Access Management - Role Mining Tutorial

This tutorial shows the use of roleAnalyze to mine roles from an application dump of identities and their responsibilities. AMX tools such as identityReport can prepare these files from Resources such as the Active Directory, and roleAnalyze can prepare reports and batch files to create roles for identitySync.

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.

Identity and Responsibility Application Reports.

The AMX install has reports from an application for use with roleAnalyse in the Tutorial3 directory.

1. Review the roleAnalyzer Properties File

Open the roleAnalyzer1.properties file. The full description of the properties are described in the AMX Access Management Document. The key ones are:

- IdentityResource1, the name of the file containing the identities
- RespResource1, the name of the file containing the responsibilities
- roleReport, the file which will have the results of the analysis.

2. Review the Identities File

This is a dump from an Enterprise CRM system, the file users.csv contains the account names and their roles. This is the only Attributes that roleAnalyzer uses, all other information has been removed.

3. Review the Identities Schema

The roleAnalyzer1.properties file has the name of a Schema file in IdentitySchema1. This contains the Staging Attribute name which corresponds to the column name in the header of the Identities file, and the Metaverse attribute name. Notice that the Staging name has “’”s, which are removed using the “replace” attribute modifier. AMX has a rich set of Attribute Modifiers that are described in the Reference documentation.

roleAnalyzer requires a Metaverse Attribute named role. This is constructed by concatenating the MRU and the BU with the Attribute Modifier “concat”.

4. Review the Responsibilities File

The file resps.csv contains user account names and their responsibilities. Where an individual has multiple responsibilities these are on subsequent lines. Notice this application use single quotes.

```
'personID','responsibility'
```

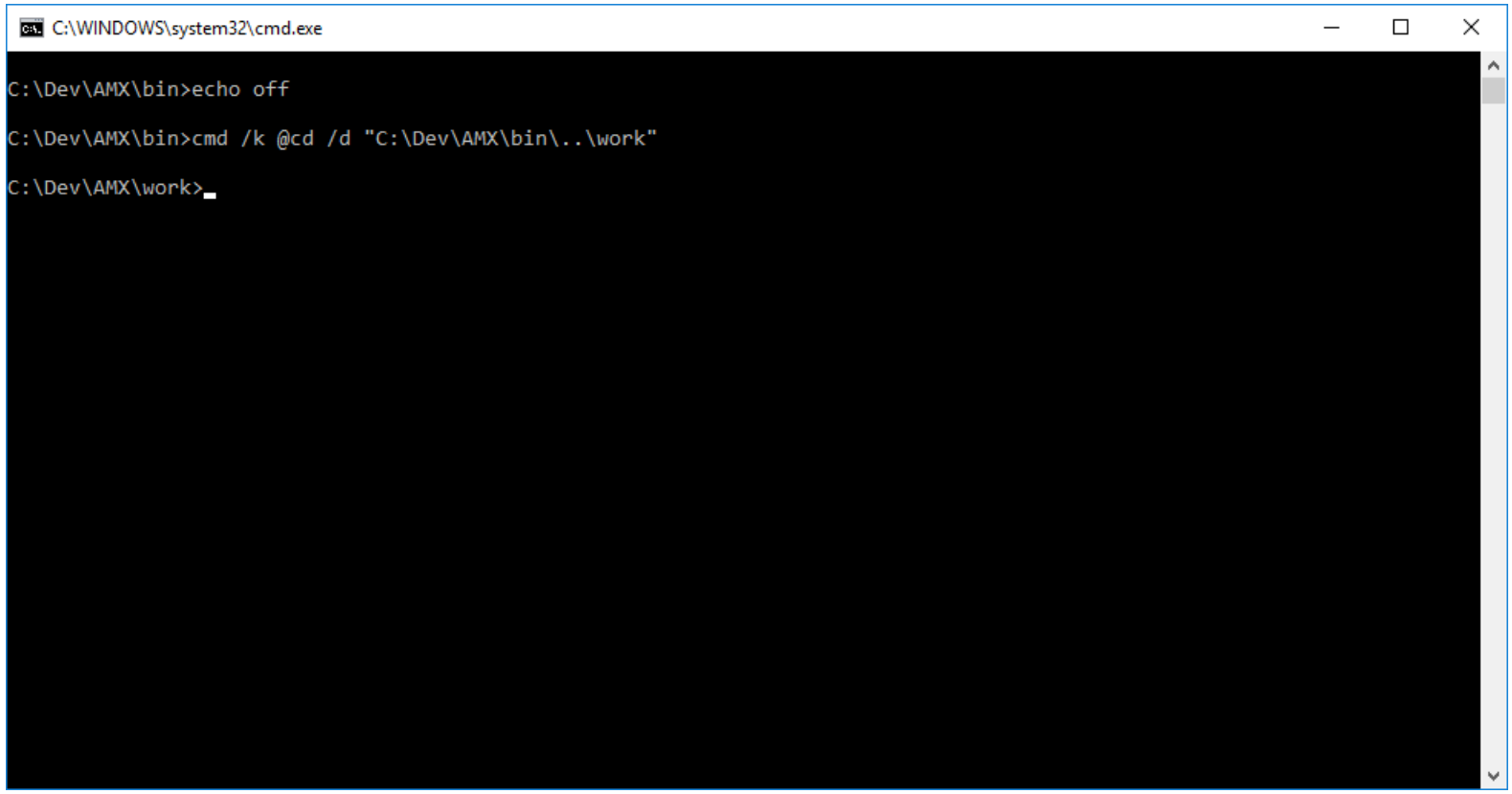
```
'00000528','Agreements - RO'
'00000528','Common User'
```

