DuraCloud Administration

This document details some of the considerations of concern to a DuraCloud administrator.

Naming restrictions

1. Space names
    a. The following restrictions apply to user-defined space names
        - only lowercase letters, numbers, periods, and dashes
        - no adjacent pair of "-" and/or "."
        - no number immediately following the last "."
        - between 3 and 42 characters
        - must start with a letter
        - may not end with a dash
    b. Note: Users can provide space names through the REST-API that do not follow these conventions, but the space actually created will have a different name under the covers.
2. Reserved space names
    a. Due to some specific operations exposed through the durastore REST-API, the following names are unavailable as user-defined space names
        - init
        - stores
        - spaces
        - security
        - task
3. Content object names
    a. The only restrictions are that a content object name
        - cannot include a question mark '?' character
        - cannot include a reverse solidus (backslash) '\' character
        - is limited to 1024 bytes (byte count is checked after URL and UTF-8 encoding)

Access Control Lists (ACLs)

Access control in DuraCloud is set at the space level. Users and groups can be provided read and write access to a space.

1. Users and Groups
    a. Access is granted to *users*, *groups*, or combinations thereof
    b. *Users* are those with credentials to access an account
    c. *Groups* are collections of users that are created in the Management Console
2. Rights
    a. When assigning a space ACL, *users* and/or *groupsv* are granted one of two rights
        i. *READ* allows reading any content within that space
        ii. *WRITE* allows reading, adding, and modifying any content within that space
3. Public (anonymous) Access
    a. There is a special group named 'public' that can only be granted *READ* access to a space
    b. If the 'public' group has *READ* access, then unauthenticated (anonymous) reads of content are permitted on that space
4. Use
    a. REST API can be used to programmatically create, update, and delete space ACLs
        - Get Space ACLs
        - Set Space ACLs
    b. DurAdmin provides authorized users to update space ACLs in the web interface