HP VAN SDN Controller 2.5.20 Release Notes

Abstract

This document contains important information on the HP VAN SDN Controller version 2.5 software.

HP Part Number: 5998-8736
Published: October 2015
Edition: 1

Acknowledgments

Warranty

For the software end user license agreement and the hardware limited warranty information for HP Networking products, visit http://www.hp.com/networking/support.

Open Source Software

For information on licenses for the open source software used by the HP VAN SDN Controller, see the *HP VAN SDN Controller Open Source and Third-Party Software License Agreements*.

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by HP. For information about acquiring the open source code for the HP VAN SDN Controller, send an email to **HPN-Open-Source-Query@lists.hp.com**, listing the product name and version information for which the source code is being requested. Because such information can become outdated quickly, HP does not publish mailing addresses and telephone numbers for open source queries. Available source code distribution methods include network transmission of the source code and sending the source code on physical media to a mailing address. Physical media distribution might require a fee to cover the media and mailing costs. .

NOTE: The HP VAN SDN Controller includes both proprietary software that is closed source in addition to the open source software listed in the *HP VAN SDN Controller Open Source and Third-Party Software License Agreements*. In response to queries to HP for source code on the HP VAN SDN Controller, HP distributes the source code for open source software only. HP does not distribute source code for closed source software.

Contents

1 HP VAN SDN Controller 2.5.20 Release Notes

Description

This document describes the changes to the controller software for releases 2.5.20, 2.5.15, and 2.5.14.

This software supports the HP VAN SDN Controller version 2.5.20.

Important information

Controller upgrades

To upgrade the controller from release 2.5.14 or 2.5.15 to release 2.5.20, see edition 2 or greater of the *HP VAN SDN Controller 2.5 Installation Guide*.

To upgrade the controller from release 2.4 to release 2.5.20, see edition 2 or greater of the *HP VAN SDN Controller 2.5 Installation Guide*.

To upgrade the controller from release 2.3 or earlier to release 2.5.20, do either one of the following:

- Upgrade the controller through each successive release. See the installation guide for each successive release, or
- Uninstall the current release, then perform a new 2.5.20 controller installation using the procedures described in the *HP VAN SDN Controller 2.5 Installation Guide*. (See the chapter titled "Uninstalling the controller and the Keystone server" in the *HP VAN SDN Controller Installation Guide*.)

NOTE: Uninstalling either an application or the controller erases any related licenses. Before you uninstall an application or the controller, you must first properly uninstall the related licenses so that they can be re-used in a new installation. See the chapter titled "License Registration and Activation" in the latest edition of the *HP 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 your controller.
- Do not allow other users besides 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 under /opt/sdn/Cassandra and /opt/sdn/Hazelcast.
- 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.
- 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.
- Make sure 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: 2.5.15

Version history

HP fully supports all released versions unless noted in the following table:

Version	Based on	Release date	Remarks
2.5.20	2.5.15	2015–10–02	Released, fully supported, and posted on the web.
2.5.15	2.5.14	2015–05–20	Released, fully supported, and posted on the web.
2.5.14	2.4.5	2015–05–08	Released, fully supported, but *not* posted on the web.
2.4.5	2.4.3	2014–11–19	Released, fully supported, and posted on the web.
2.4.3	2.3	2014–11–07	Released, fully supported, and posted on the web.
2.3	2.2.5	2014–07–30	Released, fully supported, and posted on the web.
2.2.5	2.0.	2014–03–31	Released, fully supported, and posted on the web.
2.0.0.4253	—	2013–11–08	Released, fully supported, and posted on the web.

Products supported

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

Operating systems

- Ubuntu 12.04 LTS 64–bit Server

Compatibility/interoperability

For compatibility and interoperability information, see the latest *HP VAN SDN Controller and Applications Support Matrix*.

Enhancements

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

Version 2.5.20

Localized support added for Chinese and Japanese

The SDN Controller web interface is localized to enable controller use in English, Chinese, or Japanese language. See the latest version of the *HP VAN SDN Controller Administrator Guide* for information on selecting a localized view.

NOTE: Applications running on the controller might not support localization.

Upgrade to Cassandra 1.2.19

The Cassandra upgrade adds these benefits:

- Improved consistency of availability for the Cassandra Persistence Service for applications
- Better consistency in team formation
- Better performance in Cassandra compaction
- More effective repair scripts

Version 2.5.15

No enhancements in this release.

