Hewlett Packard Enterprise

HPE VAN SDN Controller 2.7.16 Release Notes

HPE VAN SDN Controller 2.7.16 Release Notes

This document contains important information on the HPE VAN SDN Controller version 2.7 software.

Part Number: 5200-1984
Published: July 2016
Edition: 1

Acknowledgments

Contents

1 HPE VAN SDN Controller 2.7.16

Description

This document describes the changes to the HPE VAN SDN Controller software for release 2.7.16.

This software supports the HPE VAN SDN Controller version 2.7.16.

Important information

Internationalization (I18N)

The HPE VAN SDN Controller 2.7.16 supports internationalization (I18N).

NOTE: Although the controller supports internationalization, HPE no longer ships Chinese and Japanese language localized resource bundles with the controller. For more information, see the latest version of the *HPE VAN SDN Controller Administrator Guide*.

Security best practices

Observing these rules can help to prevent unauthorized access to the controller:

- Do not enable shell history on the server on which your controller is installed.
- Do not allow users other than `sdn` and `sdnadmin` to have access to your controller system.
- Do not store your authentication token in plain text, such as a non-encrypted cookie.
- Do not use self-signed certificates in a production environment.
- Do not alter contents in the `/opt/sdn/Cassandra and /opt/sdn/Hazelcast` directory.
- Do not delete any chains with the name `hazelcast`, `cassandra-default`, or `cassadra-team`, or any rules with the following ports: 5700, 7000, 7001, 7199, 9160.
- Do not manually override the firewall rules to allow or deny ports 5700, 7000, 7001, 7199, and 9160.

To prevent authentication tokens from being stolen:

- Always log out of the UI and close the web page after you finish using it.
- Never leave browser access to the UI open and unattended.
- Never let someone who does not have access rights to the controller “look over your shoulder” while you access the UI.
- Ensure that Keystone is configured to expire tokens after a short period of time. (A common industry practice is to expire tokens after 20 minutes.)

Supersede information

Supersedes: 2.7.10

Version history

Hewlett Packard Enterprise fully supports all released versions unless noted in the following table:

Version	Release date	Based on	Remarks
2.7.16	2016-07-13	2.7.10	Released, fully supported, and posted on the web.
2.7.10	2016-02-19	2.6.11	Released, fully supported, and posted on the web.

Version	Release date	Based on	Remarks
2.6.11	2016-01-15	2.6.8	Released, fully supported, and posted on the web.
2.6.8	2015-10-16	2.5.20	Released; no longer maintained.
2.5.20	2015-10-02	2.5.15	Released; no longer maintained.
2.5.15	2015-05-20	2.5.14	Released; no longer maintained.
2.5.14	2015-05-08	2.4.5	Released, but *not* posted on the web. Release; no longer maintained.

Products supported

Product number	Description
J9863AAE	HPE VAN SDN Controller Base Software with 50–node License E-LTU
J9864AAE	HPE VAN SDN Controller Additional 50–node License E-LTU
J9865AAE	HPE VAN SDN Controller High Availability License E-LTU

Operating systems

- Ubuntu 14.04 LTS 64-bit Server
- Debian GNU/Linux 8 based HPE Linux

Enhancements

This section lists released builds that include enhancements. Software builds are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

NOTE: The number that is included in the enhancement title is used for tracking purposes.

Version *2.7.16*

No enhancements are included in version 2.7.16.

Version *2.7.10*

- Virtual appliance (OVA):
  - Initial configuration during OVA deployment of hostname, IP address (static or DHCP) netmask, gateway, and DNS.

  (See the *HPE VAN SDN Controller Installation Guide*.)
- The topology viewer has a completely new display with features such as the ability to zoom in and zoom out, expand or collapse clients connected a switch in the topology, and drag (PAN) the topology diagram to a specific place on the screen to locate a node. (See the *HPE VAN SDN Controller Administrator Guide*.)
- Automatic ARP filtering to reduce the number of ARP packets sent to the controller; achieved by automatically configuring rules on switches to forward ARP packets sent from infrastructure ports instead of sending such packets to the controller.
- Client Mapper Service: Combines information known about a network client by the controller, such as host IP address, host MAC addresses, and the connected datapath and port, with information about the network client known by an outside policy manager, such as the Aruba ClearPass policy manager, to provide information about network clients, including user

information, device information, and location information. This information is available via the REST API only. (See the *HPE VAN SDN Controller REST API Reference*.)

