Understanding TAXII 2

June 06, 2018 Training

Training Objectives / Agenda

- Architecture
- Core Features
- TAXII 2 API
- Implementation Considerations
- TAXII 2.1 and Beyond

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

What is TAXII 2?

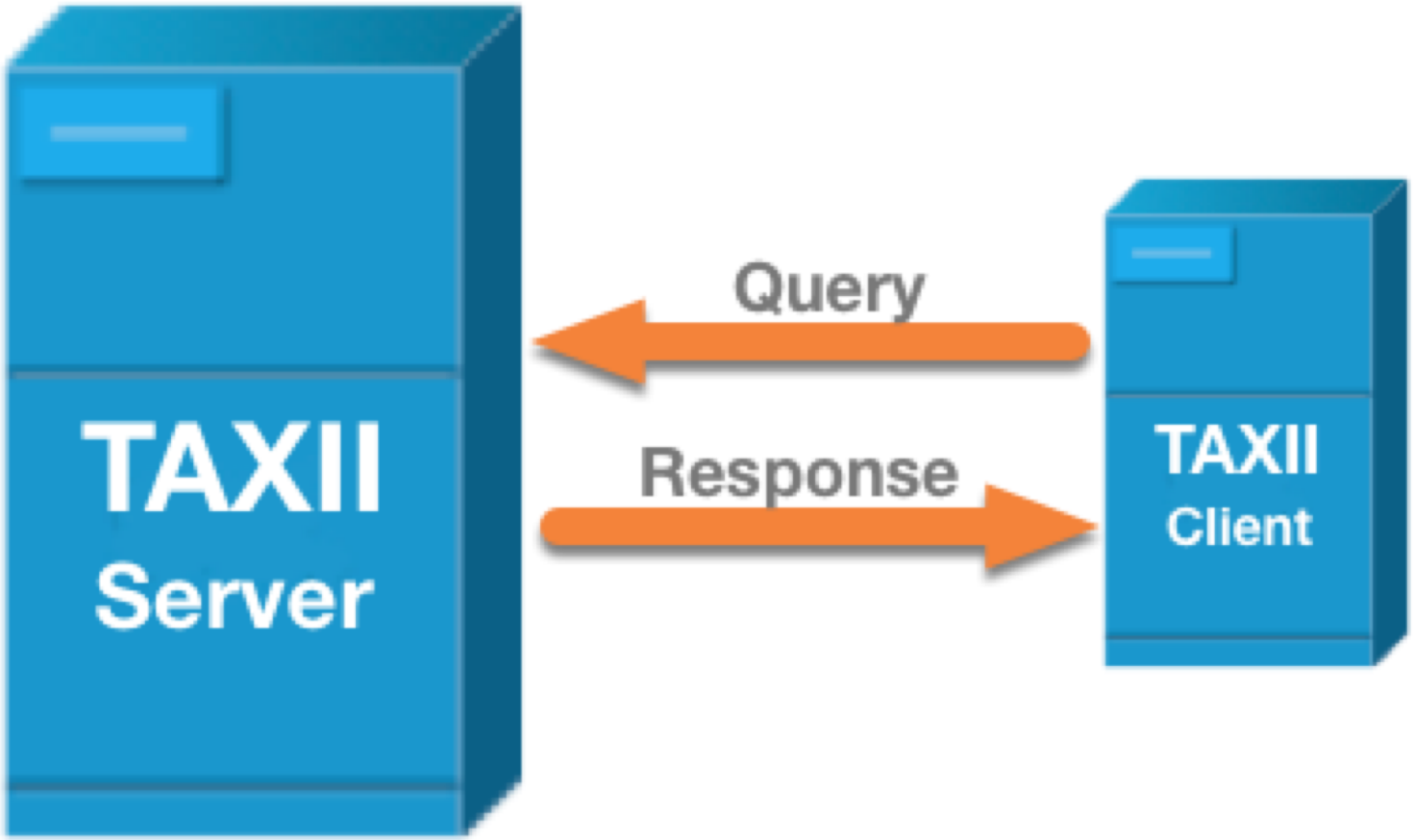
- TAXII 2.0 is a minimally viable product release (MVP)
- JSON based, no longer uses XML
- Uses HTTPs (TLS 1.2 or higher) with RESTful API design
- Support for Collections (Request / Response)
- Future support for Channels (Publish / Subscribe)