Version 2.5.14 (not posted on the web)

High availability infrastructure changes

Introduces the startup and shutdown sequencer framework. The new sequencer framework facilitates the movement of the SDN Controller in an ordered manner through a defined set of stages when the controller service starts up or is suspended. Includes changes to the controller SystemStatus and the role and region services. Adds a new peer monitoring service, and requires all team members to be active to accommodate user-driven changes. For more information, see the *HP VAN SDN Controller Programming Guide*.

Virgo console access disabled by default

To access the Virgo Admin WEB UI (web interface), copy the `org.eclipse.virgo.management.console_3.6.2.RELEASE.jar` file from the `/opt/sdn/admin`directory to the `/opt/sdn/virgo/`pickup directory.

NOTE: File ownership must belong to the “sdn” user. This means that the administrator must either use the sdn user on the controller to copy the file, or ensure that the file ownership is changed to the sdn user once the file is moved.

Controller web interface changes

- Adds a new Team screen to the web interface. The details pane of the read-only Team screen summarizes teaming and region information in team configuration and status, region configuration, and device/datapath information with region and current owner information.
- Also includes changed defaults for device labels in the OpenFlow topology screen, where the OpenFlow Topology screen defaults to displaying devices labeled with their IP Address:OpenFlow VLAN ID. The user can switch from displaying IP:VLAN ID to DPID using the “N” option as detailed in the “?” button of the Topology Screen.

For more information, see the *HP VAN SDN Controller Administrator Guide*.

Topology Viewer classes deleted

The private topology viewer classes have been removed from the topology viewer package (com.hp.sdn.tvue). See "Deleted Java API classes" under "New, changed, deprecated, and deleted APIs" (page 10).

Cassandra start and connection retry behavior changes

- Cassandra server start behavior changed. In previous versions of the controller, Cassandra Server was started by the 'sdn' user from within the OSGI container, which resulted in the Cassandra Server shutting down when the OSGI container was shut down and users of Cassandra Data Store Service being unable to write to the database as applications were being unloaded from the controller during shutdown. Beginning with HP VAN SDN Controller 2.5, the Cassandra Server is started by the 'sdnadmin' user from within the sdn admin service (sdna). The Cassandra Data Store service remains available for application access while the OSGI container is shutting down.
- New retry behavior for lost connections to the Cassandra database. In previous versions of the controller, when a connection problem between the controller and the Cassandra database was detected, the Cassandra Data Store service was unregistered from OSGi, causing all components with a mandatory dependency on it to be deactivated. When the connection was re-established, the Data Store Service was registered back to OSGi. Beginning with HP VAN SDN Controller 2.5, if a connection problem between the controller and the Cassandra database is detected, the Cassandra Data Store Service is not unregistered from OSGi, so components remain active. If a query is executed and the connection fails, the Cassandra Data Store Service makes several attempts to reconnect and then retry the query. If the Data Store Service is not able to reconnect after a few retries, the query execution throws a PersistenceException. The next time a query is executed with no connection to Cassandra, the Cassandra Data Store service repeats the process of trying to reconnect before executing the query.

New application health monitoring capability

The sdna service, installed as part of the controller package, has a new capability for monitoring the health of applications.

The HealthManager utility registers for alerts of topic HealthMonitor, receives the alerts posted by situations in the following list, and automatically takes the action specified in a configuration file. Includes these two situations:

- Unresponsive or stopped application
- Active application reports critical alert

With the configuration file, the administrator can configure the action taken for specific combinations of applications and alerts by including entries such as the following in the /etc/sdn/autoShutdown.properties configuration file:

HealthMonitorID+Alert=Action

Where:

- HealthMonitorID – Specified in an alert description as a unique identifier for the application to be affected. Example: com.hp.sdn.adm.system.impl.QuorumRegistar
- Alert – Health code. Can be either "Critical" or "Hung". Hung corresponds to the state of "Not Responding".
- Action - Action to take. Can be either "shutdown" or "restart". The action is taken on the controller and not on the application.

Simplified method for configuring file signing verification on the controller

The controller enforces signing validation for all application zip and and jar files by default. For an experimental or development environment, you can configure the controller to turn off this validation requirement. Beginning with HP VAN SDN Controller 2.5, the verifyZips key of the `com.hp.sdn.adm.mgr.impl.AppManager` configurable component has been removed, and you configure both zip and jar file signing verification using a single option in the `/opt/sdn/virgo/bin/dmk.sh` script. For more information about this feature, see the *HP VAN SDN Controller Administrator Guide*.

