128T Release Notes
Version 4.2.5-2

Abstract

128T Release Notes

28 March 2020

Contents

128T 4.2.5-2 Release Notes

Note: The 4.2.5-2 release is a superset of the 4.2.4 release. Features and corrections in the 4.2.4 release are not provided in these release notes. Please refer to the 4.2.4 Release notes for further information.

Special Considerations

- Validation has been added to prevent issues when destination service address and port overlaps with interface (waypoint) address and wayport. If your configuration has an overlapping port range prior to the upgrade, you will now receive a validation error. The configuration must be remediated in order to make any additional changes. (I95-33556)
- Support has been added to provision management interfaces. Typically, these are Linux interfaces that are not part of the 128T configuration. These interfaces are called non- forwarding interfaces. It is strongly recommended that non-forwarding interfaces now be configured within the 128T. When the Conductors are upgraded to 4.2.X, the configuration validation will provide a warning when non-forwarding interfaces are not configured for 128T routers configured in a HA pair. If non-forwarding interfaces are configured prior to upgrading the Conductors to 4.2.X, the shared or fabric device interface type must be explicitly set. DHCP however is not supported. Note: 4.1.5 does not raise a validation error if the interface had DHCP. (I95-30831)
- When creating non-forwarding interfaces on pre 4.2.0 routers, these interfaces should not be configured with default routes until after upgrading the routers to 4.2.0 or greater. (I95-30940)
- Support has been added to allow the 128T Software to automatically determine the number of CPU forwarding cores that the router will use. In previous releases the "automatic/manual" parameter was not available and the core count was defined in environment config or within the UI. If set within the environment config (local.init), 4.2.X will set core count to automatic and determine the number of cores to use. If set in the UI, this parameter will be set to manual and the existing value will be used. Note that if automatic is set and the core count is changed in the PCLI, the change will be accepted as valid configuration but the automatic parameter will override as this parameter takes precedence over the value in the forwarding core count. (I95- 30884)
- Prior to 4.1.5, peering with routers that have the same IP addresses was not supported. In 4.1.5 or greater remote peers having the same IP address is now supported in one direction, with the use of "outbound-only". 128T currently does not support ALL routers having the same IP address, the same IP address support is unidirectional. For example:

  The following is supported:

  ```
  R1(172.16.1.1) --- peered --- R2 (192.168.1.1)
          |------- peered --- R3 (192.168.1.1)
  ```

  The following is not supported:

  ```
  R1(192.168.1.1) --- peered --- R2 (192.168.1.1)
            |------- peered --- R3 (192.168.1.1)
  ```

- On 128T nodes installed after July 1, 2019 on pre 4.2.X versions, Chrome running on MAC OSX Catalina does not consider the 128T self-signed web certificates valid. Apple has put out an advisory: https://support.apple.com/en-us/HT210176 . Once the node is upgraded to 4.2.X, create a new self-signed web cert in the PCLI `create certificate self-signed webserver` (I95-31672)

Issues Fixed

- **I95-18857** Support for automatic loopback has been added to Sangoma T1 devices

- **I95-27764** `write log snapshot` does not work for process highway

- **I95-28190** Addressed issue causing PPPoE passwords to be incorrectly changed to (removed).
  Symptom: `device-interface > pppoe > password` gets converted to (removed) upon changing `device-interface > name`.
  Conditions: Changing the object's key, in this case `device-interface > name` causes secure fields to be incorrectly converted to (removed). Until the system is upgraded to 4.2.5, this issue can be mitigated by deleting the existing `device-interface` object and recreate it.

- **I95-30011** HA router nodes may take upwards of 40 seconds to achieve quorum.
  Symptom: SVR traffic may be dropped while a redundant node is restarting.
  Conditions: The hostname of the platform cannot be resolved
  Until the system is upgraded to 4.2.5, this issue can be mitigated by setting the hostname of the node to a value that can be resolved or add an address for the system in `/etc/hosts`

- **I95-31597** Configuring a static ARP entry within a `neighbor` configuration is not honored
  Symptom: Dynamic ARP entries take precedence over statically configured ARP entries

- **I95-32244** Cannot upgrade after software download completes
  Conditions: Managed router being upgraded via Conductor can intermittently fail due to transient network conditions, 4.2.5 will now perform multiple attempts to verify the download completed.
  Until the system is upgraded to 4.2.5, this issue can be mitigated by performing the Download operation again.

- **I95-32509** Generated configuration objects are shown by default in GUI and PCLI

- **I95-32660** `saltMaster.log` files rotate once daily with a maximum of 25 rotated files, consuming a large amount of disk space. This has been changed to rotate hourly, with a maximum of 25 rotated files.

- **I95-33024** Specifying a `metric` value within `advertise-default` of OSPF causes advertisements to be withdrawn Until the system is upgraded to 4.2.5, this issue can be mitigated by remove `metric` value from `advertise-default` configuration

- **I95-33174** - Some LTE cards do not use the correct wireless bands for the AT&T network

- **I95-33432** Path MTU discovery could be fooled by a (bad acting) network element that fragments large packets in spite of the do-not-fragment (DF) flag

Symptom: Sessions utilizing large packets (like those in some print jobs) may result in failed attempts
Conditions: in-path network element fragments packets with DF bit set.

- **I95-33485** Upgrading a HA node of a 128T router can result in traffic being dropped
Symptom: Existing traffic for some services are blackholed during upgrade
Until the system is upgraded to 4.2.5, this issue can be mitigated by completing the upgrade of both nodes or restart non-upgraded 128T

- **I95-33506** File descriptors can leak upon incorrectly configuring a non-existent namespace within an interface type of `host`.
Symptom: 128T application will fail to run network scripts and other applications
Conditions: Setting `network-namespace` to a value that does not exist on the host platform after committing configuration
Until the system is upgraded to 4.2.5, this issue can be mitigated by removing the invalid configuration.

