Virtual Services Platform 9000
Software Release 4.1.5.0

1. Release Summary

Release Date: June 2017
Purpose: Software release to address customer found software issues.

2. Important Notes before Upgrading to This Release

None.

3. Platforms Supported

Virtual Services Platform 9000 (all models)

4. Special Instructions for Upgrade from previous releases

None.

5. Notes for Upgrade

Please see "*Virtual Services Platform 9000, Release Notes*" for software release 4.1.0.0 (NN46250-401) available at http://www.avaya.com/support for details on how to upgrade your Switch.

File Names For This Release

File Name	Module or File Type	File Size (bytes)
VSP9K.4.1.5.0.tgz	Release 4.1.5.0 archived distribution	176781679
VSP9K.4.1.5.0_modules.tgz	Encryption modules	41900
VSP9K.4.1.5.0_mib.zip	Archive of all MIB files	825761
VSP9K.4.1.5.0_mib.txt	MIB file	5493794
VSP9K.4.1.5.0_mib_sup.txt	MIB file	958305

VSP9000v410_HELP_EDM_gzip.zip	EDM Help file	3882169
VSP9K.4.1.5.0.md5	MD5 Checksums	586
VSP9K.4.1.5.0.sha512	SHA encryption	1546
VSP9000v4.1.4.0.zip	EDM WAR plugin for COM	5655812

Note about image download:

Ensure images are downloaded using the binary file transfer. Perform MD5 checksum check on downloaded files to ensure file integrity.

Check that the file type suffix is “.tgz” and the image names after download to device match those shown in the above table. Some download utilities have been observed to append “.tar” to the file name or change the filename extension from “.tgz” to “.tar”. If file type suffix is “.tar” or file name does not exactly match the names shown in above table, rename the downloaded file to the name shown in the table above so that the activation procedures will operate properly.

Load activation procedure:

```
software add VSP9K.4.1.5.0.tgz
software add-modules 4.1.5.0.GA VSP9K.4.1.5.0_modules.tgz
software activate 4.1.5.0.GA
```

6. Version of Previous Release

Software Version 3.4.x.x, 4.0.0.0, 4.0.1.0, 4.0.1.1, 4.0.1.2, 4.1.0.0, 4.1.1.0, 4.1.2.0, 4.1.3.0, 4.1.4.0

7. Compatibility

8. Changes in 4.1.5.0

New Features in This Release

Issue Number	Issue Description
VSP9000-755	New CLI command has been introduced to enable/disable ssh client functionality. By default, ssh client is enabled. Following are the details: 1) (config)#ssh client {enable} (config)#no ssh client {enable} (config)#default ssh client {enable} 2) New MIB entry for switch on/off ssh client: rcSshGlobalClientEnable OBJECT-TYPE SYNTAX TruthValue MAX-ACCESS read-write STATUS current DESCRIPTION "Enable/disable SSH Client." DEFVAL { true } ::= { rcSshGlobal 24 } 3) New error code: RC_SSH_DISABLED_SSH_CLIENT_CANNOT_ENABLE 5516 sshDisabledSshClientCannotEnable
VSP9000-729 VSP9000-758 VSP9000-762	Additional diagnostic code on Gen-2 IO modules in unresponsive datapath conditions after continuously logging the message: **"GlobalRouter VPE_COB ERROR cob_vtIndex_accessCache: sierraslice_read failed! ret=-1, VT_BRIDGED_EGR_PORT_CNT_RAW_TBL"**. Data captured from the datapath of affected slices is logged into a file /intflash/flrec/<slot no>/io_sierraLockUp_slice_X which is created on per slot, per slice basis. The following log message will be displayed when a new file is created. "**GlobalRouter VPE_DRIVER ERROR zag_debug_write_reg: Detected Sierra Lockup. Starting zagros reg dump in file: /intflash/flrec/X/io_sierraLockUp_slice_Y**"
VSP9000-773	Added support for AOBOC(Active Break out optical cable) Avaya PEC AA1404041-E6 in 9024XL IO module.