Link discovery workaround

A feature was added as a workaround to ensure links can be properly discovered in certain specific device topologies and configurations. The *HP VAN SDN Controller Administrator Guide* provides information about when to use this workaround. To support this workaround, the following two new methods have been added in the DeviceService interface:

```
/**
     * Assign a user provided linkDiscoveryVlan to the device.
     *
     * @param deviceId to set linkDiscoveryVlan for
     * @param linkDiscoveryVlan user provided linkDiscoveryVlan
     * @throws com.hp.api.NotFoundException if device not found
     */
   void setLinkDiscoveryVlan(DeviceId deviceId, VlanId linkDiscoveryVlan);

   /**
    * Get the user provided linkDiscoveryVlan from the device.
    *
    * @param deviceId to set linkDiscoveryVlan for
    * @return linkDiscoveryVlan stored for the device
    * @throws com.hp.api.NotFoundException if device not found
    */
  VlanId getLinkDiscoveryVlan(DeviceId deviceId);
```

Corresponding to these device Java API changes, new REST APIs are available to configure and query the linkDiscoveryVlan property on a device:

- `/net/devices/{uid}/linkDiscoveryVlan`
- `/net/devices/{uid}/linkDiscoveryVlan/{linkDiscoveryVlan}`

Installation process verifies that minimum hardware requirements are met

To qualify for support, the system on which you install the controller must meet the minimum requirements described in the *HP VAN SDN Controller and Applications Support Matrix*.

Beginning with HP VAN SDN Controller 2.5, the installation process checks the system hardware and stops the installation if the system does not meet the minimum requirements for the following hardware:

- Number of processor cores
- Amount for RAM, both used and available
- Amount of available disk storage on all the disks the controller is to use

You can override this check for a development or test environment by following the instructions in the *HP VAN SDN Controller Installation Guide,* but some controller features might not work correctly in environments that do not meet the minimum requirements. HP recommends that you do not override this check for controllers in production environments.

Security improvements include support for TLS instead of SSLv3

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are security protocols used to secure transmissions between web servers and web browsers.

Previous versions of the HP VAN SDN Controller included support for both SSL version 3.0 and TLS. As part of security improvements made for HP VAN SDN Controller 2.5, support for SSLv3 has been removed.

If you use SSL to secure communications with previous versions of the controller, you must ensure that any tools you use for these communications are configured to use TLS for securing communications with HP VAN SDN Controller 2.5 and later versions of the controller.

Getting an authorization token requires that the domain name be specified

Rudimentary role-based access control (RBAC) has been implemented to enable single sign-on capability.

The controller supports a single configurable role, which defaults to the following value: `sdn-admin`.

A user must have this role configured on the Keystone server for the domain (tenant) to which the user belongs. The domain name and role configured for a user on the controller must match the domain name and role configured for that user in Keystone.

Beginning with HP VAN SDN Controller 2.5, authentication requests must include the domain name that corresponds to the user in addition to the user name and password. If you do not specify a domain name, the token that is returned by this request is not valid for use with authenticated APIs.

For more information, see the *HP VAN SDN Controller Administrator Guide*.

The controller is now held in an initialized state while a Restore operation is running

When restoring the controller from a backup, it is necessary to re-install the controller. During a user-initiated Restore operation, the controller web interface is not accessible, and the controller is not fully functional until the restore is complete. For more information on Backup and Restore operation, see the *HP VAN SDN Controller Administrator Guide*.

New, changed, deprecated, and deleted APIs

Controller release 2.5 includes the following API changes:

- New Java API methods: A feature was added as a workaround to ensure links can be properly discovered in certain specific device topologies/configurations. For details on when this workaround should be configured, see the *HP VAN SDN Controller Administrator Guide*. To configure the workaround, the following two new methods have been added in the DeviceService interface:
  - setLinkDiscoveryVlan
  - getLinkDiscoveryVlan

  There is also a new DeviceOwnerService and a new DeviceOwnerEvent that applications can use to react to OpenFlow master/slave role changes:
  - The new events are OWNERSHIP_ACQUIRED and OWNERSHIP_LOST
  - The new events are available for standalone as well as teamed controllers. In most cases, you can use the same code to handle these events for standalone and for teamed controllers.
- Deleted Java API classes affecting the following packages:
  - `com.hp.sdn.adm.region`and `com.hp.sdn.adm.role`
  - topology viewer (`com.hp.sdn.tvue`)
  - DAO (`com.hp.sdn.adm.dao`)

