Role Based Access Control (RBAC)

Users and Roles

Open-AudIT has moved away from providing access via the group system to a more flexible system using Roles.

A Role contains a set of permissions (create, read, update, delete) for endpoints (devices, locations, scripts, etc).

A User in Open-AudIT is a member of one or more Roles.

There are four roles provided with Open-AudIT. These can be changed and new Roles created.

An example of a database record for a Role is below (in this case, the org_admin Role).

```
        id: 2
      name: org_admin
description: This role is used for administration of endpoints that contain an org_id.
permissions: {"charts":"crud","connections":"crud","credentials":"crud","summaries":"crud","devices":"crud","
discoveries":"crud","fields":"crud","files":"crud","graph":"crud","groups":"crud","invoice":"crud","licenses":"
crud","locations":"crud","networks":"crud","orgs":"crud","queries":"crud","scripts":"crud","search":"crud","
sessions":"crud","users":"crud"}
   ad_group: open-audit_roles_org_admin
  edited_by: system
edited_date: 2016-11-30 15:42:42
```

A user record from the database is below (in this case the Admin user).

```
        id: 1
      name: admin
    org_id: 1
  password:
0ab0a153e5bbcd80c50a02da8c97f3c87686eb8512f5457d30e328d2d4448c8968e9f4875c2eb61356197b851dd33f90658b20b32139233b
217be54d903ca3b6
  full_name: Administrator
     email: admin@openaudit
     roles: ["admin","org_admin"]
      orgs: [1]
      lang: en
    active: y
  edited_by:
      ldap:
edited_date: 2000-01-01 00:00:00
```

You can see the roles that this user has (admin * org_admin).

There is a routine in Open-AudIT that takes a user's details and the action they are requesting and compared the permission required by that action to the list of roles the user has. A response of true/false is provided and the user is allowed (or not) to proceed.

In Open-AudIT each endpoint and action has an associated permission. These mostly translate 1 to 1 with functions. IE - devices::create action would need the devices::create permission. There are a few places where this does not match 1 to 1. For example report::execute. There is only create, read, update and delete permissions. In the case of execute, depending on the endpoint, it is mapped to update or read. In the specific case of report::execute, it is mapped to devices::read. These are detailed on the individual endpoint wiki pages.

Orgs

In addition to the above Users and Roles, we also have organisations.

Every endpoint (with a few exceptions) now has an Organisation associated with it. This field in the database is always called org_id.

A user has access to a list of organisations as part of their account. This is visible in the database as the orgs column in the users table (currently oa_user).

When a user requests an action, in addition to the role based access above, another check is performed to determine if the user has access to the item based on it's org_id.

Organisations are store in a tree like format. Each organisation has a parent. In the case of the default Org, it has itself as the parent.

IMPORTANT

If a user has access to an Org, that user also has access to any of that Orgs descendant's. There is no need to select every Org for a user. Only the highest level Org need be selected and at run time the descendant's are determined. If the user has access to the Org directly (is, in their database record) or they the requested Org is a descendant of an Org the user has access to, their access is granted. There is no limit to parent, child, grandchild, etc. If the requested item has an org_id that is a descendant of the users Orgs, the user will be allow to access.

Active Directory

Active Directory (AD) can be used in conjunction with RBAC. Each Role has an associated AD group name. When a user log's in to Open-AudIT using AD, if configured to do so, Open-AudIT will ask AD for a list of groups the AD user belongs to. If the AD user belongs to a group with the name required by the role, that Role is associated to that Open-AudIT account.

In this way it is even possible to not set up any additional users in Open-AudIT, configure the Roles and AD within Open-AudIT and place AD users into the required AD groups and they will be able to log on. Open-AudIT will verify the users name and password using AD (as it did previously), check the roles and if they have at least one role, will create them an Open-AudIT account and log them in.