- **I95-33556** 128T may drop inbound SVR traffic when destination service address and port overlaps with interface (waypoint) address and wayport.
Conditions: `address` on a service matches that of the `network-interface` that participates in SVR AND `tenant` on the service matches the `tenant` on the `network-interface` depending on the service scope AND the `port-range` defined on the `network-interface` overlaps with `port-range` of the service.
Until the system is upgraded to 4.2.5, this issue can be mitigated by changing the `port-range` on the neighborhood to a range that does not overlap with the service. In 4.2.5 a configuration validation has been added to detect such overlap and provide user with appropriate error message.

- **I95-33634** 128T unable to bind to `device-interface`
Symptom: Interface will be administratively up but operationally down
Conditions: highway process faults can leave an interface unbound to any driver, resulting in the inability for the system to rebind to the interface.
Until the system is upgraded to 4.2.5, this issue can be mitigated by issuing a `reboot` on the impacted system.

- **I95-33668** Peer path fails to meet (default) SLA, triggering BGP prefix flapping
Symptom: Advertised routes are withdrawn and subsequently re-advertised with a new route metric.
Conditions: When a service with no `service-policy` configured, therefore utilizing system defaults, traverses a path below SLA.

- **I95-33683, I95-33951** When 128T Networking Platform is configured to use LDAP for authentication, login will fail if the user is a member of both `128t-user` and `128t-admin`
Symptom: User is unable to login.
Until the system is upgraded to 4.2.5, this issue can be mitigated by removing the user from one of the two LDAP groups.

- **I95-33710** Working configuration fails to validate after upgrade
  Symptom: Validation of the configuration will fail with the message `% Error: Candidate configuration is invalid: 1. name is required`.
  Conditions: `device-interface` of type `host` will fail validation if a `management-vector` does not exist.
  Until the system is upgraded to 4.2.5, this issue can be mitigated by configuring a `management-vector` on the `network-interface`s that exist within the `device-interface`.

- **I95-33793** SVR fails to recover session on multi-hop inter-node failure
  Symptoms: Security lookup failure and packet drops.
  Conditions: This scenario occurs only with multi-hop SVR, where an intermediate node WAN link fails, and the target alternate path is `outbound-only`. This only affects existing sessions. New sessions will be unaffected.

- **I95-33857, I95-33642** Short OTP Quickstart DHCP server lease time results in an initial OTP quickstart failure.
- **I95-34058** Session setup fails for outbound only when first packet exceeds MTU
  Symptoms: Session setup fails
  Conditions: Paths configured as `outbound-only`, and the first packet of the flow exceeds MTU (typically UDP).

- **I95-34090** A network-interface configured with multiple neighborhoods, where one of the neighborhoods defines a port range, will result in traffic being dropped on the defined range
  Symptoms: SVR traffic is dropped when destined for a port range configured on its peer 128T router's neighborhood

- **I95-34092** `rotate log` command does not rotate `fastLane.log`, `serviceArea.log` and `flpp.log`.

- **I95-34113** DHCP lease management in the GUI shows no client leases exist
  Conditions: firewall is running on the host 128T platform
  Until the system is upgraded to 4.2.5, this issue can be mitigated by adding the interface `veth` to the `TRUSTED` firewalld zone

- **I95-34135** CVE-2020-8597: A buffer overflow flaw was found in the ppp package

- **I95-34158** Modifying a port-range configuration value to include an overlapping range results in a list with an incorrect range.
  Conditions: An existing range list is modified to include an overlapping range
  Until the system is upgraded to 4.2.5, this issue can be mitigated by entering a unique range of values that do not overlap.

- **I95-34173** The loss of power for the routing manager standby node in a HA router configuration may lead to temporary BGP traffic drops on the primary node.

- **I95-34174** Added configuration `negotiate-capabilities` for BGP neighbor to optionally suppress sending the Capabilities Optional Parameter in the BGP OPEN message.

- **I95-34186** PPPoE interface is disconnected upon changing `device-interface` name

- **I95-34200** Influx database corruption resulting in `show entitlement` or displaying Event history from the Conductor UI to produce an error

- **I95-34209** Incorrect Zscaler plugin installed when installed via the Conductor GUI

- **I95-34310** Secure fields from the 128T configuration are in the commit audit events from config diff operations.

- **I95-34328** asset fails to set high-state and provides errors in `show asset summary`
  Symptoms: show asset summary provides errors for an asset and does not perform high-state operations. The error `error: db5 error` would be seen in `/var/log/salt/minion.log` file
  Conditions: When the centos rpmdb has been corrupted.
  Until the system is upgraded to 4.2.5, run the following commands on the target asset `mv /var/lib/rpm/__db* /tmp; yum clean all; dnf clean all`

- **I95-34408** When creating/renaming a device-interface, prefix-delegation configuration was blocked until dhcp is explicitly disabled

Caveats

- **I95-29592** Conductor UI and/or PCLI may not update the asset software version correctly

  Symptom: The Conductor UI and/or the PCLI may not correctly reflect the software version running on the asset

  Conditions: After the asset has been upgraded

  Corrective Action: If the asset is not updated after ~5 minutes after an upgrade is performed, the salt-minion will need a restart on the asset node that does not update the version. This is done with the following command on the node as the root Linux user:

  ```
  "systemctl restart salt-minion"
  ```

- **I95-27808** `sync peer addresses router force` from conductor may not trigger router to send address information from peer

  Symptom: When performing the following command on the Conductor PCLI, `sync peer addresses router force` the router may not provide the peer address information

  Conditions: Unknown

Corrective Action*:* Perform the PCLI command on the router to update the information on the conductor.