    - region management (`com.hp.sdn.adm.region`)
    - role management (`com.hp.sdn.adm.role`)
- New REST API resources: A new Owners resource supports more features relative to the deprecated Regions resource, including:
    - Better validation of regions
    - The use of device IP ranges
    - The ability to dynamically add and remove a device from a region
    - The ability to dynamically add and remove a region.
- Changed REST API resources:
    - The domain key-value pair in the request body is now required. If you do not specify a domain name, the token that is returned in the response is not valid for use with authenticated APIs.
    - The JSON schema for the keys resource has changed to support SNMPv3 keys
- Deprecated REST API resources: `/sdn/v2.0/regions` (In addition, because the device owner service introduced in HP VAN SDN Controller 2.5 automatically refreshes device ownership information, the `/sdn/v2.0/regions/{region_uid}/refresh`resource does not execute any operations.
- The ability to dynamically add and remove a device from a region
- The ability to dynamically add and remove a region.

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 2.5.20

The HpwsInstallManager services failed to load if CA signed certificates are implemented on the controller (CR_172346)

In environments having CA signed certificates in place for the `/opt/sdn/admin/keystore` and `truststore` files, the `HpwsInstallManager` used with the AppStore fails to load. This was due to the properties file for the service located in `/opt/sdn/virgo/repository/usr/com.hp.sdn.adm.mgr.impl.hpws.HpwsInstallManager.properties` not inheriting the default password; instead it was empty. Resolution required that the service have the ability to inherit the default password as used in other containers such as ServiceRest and AdminRest in order to support use of CA signed certificates over self-signed certificates.

Version 2.5.15

Controller would not start because it could not load CA certificates signed by third-parties (CR_172119)

A defect was introduced in 2.5.14 (not posted on the web) where the controller was unable to load CA signed certificates and start if the certificates were signed by a third-party certificate

authority. Controller version 2.5.15 resolves this issue and the controller can now load certificates and start when the certificates have been signed by a third-party certificate authority.

Version 2.5.14 (not posted on the web)

A host was unable to ping some other hosts on the network when multiple VLANs were used in OpenFlow—Only mode (CR_148179)

When multiple VLANs were used with a controller configured for hybrid.mode=false, a host might not be able to ping some other hosts on the network.

OpenFlow-Only traffic between two hosts in a partially-controlled network was not forwarded at line-rate (CR_148385)

You can now resolve this issue by upgrading your ProVision OpenFlow switches to release 15.16 or greater.

The controller is responsible for the forwarding decision of every packet that enters a ProVision OpenFlow switch it controls. When the controller observes a packet for any given flow, it attempts to pave the path through the network through the OpenFlow forwarding rules for that flow, so that all future packets of the same flow are handled by the switch according to the forwarding rule. In cases where two controlled switches are separated by a multi-hop link, the controller did not pave the path across that multi-hop link because it paved only a single path and the controller could not be guaranteed that multiple paths did not exist if multiple multi-hop links existed.

As a result, the controller did not pave any paths across a multi-hop link. The controller made the forwarding decision for every packet which needed to cross the multi-hop link. If a single packet needed to cross a number of multi-hop links, then the controller would be consulted those many times for the same packet. The actual throughput rate depended on the load of other processing on the controller and the number of hops that such flows took through the controlled network.

A team misconfiguration or change in NB_IP location could cause a loss of communication due to ARP caches not being updated (CR_152738)

Depending on your network configuration and ARP cache timeout, you might lose connectivity to the team IP address if it is moved from one controller to the other. This team IP address is created as an alias on one of the controllers in a team for convenience, and when it is deleted and re-created on a new controller, the ARP caches can take a while to timeout and find the new location. As of controller software release 2.5, a gratuitous ARP is sent when the leader IP is configured to force an ARP cache update. For more information, see the *HP VAN SDN Controller Administrator Guide*.

Get /systems from a blocked member returned “500” error instead of “503” error (CR_152822)

With this fix, the blocked node has a status of “Active” while other nodes are “unreachable”. On the non-blocked nodes, the blocked node shows a status of “unreachable”, while all other nodes are “active”.

Checking flows from the controller web interface in some instances produced a “500” internal server error (CR_153065)

In some situations where an OpenFlow switch became overloaded, attempts to list the current flow from the device failed, resulting in the controller web interface displaying **500: Internal Server error**. Instead, the error should display a more appropriate “Device timeout” error message in the controller web interface.

