account creates  0
Account updates  0
Account disables 0
Account deletes  0
Unix Finished Tue, 10 Feb 2015 20:21:32 GMT
Analysis Ends Tue, 10 Feb 2015 20:21:32 GMT
Ends Tue, 10 Feb 2015 20:21:32 GMT

C:\AMX\Tutorial1 >
```

Check Action.txt there will be no transactions.

Update identities

Make changes to IdentityReportUnix1.csv. For example create a new account, modify the comment, change an account from active to disabled or viceversa.

Run identitySync

Re-run identitySync and check Action.txt. It will contain transactions for each change made to account in IdentityReportUnix1.csv. No changes will be made to the Unix system until identitySync is run in the "do" mode. The changes will be made using Unix shell commands. The commands are shown in the Manual files UnixManualDo1 and UnixManualUndo1. For example:

```
# Begin 10/02/2015
```

```
sudo usermod -G HunterC,adm,mail,deleted HunterC
sudo usermod -G "adm,admin" philn
sudo usermod -G "adm,lpadmin,admin,mail" -c "Philip Ness,London,0870 085 8555,0781 409 5555,120"
philn
sudo useradd -m -G "adm,fuse" -c  "Paul OBrian,London,0870 085 8555,0781 410 5555,123" -s /bin/bash
obriano
```

These commands can be run by copying and pasting them into a shell, to run these commands automatically:

```
C:\AMX\ Tutorial1>identitySync.exe Unix2.properties do
```

Changes are reversed using the UnixManualUndo1 or the undo mode.

```
C:\AMX\ Tutorial1>identitySync.exe Unix2.properties undo
```

4. Deconstructing the Comment or GECOS field

The Comment or GECOS field, field 4 of /etc/passwd. GECOS has comma separated subfields, commonly:

- Fullname
- Location, building or room number
- Office phone number
- Other contact phone number
- Other information, for example employee number

If the comment field follows the GECOS format the subfields can be extracted transformed and loaded using g0 – g4 as below:

```
Fullname,Location,
albonw:x:1000:1000:Alban Wilson,Edinburgh,0845 085 5555,0781 409 5555,00075151:/home/albonw:/bin/bash
f0 --^
```

```
f2 -----------^
f3 ----------------^
f4 -----------------------------------------------^
g0 ------------------------^
g1 -----------------------------------^
g2 --------------------------------------------------^
g3 ----------------------------------------------------------------^
g4 --------------------------------------------------------------------------^
f5 ------------------------------------------------------------------------------------^
f6 -----------------------------------------------------------------------------------------------^
```

An alternative approach is to synchronise the whole field, so the Unix schema contains:

```
f4,comment
```

with the identity source constructing the comment field using a concat attribute modifier:

```
,comment;concat:%fullName%,%location%,%telephone%,%mobile%,%employeeID%
```

This is useful when the comment field does not have "," delimiters. If the comment field contains a Unix attribute that will be used for a join it can be extracted in the Unix schema by using the attribute modifier "left" to get the subfield from comment. "left" subfields start from zero:

```
f4,employeeID;left4,;unique;join;nosync
```

5. email

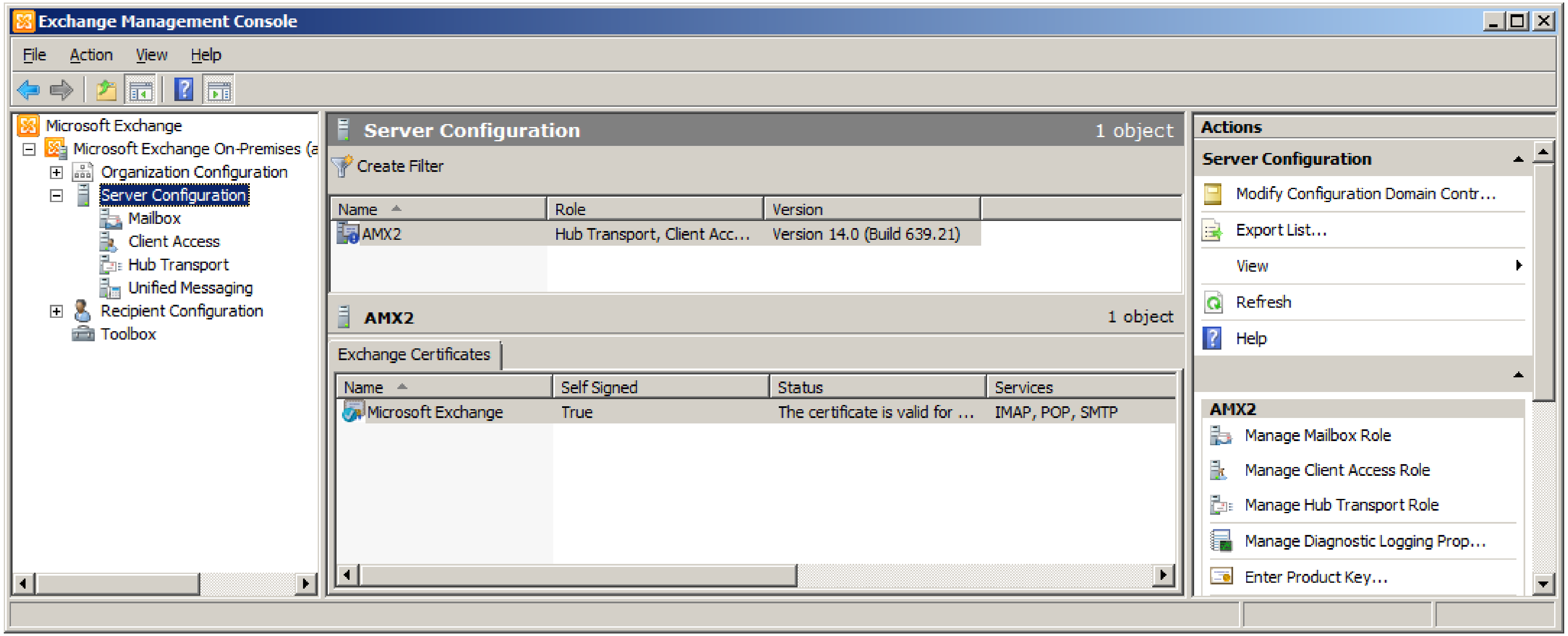
AMX is designed to be run as a scheduled task, communicating with administrators using email. identitySync email uses .NET Mail which is SMTP with Explicit SSL which opens a connection in the clear and then sends StartTLS to begin encryption. It does not open the connection using encryption, see Microsoft documentation for full details.

The eMail sends the info and debug log when configured, so any mail error message is only available on the console. It is not in the logs.

Exchange

Configuration for Exchange in Unix2.properties:

- SMTPaccount cannot be administrator, Exchange application event log shows “provided valid credentials, but is not authorized to use the server”.
- SMTPssl must be true, when false Exchange application event log shows “The SMTP server requires a secure connection or the client was not authenticated”.
- Check the certificate that SMTP is using in the Exchange Management Console / Server Configuration



Name	Role	Version
AMX2	Hub Transport, Client Acc…	Version 14.0 (Build 639.21)

Name	Self Signed	Status	Services
Microsoft Exchange	True	The certificate is valid for …	IMAP, POP, SMTP

Note that the certificate is self-signed and that it cannot be exported from the EMC. Use Certificate Management to do this, and then install it on the system running AMX.

Gmail

Configuration for gmail. https://support.google.com/a/answer/176600?hl=en . The “lesssecure” security setting must be true, or an email will be received with the subject “Google Account: sign-in attempt blocked”. To understand and activate “lesssecure” visit https://support.google.com/accounts/answer/6010255?hl=en

- SMTPserver = smtp.gmail.com

- SMTPssl = true
- SMTPport = 587
- SMTPaccount = ****@gmail.com
- SMTPpasswd = GmailPasswd.txt

Test

1. Run identitySync.exe in analyse mode, the info, debug and manual emails will be will be sent as configured.

2. Check the console for errors, the info.txt file and debug.txt files are not updatable by the email process because they are closed while being sent, so any errors are written to the console only.

3. Set mailMode back to 2 (inhibit email) in Unix2.properties.

The info message format is:

```
Begins Sun, 16 Nov 2014 19:13:12 GMT  undo

Unix System 1 AMX6.corp.example.com
Unix Load AMX6 Delete HunterC
Unix Load AMX6  Update undo philn => location=Edinburgh;gecos=Philip Ness,Edinburgh,0870 085 8555,0781
409 5555,120
Unix Load AMX6 Create undo OCreateO
Ends Sun, 16 Nov 2014 19:13:15 GMT
```

These info messages are expected to be checked by an administrator and then moved to a mail folder where they can be searched during an audit. AMX also writes an audit file when identitySync.exe is run in the do or undo mode. The audit file is not tamperproof (unlike the ActionFile), but it is tamper evident. It can be used to do multi-level undos with identitySync.

To create an Audit file:

1. Update Unix2.properties, and set the name of the audit file, for example

   ```
   LoggingAuditFile = C:\data\AMX\Audit2012\ActionAudit.txt
   ```

2. Run identitySync.exe in the do mode to write an entry in the audit file. Check the audit file, it will only contain actions that were successfully completed. The info file shows actions and their outcomes. For example:

```
16/11/2014|AMX6;HunterC|Delete|
16/11/2014|AMX6;philn|Update|location=Edinburgh;gecos=Philip Nesfield,Edinburgh,0870 085 8555,0781 409
5555,120|location=London;gecos=Philip Nesfield,London,0870 085 8555,0781 409 5555,120
16/11/2014|AMX6;OCreateO|Create|fullName=One
OCreate;accountName=OCreateO;location=London;employeeID=123;telephone=0870 085
8555;memberAdd=adm:mail;gecos=One OCreate,London,0870 085 8555,0781 410 5555,123;active=Y;mobile=0781
410 5555;passwdTemplate=CvcnCvcc
Ends|KNj3wk4560Gr8WL/hJeUgQ==
```

6. Debugging

The debug file as defined in Unix2.properties has two features, the level of detail and the account name of one user to display. The debug file is mailed to the DebugRecipents when the mailMode is < 2, and a file called debug.txt is written to the current directory.

```
    DebugSubject = Example Domain Debug
    DebugRecipients =
    LoggingLevel = 2
    DebugUser = SutherlandA
```

The DebugUser is reported when the LogLevel is 2 or greater.

LogLevels are:

1 debug log matches info. Minimal logging.

2 configurations, debugUser

3 details of configurations

4 identity and resource record names

5 details of identity and record attributes

Loglevel 5 includes a record of every identity and account extracted and therefore can be very large.

The debug.txt is overwritten on every run and is intended to be sent by email by updating the following properties in Unix2.properties:

```
DebugSubject = Ubuntu Debug
DebugRecipients = administrator@example.com
```