5. Review the Responsibilities Schema

The Responsibilities Schema has an Attribute flag “join”, this specifies how the responsibilities are matched to their owner. In this case it is using “personID”.

6. Run roleAnalyze

Right click on AMX Run in the Start Programs menu or AMXRun.bat in the installation directory bin.



```
C:\AMX\Tutorial3>roleAnalyze roleAnalyze1.properties
Begins Mon, 31 Oct 2016 12:48:58 GMT
Identity 1 users.csv
Extracted 8973 Identities
Responsibilities 1 resps.csv
Extracted 94345 Responsibilities
Number of roles skipped 154 (less than min population=10)
Number of roles in report is 150
Finished Mon, 31 Oct 2016 12:49:02 GMT

C:\AMX\Tutorial3>
```

7. Review the Results

150 roles were found and 154 were discarded because the number of users was smaller than the minimum. The results of the analysis are in file specified in the property “roleReport”. Scroll down to the third role “LCS PLS19 SERVICE CCC - PLW53 LSC”. This has a Quality Factor of 0.987.

The quality of roles are calculated from the responsibilities in the resultant role.

For each responsibility the number of persons with the responsibility is accumulated into a running total. The final total is divided by the perfect total, which is when every responsibility has every person assigned to it. A score of 1.0 is perfect, less than 1.0 is less than perfect. For example:

```
10, responsibility1
10, responsibility2
10, responsibility3
10, responsibility4
10, responsibility5
```

Is a perfect role definition. Whereas:

```
10, responsibility1
10, responsibility2
10, responsibility3
6, responsibility4
4, responsibility5
```

