VSP Operating System Software Release 6.1.3.0

1. Release Summary

Release Date: Mar 2018
Purpose: Software release to address customer found software issues.

2. Important Notes before Upgrading to This Release

If upgrading systems from either release 4.2.1.0 or release 4.2.1.1 that have ISIS enabled link(s) configured with HMAC-MD5 authentication, then you need to perform the procedure described in section (4) below in order to avoid potential network connectivity loss.

If upgrading systems running 4.1.X releases which also have TACACS+ enabled, refer to section 4 for upgrade instructions.

3. Platforms Supported

Virtual Services Platform 4000 Series
- Virtual Services Platform VSP 4850GTS
- Virtual Services Platform VSP 4850GTS-PWR+
- Virtual Services Platform VSP 4450GSX-PWR+
- Virtual Services Platform VSP 4450GSX-DC
- Virtual Services Platform VSP 4450GTS-DC
- Virtual Services Platform VSP 4450GTX-HT-PWR+

Virtual Services Platform 7200 Series
- Virtual Services Platform VSP 7254XSQ
- Virtual Services Platform VSP 7254XTQ

Virtual Services Platform 8000 Series
- Virtual Services Platform 8200
- Virtual Services Platform 8400

.

4. Special Instructions for Upgrade from previous releases

1. The following procedure should be followed when upgrading systems running one of the following two releases, 4.2.1.0 or 4.2.1.1 which also have ISIS enabled links with HMAC-MD5 authentication on:

Disable ISIS authentication throughout the network a system at a time, a link at a time by disabling it on either side of each link, ensuring the link is stable before moving to the next. When a system has been reconfigured free of ISIS HMAC-MD5 authentication in all of its links, save the configuration file and perform the upgrade to release 4.2.3.0 or greater. After all these systems have been upgraded to release 4.2.3.0 or greater, you may re-enable authentication a system at a time, a link at a time and save the configuration file in each of the involved systems.

Example:

VSP:1(config)#interface gigabitethernet x/y
VSP:1(config-if)#no isis hello-auth
VSP:1(config-if)#save config
VSP:1(config-if)# PERFORM THE UPGRADE
VSP:1(config)#interface gigabitethernet x/y
VSP:1(config-if)# isis hello-auth type hmac-md5 key <keyname> [key-id <keyed>]
VSP:1(config-if)#save config

2. The following procedure should be followed when upgrading systems running 4.1.X releases which also have TACACS+ enabled on:

   When you upgrade from VOSS 4.1.X to VOSS 4.2 or a higher release, the TACACS+ host configurations will be lost. After the upgrade, the TACACS+ host configurations will not take effect so you must reconfigure them. After you make the configurations, you must save the changes on the device. You should also save the configuration to a file to retain the configuration settings.

3. Upgrading DVR configurations from releases 6.0.1.1 and earlier to 6.0.1.2 and beyond.
   a. All DVR nodes must be upgraded to the same release.
   b. All DVR leaves should be upgraded first.

5. Notes for Upgrade

Please see “Release Notes for VSP Operating System” for software release 6.1.0 (NN47227-401, 15.05) available at http://www.avaya.com/support for details on how to upgrade your Switch.

File Names For This Release

Virtual Services Platform 4000 Series

File Name	Module or File Type	File Size (bytes)
VOSS4K.6.1.3.0.tgz	Release 6.1.3.0 archived software distribution	104467462
VOSS4K.6.1.3.0_mib.zip	Archive of all MIB files	1083039
VOSS4K.6.1.3.0_mib.txt	MIB file	7180177
VOSS4K.6.1.3.0_mib_sup.txt	MIB file	1182904
VSP4000v612_HELP_EDM_gzip.zip	EDM Help file	3282973
VSP4000v6.1.3.0.zip	EDM plug-in for COM	4876940
VOSS4K.6.1.3.0.md5	MD5 Checksums	533
VOSS4K.6.1.3.0.sha512	SHA512 Checksums	1397

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7K.6.1.3.0.tgz	Release 6.1.3.0 archived software distribution	66478054
VOSS7K.6.1.3.0_mib.zip	Archive of all MIB files	1083039
VOSS7K.6.1.3.0_mib.txt	MIB file	7180177
VOSS7K.6.1.3.0_mib_sup.txt	MIB file	1186371
VOSSv612_HELP_EDM_gzip.zip	EDM Help file	3288186
VOSSv6.1.3.0.zip	EDM plug-in for COM	5198978
VOSS7K.6.1.3.0.md5	MD5 Checksums	527
VOSS7K.6.1.3.0.sha512	SHA512 Checksums	1391

