TAXII Working Call

2016-12-19

DNS SRV

- Should the value be "taxii" or "taxii2" ?

_taxii2._tcp.example.com. 86400 IN SRV 0 5 443 taxii-hub-1.example.com

Discovery API

- Can a conformant implementation be just a Discovery API that lists out API-Roots from other servers?
- Or must a TAXII Server host at least one API Root?

added_after

- This is the date/time the record was added to the TAXII server, not the created /modified timestamp found on the STIX record.
- If TAXII gets a modified STIX record, it will probably be a "new" record in TAXII (some systems may over write data, but it seems like most will just create a new record).
- This is designed to solve the problem of give me everything that has come in since I last checked, aka the last hour.
- But there is a problem....

added_after

- What do you do when the client and server do not have synchronized time? Or do we care?
- Client has 12:01:01 and Server has 12:00:01 (off by a minute).
  - Client queries every minute.
  - Client will never get any data beyond its first request.

added_after

- Possible Solutions
  - 1) Do nothing
  - 2) Add the current server time to the Discovery API resources so the client can know about any differences in time
  - 3) Suggest clients and servers do NTP
  - 4) Do subscriptions and have the server track client requests.
- Which one do you dislike the least?

status resource

- Should we say how long, at least minimally, that a server should hold on to "status" data about a previous POST?
- Right now, nationally, we say 24 hours.
- If this is left up to the server, should the Discovery API or API-Root tell the client how long these messages are kept?

All resources

- Historically we had a "type" field on every resources. Then we got a lot of feedback from this community that we should not have a "type" field, since you know the URL Endpoint you are talking to.
- Just wanted to verify that this is still the general consensus of this group.

objects resource

- Should we have an objects_count property?