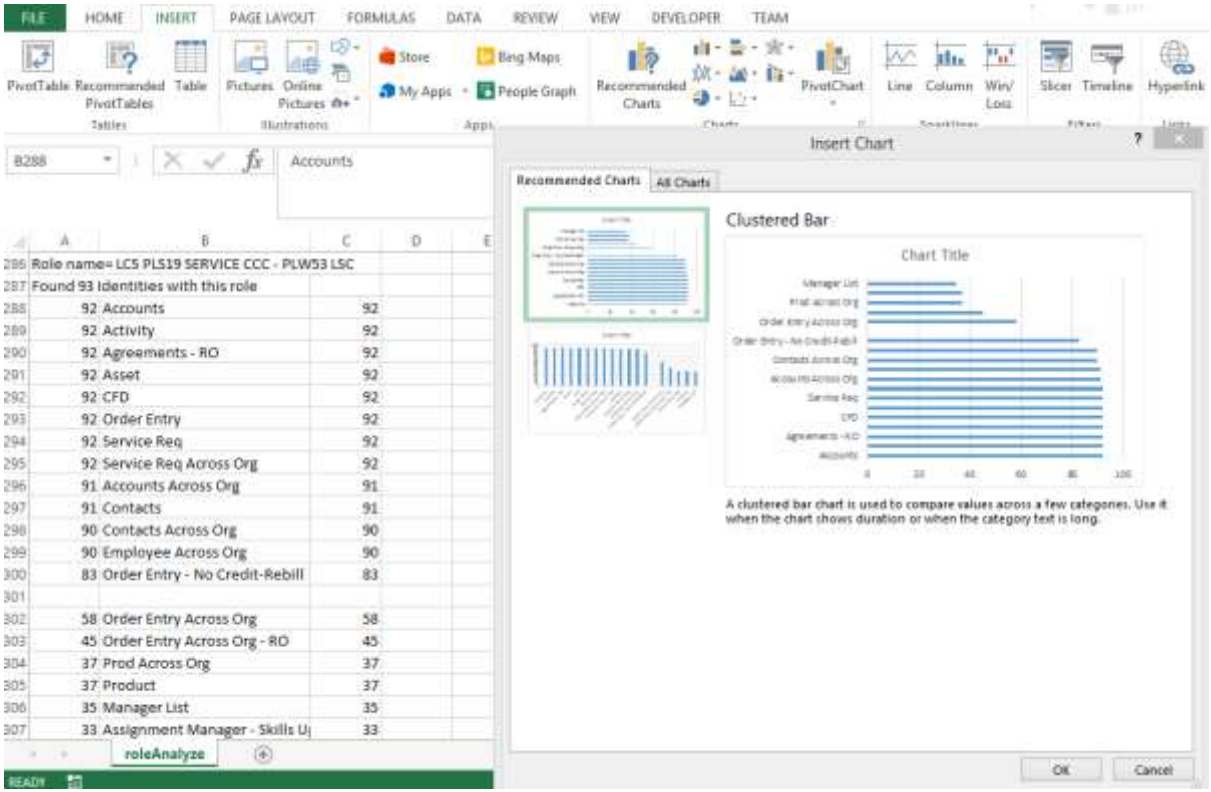
Is not. The running total is 40, compared with a perfect score of 50. The Quality Factor is 40/50 = 0.8. A poor quality such as 0.5 would be:

```
10, responsibility1
4, responsibility2
```

```
4, responsibility3
4, responsibility4
3, responsibility5
```

The running total is 25, giving a Quality Factor of 25/50 = 0.5.

The quality of “LCS PLS19 SERVICE CCC - PLW53 LSC” can be visualised by inserting a “Recommended Chart” from the “Insert” menu item.



This role will have to be discussed with the Application Specialist. Notice that every individual has “Order Entry”, most have “Order Entry – No Credit-Rebill” which must be a responsibility with less privilege. There are also about half the individuals with “Order Entry Across Org” which must be a more powerful role than “Order Entry”. These are Nested Responsibilities, often the application has a table describing them. If a Parent Role is discretionary, that is an

individual is assigned the responsibility as part of a Request and Approve process the discretionary privileges can be removed from the report by adding them to “roleIgnoreResp”.

In this case the problem is probably responsibility creep. Responsibilities have been added a required, and it has never been determined if everyone needs “Order Entry Across Org” or if it is given to individuals with some other criteria, such as only those who have been in the role 3 years, or are graded excellent in their annual reviews. Role Based Access Control need to be based on rigorous rules. roleAnalyzer can use these rules given enough information, until then its results allow these anomalies to be identified and resolved.

Active Directory Role Mining

roleAnalyzer can review Active Directory groups for consistency and identify roles for use directly by identitySync.

Only attempt this exercise if your Active Directory is well managed, has rich and accurate user attributes and you have completed the Active Directory tutorials.

1. Extract Accounts from the Active Directory

Copy the ActiveDirectory2.Properties file an earlier tutorial AD1:

- ActiveDirectoryResource1 with the DNS name of a Domain Controller
- ActiveDirectoryAccountContainer1
- ActiveDirectoryUser1 leave blank if identityReport is being run on a system that is a member of the domain

If appropriate:

- ActiveDirectoryFilterValue1

These properties are the same for all AMX tools and are fully explained in the first tutorial AD1 and the User Reference document. It will be run with a different ActiveDirectorySchema1.csv file that will extract groups.

