SZTPD Alpha-16 Release Notes

Watsen Networks

January 22, 2025

Abstract

This documentation provides release notes for the Alpha-16 release of SZTPD.

Contents

1 Introduction

The sections below cover what is and is not working in this release of the SZTPD product.

Most everything listed as “not working” will be implemented before FCS.

2 Implemented / Tested

SZTPD implements features on top of YANGcore. Please see the “Implemented / Tested” section in the YANGcore Release Notes for details about what is implemented/tested in the YANGcore layer.

For the SZTPD layer, the following are implemented/tested:

- The ‘rfc8572’ interface implementing the “bootstrap server” defined in RFC 8572.
- The ‘rfc8572’ interface supports client-auth via TLS client-certs and/or HTTP basic auth.
- Both XML and JSON supported on SBI. Strong HTTP header checking.
- Plugin-based dynamic callouts to relay progress reports
- Plugin-based dynamic callouts for ownership verification
- Plugin-based dynamic callouts for response manager[1].
- Bootstrapping log per device (including information about SZTPD’s relay to remote systems)

3 Should Work

SZTPD implements features on top of YANGcore. Please see the “Should Work” section in the YANGcore Release Notes for details about what is should work in the YANGcore layer.

SZTPD adds no new “should work” items.

4 Upcoming Features/Releases:

The following features are sorted by the expected release they might show up in. Please let us know if there is something out of place or missing.

4.1 Alpha-X

- Bootstrapping event counter. SZTPD needs to maintain bootstrapping event counters.
- Device record counters. It is planned to track when the device records are created, last modified, and the total number of modifications. Similarly, to track when the bootstrapping device first connected, last connected, and the total number of connections.
- send notifications, as currently none are.

4.2 Beta

- Run performance and soak tests. Only address issues found.

4.3 FCS

- Nothing new
- Stress tests
- Soak tests

4.4 Post 1.0

- Run the “verify-device-ownership” callouts at time of bootstrapping event (in addition to when the device record was first created). Seems like something that should be opt-ed into, and hence a feature that can be implemented later.

[1] Plugin-based dynamic callouts have been used to test support for RFC 9646.

- Support a callout to retrieve an ownership voucher from an external system. This would implement the “supply-ownership-voucher” RPC defined in the “sztpd-rpcs” module. The RPC is currently protected by a ‘feature’ statement called “supply-ownership-voucher”, thus programmatically signaling that it is not supported, though visible in the YANG.
- Support signing conveyed information sent from SZTPD using the private key associated with a configured owner certificate.
- Support encrypting conveyed information sent from SZTPD using the device’s public key from its identity certificate (e.g., IDevID).
- Support stapling revocation responses to CMS objects returned to devices.
- Update the SBI’s “get-bootstrapping-data” response to strip-out the “ietf-sztp-conveyed-info:” prefix from the “hash-algorithm” value. Since the namespace is already “ietf-sztp-conveyed-info”, the value MAY be prefixed, and while it is considered clearer to always use prefixes, it may be considered cluttering in this instance…

5 Known Limitations

SZTPD inherits known limitations from YANGcore. Please see the “Known Limitations” section in the YANGcore Release Notes for details.

SZTPD has no new known limitations.

6 Change Log

6.1 0.0.16

- Significant update!
- Completely factored YANGcore out to it’s own Python package. See YANGcore’s Release Notes for what is new in the YANGcore layer for its “0.0.1” release.
- Many nodes moved and/or renamed.
- YANG simplified: collapsed groupings from old multi-tenancy solution
- The data model is no longer a single namspace (related to collapsing the groupings).
- Documentation overhauled (more friendly and now only documents what works)

6.2 0.0.15

- Editorial fix

6.3 0.0.14

- Removed a debug statement.

6.4 0.0.13

- Fixed package_data bug from PEP 517 conversion (a false-positive prevented pytests from finding)

6.5 0.0.12

- Updated to support SQLAlchemy 2.0
- Fixed asyncio Deprecation warning
- Fixed PEP 517 based warnings

6.6 0.0.11

- Factored out “yangcore” as a submodule.
- Fixed an issues caused by an update to the SQLAlchemy package.
- Increase max client msg to 32MB, remove prefix from sha-265, only for the JSON response
- Fixed an issue caused by a ‘yangson’ package update.

6.7 0.0.10

- Created “SZTPD_ACCEPT_CONTRACT” with valid value “YES”.
- Renamed “SZTPD_MODE” to “SZTPD_INIT_MODE”.
- Renamed “SZTPD_DEFAULT_ADDR” to “SZTPD_INIT_ADDR”.
- Renamed “SZTPD_DEFAULT_PORT” to “SZTPD_INIT_PORT”.
- Reduced persistent memory usage demand for binary/base64 data.
- Improved YANG to ensure proper callout is referenced in various contexts.

6.8 0.0.9

- Enabled TLS ports to use RSA-based keys (extended deep-inspection logic)
- Enabled TLS server certs to be unordered inside the CMS structure when configured.
- Logic now removes the <content-data> wrapper from XML-based conveyed-information responses.
- Added support for the ‘relay-progress-report’ dynamic-callout. Previously only the webhook was supported.

6.9 0.0.8

- Rewrote the support for “ordered-by user” lists to be more scalable.
- Added initial support for pagination query parameters (‘limit’, ‘offset’, and ‘direction’).
- Added XML support for the SBI (now supports both JSON and XML). Strong HTTP header checking.
- Added strong validation for known base64-encoded values (public keys, private keys, end-entity certificates, and trust anchor certificates) when being configured.

6.10 0.0.7

- Changed “/transport/listen/endpoint/use-for” to be a “mandatory true” *leaf*; it was a “mandatory false” *leaf-list*, thus removing the ability for an endpoint to present more than one API, which was unnecessarily present before.
- The “ordered-by user” query parameters (point + insert) now work, per Section 4.8 of RFC 8040[There are three “ordered-by user” lists in SZTPD: download-uris, bootstrap-servers, and matched-responses (the first two are leaf-lists).] advised that the “download-uri” leaf-list uses URL as keys; the client MUST percent-encode these URL-based keys.].
- Modified the “wn-sztpd-1” YANG module to set the per-device *device-type* leafref to “require-instance true” (was false).
- Implemented the “SZTPD_DEFAULT_ADDR” environment variable, as described in the Installation Guide.

6.11 0.0.6

- Device-ownership verification callout now works using plugin-based callouts.
- The validation-layer’s cache is now rolled back when database transactions fail.
- The validation-layer now tests for uniqueness in global keys.

6.12 0.0.5

- Now supports fronting SZTPD with a TLS-terminator. Requires that the SZTP-client’s certificate is passed to SZTPD via the HTTP header “X-Client-Cert” as a PEM (urlencoded). Tested using NGINX.

6.13 0.0.4

- Now supports concurrent write requests.

6.14 0.0.3

- all unit tests now pass when SZTPD points to a MySQL database. With or without TLS, with or without client certificate. AWS Aurora MySQL also tested.
- RESTCONF error messages are now returned on the SBI (RFC 8572) interface.

6.15 0.0.2

- callback-based callouts implemented to support RFC 9646.
- fixed bugs related to bootstrapping-log and audit-log not cleaning up correctly when deleted.

6.16 0.0.1

- initial public release