- For controllers with the HPE Network Protector SDN Application enabled, the ability to launch the application from the controller UI. (See the *HPE VAN SDN Controller Administrator Guide*.)
- API changes and additions. (See the *HPE VAN SDN Controller REST API Reference*.)
- Enhanced UI to include:
  - URL to the SDN controller UI simplified to **https://*SDN-Controller-Address*:8443**
  - Ability to change the sdn password from the sdn User window in the UI
  - Enhanced Configurations screen with tabs listing configuration components for Basic, Advanced, System and Apps.
  - On the System configuration screen, added the ability to do post install configuration of NTP, networking configuration for DHCP or static IP address, and logging levels.

  (See the *HPE VAN SDN Controller Administrator Guide*.)
- Device support for the new Aruba 3810 Switch Series. (See the *HPE VAN SDN Controller and Applications Support Matrix*.)

Fixes

This section lists released builds that include fixes. Software builds are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

NOTE: The number that is included in the fix title is used for tracking purposes.

Version 2.7.16

Controller UI

CR_0000198869 Symptom/Scenario: After logging in to the SDN Controller UI, when the user clicks [user icon] sdn link (from the top-right corner) and clicks **Links: SDN Community** from the user dropdown menu, the link redirects the user to Aruba networks community site instead of HPE community site.

CR_0000199481 Symptom/Scenario: If the user navigates to **Configurations** → **System** → **Network** → **Modify** page and adds the following values,

Type: Static

IP Address: `15.255.126.61abc`

Gateway: `15.255.128.1def`

then a dialog box is displayed with the following error message:

`Error: Invalid IP Address: 15.255.126.61abc`

`Error: Invalid Gateway Address: 15.255.128.1def`

Workaround: This is just an error message format. It does not impact any functionalities.

Jasper Reports

CR_0000200139 Symptom: When rendering reports via GUI, the new installations of Network Protector (JL004AAE) or Network Optimizer (J9985AAE) might encounter `Error 500`.

Scenario: The error and steps to trigger vary slightly depending on whether the Network Protector or Network Optimizer application is used.

The **Network Protector** application might encounter an error when rendering report information in its GUI environment. This error can be seen in two locations:

- Administration > License Compliance
- Reports > System

The error is displayed as a popup dialog box with the following message:

```
Internal Server Error 500. Please contact the site administrator.
```

The **Network Optimizer** application might encounter an error when rendering report information on the **Reports** tab of its GUI environment. The error is displayed while attempting to generate any of the four reports offered under:

- Network Optimizer > Reports

After the desired report is selected, the query parameters are defined, and the **Generate Report and Download** button is selected.

A dialog box might open with the following error message:

```
HTTP Status 500 – java.lang.ExceptionInInitializationError.
```

For more information, see the customer advisory at **http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05085440**.

SSL

CR_0000200712 Symptom/Scenario: Several potential vulnerabilities have been identified in the OpenFlow Virtual Appliance (OVA) version of the HPE VAN SDN Controller using OpenSSL. These vulnerabilities could be exploited remotely to allow Denial of Service (DoS), unauthorized disclosure of information, and unauthorized modification of information.

Workaround: HPE has provided the following instructions to update the version of OpenSSL in the controller, which reduces the risk of these vulnerabilities:

- If a proxy is configured to access the Internet:
  - Edit the "`apt.conf`" file found in the `/etc/apt` directory.
  - Add the http proxy setting by adding a line similar to the following:

    ```
    Acquire::http::Proxy "http://proxy-ip:proxy-port/";
    ```

- Create and Edit the `sources.list` file in the `/etc/apt` directory:
  - Add the line: `deb http://security.debian.org/ Jessie/updates main contrib non-free`
- Run updates for apt-get indexes:
  - `sudo apt-get update`
- Run `apt-get upgrade` command to upgrade OpenSSL version:
  - `sudo apt-get upgrade openssl`
- Remove the "`sources.list`" file from `/etc/apt` directory.