Run identityReport.exe ActiveDirectory2.properties.

Possible errors are detailed in the earlier tutorial, with the addition of:

> Error: ActiveDirectory ExtractMembers circular recursion of <group> in <group>
>
> The memberNested Staging Attribute ExtractMembers has found group1 is a member of group2 and group2 is already a member of group1.

2. Review the Active Directory Report

The report are in a file IdentityReportAD2.csv as specified by the property Report. Specifically check:

- Groups are correctly extracted, they are all on a single line
- Attributes that can be used to define roles. Typically Title or Description

3. Update Identity Schema

The file IdentitySchemaAD.txt uses title as the role descriptor. If there are more suitable attributes, update the Staging Name (first name on the line) leaving the Metaverse Attribute name as “role”.

All the Metaverse Attribute modifiers described in the Reference documents are available for use. For example if the role needs to be the combination of two or more attributes use “concat”. For example:

```
description,description
department,department
,role;concat:%description% %department%
```

4. Run roleAnalyze

Run roleAnalyze and check the debug file. Locate the section

```
Role Table ============================================================
ASSURANCE SOLUTIONS DIVISION
ATM CT BUSINESS CENTER
ATM CT BUSINESS CNTR
ATM CT BUSINESS CREATION
ATM CT CENTER OF EXPERTISE
ATM CT CUSTOMER TEAM STAFF
...
```

Where there are inconsistent role names, they can be normalised using “replace” in the schema. For example:

```
title,role;replace/CNTR/CENTER/
```

Re-run roleAnalyze and repeat until the role names are consistent.

5. Review Results

The results are in the file specified in the property roleReport. Open it in Excel. Key indicator of the quality of the roles is the Quality Factor, anything less than 0.8 means that the role needs investigation.

See Reference documentation for details of the Role Quality Factor.

Issue 1 Individuals with no responsibilities.

With a population of 28 there are only 24 individuals with responsibilities. Why do some 4 individuals have no responsibilities? In this situation the administrator has perhaps removed responsibilities rather than disabled the account. It is critical that an Identity Management system does not reverse this until an alternative process is put in place for individuals that leave the organisation.

Issue 2 Individuals with missing responsibilities – Nested Responsibilities

In the example above there are 4 individuals that do not have “PI - 1b - Order Entry - No Credit-Rebill”. This needs to be investigated to see if this is an omission or if this responsibility is a subset of a responsibility they already have, for instance “PI - 1b - Order Entry”. This would have to be resolved by an application specialist, and then “PI - 1b - Order Entry - No Credit-Rebill” might be removed from the role as superfluous.

Situations where a responsibility is included in another responsibility that an individual already has is a Nested Responsibility. In situations where groups can be members of other groups makes the situation obvious. Where it is part of the application’s access control, as in the example above, this should be defined in the application’s documentation.

Issue 3 Resultant Responsibilities - Nested Roles

Nested Roles cause a problem for roleAnalyzer. The parent role will simply have all the responsibilities of the child role and some extra ones. The Individuals having the parent role are often Team Leads or Managers, or global staff as opposed to local. The difficulty for roleAnalyzer is when the roles cannot be discriminated, that is there is no information from Identity records concerning the additional responsibilities of some (unknown) number of individuals to determine who should have the parent role.