Intermittent data loss when connectivity to a team node was lost (CR_153341)

There was an intermittent issue where the team lost data when connectivity to one of the nodes in the team was lost. This could result in loss of the team leader, as well as a loss of information for links, nodes, or devices. This is now fixed.

Hazelcast removed nodes from a cluster after the master node wais partitioned and then brought back into the cluster (CR_156150)

Nodes are no longer removed when the old master rejoins the cluster.

Stopping SDN services on lead controller in a team caused teaming to fail (CR_157913)

If the team leader IP address is assigned to a different member of the team, sometimes connectivity was temporarily lost due to stale entries in various ARP caches. The frequency of this failure varieed across environments due to the ARP cache timeouts being different. Now, a gratuitous ARP is sent from the system with the new leader IP address to force an update of the ARP caches.

Firewall rules were not updated correctly (CR_158475)

When the OS was rebooted, the default drop rule used to secure the team message bus could be removed. The default drop rule should be re-applied on every restart. This is now fixed.

The Cassandra system.log was not included in captures of the support logs (CR_159054)

The controller collected only the log files under /var/log/sdn/virgo/ for support logs. All log files are now collected under /var/log/sdn/.

With Network Protector running, Cassandra sometimes became disconnected and did not come up (CR_159221)

The workaround was to stop Network Protector before stopping the controller. However this issue is now fixed.

Switches disappeared from the OpenFlow Topology view (CR_159499)

With switches connected to the controller and visible in the Topology view, clicking on the controller **Reload** button sometimes resulted in one or more switches disappearing from the browser Topology view during the reload. The workaround was to refresh the browser.

The controller failed to parse a REST response in a team environment (CR_159664)

An unexpected character ('<' (code 60) was observed while deleting the team. This is now fixed.

Unable to change the default password for the Cassandra keystore and truststore.(CR_159776)

You can now change the default password for the keystore and truststore used by Cassandra. See the section titled "Creating the Cassandra keystore and truststore" in the "Security Features" chapter in the *HP VAN SDN Controller Administrator Guide*.

End-hosts were discovered on VLAN 0 on ProVision switches in virtualized mode with OpenFlow 1.0 instances (CR_160767)

When hosts were discovered through a ProVision switch in virtualized mode (that is, one OpenFlow instance per VLAN), when that instance was using OpenFlow 1.0, the discovered hosts were not learned on the correct VLAN. In this case, they were learned on VLAN 0 because the only information about the VLAN was contained in the datapath ID. Now, the correct VLAN is discovered.

Teaming subsystem should not run if Iptable Rule programming for Hazelcast fails (CR_161066)

If the iptable rule programming for the teaming framework (Hazelcast) fails, the teaming framework will not come up. In previous releases, the service would come up regardless of the iptable rule programming.

The cassandra server does not start if the iptable rules fail (CR_161067)

In previous releases, the Cassandra server would come up regardless of the iptable rule programming. This change in functionality prevents the Cassandra server from coming up if the iptable rule programming for cassandra fails.

The sdna service was reading stdin, stealing input from the OS, and restarting when run from the console (CR_161380)

The Admin service was updated to no longer read stdin.

The ARPing package caused installation failures and loss of the network configuration (CR_161462)

Replaced ARPing with iputils-arping.

The Cassandra server was stopped with SDNC stopped (CR_161493)

The implemented a start/stop/restart of the Cassandra server from the SDN Admin instead of the SDN user. The controller start and stop do not have any effect on Cassandra, and Cassandra remains available even if sdnc is stopped.

The controller threw unsupported flow exceptions for a flow supported in table 200. (CR_161512)

Relates only to ProVision switches. When creating a flow mod that sets a particular field in the packet, customers were formerly limited to only those fields that are settable on ProVision switches running software release 15.15. With this fix, you can set any fields that the switch itself reports in the OpenFlow handshake.

The Cassandra server didn't start if the controller was rebooted soon after a team was created (CR_162770)

A quick restart of sdnc immediately after creating a team caused the Cassandra server to not start. Rebooting did not recover from this condition. This is now fixed.

No notification to the Admin that nodetool repair has not been run (CR_162860)

Cassandra recommends running nodetool repair once every ten days. The controller now generates an alert to remind the Admin to run nodetool repair if it has not been run in the last ten days.

Preventing an invalid IP address to be set in the controller (CR_163284)

When an invalid IP Address was set to the controller via REST API at systems/{system_uid}, the operation failed with an exception. However the invalid IP Address was set to the controller and it was only cleared after restarting the controller. This issue was fixed and now the IP Address is not set unless it is valid.

