draft-kwatsen-netconf-server

Configuration Model for SSH and TLS Transports

Introduction

The IETF 88 meeting agreed to unify the configuration data model used between RFC 5539bis and draft-ietf-netconf-reverse-ssh.

The resulting data-model defined in this draft supports the SSH and TLS transports simultaneously, for both the listening and call-home use cases.

Updates since -00

- From -00 to -01
  - Restructured YANG module slightly, to provide groupings useful to the ZeroTouch draft.

- From -01 to -02 (not posted yet!)
  - YANG
    - Moved transport selection deeper into tree
    - Renamed “application” to “network-manager”
    - Renamed “server” to “endpoint”
  - Text
    - Enhanced definition for Keep Alives
    - Clarified persistent connection behavior if app closes connection

Objectives

- Support all NETCONF transports
- Align transport-specific configurations
- Support transport-independent configuration
- Support both inbound and outbound connections

- For Outbound Connections
  - Support More than one Network Manager
  - Support Network Managers having more than one endpoint
  - Support a reconnection strategy
  - Support both persistent and periodic connections
  - Keep-Alives for persistent connections
  - Customizations for periodic connections

Data Model

- Module’s Top-Level Container

```
container netconf {
    description
      "Top-level container for NETCONF server configuration.";
    container listen {
      uses listen-config;
    }
    container call-home {
      uses call-home-config;    // grouping reused by zerotouch
    }
    container tls {
      if-feature tls;
      uses tls-global-config;   // grouping reused by zerotouch
    }
  }
```

Data Model (cont.)

- The “listen” grouping

```
+--rw listen
   +--rw ssh {inbound-ssh}?
   |  +--rw (one-or-many)?
   |     +--:(one-port)
   |     |  +--rw port?        inet:port-number
   |     +--:(many-ports)
   |        +--rw interface* [address]
   |           +--rw address    inet:ip-address
   |           +--rw port?      inet:port-number
   +--rw tls {inbound-tls}?
      +--rw (one-or-many)?
         +--:(one-port)
         |  +--rw port?        inet:port-number
         +--:(many-ports)
            +--rw interface* [address]
               +--rw address    inet:ip-address
               +--rw port?      inet:port-number
```

Data Model (cont.)

- The “call-home” grouping

```
+--rw call-home
   +--rw network-managers
      +--rw network-manager* [name]
         +--rw name                  string
         +--rw description?          string
         +--rw endpoints
         |  +--rw endpoint* [address]
         |     +--rw address    inet:host
         |     +--rw port?      inet:port-number
         +--rw transport
         |  +--rw ssh {outbound-ssh}?
         |  |  +--rw host-keys
         |  |     +--rw host-key* [name]
         |  |        +--rw name    string
         |  +--rw tls! {outbound-tls}?
         +--rw connection-type
            ...
         +--rw reconnect-strategy
            ...
```

Data Model (cont.)

- The “connection-type” and “reconnect-strategy” containers

```
+--rw connection-type
|  +--rw (connection-type)?
|     +--:(persistent-connection)
|     |  +--rw persistent
|     |     +--rw keep-alives
|     |        +--rw interval-secs?   uint8
|     |        +--rw count-max?       uint8
|     +--:(periodic-connection)
|        +--rw periodic
|           +--rw timeout-mins?   uint8
|           +--rw linger-secs?    uint8
+--rw reconnect-strategy
   +--rw start-with?      enumeration
   +--rw interval-secs?   uint8
   +--rw count-max?       uint8
```

Data Model (cont.)

- The “tls” grouping

```
+--rw tls {tls}?
        +--rw cert-maps {tls-map-certificates}?
        |  +--rw cert-to-name* [id]
        |     +--rw id             uint32
        |     +--rw fingerprint    x509c2n:tls-fingerprint
        |     +--rw map-type       identityref
        |     +--rw name           string
        +--rw psk-maps {tls-map-pre-shared-keys}?
           +--rw psk-map* [psk-identity]
              +--rw psk-identity        string
              +--rw user-name           nacm:user-name-type
              +--rw not-valid-before?   yang:date-and-time
              +--rw not-valid-after?    yang:date-and-time
              +--rw key                 yang:hex-string
```

Security Considerations

This document defines a YANG module to configure NETCONF's SSH and TLS transports. Please see the Security Considerations section in those RFCs for transport-specific security issues.

IANA Considerations

Registers one URI in the IETF XML registry:

```
URI: urn:ietf:params:xml:ns:yang:ietf-netconf-server
Registrant Contact: The NETCONF WG of the IETF.
 XML: N/A, the requested URI is an XML namespace.
```

Registers one YANG module in the YANG Module Names registry:

```
name:          ietf-netconf-server
namespace:     urn:ietf:params:xml:ns:yang:ietf-netconf-server
prefix:        ncserver
reference:     RFC XXXX
```

Open Issues

In the “listen” grouping:

- Is the “one-or-many” choice OK?

In the “call-home” grouping:

- Rethink persistent/periodic choice?
  - Add a “schedule” and then use it to configure “periodic” connections?

Questions / Concerns ?