Example Role Mining & Peer Analytics Endpoint

What is Role Mining & Peer Analytics?

The process of creating role objects or functional groupings (peers), through the analysis of users and their functional characteristics (top down mining), or via their associated system entitlements (bottom up mining). A mixture of the two (hybrid mining) is the most scalable and pragmatic.

What are Roles & Peer Groupings?

Groupings of users and associated entitlements to make system provisioning faster and less error prone, whilst also identifying user entitlement exceptions that fall outside of a peer comparison. Peer comparison is a natural byproduct of creating roles based on functional groupings and can dramatically reduce the need and time of certification and attestation project, by simply analysing the most high-risk entitlements, or entitlements that are unique across peer workers.

The following example, goes through an example 3-step approach to firstly create roles and associated users, secondly to identify entitlements associated with those roles by analysing a target system and finally to identify any user exceptions - that is, entitlements that fall outside of the role framework.

Note, this is a set of examples, with limited security, error checking or performance testing (tested against 1000 users).

Setup

All code is available for download here - https://github.com/smof/openIDM_peer_analytics_extension. This contains Javascript analyzers and .json endpoint configuration files. You will also need to edit the access.js file with appropriate permissions to access the endpoints. Copy the Javascript files into the ../script directory and any *.json files into ../conf. There is an assumption that the managed/user object has an attribute that contains a functional grouping such as job title, project, business unit and so on. A target system that contains an entitlement attribute should also be present. For example AD and the memberOf attribute.

peerAnalysis

GET http://idm.example.com:8080/openidm/endpoint/peerAnalysis?sourceSystem=managed/user&sourceAttribute=jobTitle&userAttribute=_id

sourceSystem: system to analyse that will contains user and functional grouping. Defaults to managed/user but could be any integrated system

sourceAttribute: attribute within sourceSystem that contains functional grouping

userAttribute: unique user attribute that will be saved within the role object

Returns: {"roleName" : ["user1", "user2"] ...}

peerEntitlements

POST http://idm.example.com:8080/openidm/endpoint/peerEntitlements?sourceSystem=AD&sourceAttribute=groups

sourceSystem: system to analyse that will contains user and their respective entitlements

sourceAttribute: attribute within sourceSystem that contains user entitlements

payload: JSON from createRoles

Returns: {"roleName" : ["entitlement1", "entitlement2"] ...}

Only entitlements that are common across ALL users in a given role are returned.

peerExceptions

POST http://idm.example.com:8080/openidm/endpoint/peerExceptions?sourceSystem=AD&sourceAttribute=groups&user=J10000

sourceSystem: system to analyse that will contains user and their respective entitlements

sourceAttribute: attribute within sourceSystem that contains user entitlements

user: user ID analyse

payload: JSON from createRoleEntitlements

Returns: {"Exceptions" : ["entitlement1", "entitlement2"], "User_Effective_Entitlements" : ["entitlement1", "entitlement2"], "Role_Effective_Entitlements" : ["entitlement1", "entitlement2"].}

Example Run Through

System Entitlements:

```
id,groups
J100000,cn=App_cyclops;cn=backup_operators;cn=App_salestracker2.1;cn=Sage;cn=Intranet_news;cn=backup_operators;cn=Intranet_dept;cn=App_aptana;cn=Distribution_List_Liverpool
G100000,cn=App_cyclops;cn=backup_operators;cn=App_salestracker2.1;cn=Sage;cn=Intranet_news;cn=Sharepoint_intranet_edit
R100000,cn=App_cyclops;cn=backup_operators;cn=App_salestracker2.1;cn=Sage;cn=Intranet_news;cn=Sage;cn=App_partner_register_0.8
P100000,cn=App_cyclops;cn=backup_operators;cn=App_salestracker2.1;cn=Sage;cn=Intranet_news;cn=App_eniga_research_engine;cn=York_Printing
```

1 - GET ../peerAnalysis?sourceSystem=managed/user&sourceAttribute=jobTitle&userAttribute=_id

Result:

```
{"Managers":["G100000","P100000","J100000","R100000"]}
```

2 - POST ../peerEntitlements?sourceSystem=AD&sourceAttribute=groups

```
Data = {"Managers":["G100000","P100000","J100000","R100000"]}
```

Result:

```
{"Managers":["cn=App_cyclops","cn=backup_operators","cn=App_salestracker2.1","cn=Sage","cn=Intranet_news"]}
```

3 - POST ../peerExceptions?sourceSystem=AD&sourceAttribute=groups&user=J100000

```
Data = {"Managers":["cn=App_cyclops","cn=backup_operators","cn=App_salestracker2.1","cn=Sage","cn=Intranet_news"]}
```

Result:

```
{Exceptions: ["cn=Intranet_dept", "cn=App_aptana", "cn=Distribution_List_Liverpool"] ,
Roles_Effective_Entitlements: ["cn=App_cyclops", "cn=backup_operators", "cn=App_salestracker2.1", "cn=Sage", "cn=Intranet_news"] ,
J100000_Effective_Entitlements: ["cn=App_cyclops", "cn=backup_operators", "cn=App_salestracker2.
1", "cn=Sage", "cn=Intranet_news", "cn=backup_operators", "cn=Intranet_dept", "cn=App_aptana", "cn=Distribution_List_Liverpool"] }
```