OpenFlow match on IPv6 flow label appeared not to be supported even though the switch indicated it is supported (CR_163381)

For ProVision switches running software release 15.15.0005, the HP VAN SDN Controller was unable to install an IPv6 flow based on the IPV6_FLABEL field. The switches reported the flow was not supported in the protocol response, while indicating in the output of `show openflow instance vlan2 flow-table 200 table-capability` that the flow is supported. This was the result of an ambiguity in the Openflow specification regarding the length of the IPv6_FLABEL and MPLS_LABEL fields, stating that they could be either three or four bytes. The HP VAN SDN Controller chose to create the field as three bytes, but the ProVision switches parse it as four bytes. Thus, the switches rejected flows from the controller that included either of these fields. The OpenFlow specification has since been clarified to state that this field should be four bytes long. The controller has been updated to now send out these fields as four bytes, resulting in the switches being able to accept the flows.

Apps were unable to push flow_mods with empty instructions (CR_164458)

This occurred on all ProVision and H3C 5500HI devices because the device driver framework was rejecting such flows. The issue was seen with OpenFlow 1.3. Flow mods with empty instructions in OpenFlow 1.3 are now successfully installed on the switches.

For an 8GB Ram VM, a backup could fail if the data volume was greater than approximately 130MB and, for a 16GB RAM VM, if the data was greater than approximately 200MB (CR_165514)

For large Cassandra databases , the backup could fail due to the lock of the database not waiting long enough. There is a configurable cassandra lock timer, `backupLockSeconds`. This configuration must be set based on the size of the data being backed up. The default value is 10 minutes. The applications that sort data in Cassandra have up to this timer value in case they encounter the lock timeout error during backup. (The specific error is - "Cassandra lock timed out before backup was finished.") The Cassandra `backupLockSeconds` timer setting is in the `com.hp.sdn.teaming.impl.CassandraProcessManager` component of the **General/Configuration** screen. See the latest version of the *HP VAN SDN Controller Administrator Guide* for more information on how to change the lock timeout.

Controller access failed using Google Chrome browser version 41.0.2272.118 or Firefox browser version 37.0.1 (CR_168809)

Using Chrome windows version 41.0.2272.118 or Firefox windows version 37.0.1 generated one of the following messages when trying to access the controller web interface:

```
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
```

or

```
Error code: ssl_error_no_cypher_overlap
```

The mismatch was due to the controller attempting to generate self-signed certificates using the DSS cipher, which is not supported in Chrome and Foxfire versions cited above. This problem is resolved in release 2.5 by changing the controller's certificate self-signing cipher from DSS to RSA.

NOTE: If you did not experience this error when using the above cited versions of Chrome or Firefox with controller version 2.4, the browsers will continue to operate with a controller upgrade to version 2.5 as long as you do not also upgrade Chrome or Firefox to the versions cited above, which introduce the problem.

If you experienced this error with controller version 2.4, upgrading to version 2.5 does not fix the error condition. The resolution for upgrading to version 2.5 with the Chrome and Firefox versions cited above installed is provided on the HP Support center page at this Support Communication — Customer Advisory link. You can also resolve the problem by uninstalling the controller (and the Keystone server if you are using a local Keystone server) and performing a fresh controller installation. To do so, see the following chapters in the HP VAN SDN Controller Installation Guide for controller release 2.5:

1. "Uninstalling the controller and the local Keystone server"
2. Either "Installing a new controller with a local Keystone server" or "Installing the controller to operate with a remote Keystone server", depending on your choice of Keystone server environment.

Earlier fixes

For information about software fixes prior to Version 2.5, see the *HP VAN SDN 2.4.6 Release Notes*.

Issues and workarounds

The following issues exist in this release:

- **Switch in topology viewer occasionally moves around in the display** (CR_146636): May occur before end-nodes are discovered on the switch or before Pin All (in the View drop-down menu) is selected.
- **Data plane traffic to or from a host that is indirectly connected to a controlled switch is not forwarded at line-rate if the controller is configured with hybrid.mode=false (OpenFlow-only)** (CR_148324): A host is indirectly connected to a controlled switch when there is an uncontrolled switch between the edge-most controlled switch and the host. In any instance where a host is connected to the controlled network in this manner, the controller does not learn where the host is located because the controller assumes that no hosts will appear on infrastructure ports. Since the controller does not learn where the host is located, any traffic flows to or from this host cannot be paved and will therefore be handled by the controller at each hop through the controlled network. If a single packet to or from such a host needs to cross *N* controlled switches, then the controller will be consulted *N* times for the same packet. The actual throughput rate depends upon the load of other processing on the controller and the number of hops that such flows take through the controlled network.