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

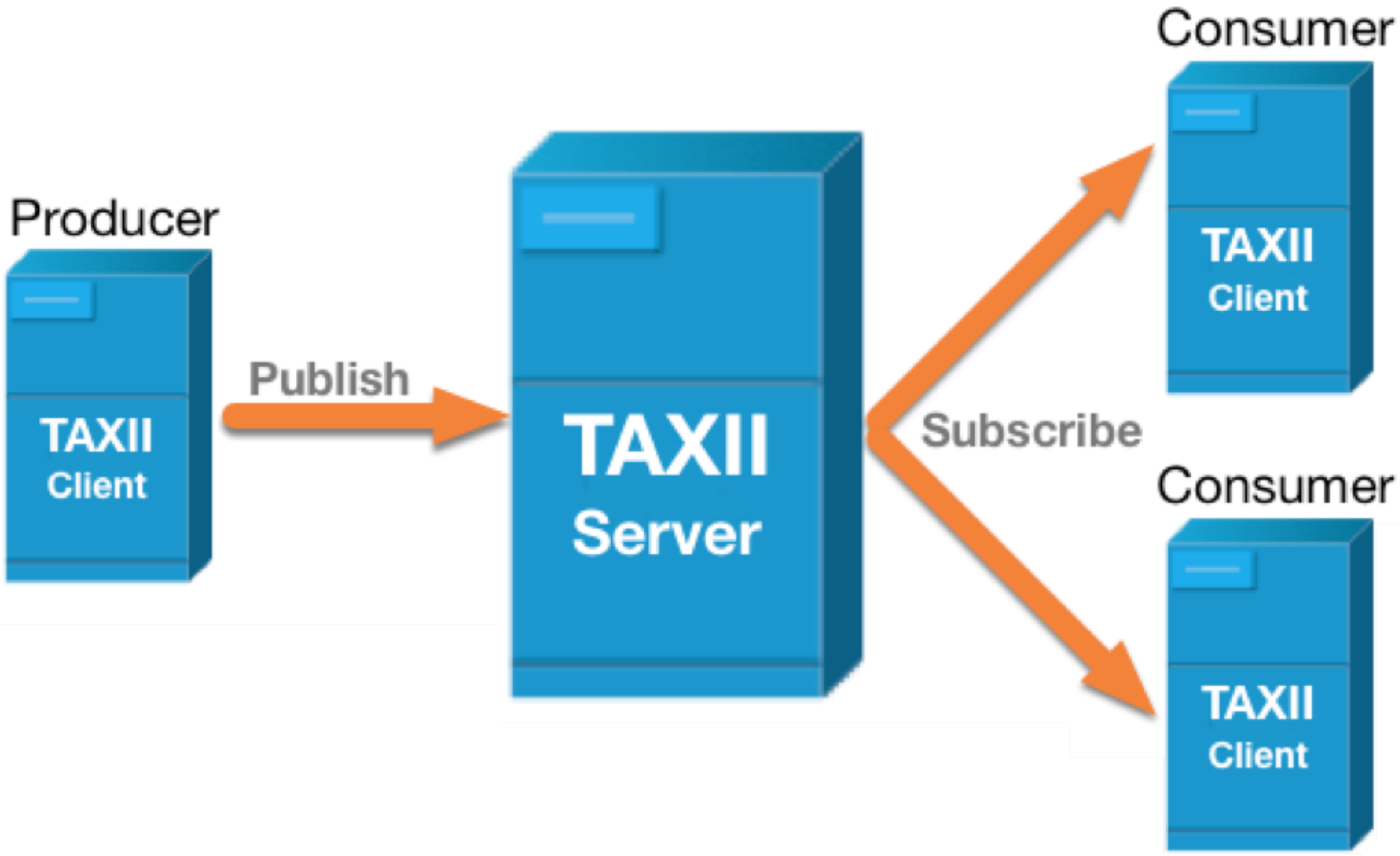
TAXII Architecture

TAXII Architecture



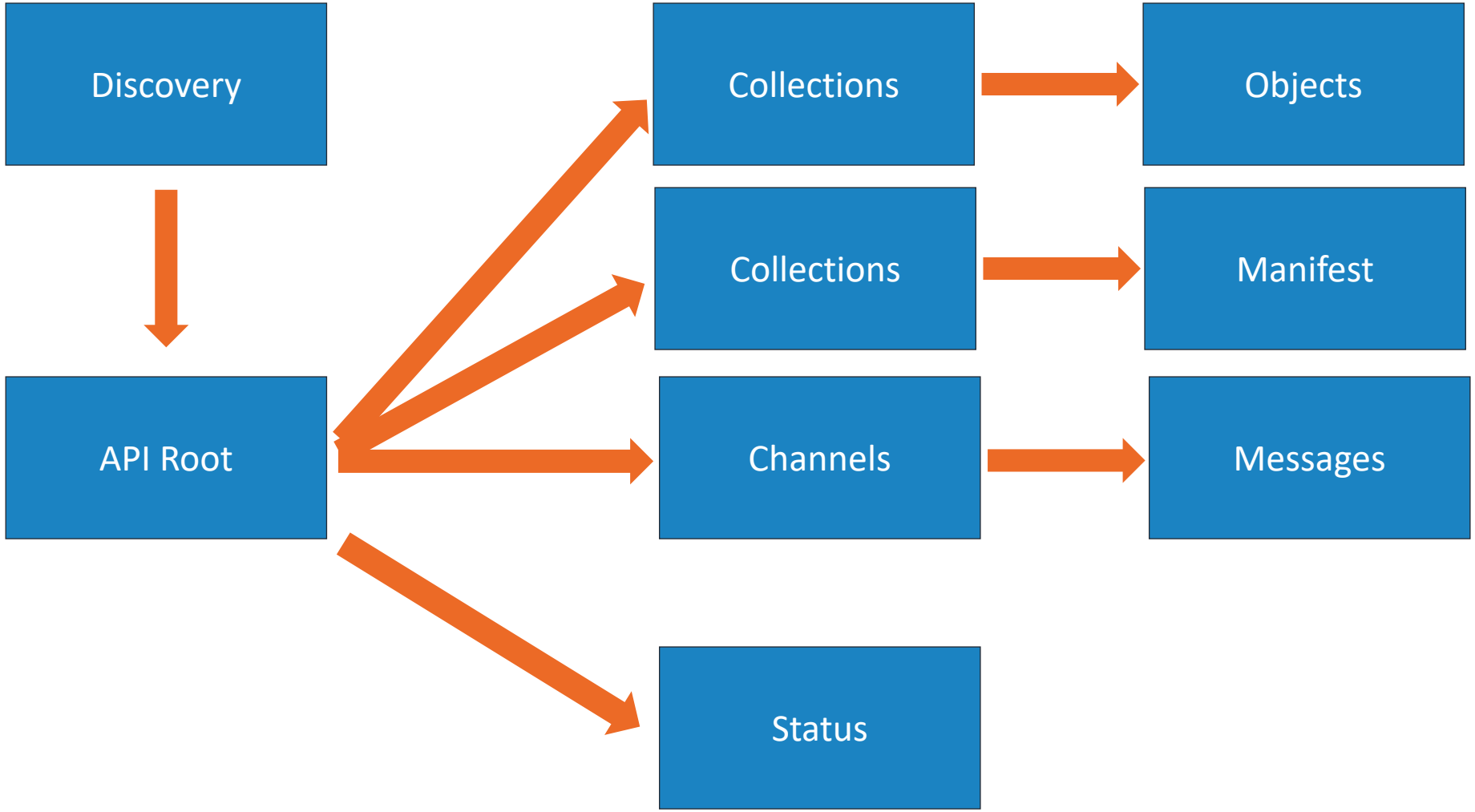
Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

TAXII Architecture



Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

TAXII Architecture



Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Core Features of TAXII 2.0

Core Features

- Initial Client Discovery
- Server Discovery
- Trust Group Support
- Collections
- Authentication
- Content Negotiation / Media Types
- Filtering Options
- Sorting
- X Headers
- Error Messages

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Initial Client Discovery

- What is it?
- Requirements
  - Must be called "taxii"
  - This is changed to "taxii2" in 2.1
- Example:
  - _taxii._tcp.example.com. 86400 IN SRV 0 5 443 taxii-hub-1.example.com
  - Note the leading underscore (_)
- How does it work?

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Server Discovery

- What is it?

