RPKI validated cache Update in SLURM over HTTPs (RUSH)
draft-madi-sidrops-rush-00

Abstract

This document defines a method for transferring RPKI validated cache update information in JSON object format over HTTPs.

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on June 26, 2020.

Copyright Notice

Copyright (c) 2019 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 (https://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.
1. Introduction

This document defines a mechanism called "RPKI validated cache Update in SLURM [RFC 8416] over HTTPs (RUSH)" for the use of SLURM in updating RPKI cache data over HTTP [RFC7540] using HTTPs [RFC2818] URIs (and therefore TLS [RFC8446] security for integrity and confidentiality). Integration with HTTP provides a secure transport for distributing cache data, which is in alignment with SLURM file format in order to take advantage of using one same API for a cache server to do both remote update and local override.

The RPKI validated cache in this document refers to the validated data of assertion information certified by corresponding RPKI signed objects such as ROA [RFC6482] and BGPsec router certificate [RFC8209], which are transferred from the RPKI cache server to routers by RTR protocol [RFC8210] for the use of the RPKI. While this document is intended for the RPKI cache update between two cache servers. SLURM offers a standardized method for describing RPKI cache data in JSON format [RFC8259], and SLURM is designed to carry out incremental update.

The primary use of RUSH is to distribute RPKI validated cache within an ISP or an ICP composed of a number of ASes. A small site or enterprise network MAY also use RUSH by synchronizing with a third-party RPKI cache provider over networks.

Note that RUSH merely focuses on a standardized transport and data format of the RPKI cache data. RUSH has nothing to do with synchronization at the RUSH end system, that is, more sophisticated functions such as automatic re-synchronization and access control is out of this scope and MAY be left to private implementation.
2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. RUSH Operations

3.1. Use of SLURM

RUSH uses SLURM file format to indicate the intended update. A SLURM file consists of a single JSON object containing some members. Among others, "validationOutputFilters" [Section 3.3 of [RFC8416]] and "locallyAddedAssertions" [Section 3.4 of [RFC8416]] are defined to describe actions of deleting some of existing data items and adding new data items respectively.

Note that RUSH re-uses the JSON members of SLURM object, not implying the very actions are taken locally to any extent. Typically, RUSH takes place over networks remotely while take effects to the cache in question locally.

The RUSH-aware HTTP server/client MUST be prepared to parse SLURM object.

3.2. Use of HTTP as Transport

HTTP is employed by RUSH to transfer RPKI validated cache update information as expressed as a SLURM object. A new data type is therefore defined to identify SLURM object in HTTP message body.

The RUSH-aware HTTP server/client MUST be prepared to process media type "application/json-slurm".

3.3. RUSH Example

Figure 1 shows an example of using RUSH to carry out RPKI validated cache by HTTP POST method.

POST /rpki-cache HTTP/2
Host: rpki.example.com
Content-Type: application/json-slurm
Content-Length:964
<964 bytes represented by the following json string>
|
"slurmVersion": 1,
"validationOutputFilters": {
  "prefixFilters": [
    {
      "prefix": "192.0.2.0/24",
      "comment": "All VRPs encompassed by prefix"
    },
    {
      "asn": 64496,
      "comment": "All VRPs matching ASN"
    },
    {
      "prefix": "198.51.100.0/24",
      "asn": 64497,
      "comment": "All VRPs encompassed by prefix, matching ASN"
    }
  ],
  "bgpsecFilters": [
    {
      "asn": 64496,
      "comment": "All keys for ASN"
    },
    {
      "SKI": "Zm9v",
      "comment": "Key matching Router SKI"
    },
    {
      "asn": 64497,
      "SKI": "YmFy",
      "comment": "Key for ASN 64497 matching Router SKI"
    }
  ]
},
"locallyAddedAssertions": {
  "prefixAssertions": [
    {
      "asn": 64496,
      "prefix": "198.51.100.0/24",
      "comment": "My other important route"
    },
    {
      "asn": 64496,
      "prefix": "2001:DB8::/32",
      "maxPrefixLength": 48,
      "comment": "My other important de-aggregated routes"
    }
  ],
  "bgpsecAssertions": [}
Figure 1. Example of an HTTP message for use of RUSH

4. IANA Considerations

Type name: application
Subtype name: json-slurm
Subtype name: json-slurm
Optional parameters: N/A
Encoding considerations: This is a JSON object.
Security considerations: N/A
Interoperability considerations: [RFC8416]
Published specification:
Applications that use this media type:
Systems that want to exchange RPKI cache data update information in SLURM file format [RFC8416] over HTTP.
Person & email address to contact for further information: Di Ma<br/>madi@zdns.cn
Intended usage: COMMON
Restrictions on usage: N/A
Author: Di Ma <madi@zdns.cn>
Change controller: IESG
5. Security Considerations

Updating RPKI validated cache over HTTPs relies on the security of the underlying HTTP transport. Implementations utilizing HTTP/2 benefit from the TLS profile defined in Section 9.2 of [RFC7540]. An HTTPS connection provides transport security for the interaction between servers, but it does not provide data integrity detection. An adversary that can control the cache used by the subscriber can affect that subscriber’s view of the RPKI. The RPKI cache server security and the trust model for the interaction between cache server and subscriber is out of the scope of this document.

6. Acknowledgments

7. References

7.1. Normative References


7.2. Informative References


Authors' Addresses

Di Ma  
ZDNS  
4 South 4th St. Zhongguancun  
Haidian, Beijing  100190  
China  

Email: madi@zdns.cn

Hanbing Yan  
CNCERT  

Email: yhb@cert.org.cn