- If a proxy is configured in the first step:
  - Edit the "`apt.conf`" file found in the `/etc/apt` directory.
  - Remove the http proxy setting by removing the line added in step 1:
    `Acquire::http::Proxy "http://proxy-ip:proxy-port/";`
- Reboot the system to use the newer version of OpenSSL.

Version 2.7.10

Controller Access

CR_0000182850 Symptom: The customer is not able to access the controller after rebooting the system.

Scenario: When the customer creates a team and reboots the controller on version 2.5 along with the Cassandra version 1.2.4, he is not able to access the controller after rebooting the system.

Workaround: Update the version of Cassandra on the customer side from 1.2.4 to 1.2.19.

Controller Reboot

CR_0000186648 Symptom: If there are more than 10000 interfaces present in the database used to store the interfaces by the controller, the controller restarts.

Scenario: When there are more than 10000 interfaces present in the database during the load time in the controller, the controller restarts. This difference is caused by a 30-second timeout in the controller when reading the contents of the database. With a large number of interfaces present in the database, the timeout expires before the data can be returned.

Workaround: Manually delete all device entries from the controller's database, using the following SQL commands as the 'sdn' user:

```
> psql sdndb
sdndb=> delete * from interface;
sdndb=> \q
```

then restart the controller service with "`sudo service sdnc restart`". Devices will be re-learned by the controller when they reconnect after the restart.

Controller Support Log

CR_0000168028 Symptom: The controller support log exceeds its configured maximum size and potentially consumes all available disk space on the system on which the controller is installed. The log contains multiple instances of the following message:

`Unable to accept incoming connection: java.io.IOException: Too many open files.`

Scenario: The system on which the controller is installed has run out of file descriptors, either because it controls too many devices, links, or hosts, or some other process on the system has consumed a large number of file descriptors.

Workaround: Ensure that the system on which the controller is installed conforms to the recommended hardware requirements for the number of devices, links, and hosts. For hardware recommendations, see the support matrix. Take one or more of following actions:

- Form a controller team and distributing ownership of the switches in the network across the team members such that each controller in the team controls one third of the switches in the network.
- Increase the system resources, such as the file descriptors, on the system on which the controller is installed.
- Install the controller on a larger system, such as one that conforms to the hardware recommendations appropriate to the size of the network deployment.

Controller UI

CR_0000192190 Symptom: The customer sees multiple established TCP connections between the same datapath and the controller.

Scenario: When a fault is observed in the switch that causes the switch to reconnect continuously to the connector, multiple established TCP connections are observed between the same datapath and the controller.

DHCP

CR_0000186609 Symptom: If malformed DHCP packets exist on the data-plane networks being controlled by the SDN controller, the SDN controller logs a detailed message for each malformed DHCP packet that it observes. Since the controller receives copies of DHCP packets from all switches, this may result in a significant rate of logging that consumes an inappropriate percentage of the system logs. Since the log size is bound, this does not consume more than the capped storage space for the logs, however it negatively impacts the usefulness of the logs for identifying and solving other issues in the network.

Scenario: This problem can be in the 2.6 and prior releases by having malformed DHCP packets in the data-plane of the network controlled by the controller.

OpenFlow

CR_0000175131 Symptom: After rebooting the switch with software release 15.17 or later, the connection between the teamed controller and the switch is lost.

Scenario: When updating a 5400R or 3800 switch in a teamed controller environment by rebooting the switch from flash memory using software release 15.17 or later for the first time, the controller team loses connectivity with the switch. (This does not occur where a single node controller is in use.)

Workaround: Disable and then re-enable OpenFlow on the affected switch.

