Internet Engineering Task Force C. Ma
Internet Draft J. Chen
Intended status: Informational X. Fan
Expires: June 21, 2022 M. Chen
Z. Li
China Academy of Information and Communications Technology
December 21, 2021

Finding the Authoritative Registration Data (IIIDAP) Service
draft-mcd-identifier-access-authority-04

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on June 21, 2022.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this

document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Abstract

This document specifies a method to find which Industrial Internet Identifier Data Access Protocol (IIIDAP) server is authoritative to answer queries for a request of identifier data.

Table of Contents

1. Introduction

Querying and retrieving identifier data from registry are defined in Industrial Internet Identifier Data Access Protocol (IIIDAP) [IDENTIFIER-HTTP] [IDENTIFIER-QUERY] [IDENTIFIER-RESPONSES]. These documents do not specify where to send the queries. This document specifies a method to find which server is authoritative to answer queries for a request of identifier data.

Identifier data of Enterprise-Level Nodes (ELN) are delegated by SLN, and identifier data of Second-Level Nodes (SLN) are also stored in SLN. Thus, the bootstrap information needed by IIIDAP clients is best generated from data and processes already maintained by SLN;

Per this document, Top-Level Node (TLN) SHOULD create a registry based on a JSON format specified in this document, herein named IIIDAP Bootstrap Service Registry. TLN will create and update IIIDAP

Bootstrap Services Registry as the registry is updated. TLN has provided a mechanism for collecting the IIIDAP server information. The IIIDAP Bootstrap Services Registry will start empty and will be gradually populated as registrants of identifiers and address spaces provide IIIDAP server information to TLN. An IIIDAP client fetches the IIIDAP Bootstrap Service Registry, extracts the data, and then performs a match with the query data to find the authoritative identifier data server and appropriate query base URL.

Entries in this registry contain at least the following:

o an identifier of SLN of ELN.

o one or more URLs that provide the IIIDAP service regarding this registration.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.1. Acronyms and Abbreviations

IIIDAP: Industrial Internet Identifier Data Access Protocol

TLN: Top-Level Nodes

SLN: Second-Level Nodes

ELN: Enterprise-Level Nodes

3. Structure of the IIIDAP Bootstrap Service Registry

The IIIDAP Bootstrap Service Registry, as specified below, have been made available as JSON [RFC8259] objects, which can be retrieved via HTTP from locations specified by TLN. The JSON object for each registry contains a series of members containing metadata about the registry such as a version identifier, a timestamp of the publication date of the registry, and a description. Additionally, a "services" member contains the registry items themselves, as an array. Each item of the array contains a second- level array, with two elements, each of them being a third-level array.

Each element of the Services Array is a second-level array with two elements: in order, an Entry Array and a Service URL Array.

The Entry Array contains all entries that have the same set of base IIIDAP URLs. The Service URL Array contains the list of base IIIDAP URLs usable for the entries found in the Entry Array. Elements within these two arrays are not sorted in any way.

The JSON output of identifier registry, grouped by base IIIDAP URLs, as shown in this example.

```
{
    "version": "1.0",
    "publication": "YYYY-MM-DDTHH:MM:SSZ",
    "description": "Some text",
    "services": [
      [
        ["86.100", "86.100.1"],
        [
          "https://registry.example.com/myiiidap/"
        ]
      ],
      [
        ["86.101"],
        [
          "http://example.org/"
        ]
      ]
    ]
}
```

The "version" corresponds to the format version of the registry. This specification defines version "1.0".

The syntax of the "publication" value conforms to the Internet date/time format [RFC3339]. The value is the latest update date of the registry by IANA.

The optional "description" string can contain a comment regarding the content of the bootstrap object.

Per [RFC7258], in each array of base IIIDAP URLs, the secure versions of the transport protocol SHOULD be preferred and tried first. For example, if the base IIIDAP URLs array contains both HTTPS and HTTP URLs, the bootstrap client SHOULD try the HTTPS version first.

Base IIIDAP URLs MUST have a trailing "/" character because they are concatenated to the various segments defined in [IDENTIFIER-QUERY].