- Requirements
  - Must be located at the root of the server
  - Must be called "/taxii/"
  - This is changed to "/taxii2/" in 2.1

- Implementation Considerations
  - Example: "Accept: application/taxii+json"

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Trust Group Support

- Can host multiple instances
- API Root
- Location
- Independent data and controls

- Examples
  - https://taxii-server-us-01.example.com/
  - https://ts.example.com/api1/
  - https://demo.example.com/trustgroup1/

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Collections

- Unique content

- Unique permissions / authentication
  - Read-only
  - Write-only
  - Read and Write

- Requirements
  - UUIDv4 identifiers

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Authentication

- Native semantics
- Basic authentication
  - Minimum authentication
- Other authentication mechanisms
- No auto negotiate authentication

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Content Negotiation

- HTTP Media Types
  - Accept HTTP header
  - Content-type HTTP header

- Tells client and server what content is being used

- STIX endpoints (object, object-by-id)

- TAXII endpoints (everything else)†

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Content Negotiation

- Client does not use optional version parameter
  - Accept: application/taxii+json

- Server must respond with latest version
  - Content-Type: application/taxii+json;version=2.1

- Error Codes
  - HTTP 406 (Not Acceptable)
  - HTTP 415 (Unacceptable Media Type)

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Content Negotiation

- Client requests TAXII content (HTTP GET)

```
GET /api1/collections/ HTTP/1.1
Host: example.com
Accept: application/taxii+json;version=2.1
```

- Server response

```
HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.1
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Content Negotiation

- Client requests STIX content (HTTP GET)

```
GET /api1/collections/91a7b528-80eb-42ed-a74d-c6fbd5a26116/object/indicator--
252c7c11-daf2-42bd-843b-be65edca9f61/ HTTP/1.1
Host: example.com
Accept: application/stix+json;version=2.1,application/taxii+json;version=2.1
```

- Server response

```
HTTP/1.1 200 OK
Content-Type: application/stix+json;version=2.1
X-TAXII-Date-Added-First: 2018-05-12T03:05:09.15811Z
X-TAXII-Date-Added-Last: 2018-05-12T03:05:17.275544Z
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Content Negotiation

- Client sends STIX content (HTTP POST)

```
POST /api1/collections/91a7b528-80eb-42ed-a74d-c6fbd5a26116/objects/ HTTP/1.1
Host: example.com
Accept: application/taxii+json;version=2.1
Content-Type: application/stix+json;version=2.1
```

- Server response

```
HTTP/1.1 202 Accepted
Content-Type: application/taxii+json;version=2.1
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Filtering Options

- Filters

```
- added_after  - a timestamp              (e.g., ?added_after=...)
- id           - an id of an object       (e.g., ?match[id]=...)
- type         - the type of an object    (e.g., ?match[type]=...)
- version      - the version of an object (e.g., ?match[version]=...)
```

- ID: indicator--3600ad1b-fff1-4c98-bcc9-4de3bc2e2ffb

- Type: indicator, attack-pattern, relationship, sighting, etc..

- Version: 2017-11-03T02:34:23.312Z

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Filtering Options

- AND'ing filters
  - A "match[<field>]=…" can appear more than once.
  - Example: ?match[type]=incident&match[version]=2016-01-01T01:01:01.000Z

- OR'ing filters
  - Example: ?match[type]=indicator,attack-pattern,malware

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Filtering Strategies

- Use X-Headers and added_after to sync a data feed

- Example
  - Client wants all data from collection
  - Provides no added_after
  - Sever sends first batch of data
  - Client uses X-Header value in next added_after to fetch more data

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Filtering Strategies

- Server responds to query with:
  - HTTP 206 (Partial Content)
  - Some number of records
  - X-TAXII-Date-Added-First
  - X-TAXII-Date-Added-Last

- Client knows more content is available
  - Use date from X-TAXII-Date-Added-Last as value for next "added_after" query

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Sorting

- Objects sorted in ascending order by the date it was added
  - NOT the version, STIX modified date, or STIX created date
- Most recently added objects are last in the list
- If no added_after is provided, server sends oldest first

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Sorting - Example

- Server has 10 million records
- Collections goes back to 2015
- Sever limits clients to 100 records
- Client asks for all records
- Server responds with records 0-99 sorted 0-99

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

X Headers

- Two X headers
  - X-TAXII-Date-Added-First
  - X-TAXII-Date-Added-Last

- Enables clients to request content on either side of time window

- Examples
  - will be shown in the API endpoints in the next section

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Error Messages

- Optional Error Resource
- Resource

```
{
  "title": "Error condition XYZ",
  "description": "This error is caused when the application tries to access data...",
  "error_id": "1234",
  "error_code": "581234",
  "http_status": "409",
  "external_details": "http://example.com/ticketnumber1/errorid-1234",
  "details": {
    "somekey1": "somevalue",
    "somekey2": "some other value”
  }
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Core Features - Review

