Multiple ALTO Resources Query

draft-zhang-alto-multipart-01

J. Jensen Zhang

ALTO Interim Meeting
Dec 11, 2018

Quick Updates

- The document is still in the very early stage.
- Updates since IETF 102:
  - Update text and terms
  - Clarify the requirements for the query languages and programs
  - Update the protocol errors
  - Add some security considerations

Requirements for Query Languages and Programs

- General requirements for query languages (JSON process capability):
  - The query language MUST be able to read a JSON variable as the input.
  - The query language MUST be able to process the JSON variable.
  - The query language MUST be able to generate the JSON variable.
  - If the server wants to support query language X, it MUST declare the API to get all available ALTO resources in the current query session.
- Requirements for query programs used in multipart service requests:
  - The return value of a query program MUST be a JSON variable.

```
{ "resource-id": "endpoint-path-vector",
  "input": {...},
{ "resource-id": "propmap-availbw",
  "input": `let $propmap :=
    collection("endpiont-path-vector")
            .("endpoint-cost-map")
    return ...`}
```

collection() is just such an API. The query program can use it to get the response data of another resource in this query session.

Protocol Errors Definition

Multipart service considers two types of errors:

- Partial error:
  - When: "resource-id" is not available, or attribute "input" of a resource in the request conducts error.
  - How: still return "multipart/related" response; only report the error in the corresponding parts.
- Entire error:
  - When: for every other error cases.
  - How: return "application/alto-error+json" response.

```
{ "resources": [
  { "resource-id": "endpoint-path-vector",
    "input": {...},
  { "resource-id": "propmap-availbw",
    "input": [...]}]
```

Partial Error

```
{ "resources": {
  "endpoint-path-vector": {
    "input": {...}},
  "propmap-availbw": {
    "input": {...}}}
```

Entire Error

Security Considerations

The client can inject harmful code snippets in the input program.

- Potential attack: read secure database
  - Suggestion: database isolation
- Potential attack: get system control
  - Suggestion: application container isolation
- Potential attack: consume server resources
  - Suggestion: limit memory usage and execution time

Open discussion: is it possible to design a domain-specific query language for ALTO?

Next Steps

- Consider requirements for domain-specific language instead of general-purpose query language
- Implement it in current Unicorn / Mercator system
- Call for reviews

Backup Slides