Runtime Infrastructure - Feature #5262

add access control for resources exposed via web services/protocols using the SecurityManager

04/17/2021 09:31 AM - Greg Shah

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
billable:	No	**version:**	
vendor_id:	GCD		

Description

Related issues:

Related to Runtime Infrastructure - Feature #4405: provide the capability to ...	**Closed**

History

#1 - 04/17/2021 09:31 AM - Greg Shah

- Related to Feature #4405: provide the capability to deliver static HTML and resources via the FWD server's Jetty added

#2 - 04/17/2021 09:48 AM - Greg Shah

Support for static web content was added in #4405. This support is just for GET and is currently unsecured (all resources are available to any requester with no authentication or access control).

The purpose of this task is to add security:

- We will use the built-in security model of FWD, which is based on the SecurityManager.
- We will add a web-content security plugin to define the resource and provide access control.
- The authentication will be assumed to be handled separately, with any valid FWD authentication method.
- We need to provide a mechanism to obtain an authentication token from a valid (authenticated and active) FWD session. This token would be written as a cookie and provided with any request for web content.
- As part of the web content processing, we would read the authentication cookie (if present), use it to define the security context for the request. Then we would ask the web content security plugin to decide if the requested access is allowed. If not, reject the request with the appropriate status code. If allowed, return the resource.
- We should plan for a range of access rights, based on REST:
- GET (read)
- POST (create)
- PUT (write or replace the entire resource)
- DELETE (delete)
- PATCH (a partial write)

I would want this to support securing both the static web content of #4405 as well as any REST or other web resources.

I'm not sure what needs to be done to secure SOAP or other arbitrary servlet access, but I would like to provide a generic mechanism to secure any access to Jetty.

#3 - 04/22/2021 10:11 AM - Greg Shah

- Subject changed from add access control for static web content using the SecurityManager to add access control for resources exposed via web services/protocols using the SecurityManager