- Discovery Services
  - DNS SRV Records, TAXII Server Information, List API Roots
- Support for Trust Groups and Collections of Content
- HTTP Support
  - Authentication, Content Negotiation / Media Types
  - Filtering Options and Sorting
  - X Headers
- Error Messages

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Understanding the TAXII API

TAXII API Endpoints

- Server Discovery
- API Root
- List of Collections
- Manifest of all Objects
- All Objects
- Object By ID
- Object Versions
- Status

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

General Requirements

- All endpoints must end in a slash.
  - Example of a request for a resource without any filter parameters
  - /{api-root}/collections/{id}/objects/{object-id}/

  - Example of a request for a resource with some filter parameters
  - /{api-root}/collections/{id}/objects/{object-id}/?match[type]=indicator

- Collection IDs are UUIDv4 identifiers, so they are globally unique

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

TAXII API Endpoints Summary

URL	Methods	Resource Type
Core Concepts (section 4)		
/taxii2/	GET	`discovery`
{api-root}/	GET	`api`
{api-root}/status/**{status-id}**/	GET	`status`
Collections (section 5)		
{api-root}/collections/	GET	`collections`
{api-root}/collections/**{id}**/	GET	`collection`
{api-root}/collections/**{id}**/manifest/	GET	`manifest`
{api-root}/collections/**{id}**/objects/	GET, POST	`object`*
{api-root}/collections/**{id}**/objects/**{object-id}**/	GET, DELETE	`object`*
{api-root}/collections/**{id}**/objects/**{object-id}**/versions/	GET	`versions`

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Server Discovery

- Get server information and a list of API Roots that this server knows about
- Example: https://ts01.example.com/taxii2/
- Resource

```
{
  "title": "Some TAXII Server",
  "description": "This TAXII Server contains a listing of...",
  "contact": "string containing contact information",
  "default": "https://example.com/api2/",
  "api_roots": [
    "https://example.com/api1/",
    "https://example.com/api2/",
    "https://example.net/trustgroup1/"
  ]
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

API Root

- Get information about a specific API Root
- Example: https://ts01.example.com/api1/
- Resource

```
{
  "title": "Malware Research Group",
  "description": "A trust group setup for malware researchers",
  "versions": [
    "application/taxii+json;version=2.1”
  ],
  "max_content_length": 104857600
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Collections

- Get a list of collections that this client has access to
- Example: https://ts01.example.com/api1/collections/
- Resource

```
{
  "collections": [
    <list of collection resources>
  ]
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Collection by ID

- Get details about a specific collection that this client has access to
- Example: https://ts01.example.com/api1/collections/91a7b528-80eb-42ed-a74d-c6fbd5a26116/
- Resource


```
{
  "id": "91a7b528-80eb-42ed-a74d-c6fbd5a26116",
  "title": "High Value Indicator Collection",
  "description": "This data collection contains high value IOCs",
  "can_read": true,
  "can_write": false,
  "media_types": [
    "application/stix+json;version=2.1”
  ]
}
```


Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Manifest Data

- Get summary information about objects in a collection

- Example https://ts01.example.com/api1/collections/91a7b528-80eb-42ed-a74d-c6fbd5a26116/manifest/

- URL Filtering Parameters

```
- added_after  - a timestamp              (e.g., ?added_after=...)
- id           - an id of an object       (e.g., ?match[id]=...)
- type         - the type of an object    (e.g., ?match[type]=...)
- version      - the version of an object (e.g., ?match[version]=...)
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Manifest Data

- GET Resource Response

```
HTTP/1.1 200 OK
Content-Type: application/taxii+json;version=2.1
X-TAXII-Date-Added-First: 2018-05-12T03:05:09.15811Z
X-TAXII-Date-Added-Last: 2018-05-12T03:05:17.275544Z

{
  "objects": [
    {
      "id": "indicator--29aba82c-5393-42a8-9edb-6a2cb1df070b",
      "date_added": "2016-11-01T03:04:05Z",
      "version": "2016-11-03T12:30:59.000Z",
      "media_type": "application/stix+json;version=2.1”
    }
  ]
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Objects

- Get or add actual objects from a collection

- Example: https://ts01.example.com/api1/collections/91a7b528-80eb-42ed-a74d-c6fbd5a26116/objects/

- URL Filtering Parameters

