

I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: May 16, 2018

S. Hares
Hickory Hill Consulting
A. Clemm
Huawei
November 12, 2017

I2RS Ephemeral Datastore
draft-hares-i2rs-ephemeral-ds-00.txt

Abstract

This document the Yang module for the I2RS ephemeral datastore.

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 May 16, 2018.

Copyright Notice

Copyright (c) 2017 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.

Table of Contents

1. Introduction	2
2. Definitions	2
2.1. Requirements language	2
2.2. I2RS Definitions	2
3. Operational Options	3
4. Publishing non-Secure Data	3
5. Yang for Ephemeral Datastore	4
6. IANA Considerations	6
7. Security Considerations	6
8. Acknowledgements	6
9. References	6
9.1. Normative References:	7
9.2. Informative References	8
Authors' Addresses	8

1. Introduction

The I2RS architecture [RFC7921] defines the I2RS interface "a programmatic interface for state transfer in and out of the Internet routing system". The I2RS interface consists of the I2RS ephemeral dynamic datastore populated with modules which operate within that ephemeral datastore plus a protocol to access this datastore. This document provides the yang for the I2RS ephemeral dynamic datastore as a basic for developers who wish to populate it with specific modules.

The protocol which access the ephemeral datastore is an IETF management protocol (NETCONF [RFC6241], RESTCONF [RFC8040]) which have been extended in the revised data stores module ([I-D.ietf-netconf-nmda-restconf], [I-D.ietf-netconf-nmda-netconf]). These basic protocols meet the I2RS requirements for ephemeral state [RFC8242] and protocol security [RFC8241].

2. Definitions

2.1. Requirements language

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].

2.2. I2RS Definitions

The I2RS architecture [RFC7921] defines the following:

ephemeral data: is data which does not persist across a reboot (software or hardware) or a power on/off condition. Ephemeral data can be configured data or data recorded from operations of the router. Ephemeral configuration data also has the property that a system cannot roll back to a previous ephemeral configuration state. (See [RFC7921] for an architectural overview, [RFC8242] for requirements, and [I-D.ietf-netmod-revised-datastores] for discussion of how the ephemeral datastore as a dynamic datastore interacts with intended configuration datastore, the dynamic configuration protocols, and control planes datastore to create the applied datastore and operational state datastore.

3. Operational Options

The I2RS ephemeral datastore requires the revised datastores ([I-D.ietf-netmod-revised-datastores]).

It is suggested that any implementation provide the following operator options as "knobs" the operator can set:

- o Knobs to determine whether local policy or I2RS has precedence.
- o Knob for allowing only secure transport (e.g. TLS) or allowing both secure and insecure transport. Insecure transport can only support for items denoted as "data-not-sensitive" in the module. The recommend default setting for this knob is not allow insecure transport.

4. Publishing non-Secure Data

Non-Secure data may be published from an I2RS datastream as a stream of notifications or a set of data read. For example, if the routing system attaches to a web site which is up via multiple links, the I2RS may want to publish the availability or non-availability of such a web site via a notification stream. In this case, the notification stream in RESTCONF might run over HTTP over TCP instead of HTTP over TLS.

Any data module which uses this feature should undergo additional security review to determine that this non-secure stream does not provide an additional attack surface. Any yang data module being standardized in the IETF which utilizes non-secure data should be reviewed by IETF experts in routing, operations, and security to determine if the non-secure data provides an acceptable mitigation of security risks.

5. Yang for Ephemeral Datastore

1. Name : ephemeral
2. YANG modules : all (default)
3. YANG statements : config false + ephemeral true
4. How applied : automatic
5. Protocols : NC/RC (default)
6. YANG Module : (see below)
 7. Ephemeral-capable modules: (see IANA registry)
 8. illegal features: (features illegal for I2RS datastore)
 9. Property :

```
<CODE BEGINS> file "ietf-i2rs-ephemeral-ds@2017-11-11.yang"
module ietf-i2rs-ephemeral-ds {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-i2rs-ephemeral-ds";
  prefix i2rs;

  import ietf-datastores {
    prefix ds;
  }
  import ietf-origin {
    prefix or;
  }

  organization
    "IETF I2RS (Interface to the Routing System)
    Working Group";

  contact
    "WG WB: <http://tools.ietf.org/wg/i2rs>
    WG List: <mailto:i2rs@ietf.org>
    Editor: Susan Hares
    <mailto:shares@ndzh.com>

    Editor: Alex Clemm
    <mailto:ludwig@clemm.org>";

  description
    "This module defines the I2RS ephemeral datastore.
    Deployed copies will augment the

    Copyright (c) 2017 IETF Trust and the persons
    identified as authors of the code. All rights reserved.

    Redistribution and use in source and binary forms,
    without modification, is permitted pursuant to,
```

and subject to the license terms contained in, the Simplified BSD License set form in Section 4.c of the IETF Trust's Legal Provisions related to the IETF documents (<http://trusee.ietf.org/license-info>).