RSDoc

CR_0000169890 Symptom: After creating a team, accessing the team IP address RSDoc page, if certain embedded RESTful API with GET methods are used, the following error message is displayed:

```
Unable to parse JSON
```

Scenario: Create a team, access the RSDoc page using the northbound IP address. Using certain embedded RESTful API with GET methods, an `unable to parse JSON` error message displays.

Workaround: Use the member controller IP address for RSDoc (leader controller IP address cannot guarantee to work).

Issues and workarounds

App Access

CR_0000182811 Symptom: The customer is not able to access the Network Protector UI.

Scenario: When the customer disables the Network Visualizer app, he is not able to access the Network Protector UI.

Workaround: The user needs to login to the Network Protector UI again and check if Network Visualizer has been disabled. If so, re-enable Network Visualizer.

Application Manager

CR_0000169043 Symptom: If an application fails to start, the Application Manager does not disable it when the controller is restarted.

Scenario: When an application is installed for the first time and if it fails to start, the application management framework moves it to a disabled stage. However, if an application, which is supposed to be running, fails to restart as part of a controller restart, the application management framework leaves it in the Active state even though it is not running.

Workaround: If the application runs into that state, just disable and then re-enable the application manually.

Controller UI

CR_0000184096 Symptom: The customer is not able to access the controller UI.

Scenario: When the customer throttles 140 requests/sec along with 40k users, he is not able to access the controller UI.

Workaround: When the controller is unavailable, the customer needs to reboot the controller to continue the operation.

IP Communication

CR_0000170393 Symptom: REST calls throughput is less while using Northbound IP than while using the switch's Master Controller IP.

Scenario: In a HA/teaming setup, when the user makes REST calls through the Northbound IP, the Northbound IP might affect its performance.

Workaround: It is preferable to use the Master Controller's IP whenever possible as the Northbound IP might affect the performance.

LLDP

CR_0000176812 Symptom: Controller link-discovery packets (LLDP and BDDP) are forwarded to the SI copy tunnel interface.

Scenario: LLDP and BDDP packets are forwarded to the SI copy tunnel interface when they shouldn't be. These packets will be injected into the SI copy tunnel interface by the controller at the rate specified in the OpenFlow Link Discovery configuration.

Workaround: Change the "enable.tunnel_discovery" setting in OpenflowLinkDiscoveryComponent to 'false'. Once this setting is changed, the link discovery packets are not sent to the tunnel ports for HPE Aruba switches. This resolution does not apply to other product lines or manufacturers.

OpenFlow

CR_0000210505 When the VAN controller re-establishes a connection with an OpenFlow switch, there will be a small duration of packet loss on the data-plane VLANs. The packet loss duration should not last longer than 1 second.

The VAN controller will re-establish a connection with an OpenFlow switch due to any of the following events:

- The VAN controller is rebooted.
- The VAN controller process (sdnc) is restarted.
- The switch is rebooted.
- The switch OpenFlow state is changed (global or per-instance).
- The network connection (control-plane) between the switch and the controller experiences an outage.

Teaming

CR_0000176684 Symptom: Alerts generated on a controller won't be seen on IMC when the controller is in a team.

Scenario: After creating a team of controllers and discovering them in IMC using the team IP address, alerts generated by any of the teamed controller are not displayed in IMC. However, the alerts are displayed on the controller.

CR_0000180777 Symptom/Scenario: When the customer tries to backup and restore a 3-node team, the restoration fails on all the three nodes.

Workaround: The backup-restore should be run sequentially and not parallely across the 3 nodes.

Web UI

CR_0000193130 Symptom: Log level in the Web UI does not display the expected value.

Scenario: When changing the log level via RSDOC, the expected value may not be displayed in the Web UI.

Workaround: Do not change the log level via RSDOC.

Deprecated, obsolete, or changed features

New and changed information for the HPE VAN SDN Controller 2.7 REST API

The following table contains a list of resources that were added, changed, or removed from the HPE VAN SDN Controller 2.7 REST API.