Old Features Removed From This Release

None

Problems Resolved in This Release

Issue Number	Issue Description
VSP9000-722	Some IP hardware records are not displayed correctly in Gen-1 IO module.
VSP9000-726	When TACACS is enabled and switch is accessed using SSH, some of the TCP connections from TACACS server to the switch are suspended in CloseWait state.
VSP9000-742	VSP platforms come with a trial license by default to enable premier features. When this license expires, the switch logs the message: "**GlobalRouter SW INFO Premium License trial period has expired. Base Licensing is running.** "once per day. After the trial license expires, this log generation can be stopped with system reset.
VSP9000-757 [Also in 4.1.4.1]	During VLAN migration from GRT to VRF, VPE_ARP ERRORs may be continuously logged for Gen-2 IO modules indicating failure to add records to the ARP table
VSP9000-761 [Also in 4.1.4.1]	Connectivity issues observed due to nodal BMAC association to certain ARP entries not populated on Gen-2 IO modules. The missing of nodal BMAC for ARP entries causes transmission of SPB traffic without BMAC encapsulation and results in reachability issues.
VSP9000-765	CPP RX packet dump messages may be logged continuously in high volumes due to ingress of packets with invalid MAC Ether type in CP due to fabric issues. The packet logging logic has been modified to limit the messages to one invalid packet per minute.
VSP9000-766, VSP9000-768, VSP9000-775 [Also in 4.1.4.1]	The size of RSP Exception capture file, which is created when exception packets are generated at RSP, increments continuously increasing buffer utilization on internal flash memory. In addition to fixing the issue, a flag has been introduced to disable or enable the RSP Exception packet capture feature from the IO shell, as follows. In the privilege mode, from the IO card shell: To disable the feature: setflag ("rspExpDebug", 3) To enable the feature: setflag ("rspExpDebug", 0) The feature is enabled by default
VSP9000-767	Re-added the functionality to support 1 Million IP routes with Premier and Premier+MACsec license in Gen-2 compatibility mode that was accidentally removed in VSP9000 4.1.0.0-4.1.4.0 software versions.

VSP9000-771 [Also in 4.1.4.1]	Traceroute to IP interface does not work on inter-VRF routes accepted using ISIS accept policies.
VSP9000-772 VSP9000-777 [Also in 4.1.4.1]	Latency issues may be observed on both Gen-1 and Gen-2 IO modules for inter-VRF routes redistributed using ISIS accept policies. Elevated CPU utilization may be observed as packets are forwarded through the control plane.
VSP9000-780	When ISIS adjacency bounces, the SPB ARP index associated with L3VSN record is leaked in systems with Gen-2 IO module. Continuous flapping of ISIS adjacencies may result in the exhaustion of heap memory associated with SPB ARP table. This heap memory exhaustion may cause system instability and network connectivity issues.
VSP9000-794	Withdraw messages are leaked that are not included in route policies configured via route-map. To fix the issue the following CLI commands have been introduced: 1) Router BGP mode: (router-bgp)# neighbor <ipaddr|peer-group> always-send-withdraw enable 2) Router VRF mode: (router-vrf)# ip bgp neighbor <ipaddr|peer-group> always-send-withdraw enable The command is enabled by default. The behavior with the introduction of new commands is as below: Enabled (Default): Even though BGP does not advertise the routes due to output policy, it sends withdraw messages so that this BGP peer receives only Update messages with withdraw routes. Disabled: BGP won't send withdraw messages if it did not advertise the routes (NLRI) so that this BGP peer does not receive any Update messages (NLRI/WITHDRAW).

10. Outstanding Issues

Please see “Virtual Services Platform 9000, Release Notes” for software release 4.1.0.0 (NN46250-401), 4.1.1.0, 4.1.2.0, 4.1.3.0 and 4.1.4.0 available at http://www.avaya.com/support for details regarding Known Issues.

11. Known Limitations

Please see "Virtual Services Platform 9000, Release Notes" for software release 4.1.0.0 (NN46250-401), 4.1.1.0, 4.1.2.0, 4.1.3.0 and 4.1.4.0 available at http://www.avaya.com/support for more details regarding Known Limitations.

VSP 9000 does not support the use of local interfaces as next hop for static default routes to route between VRF contexts. Using such configurations may result in traffic loss and elevated CPU utilization on the CP module as packets are forwarded to the CP for software forwarding. Inter-VRF routing must be accomplished by using routes that point to next hops that are not local.

9024XL I/O modules with hardcopy Zagros FPGA cannot reliably mirror heavy egress traffic. When the egress mirror port bandwidth is exceeded by the combined burst rate of the mirrored traffic and the incoming traffic of the ports on the slice, it might result in Egress Mirror Block (EMB) overflow condition which results in corrupting the egress packets. These packets cause a series of cascading errors in the data path which includes forwarding bad frames to the destination slot (examples of said bad frames would be registered in the log file as follows "GlobalRouter CPU ERROR CPP RX: Unexpected source for packet. CPU_MAC_EtherType = 0xF38E. Dropping Packet." and "GlobalRouter SW WARNING CppIoHbProcessPacket:Received invalid/corrupt heartbeat packet from RSP. Slice 84, lane 32, rtnSlice 80."). As an alternative, "slice" method of doing port mirroring is supported to supplement diag port mirroring to provide higher performance mirroring with restriction that ports must be local to the same slice.

12. Documentation Corrections

For other known issues, please refer to the product release notes and technical documentation available from the Avaya Technical Support web site at: http://www.avaya.com/support .

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Avaya.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web at: http://www.avaya.com/support