  A common instance of this issue occurs if multiple controlled switches are connected to the same VLAN of an uncontrolled router. The port that a switch uses to connect to the router is considered an infrastructure port, because that port has an indirect or multi-hop link to other controlled switches. In that instance, all hosts reachable through the router appear to the controller as though they were indirectly connected to an infrastructure port. Such hosts experience performance levels significantly lower than line-rate. If this router were a gateway router to the internet, then all traffic to or from internet hosts would be directed by the controller at a performance level significantly lower than line-rate.

  Workarounds:

  1. Change the controller's hybrid.mode setting to "true". See the *HP VAN SDN Controller Administrator Guide* for information on what such a change implies for the controlled network.
  2. If workaround number 1 is unacceptable, connect all hosts to the ports of controlled switches that are not also connected to other controlled switches. Avoid connecting multiple controlled switches to ports on the same VLAN of a router (especially a gateway router).

- **The interface status is not updated for a port in the spanning tree BLOCKED state** (CR_152839): Ports that are in STP BLOCKED state are not reported correctly via OpenFlow when their status changes. This may result in the controller showing incorrect port information because the controller is not updated regarding BLOCKED ports.
- **5406 zl ProVision switch (J8697A) discovered as J9642A** (CR_155563): The J8697A HP 5406 zl switch was replaced with the J9642A HP 5406zl Switch with Premium Software.
- **The controller learns nodes from DHCP "release" packets** (CR_160368): Fixed with this caveat: IP learning looks at DHCP release packets and learns from them. Rather than insert DHCP specifics into the IP learning code, HP recommends disabling IP learning if you want DHCP release packets to instantly cause the node to be removed from the cache. To disable IP learning, start the controller and do the following:
  1. Select **Configurations**.
  2. In the **Component** window, select `com.hp.sdn.disco.of.node.impl.OflpDiscoveryComponent`.
  3. Click on **Modify**.
  4. In the `learn.ip` **Value** field, enter `false`.
  5. Click on **Apply**.

- **The controller stays in an initialized state and an HTTP Status 404 — Not Found error appears when CTL_RESTORE_INSTALL_MODE=True** (CR_164548): The controller web interface is not accessible while a Restore is running, and the controller is not fully functional until a user-initiated restore is complete.
- **Pushing a meter or group mod to a connected switch from a controller that is a slave will not return the proper error message if the switch returns an error** (CR_165154): Pushing flows, groups, and meters via northbound REST API to any controller in the team is supported even if that controller is not the master of the given device. However, if the controller receiving the request is not the master for the destination switch (DPID), then that slave will contact the master to handle it. If the switch returns an error from the given request (for example, the meters table is full), the switch responds to the master controller with a proper Openflow error such as:

  `METER_MOD_FAILED/OUT_OF_METERS`

  with a json code of 400. When that error is sent back to the requesting controller, though, it is not parsed properly and results in an error of: :

  `java.lang.IllegalStateException`

  with a json code of 500 instead of the meter configuration error message.
- **org.postgresql.util.PSQL Exception: Connection refused. Exceptions generated when the VM is shut down** (CR_165333): During the shut down of the VM, sdnc is trying to send alerts while many PostgreSQL exceptions are being thrown. This delays the sdnc shutdown, causing a delay in the controller shut down and generation of exceptions. As a workaround, stop the sdnc service and verify that it has stopped before shutting down the VM. This ensures that the PostgreSQL service is available when sdnc is shutting down. This avoids exceptions, and allows detection of the node leaving the cluster faster for high availability services.
- **Reinstalling the controller in Restore mode fails when the user "sdn" existed before the installation** (CR_166583): If the user "sdn" existed before the installation, the controller terminal displays this warning when the `sudo apt-get install -f` command is executed to install the downloaded HP VAN SDN Controller software.

```
****************************** WARNING ******************************

THE USER 'sdn' EXISTED PRIOR TO THE INSTALLATION OF THE CONTROLLER.  THE
CONTROLLER REQUIRES THE USER 'sdn' TO HAVE CERTAIN ATTRIBUTES AND
PERMISSIONS.  IT IS RECOMMENDED THAT YOU DELETE THE 'sdn' USER, AND THEN
RE-INSTALL THE CONTROLLER TO ENSURE CORRECT FUNCTIONALITY.

*********************************************************************
```

  To avoid a restore failure when the above warning appears, delete the "sdn" user and use `sudo apt-get install -f` to re-install the controller.

