draft-ietf-netconf-server-model-01

NETCONF Server Configuration Model

Updates since IETF 89

- From I-D to -00
  - Changed title to "NETCONF Server Configuration Model”
  - Mapped inbound/outbound to listen/call-home
  - Restructured YANG module to place transport selection deeper into the tree, providing a more intuitive data model
  - Added section "Keep-Alives for SSH and TLS”
  - Updated the Security Considerations section
  - Added section for supporting VRFs via augments
  - Added the “ietf-system-tls-auth” module
- From -00 to -01
  - Restructured document so it flows better
  - Added trusted-ca-certs and trusted-client-certs objects into the ietf-system-tls-auth module
  - Moved “Support for Virtual Routing and Forwarding” section to “Other Considerations” section near end.

Module netconf-server

Top-Level Container

```
container netconf-server {
       description
         "Top-level container for NETCONF server configuration.";
       container listen {
         uses listen-config;
       }
       container call-home {
         uses call-home-config;
       }
     }
```

The “listen” Grouping

```
module: ietf-netconf-server
     +--rw netconf-server
        +--rw listen
           +--rw ssh {ssh-listen}?
           |  +--rw (one-or-many)?
           |     +--:(one-port)
           |     |  +--rw port?        inet:port-number
           |     +--:(many-ports)
           |        +--rw interface* [address]
           |           +--rw address    inet:host
           |           +--rw port?      inet:port-number
           +--rw tls {tls-listen}?
              +--rw (one-or-many)?
                 +--:(one-port)
                 |  +--rw port?        inet:port-number
                 +--:(many-ports)
                    +--rw interface* [address]
                       +--rw address    inet:host
                       +--rw port?      inet:port-number
```

The “call-home” Grouping

```
module: ietf-netconf-server
     +--rw netconf-server
        +--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 {ssh-call-home}?
                 |  |  +--rw host-keys
                 |  |     +--rw host-key* [name]
                 |  |        +--rw name    string
                 |  +--rw tls! {tls-call-home}?
                 |
```

[Continued on next slide]

The “call-home” Grouping (cont.)

[Continuation from previous slide]

```
        |
        +--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
```

Module ietf-system-tls-auth

```
module: ietf-system-tls-auth
  augment /sys:system/sys:authentication:
     +--rw tls
        +--rw trusted-ca-certs
        |  +--rw trusted-ca-cert*   binary
        +--rw trusted-client-certs
        |  +--rw trusted-client-cert*   binary
        +--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
```

Open Issues

1. **In the "listen" grouping, the "one-or-many" construct is inconsistent with other models**
   - replaced with a simple list

2. **In the "call-home" grouping, the "address" node is a key field, preventing extensions such as for VRFs**
   - remove key

3. **Aslo in the "call-home" grouping, "network-manager" is inconsistent with RFC 6244 terminology**
   - Replace with "application"

4. **The "host-key" is currently the *name* of the host key (i.e. ssh_hostkey.pem), which may be underspecified**
   - use fingerprint instead? (or use instance-identifier, see #5 below)

Open Issues (cont.)

5. **Currently no way to config NETCONF server's SSH host-keys or TLS certificates**
   - Add "netconf-server/ssh" and "netconf-server/tls" containers to config and then use instance-identifier to identify which should be used for "listen" and "call-home" use-cases?
   - Do we need to config SSH host-key at the system level? - ietf-system?

6. **Should system-wide SSH Keep-Alives be configurable?**
   - Since not NETCONF-specific, augment ietf-system?

7. **The "ietf-system-tls-auth" module augments "ietf-system", but if only for NETCONF users (not system users), then better in "ietf-netconf-server"**
   - Move the "tls" container directly under /netconf-server (no augmentation)

Questions / Concerns ?