avaya.com

Virtual Services Platform 9000
Software Release 4.2.0.0

1. Release Summary

Release Date: August 11, 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.4.2.0.0.tgz	Release 4.2.0.0 archived distribution	177253722
VSP9K.4.2.0.0_modules.tgz	Encryption modules	41914
VSP9K.4.2.0.0_mib.zip	Archive of all MIB files	826188
VSP9K.4.2.0.0_mib.txt	MIB file	5495987
VSP9K.4.2.0.0_mib_sup.txt	MIB file	958527

VSP9000v410_HELP_EDM_gzip.zip	EDM Help file	3882169
VSP9K.4.2.0.0.md5	MD5 Checksums	586
VSP9K.4.2.0.0.sha512	SHA encryption	1546
VSP9000v4.2.0.0.zip	EDM WAR plugin for COM	5657179

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.4.2.0.0.tgz
software add-modules 4.2.0.0.GA VSP9K.4.2.0.0_modules.tgz
software activate 4.2.0.0.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, 4.1.5.0

7. Compatibility

8. Changes in 4.2.0.0

New Features in This Release

MACsec enhancement

MACsec updates in this release enable enhanced security where multiple Secure Association (SA) Keys are internally derived from the configured Connectivity Association Key (CAK), to secure communication on the link. These SA Keys are periodically refreshed to ensure that the same key is not used for an extended period of time. From a provisioning perspective, the administrator still configures a single shared CAK on the two ends of the MACsec enabled link. This CAK is now used to internally derive multiple SA Keys. In order to differentiate the

transmit and receive SA keys used between two ends of a MACsec enabled link, one additional parameter has been added (`key-parity <even|odd>`). MACsec links should always be provisioned as odd/even pair.

After the upgrade, previously configured MACsec links will continue to be operational with earlier MACsec implementations where fewer SAs were used to secure the link. In order to utilize the enhanced security, it is strongly recommended to add the `key-parity` configuration, which will enable multiple SA keys to be used to secure the link.

Note:
With this release, `key-parity` is an optional parameter. Future releases will make this a mandatory parameter. As such, to avoid configuration breaks during upgrade to future releases, it is strongly recommended that once you upgrade to 4.2.0.0, you should update your existing MACsec configuration to include the `key-parity` keyword and provision the MACsec links as odd/even pairs.

Due to changes in password file format for MACSec CA Entries to support 4AN mode, MACSec CA configs will fail during downgrade to older release prior to 4.2.0.0. User Should delete the MACSec entries, proceed to downgrade and re-configure CA after downgrade is completed. This is applicable to 2AN mode CAs also.

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 regarding MACsec feature.

SSL enhancement

RC4 ciphers are disabled to resolve Security Vulnerability Found CVE-2013-2566 CVE-2015-2808 CVE-2009-3555. A new boot flag `ssl-support-rc4` has been added to provide RC4 support if needed. The flag will be disabled by default.

Unicast FIB Hash Collision Algorithm enhancement

The BVID and BMAC hashing function for SPBM Unicast FIB table Indices cannot accommodate all permutations for all customers. Two new hash algorithms (correlation and random) have been introduced to help in avoiding collisions when storing ISIS SPBM Unicast FIB entries in the SPBM Unicast FIB table on Gen-2 IO module. This option should only be changed if log event **“0x00338602 00000000 GlobalRouter VPE_TBLMGR ERROR tblmgr_hash_addOrUpdateRecord: failed to add an entry due to hash collision in all 8 segments in VST_SPB_UC_FIB_TBL”** has been observed on Gen-2 IO modules.

CLI/SNMP support has been provided to switch between the default, correlation and random algorithms. This applies to GEN-2 modules only. The IO module(s) needs to be rebooted once the hash algorithm has been changed for it to take effect.

CLI command:

```
spbm uc-fib-hash-alg <correlation | default | random>
```

Example:

```
VSP9000:1(config)#spbm uc-fib-hash-alg correlation
Warning: The modified hash algorithm will only be applied to Unicast FIB
table on the Gen 2 IO module(s) after a reboot of the IO module{s)

VSP9000:1(config)#show spbm
                    spbm : enable
               ethertype : 0x8100
           uc-fib-hash-alg : correlation
```

MIB details:

```
rcPlsbGlobalUcFibHashAlg OBJECT-TYPE
SYNTAX INTEGER {default(1), correlation(2), random(3)}
MAX-ACCESS read-write
STATUS current
DESCRIPTION "SPBM UC FIB Table Hash Algorithm"
DEFVAL {default}
::= { rcPlsbGlobal 6}
```

The config needs to be set to "`default spbm uc-fib-hash-alg`" and saved prior to downgrade to earlier releases. The default algorithm will be enabled on downgrade and the hash table collisions may reoccur.

Old Features Removed From This Release

None

Problems Resolved in This Release

Issue Number	Issue Description
VSP9000-778	The following error messages may be logged continuously on Gen-2 I/O modules after recurrent rebooting of IST peer or toggling of ISIS interfaces when ECMP is enabled on ISIS routes and routes are redistributed using ISIS accept policy. **"GlobalRouter VPE_VL ERROR mw_getIndex heap_getindex failed! HEAP_ECMP_TBL cellIndexCnt=8 starting_index=-1"** **"GlobalRouter VPE_IPV4 ERROR ioIpv4EcmpRouteAdd: Failed to add/update ECMP Route in Route Table IPv4 <addr> Mask <subnet-mask> NH <addr> VRF X numEcmp Y - reason IO_HEAPMGR_GET_FAILED"**
VSP9000-798	IP hardware records which have 'F' in hexadecimal representation of network addresses are not displayed correctly in Gen-1 IO module.

VSP9000-801	"show fabric io" command output is incomplete for slots 11 and 12. SFI information is incomplete for slot-11 and no SFI/SCI information is displayed for slot-12.
VSP9000-808	SSH client functionality can be enabled via ACLI command only when SSH is enabled.
VSP9000-812	High CPU utilization and memory leak when responding to large ICMP echo request packets that required fragmentation

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, 4.1.4.0 and 4.1.5.0 available at http://www.avaya.com/support for details regarding Known Issues.

11. Known Limitations

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.

PCAP will not capture LACP TX packets on Gen-1 I/O modules. As an alternative, mirroring of packets can be used or LACP RX packets can be captured on the other end.

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, 4.1.4.0 and 4.1.5.0 available at http://www.avaya.com/support for more details regarding Known Limitations.

12. Software Scaling Capabilities

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 more details regarding scaling capabilties.

13. 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 .

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