Virtual Services Platform 8000 Series

File Name	Module or File Type	File Size (bytes)
VOSS8K.6.1.3.0.tgz	Release 6.1.3.0 archived software distribution	120546892
VOSS8K.6.1.3.0_mib.zip	Archive of all MIB files	1083039
VOSS8K.6.1.3.0_mib.txt	MIB file	7180177
VOSS8K.6.1.3.0_mib_sup.txt	MIB file	1186371
VOSSv612_HELP_EDM_gzip.zip	EDM Help file	3288186
VOSSv6.1.3.0.zip	EDM plug-in for COM	5198978
VOSS8K.6.1.3.0.md5	MD5 Checksums	527
VOSS8K.6.1.3.0.sha512	SHA512 Checksums	1391

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 procedures:

software add VOSS4K.6.1.3.0.tgz
software activate VOSS4K.6.1.3.0.GA

or

software add VOSS7K.6.1.3.0.tgz
software activate VOSS7K.6.1.3.0.GA

or

software add VOSS8K.6.1.3.0.tgz
software activate VOSS8K.6.1.3.0.GA

6. Version of Previous Release

Virtual Services Platform 4000 Series

Software Version 3.0.0.0, 3.0.1.0, 3.1.0.0, 3.1.0.2, 3.1.0.3, 4.0.0.0, 4.0.0.1, 4.0.0.2, 4.0.0.3, 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0 and 6.1.2.1 for VSP 4850GTS platforms

Software version 4.0.0.0, 4.0.0.1, 4.0.0.2, 4.0.0.3, 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0 and 6.1.2.1 for VSP 4450GSX platform

Software Version 4.0.50.0 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0 and 6.1.2.1 for VSP 4450GSX DC and VSP 4450GTS DC platforms

Software Version 4.0.40.0**,** 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0 , 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0 and 6.1.2.1 for VSP 4450GTX-HT-PWR+ platform

Virtual Services Platform 7200 Series

Software Version 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0 , 6.0.1.1, 6.0.1.2, 6.1.0.0**,** 6.1.1.0, 6.1.2.0 and 6.1.2.1.

Virtual Services Platform 8000 Series

Software Version 4.0.0.0, 4.0.1.0, 4.0.1.1, 4.0.1.2, 4.0.1.3, 4.0.1.4, 4.1.0.0, 4.1.0.1, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0**,** 6.0.1.0 , 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0 and 6.1.2.1 for VSP8200 platform

Software Version, 4.2.0.0, 4.2.0.1, 4.2.1.0, 4.2.1.1, 4.2.2.0, 4.2.3.0, 5.0.0.0, 5.0.1.0, 5.1.0.0, 5.1.1.0, 5.1.1.1, 5.1.1.2, 5.1.1.3, 5.1.1.4, 6.0.0.0, 6.0.1.0, 6.0.1.1, 6.0.1.2, 6.1.0.0, 6.1.1.0, 6.1.2.0 and 6.1.2.1 for VSP8404 platform

Software Version, 5.3.0.0, 6.1.0.0, 6.1.1.0, 6.1.2.0 and 6.1.2.1 for VSP8404c platform

7. Compatibility

8. Changes in 6.1.3.0

Inserting an ESM into a slot from which an ESM has been removed will wait for 15 seconds before being allowed to power on. The following log message will appear when this condition occurs.

> CP1 [03/27/18 04:00:04.304:UTC] 0x00010822 00000000 GlobalRouter HW INFO Slot 1 is re-inserted within 15 seconds. Delay 7 seconds to power it on

Problems Resolved in This Release

ID	Description
VSP4000-198	Unable to change the ISIS L1 metric value from the on box EDM for MLT interface
VSP4000-200	High CPU Utilization lasting 2-3 min on multiple VSP nodes because ISIS packets sent to wrong priority internal queue. VSP4000 specific issue.
VSP4000-201	Fix to display the complete filtered bridge table output on EDM
VSP4000-206	DHCP Clients physically disconnected and reconnected are no longer able to receive a DHCP IP address where DHCP_RELAY forwarding path was using a VRRP IP address.
VSP4000-209	Memory corruption caused node to reset when a vIST interface goes down due to peer interface going down
VSP7200-53	Upgrade from 6.1.1.1 to 6.1.2.0 resulted in CLI “show sys-info” to display airflow as front to back
VSP7200-37 VSP8000-265	Switch management becomes non-responsive for many minutes when vlan experiences a down event after it has not been in the down state for a long time.
VSP8000-252 VSP8000-260	Dynamically changing the Metric Type in an ISIS redistribution Policy does not always take effect when those routes are imported into other VRFs.
VSP8000-256	Running show fulltech produces a large number of macsec stat get errors in /var/log/messages file when macsec is not configured.
VSP8000-258	Unable to access node via SSH/Telnet/Console after a session times out and cleanup causes node reset.
VSP8000-259	Toggling ISIS or booting a node may make inter-vrf redistributed routes disappear leaving less preferred routes.
VSP8000-263	HW watchdog may go off (silently) when system gets busy. Logic changed to not falsely trigger error and added logs to console and syslog to help identify actual SW watchdog failure.
VSP8000-264	Sflow packets received from VSP8200 do not egress through an adjacent ERS 8800 even though S-flow collector is reachable and IP Shortcuts is enabled.
VSP8000-266	VSP8404/VSP8404C show pluggable-optical-modules detail for 40G optics may cause link down
VSP8000-269	IGMP record cleanup may crash node.
VSP8000-270	MACSEC enabled Interfaces may fail after rekey. Changing between 4AN and 2AN mode may cause rekey to fail.
VSP8000-272	Node crashed after executing vlan action command
VSP8000-274	Multicast group address is subscribed by two VLANs. Multicast traffic should hit both the VLANs but it’s not happening.
VSP8000-275	ACL configured not working after upgrade to 6.1.0.0/6.1.1.0 from 5.1.1.1. MinM packets ingressing NNI are matching vlan qualifier on inVlan (CVID) ACL (the inner vlanID). Fix