REST API Resource	Method	Change	Description
/of/classes	GET	Added to documentation	Gets the set of currently-registered OpenFlow classes.
/of/classes/{id}	GET, PUT, DELETE	Added to documentation	Lists, adds, or deletes the OpenFlow class that has the specified id.
/of/sequencer	GET	Added	Lists information about the packet listeners that are registered on the controller.
/net/nodes	GET	Changed syntax	You can get the end node detail for a given IP address without being required to also provide the VLAN ID.

REST API Resource	Method	Change	Description
/cms/client/events	GET	Added	Gets events posted to the controller by the external policy managers, such as the Aruba ClearPass Policy Manager.
/cms/client/event	POST	Added	Used by an external policy manager, such as Aruba ClearPass, to add information about network client events to the controller.

Java API changes for HPE VAN SDN Controller 2.7.16

No changes were made to the Java API for HPE VAN SDN Controller 2.7.16. However, Hewlett Packard Enterprise recommends that Java applications compiled with earlier versions of the JDK be recompiled using OpenJDK version 8.

Upgrade information

Upgrading restrictions and guidelines

See the *HPE VAN SDN Controller Installation Guide*.

Contacting Hewlett Packard Enterprise

For additional information or assistance, contact Hewlett Packard Enterprise Networking Support:

http://www.hpe.com/networking/support

Before contacting Hewlett Packard Enterprise, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Hewlett Packard Enterprise security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

To find security bulletins:

1. Go to the Hewlett Packard Enterprise Support Center website at **http://www.hpe.com/support/hpesc**.
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email, sign up at:

https://h41360.www4.hpe.com/signup_alerts.php?jumpid=hpsc_secbulletins

Related information

Documents

To find related documents, see the Hewlett Packard Enterprise Support Center website:

http://www.hpe.com/support/manuals

Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.

Related documents

The following documents provide related information:

- *HPE VAN SDN Controller and Applications Support Matrix*
- *HPE VAN SDN Controller 2.7 Installation Guide*
- *HPE VAN SDN Controller 2.7 Administrator Guide*
- *HPE VAN SDN Controller 2.7 Programming Guide*
- *HPE VAN SDN Controller 2.7 REST API Reference*
- *HPE VAN SDN Controller 2.7 Troubleshooting Guide*
- *HPE VAN SDN Controller 2.7 Open Source and Third-Party Software License Agreements*

Websites

Website	Link
SDN websites	
Hewlett Packard Enterprise Information Library for SDN	**www.hpe.com/info/sdn/infolib**
Hewlett Packard Enterprise Software-Defined Networking website	**www.hpe.com/info/sdn**
Hewlett Packard Enterprise SDN community discussion forum	**www.hpe.com/networking/sdnforum**
Hewlett Packard Enterprise SDN App Store	**www.hpe.com/networking/sdnappstore**
Hewlett Packard Enterprise SDN Dev Center website	**www.sdndevcenter.hp.com**
Hewlett Packard Enterprise Open Source download website	**www.hpe.com/software/opensource**
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	**www.hpe.com/networking/resourcefinder**
Hewlett Packard Enterprise Networking website	**www.hpe.com/info/networking**
Hewlett Packard Enterprise My Networking website	**www.hpe.com/networking/support**
Hewlett Packard Enterprise My Networking Portal	**www.hpe.com/networking/mynetworking**
Hewlett Packard Enterprise Networking Warranty	**www.hpe.com/networking/warranty**
General websites	
Hewlett Packard Enterprise Information Library	**www.hpe.com/info/enterprise/docs**
Hewlett Packard Enterprise Support Center	**www.hpe.com/support/hpesc**
Hewlett Packard Enterprise Support Services Central	**www.ssc.hpe.com/portal/site/ssc/**

Website	Link
Contact Hewlett Packard Enterprise Worldwide	**www.hpe.com/assistance**
Subscription Service/Support Alerts	**www.hpe.com/support/e-updates**
Software Depot	**www.hpe.com/support/softwaredepot**
Customer Self Repair (not applicable to all devices)	**www.hpe.com/support/selfrepair**
Insight Remote Support (not applicable to all devices)	**www.hpe.com/info/insightremotesupport/docs**

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.