UAA Developer Issues

25 Feb 2013

scopes enforced by uaa user and group management

- scim.read, scim.write: read/write users and groups
- password.write: user can change own password
- scim.userids: can access ids/User endpoint if uaa is configured to support it.
- scim.me: finer grained group access when combined with group reader, writer attributes

scopes enforced by uaa client registration apis

- clients.read, clients.write: read/write client registrations
- clients.secret: allow clients to change their own client secret.

miscellaneous scopes enforced by uaa

- openid: get user info from token
- uaa.admin: can set user password
- uaa.user: I have no idea what this is for. All users have it automatically
- uaa.resource: not actually used as a scope in a token. Clients can call the check_token and token_key endpoints with basic auth if they have this authority.

scopes enforced by the cloud_controller

- cloud_controller.admin: provides admin access in ccng
- cloud_controller.read and cloud_controller.write are NOT yet directly supported
- however, the cloud controller does enforce that it is the correct audience of a token, so the token must have a cloud_controller.* scope

automatic groups

users are automatically added to these groups and so can have these in a token scope (if they are also in the client registration and approved)

- openid
- uaa.user
- scim.me,
- cloud_controller.read
- cloud_controller.write
- password.write
- scim.userids
- uaa.user
- approvals.me

creating a new app to use a uaa token and scope

- add group, e.g. dashboard.user
- register dashboard client with scope
- put users in the group
- change app to accept tokens and check for dashboard.user scope
    - can validate tokens locally but must get uaa token verification key first from /token_key endpoint
    - can have the uaa validate the token via the /check_token endpoint

creating a new resource server for client token access

- register client with appropriate authority, e.g. billing.charger
- client app gets a token with client credentials grant
- change resource server to accept tokens and check for billing.charger scope
  - can validate tokens locally but must get uaa token verification key first from /token_key endpoint
  - can have the uaa validate the token via the /check_token endpoint

tour of uaa source code tree?
tour or cf-uaa-lib doc on rubygems?
demo uaac?