```
- added_after  - a timestamp              (e.g., ?added_after=...)
- id           - an id of an object       (e.g., ?match[id]=...)
- type         - the type of an object    (e.g., ?match[type]=...)
- version      - the version of an object (e.g., ?match[version]=...)
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Objects

- GET Resource Response

```
HTTP/1.1 200 OK
Content-Type: application/stix+json;version=2.1
X-TAXII-Date-Added-First: 2018-05-12T03:05:09.15811Z
X-TAXII-Date-Added-Last: 2018-05-12T03:05:17.275544Z

{
  "type": "bundle",
  ...
  "objects": [
    {
      "type": "indicator",
      ...
    }
  ]
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Objects

- POST Resource Response

```
HTTP/1.1 202 Accepted
Content-Type: application/taxii+json;version=2.1

{
  "id": "2d086da7-4bdc-4f91-900e-d77486753710",
  "status": "pending",
  "request_timestamp": "2016-11-02T12:34:34.12345Z",
  "total_count": 4,
  "success_count": 1,
  "successes": [
    {
      "id": "indicator--c410e480-e42b-47d1-9476-85307c12bcbf",
      "version": "2017-12-01T12:15:13.142Z"
    }
  ],
  "failure_count": 0,
  "pending_count": 3
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Object by ID

- Get actual objects from a collection

- Example: https://ts01.example.com/api1/collections/91a7b528-80eb-42ed-a74d-c6fbd5a26116/objects/indicator--252c7c11-daf2-42bd-843b-be65edca9f61/

- URL Filtering Parameters

```
- added_after  - a timestamp              (e.g., ?added_after=...)
- version      - the version of an object (e.g., ?match[version]=...)
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Object by ID

- GET Resource Response

```
HTTP/1.1 200 OK
Content-Type: application/stix+json;version=2.1
X-TAXII-Date-Added-First: 2018-05-12T03:05:09.15811Z
X-TAXII-Date-Added-Last: 2018-05-12T03:05:17.275544Z

{
  "type": "bundle",
  ...
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--252c7c11-daf2-42bd-843b-be65edca9f61",
      ...
    }
  ]
}
```

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

TAXII API Endpoints Review

URL	Methods	Resource Type
Core Concepts (section 4)		
/taxii2/	GET	`discovery`
{api-root}/	GET	`api`
{api-root}/status/**{status-id}**/	GET	`status`
Collections (section 5)		
{api-root}/collections/	GET	`collections`
{api-root}/collections/**{id}**/	GET	`collection`
{api-root}/collections/**{id}**/manifest/	GET	`manifest`
{api-root}/collections/**{id}**/objects/	GET, POST	`object`*
{api-root}/collections/**{id}**/objects/**{object-id}**/	GET, DELETE	`object`*
{api-root}/collections/**{id}**/objects/**{object-id}**/versions/	GET	`versions`

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Implementation Considerations

Design Considerations

- Associating Objects to a Collection
- Date Added
- Storing Objects by Version
- Storing Base Properties Separately
- Storing Exact Copies
- Synchronous / Asynchronous POSTs

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Associating Objects to a Collection

- Store just the STIX Object ID

- This allows
  - Object to exist in multiple collections
  - Update object everywhere

- If not, book keeping will be significant

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Date Added

- Date added timestamp for each object version
- Date added when first added to a collection
- Micro second precision, example:
  2017-11-29T01:01:01.123456Z
- Records batch processed with same timestamp may have performance problems

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Storing Objects by Version

- Central object store

- Index STIX ID and modified timestamp (aka the version).

- No requirement keep any content
  - How long to keep data (data retention)
  - Keep older versions, and if so, how many.

- Some might keep everything, some may only keep current version of objects less than say a month old.

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Storing Base Properties Separately

- Store base object properties separate from object specific properties
- Easier to add new common properties
- Eases summarization of records

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Storing Exact Copies

- Custom Properties
- Digital Signatures

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Synchronous / Asynchronous POSTs

- Can process synchronously or asynchronously
  - Response on success is always an HTTP 202 (Accepted)

- Asynchronous
  - Status resources shows pending
  - Client query status resource ID to get final status

- Synchronous
  - Status resource shows complete

OASIS

Copyright © OASIS Open 2018. Portions copyright LookingGlass Inc. and Symantec Inc. All Rights Reserved

Demo

Q/A