This version of this YANG Module is part of draft-hcww-i2rs-ephemeral-ds-00.txt. See the RFC itself for full legal notices.

Note to RFC Editor: Please replace above reference to the draft-hcww-i2rs-ephemeral-ds-00.txt with RFC umber when published (i.e. RFC xxx).";

```
revision 2017-11-11 {
  description
    "initial revision.
     Note to RFC EDITOR:
     (1) Please replace the following reference with
     to draft-hwcc-i2rs-ephemeral-ds with
     RFC number whe published (i.e. RFC xxx)";

    reference "draft-hcww-i2rs-ephemeral-ds-00.txt";
}
```

```
// add datastore identity
identity ds-ephemeral {
  base ds:datastore;
  description
    "The 'ephemeral' datastore.";
}
```

```
// add origin identity
identity or-ephemeral {
  base or:dynamic;
  description
    "Denotes data from the ephemeral dynamic datastore.";
}
```

```
extension data-not-sensitive {
  argument "value";
  description
    "This extension indicates that this
     read-only data node is not sensitive
     and should be allowed to
```

```
        access via a non-secure transport.
        The value is either true or false.
        ";
    }

    // modules which can be used this draft are included here
    // topology drafts:
    //ietf-network, ietf-network-topology
    // with state modules (ietf-network-state,
    // ietf-network-topology-state)
    // ietf-l3-unicast-topology
    // with state modules
    // (ietf-l3-unicast-topology-state)
    // ietf-i2rs-rib
    // (additional models can be added here

}
<CODE ENDS>
```

6. IANA Considerations

The IANA URI for the I2RS ephemeral datastore go here.

7. Security Considerations

The security requirements for the I2RS protocol are covered in [RFC8241]. The security environment the I2RS protocol is covered in [I-D.ietf-i2rs-security-environment-reqs]. Any person implementing or deploying these yang additions for an I2RS protocol should consider both security requirements.

8. Acknowledgements

The NETMOD and NETCONF working group have worked out the majority of the issue for support of the ephemeral datastore. The authors want to specifically thank Kent Watsen, Robert Wilton, Lou Berger, Andy Bierman, Phil Shaffer, and all the members of the netmod and netconf working group for their work on revised datastores.

9. References

9.1. Normative References:

- [I-D.ietf-netconf-nmda-netconf]
Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K.,
and R. Wilton, "NETCONF Model for NMDA", draft-ietf-
netconf-nmda-netconf-01 (work in progress), October 2017.
- [I-D.ietf-netconf-nmda-restconf]
Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K.,
and R. Wilton, "RESTCONF Update to Support the NMDA",
draft-ietf-netconf-nmda-restconf-01 (work in progress),
October 2017.
- [I-D.ietf-netmod-revised-datastores]
Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K.,
and R. Wilton, "Network Management Datastore
Architecture", draft-ietf-netmod-revised-datastores-06
(work in progress), October 2017.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119,
DOI 10.17487/RFC2119, March 1997,
<<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed.,
and A. Bierman, Ed., "Network Configuration Protocol
(NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011,
<<https://www.rfc-editor.org/info/rfc6241>>.
- [RFC7921] Atlas, A., Halpern, J., Hares, S., Ward, D., and T.
Nadeau, "An Architecture for the Interface to the Routing
System", RFC 7921, DOI 10.17487/RFC7921, June 2016,
<<https://www.rfc-editor.org/info/rfc7921>>.
- [RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language",
RFC 7950, DOI 10.17487/RFC7950, August 2016,
<<https://www.rfc-editor.org/info/rfc7950>>.
- [RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF
Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017,
<<https://www.rfc-editor.org/info/rfc8040>>.
- [RFC8241] Hares, S., Migault, D., and J. Halpern, "Interface to the
Routing System (I2RS) Security-Related Requirements",
RFC 8241, DOI 10.17487/RFC8241, September 2017,
<<https://www.rfc-editor.org/info/rfc8241>>.

[RFC8242] Haas, J. and S. Hares, "Interface to the Routing System (I2RS) Ephemeral State Requirements", RFC 8242, DOI 10.17487/RFC8242, September 2017, <<https://www.rfc-editor.org/info/rfc8242>>.

9.2. Informative References

[I-D.ietf-i2rs-security-environment-reqs] Migault, D., Halpern, J., and S. Hares, "I2RS Environment Security Requirements", draft-ietf-i2rs-security-environment-reqs-06 (work in progress), September 2017.

Authors' Addresses

Susan Hares
Hickory Hill Consulting
Saline
US

Email: shares@ndzh.com

Alex Clemm
Huawei

Email: ludwig@clemm.org