JSON names MUST follow the format recommendations of [IDENTIFIER-HTTP]. Any unrecognized JSON object properties or values MUST be ignored by implementations.

All labels used as entries or base IIIDAP URLs in the registry defined in this document MUST be only represented in lowercase.

Authoritative identifier data service is found by doing the label-wise longest match of the target identifier with the identifier values in the Entry Arrays in the TLN Bootstrap Service Registry. The match is done per label, from right to left. If the longest match results in multiple entries, then those entries are considered equivalent. The values contained in the Service URL Array of the matching second-level array are the valid base IIIDAP URLs as described in [IDENTIFIER-QUERY].

For example, an identifier IIIDAP query for 86.100.1 matches the 86.100 entry in one of the arrays of the registry. The base IIIDAP URL for this query is then taken from the second element of the array, which is an array of base IIIDAP URLs valid for this entry. The client chooses one of the base URLs from this array; in this example, it chooses the only one available, "https://registry.example.com/myiiidap/". The segment specified in [IDENTIFIER-QUERY] is then appended to the base URL to complete the query. The complete query is then "https://registry.example.com/myiiidap/identifier/86.100".

If a domain IIIDAP query for 86.100.1 matches both 86.100 and 86.100.1 entries in the registry, then the longest match applies and the 86.100.1 entry is used by the client.

4. Entity

Names of identifier nodes can be queried by handle as described in [IDENTIFIER-QUERY], since there is no global namespace for names, this document does not describe how to find the authoritative IIIDAP server for names. However, it is possible that, if an identifier was received from a previous query, the same IIIDAP server could be queried by its name.

5. Non-existent Entries or IIIDAP URL Values

The registry may not contain the requested value. In these cases, there is no known IIIDAP server for that requested value, and the client SHOULD provide an appropriate error message to the user.

6. Deployment and Implementation Considerations

This method relies on the fact that IIIDAP clients are fetching the TLN registry to then find the servers locally. Clients SHOULD NOT fetch the registry on every IIIDAP request. Clients SHOULD cache the registry, but use underlying protocol signaling, such as the HTTP Expires header field [RFC7234], to identify when it is time to refresh the cached registry. It is important for that header field to be properly set to provide timely information as the registry change, while maintaining a reasonable load on the IANA servers. The HTTP Content-Type returned to clients accessing these JSON-formatted registry MUST be "application/json", as defined in [RFC8259].

If the query data does not match any entry in the client cached registry, then the client may implement various methods. For example, if the client knows the existence of an IIIDAP aggregator or redirector and its associated base URL, and trusts that service, then it could send the query to the redirector, which would redirect the client if it knows the authoritative server that client has not found.

Some authorities of identifier data may work together on sharing their information for a common service, including mutual redirection [REDIRECT-IIIDAP].

When a new object is allocated, there is no guarantee that this new object will have an entry in the corresponding bootstrap IIIDAP registry, since the setup of the IIIDAP server for this new entry may become live and registered later.

7. Limitations

In particular, the following objects are not bootstrapped with the method described in this document:

- queries using search patterns that do not contain a terminating string that matches the identifiers in the registry
- names
- help

8. Formal Definition

This section is the formal definition of the registry. The structure of JSON objects and arrays using a set of primitive elements is

defined in [RFC8259]. Those elements are used to describe the JSON structure of the registry.

8.1. Imported JSON Terms

- OBJECT: a JSON object, defined in Section 4 of [RFC8259]
- MEMBER: a member of a JSON object, defined in Section 4 of [RFC8259]
- MEMBER-NAME: the name of a MEMBER, defined as a "string" in Section 4 of [RFC8259]
- MEMBER-VALUE: the value of a MEMBER, defined as a "value" in Section 4 of [RFC8259]
- ARRAY: an array, defined in Section 5 of [RFC8259]
- ARRAY-VALUE: an element of an ARRAY, defined in Section 5 of [RFC8259]
- STRING: a "string", as defined in Section 7 of [RFC8259]

8.2. Registry Syntax

Using the above terms for the JSON structures, the syntax of a registry is defined as follows:

- iiidap-bootstrap-registry: an OBJECT containing a MEMBER version and a MEMBER publication, an optional MEMBER description, and a MEMBER services-list
- version: a MEMBER with MEMBER-NAME "version" and MEMBER-VALUE a STRING
- publication: a MEMBER with MEMBER-NAME "publication" and MEMBER-VALUE a STRING
- description: a MEMBER with MEMBER-NAME "description" and MEMBER-VALUE a STRING
- services-list: a MEMBER with MEMBER-NAME "services" and MEMBER-VALUE a services-array
- services-array: an ARRAY, where each ARRAY-VALUE is a service

- o service: an ARRAY of 2 elements, where the first ARRAY-VALUE is an entry-list and the second ARRAY-VALUE is a service-uri-list

- o entry-list: an ARRAY, where each ARRAY-VALUE is an entry

- o entry: a STRING

- o service-uri-list: an ARRAY, where each ARRAY-VALUE is a service-uri

- o service-uri: a STRING

9. Security Considerations

By providing a bootstrap method to find IIIDAP servers, this document helps to ensure that the end users will get the IIIDAP data from an authoritative source, instead of from rogue sources. The method has the same security properties as the IIIDAP protocols themselves. The transport used to access the registry can be more secure by using TLS [RFC5246], which IANA supports.

Additional considerations on using IIIDAP are described in [IDENTIFIER-SECURITY].

10. IANA Considerations

11. References

References to IIIDAP are subject to the latest edition.

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002, <http://www.rfc-editor.org/info/rfc3339>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, August 2006, <http://www.rfc-editor.org/info/rfc4632>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, August 2010, <http://www.rfc-editor.org/info/rfc5890>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

11.2. Informative References

[REDIRECT-IIIDAP] Martinez, C., Zhou, L., and G. Rada, "Redirection Service for Industrial Internet Identifier Data Access Protocol", Work in Progress, draft-ietf-weirds-redirects-04, July 2014.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC7071] Borenstein, N. and M. Kucherawy, "A Media Type for Reputation Interchange", RFC 7071, November 2013, <http://www.rfc-editor.org/info/rfc7071>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", RFC 7234, June 2014, <http://www.rfc-editor.org/info/rfc7234>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[asreg] IANA, "Autonomous System (AS) Numbers", <http://www.iana.org/assignments/as-numbers>.

[domainreg] IANA, "Root Zone Database", <http://www.iana.org/domains/root/db>.

[ipv4reg] IANA, "IPv4 Address Space Registry", <http://www.iana.org/assignments/ipv4-address-space>.

[ipv6reg] IANA, "IPv6 Global Unicast Address Assignments", <http://www.iana.org/assignments/ipv6-unicast-address-assignments>.

[IDENTIFIER-HTTP]
Ma, C., "HTTP Usage in the Industrial Internet Identifier Data Access Protocol (IIIDAP)", Work in Progress, draft-ma-identifier-access-http, June 2022.

[IDENTIFIER-SECURITY]
Ma, C., "Security Services for the Industrial Internet Identifier Data Access Protocol (IIIDAP)", Work in Progress, draft-mcd-identifier-access-security, June 2022.

[IDENTIFIER-QUERY]
Ma, C., "Industrial Internet Identifier Data Access Protocol (IIIDAP) Query Format", Work in Progress, draft-mcd-identifier-access-query, June 2022.

[IDENTIFIER-RESPONSES]
Ma, C., "JSON Responses for the Industrial Internet Identifier Data Access Protocol (IIIDAP)", Work in Progress, draft-mcd-identifier-access-responce, June 2022.

Authors' Addresses

Chendi Ma
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 177 1090 9864
Email: machendi@caict.ac.cn

Chen Jian
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 138 1103 3332
Email: chenjian3@caict.ac.cn

Xiaotian Fan
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 134 0108 6945
Email: fanxiaotian@caict.ac.cn

Meilan Chen
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 139 1143 7301
Email: chenmeilan@caict.ac.cn

Zhiping Li
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 185 1107 1386
Email: lizhiping@caict.ac.cn