VSP Operating System Software Release 5.1.1.3

1. Release Summary

Release Date: September 2016
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.

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

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
```

5. Notes for Upgrade

Please see “Release Notes for VSP Operating System” for software release 5.1.1 (NN47227-401, 09.04) 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.5.1.1.3.tgz	Release 5.1.1.3 archived software distribution	97254476
VOSS4K.5.1.1.3_mib.zip	Archive of all MIB files	996309
VOSS4K.5.1.1.3_mib.txt	MIB file	6680463
VOSS4K.5.1.1.3_mib_sup.txt	MIB file	986407
VSP4000v511_HELP_EDM_gzip.zip	EDM Help file	2996205
VSP4000v5.1.1.3.zip	EDM plug-in for v5.1.1.3/vsp4000	4501306
VOSS4K.5.1.1.3.md5	MD5 Checksums	642

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7K.5.1.1.3.tgz	Release 5.1.1.3 archived software distribution	62839489
VOSS7K.5.1.1.3_mib.zip	Archive of all MIB files	996309
VOSS7K.5.1.1.3_mib.txt	MIB file	6680463
VOSS7K.5.1.1.3_mib_sup.txt	MIB file	979385
VOSSv511_HELP_EDM_gzip.zip	EDM Help file	3017523
VOSSv5.1.1.3.zip	EDM plug-in for v5.1.1.3/vsp7200	4635216
VSP7K.5.1.1.3.md5	MD5 Checksums	636

Virtual Services Platform 8000 Series

File Name	Module or File Type	File Size (bytes)
VOSS8K.5.1.1.3.tgz	Release 5.1.1.3 archived software distribution	62836868
VOSS8K.5.1.1.3_mib.zip	Archive of all MIB files	996309
VOSS8K_5.1.1.3_mib.txt	MIB file	6680463
VOSS8K.5.1.1.3_mib_sup.txt	MIB file	979385
VOSSv511_HELP_EDM_gzip.zip	EDM Help file	3017523
VOSSv5.1.1.3.zip	EDM plug-in for v5.1.1.3/vsp8000	4635216
VSP8K.5.1.1.3.md5	MD5 Checksums	636

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.5.1.1.3.tgz
software activate VOSS4K.5.1.1.3.GA
```

or

```
software add VOSS7K.5.1.1.3.tgz
software activate VOSS7K.5.1.1.3.GA
```

or

```
software add VOSS8K.5.1.1.3.tgz
software activate VOSS8K.5.1.1.3.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 and 5.1.1.2 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 and 5.1.1.2 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 and 5.1.1.2 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 and 5.1.1.2 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 and 5.1.1.2

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 and 5.1.1.2 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 and 5.1.1.2 for VSP8400 platform

7. Compatibility

8. Changes in 5.1.1.3

New Features in This Release

1. Enable/disable ssh client Functionality

New CLI command to enable/disable ssh client functionality. By default, ssh client is enabled. Following are 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
```

Old Features Removed From This Release

Problems Resolved in This Release

ID	Description
VSP4000-115	EDM access fails when using Radius authentication with password length more than 20 characters
VSP4000-120	EDM access fails when User ID uses TACACS+ authentication with access level 15. Access level 15 is mapped to 6 which is rwa.
VSP8000-128	ARP entries for L3VSN routes were not being cleaned up when the last L3VSN route from a remote BEB was removed. These stale entries could cause connectivity problems if a new SPB node is then introduced into the topology and is participating in the same L3VSN.
VOSS-3808	SSH login may fail with ASG user ID when ASG is enabled.
VOSS-3837	Polling "if name" OID returns wrong value for the port on card 8408QQ
VOSS-3862	Global Router IP routes that are ISIS Accepted into L3VSN VRF are broken; Packets go out with null source BMAC
VOSS-3922	Add ACLI command to disable SSH client functionality.
VOSS-4259	EAP is failing when server first authentication method does not match.

9. Outstanding Issues

Please see “Release Notes for VSP Operating System” for software release 5.1.1 (NN47227-401, 09.04) available at http://www.avaya.com/support for details regarding Known Issues.

In addition, the following issues have been identified:

ID	Problem Description	Workaround
VSP8000-113	EDM display for 40G QSFP DDI Stats shows incorrect values	Use CLI to display values

10. Known Limitations

Please see “Release Notes for VSP Operating System” for software release 5.1.1 (NN47227-401, 09.04) available at http://www.avaya.com/support for details regarding Known Limitations.

The VSP8284XSQ platform may experience a watchdog timeout induced reset when a momentary power loss to the system occurs. In this situation the datapath has been reinitialized even though there is enough power left in the system for the Control Plane to generate a coredump. The reset is needed for the system to be fully functional again. Using a UPS is recommended to mitigate momentary power interruption.

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.

Firefox 38 introduced more stringent crypto cipher requirements. Set Firefox user configuration to enable fallback to RC4. Otherwise use older version of Firefox or other supported browsers.

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 .

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