	prevents the application of inVlan ACL on NNI traffic.
VSP8000-280	VSP8000 platforms generating coredump exceptions when last power supply goes off line.
VSP8000-291	VRRP PDU rate much higher than expected.
VSP8000-292	Node resets when out of memory. Memory leak seen when rcIsisSpbmMcastFibUniEntry MIB object is polled over time.
VSP8000-293	OSPF area mismatch caused by configuration error due to OSPF enabling placed VLAN into OSPF backbone area. Warning added.
VSP8000-295	Radius authenticated RWA user not allowed through SCP
VSP8000-299	EDM is not displaying optical transmit power level information
VSP8000-305	Fixed security issue when authenticating through TACACS
VSP8000-304	Fixed security issue when authenticating through TACACS
VOSS-8749	Add counter for received STP packets with TC bit set. #show spanning-tree mstp port statistics 1/13 ========== MSTP Cist Port Statistics ========== Port Number : 1/13 Cist Port Fwd Transitions : 2 Cist Port Rx MST BPDUs Count : 0 Cist Port Rx RST BPDUs Count : 0 Cist Port Rx Config BPDUs Count : 1 Cist Port Rx TCN BPDUs Count : 0 Cist Port Rx TC BPDUs Count : 1 <- TC is now included and counted for STP packets with TC Cist Port Tx MST BPDUs Count : 0 Cist Port Tx RST BPDUs Count : 0 Cist Port Tx Config BPDUs Count : 6 Cist Port Tx TCN BPDUs Count : 0 Cist Port Invalid MSTP BPDUs Rx : 0 Cist Port Invalid RST BPDUs Rx : 0 Cist Port Invalid Config BPDUs Rx : 0 Cist Port Invalid TCN BPDUs Rx : 0 Cist Port Proto Migr Count : 0
VOSS-8836	SVIST Peer switch local MAC is learned on a non SVIST port/tunnel on different vlan (due to loop condition)
VOSS-8923	Problem installing 3rd party digital certificate
VOSS-9052	LLDP: Interface name id is not correct on subport 2/3/4 of channelized port
VOSS-9200	SM Multicast traffic is filtered on vIST interface in single homed scenario with sender off local interfaces and receiver on the vIST peer
VOSS-9317	XMC failed to configure PVID when a port is not in the VLAN
VOSS-9339	IPV6 tagged / untagged traffic action does not work with IPV6 INVLAN ACL Filters
VOSS-9413	Fixed rcErrorReturnCode attribute in mib.txt object
VOSS-9436	Failed to recognize or bring online JDSU, Finisar, Avago 40G optics and 40G DAC pluggable in VSP8404/VSP8404c
VOSS-9554	Intermittently a channel in a 40Gig channelized port is not recognized at bootup
VOSS-9591	Ability to display the Module revision number for the ESMs on VOSS platforms
VOSS-9787	For ESM card re-insert, device should wait for 15 seconds to power it up

9. Outstanding Issues

Please see “Release Notes for VSP Operating System” for software release 6.1.0 (NN47227-401, 15.05) available at http://www.avaya.com/support for details regarding Known Issues.

10. Known Limitations

Please see “Release Notes for VSP Operating System” for software release 6.1.0 (NN47227-401, 15.05) available at http://www.avaya.com/support for details regarding Known Limitations.

Regular cleanup of unneeded files on USB drives is recommended to minimize possibility of USB corruption when a system is reset, shutdown or power is lost.

Redistribution of "direct" interfaces between VRFs will cause replication of arp entries in the hardware tables for each of the redistributed VRFs.
Care should be taken when planning the redistribution of directs between VRFs to ensure arp counts remain within the scaling limits of the platform.
If platform scaling limits are exceeded the following message will be observed:
IO1 [09/17/17 20:41:01.049:EDT] 0x00140592 00000000 GlobalRouter COP-SW ERROR ercdUpdateArpAcrossVrf: Failed to add IPv4 Host in BCM for 10.1.4.39 vrf=15: reason=-6(Table full)
To avoid this situation, design consideration should be taken to plan for direct route redistribution between VRFs only where needed to reduce unnecessary extra ARP copies.

11. 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