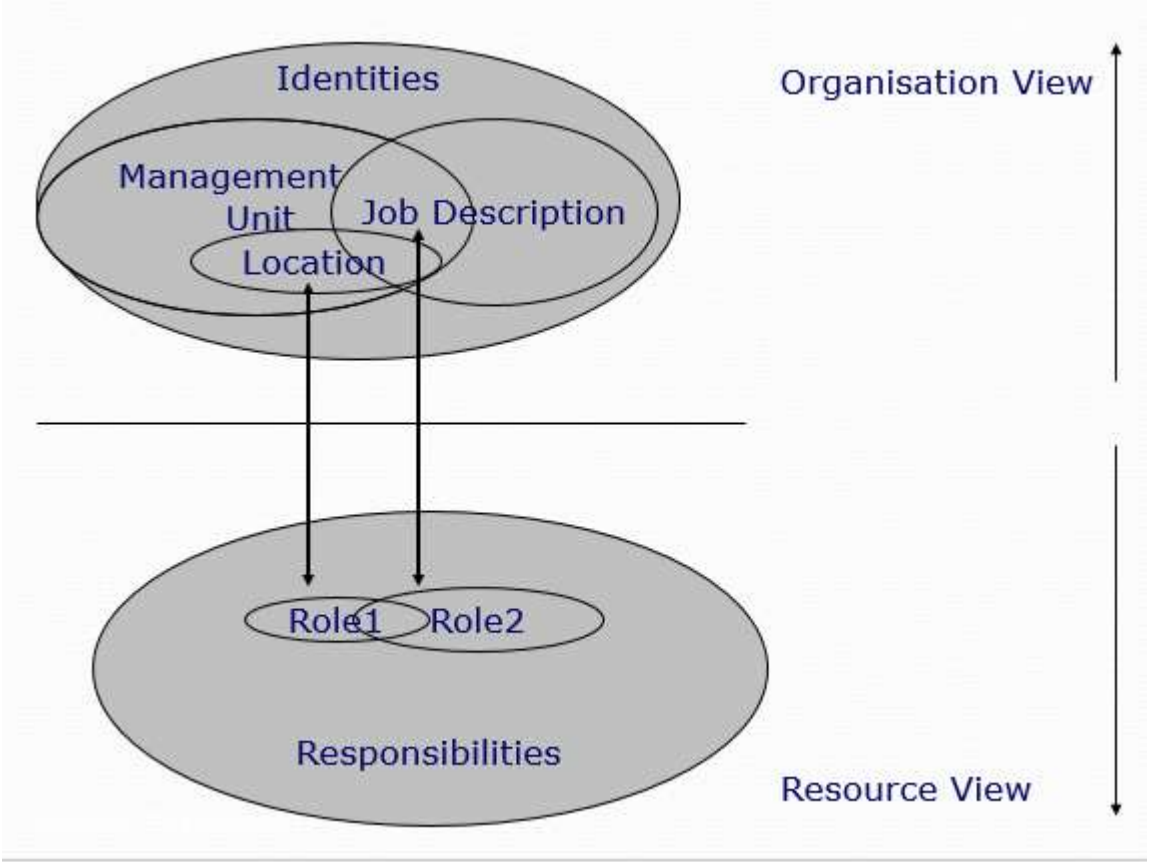
In some cases the parent role is discretionary, and the extra responsibilities have been given after a Request and Approve process rather than as part of a role. Responsibilities provisioned in this way must be excluded from roleAnalyzer. Often this is simple, the Request and Approve process has a database of responsibilities that it provisions, and an extract, a file containing the responsibilities can be given to roleAnalyzer to ignore in the property roleIgnoreResp.

Issue 4 Resultant Responsibilities – Multiple Roles

When responsibilities are given to a few individuals because they are performing multiple roles, as in this example below, the combined roles, the one with the largest number of individuals has a poor consistency. When better granularity is used and the role is split into two sub-roles, it can be seen that each sub-role has better consistency.

Issue 5 Incorrect Role Definition

Another issue that has caused problems is when Roles are defined differently when viewed by the Organisation compared to the Application Owner. In the example below, Role1 is based on the Management Unit and Location, while Role2 is based Management Unit and Job Description.



When roleAnalyze reports the Responsibilities associated with each Role, they will be different. Only the Application Administrator can define the Roles, the bigger Issue is when Role characteristics used by the Administrator are not available to roleAnalyzer. In this case it is necessary to find where the Administrator got the information, so that it can be used by roleAnalyze.

6. CreateRoles

The Role Create file name is defined in the property roleOutFile. It is intended to be used as a batch file to create the roles in the application. The template allows text and substitution of %role% and %responsibilities%. For example a template:

dsadd CN=%role%,OU=Roles,DC=corp,DC=Example,DC=com -samid %role% -desc Role Definition -memberof %responsibilities%

will create a batch file for the Active Directory to make role templates for identitySync. When identitySync is configured to use roles with the same role definition in the Schema, the roles will be managed as individual's attributes change.

Make changes to the template to create roles in the Active Directory, for example changing the Distinguished Name.