DuraCloud Security

AWS

The DuraCloud service runs on Amazon Web Services cloud infrastructure. AWS is the datacenter used to manage all servers running DuraCloud software. Information about AWS security can be found at the following links:

- AWS Cloud Security: https://aws.amazon.com/security/
- AWS Whitepapers (many security-related papers can be found here): https://aws.amazon.com/whitepapers/

Overview

The security approach is divided into two distinct spheres of responsibility

1. Channel security (encryption)
2. Application security (AuthN / AuthZ)

The configuration of any given user compute instance will consist of an Apache HttpServer layered on top of Tomcat.

1. Apache HttpServer
    - All requests will come through Apache on port 443 (https) of the instance
    - The requests will internally be unencrypted, where encryption exists, and redirected to tomcat as open text
2. Tomcat
    - A defined set of resource endpoints will require AuthN and AuthZ
    - Spring-security is being leveraged to wire AuthN and AuthZ across relevant resources

Channel Security Implementation

1. Apache HttpServer is configured to require all requests to the DuraCloud web applications go over https.
2. Below are the https enforcement rules configured in Apache. The X-Forwarded-Proto header is provided by AWS Elastic Load Balancers.

```
RewriteEngine On
RewriteCond %{HTTP:X-Forwarded-Proto} !https
RewriteRule !/status https://%{SERVER_NAME}%{REQUEST_URI} [L,R]
```

Application Security Implementation

The basic AuthN flow is as follows

1. User requests secured resource
2. If credentials not in request
    - response 401
3. Spring AuthenticationProvider performs AuthN
    a. AuthProvider asks UserDetailsService for GrantedAuthorities for given Principal
    b. notes
        i. DuraCloud provides custom UserDetailsService implementation to return UserDetails of requesting Principal
        ii. AbstractSecurityInterceptor permanently caches user AuthN decisions by default
4. Authentication object and "configuration attributes" are passed to AccessDecisionManager for AuthZ

Security Servlet Filters

DuraCloud leverages Spring's mechanism for wiring AuthN/Z into an application across servlet url patterns.
The following access rules are placed across the durastore and duraservice REST-APIs:

DuraStore REST Methods

Action	Role
Get Stores	ROLE_USER
Get Spaces	ROLE_USER
Get Space	ROLE_ANONYMOUS if space ACL allows public read, else ROLE_USER
Get Space Properties	ROLE_ANONYMOUS if space ACL allows public read, else ROLE_USER
Get Space ACLs	ROLE_ANONYMOUS if space ACL allows public read, else ROLE_USER
Create Space	ROLE_ADMIN
Set Space ACLs	ROLE_ADMIN
Delete Space	ROLE_ADMIN
Get Content	ROLE_ANONYMOUS if space ACL allows public read, else ROLE_USER
Get Content Properties	ROLE_ANONYMOUS if space ACL allows public read, else ROLE_USER
Store Content	ROLE_USER
Copy Content	ROLE_USER
Set Content Properties	ROLE_USER
Delete Content	ROLE_USER
Get Audit Log	ROLE_ADMIN
Get Manifest	ROLE_USER
Get Storage Reports by Space	ROLE_USER
Get Storage Reports by Store	ROLE_ADMIN
Get Storage Reports for all Spaces in a Store	ROLE_ADMIN
Get Bit Integrity Report	ROLE_USER
Get Bit Integrity Report Properties	ROLE_USER
Get Tasks	ROLE_ADMIN
Perform Task	ROLE_ADMIN
Perform Task (restore-content, restore-snapshot)	ROLE_ROOT

All ROLE_USER permissions are limited to spaces for which space ACLs permit read and/or write access

Roles

The fixed set of users/roles listed below are provided in DuraCloud. Each role in the list below represents a super set of the privileges of those above it.

1. ROLE_ANONYMOUS
   - no username/password
2. ROLE_USER
   - user created by DuraCloud-account admin
3. ROLE_ADMIN
   - administrator of DuraCloud-account
4. ROLE_ROOT
   - DuraSpace personnel

User Management and Access Control

- Users are managed via the DuraCloud Management Console. In the Management Console, an account administrator has the ability to:
  1. Add and remove users to the DuraCloud account
  2. Create Groups and add users to groups in order to simplify access control
- Access Control is managed at the space level

- Within DuraCloud (via the UI or the REST API), an account administrator has the ability to define which users and groups have access to a space, as well as the type of access (read or write) that is available.