  NOTE: The `sudo apt-get install -f` command runs a script that creates a correct sdn user.

- **Creating a FlowMod with empty actions inside an instruction causes the FlowMod to mistakenly choose the default table in ProVision switches** (CR_168239): Applications can create empty instructions for a FlowMod. This translates to a DROP. However, if you create an instruction with an empty action, the FlowMod is incorrectly directed to a read-only table in ProVision devices. Workaround: If there is no discernable action to include in an instruction, the application should create no instruction rather than putting an empty action inside.
- **Log rolling feature fails to roll logs. Fills the drive to capacity with log messages** (CR_168028): The SDN logging system depends on the ability of the underlying OS to provide a new file when the time comes for the log file to roll over. The default configuration is for the log files to roll once they reach 10 MB in size, maintaining four previous versions of the file. If the total

number of available file descriptors is consumed to the point where the OS cannot provide a new log file, the log file rollover fails. When this condition occurs, it can be observed that the SDN controller continues logging to the last log file it was able to create. It is then possible for the SDN controller to produce a single very large log file (as rollover is not possible due to the inability of the OS to provide a new file) which can grow to consume all available disk space.

Workaround: The SDN controller captures and records metrics concerning the total number of open File Descriptors and the ratio of open File Descriptors to the maximum number of File Descriptors configured on the OS. These values should be monitored periodically to help detect the condition where all available File Descriptors have been consumed.The File Descriptor metric data can be obtained via the "metrics" REST API, and are reported for the application `com.hp.sdn`. The metric values for monitoring the File Descriptor usage are the `fileDescriptorUsage` and `fileDescriptorsOpen` metrics. Please see the chapter titled "Metrics" in the *HP VAN SDN Controller Administrator Guide* for more information.

- **Code fails after requesting FlowService API implementation** (CR_169321): Both FlowService APIs listed in Javadocs are not available for use. To interact with the built-in OpenFlow controller, use the `ControllerService` interface in the `com.hp.of.ctl` package or the `TeamControllerService` interface in the `com.hp.sdn.teamcs` package.
- **The Controller's flow monitor UI may time-out when making REST calls on switches having a large number of flows** (CR_171357 and CR_171777): When a switch has 800 or more flow entries, an OpenFlow Monitor can time-out when either monitoring OF multipart messages having more than one packet, or performing actions--such as getting the flow statistics for all flows in the flow table. This issue is automatically resolved as flows expire and the number of flow entries on the switch is reduced. For the HP Network Optimizer application, there may be a delay in displaying Microsoft Lync sessions as closed in the UI, but this issue does not impact either the prioritization of the calls or the overall call quality.

  Multipart messages occur when the controller exchanges messages with a switch in a series of OpenFlow transactions that are part of the same request and reply stream. To ease implementation, the controller is allowed to send requests, and the switch is allowed to send replies, with no additional entries. However, another message must always follow a message with the "more" flag set. A request that spans multiple messages (that is, one or more messages with the "more" flag set) must use the same transaction ID (xid) for all messages in the request stream. Messages from a multipart request may also be interleaved with other OpenFlow message types, including other multipart requests. Such messages must have distinct transaction IDs if multiple, unanswered, multipart requests are simultaneously in transit.

  Cause: The "more" flag is set to 1 in a multipart packet if there are additional packets expected for the same request. However, the last packet must be set to 0. On a ProVision switch experiencing a large number of flows, the last packet setting of 0 does not occur, resulting in the controller waiting for a new multipart message that does not arrive. After waiting 10 seconds in this state, the controller times-out.

  Another issue affecting only Comware switches is when messages from a multipart request are interleaved with other OpenFlow message types. In this case, the transaction ID becomes corrupted and the controller times-out while waiting for the next multipart message.

- **All available inodes used** (CR_171438): Old JVM metrics data is not being deleted as scheduled. Consequently all available inodes on the file system are consumed over time.

  Workaround: Delete the old JVM metrics data by deleting the "year" subdirectories (such as "2015") under the `/opt/sdn/virgo/` metrics directory. The "year" subdirectories will be rebuilt as needed as new data is collected. For example, to remove a subdirectory named 2015:

  ```
  cd /opt/sdn/virgo/metricsrm -rf 2015
  ```

CAUTION: Do not delete the `.csv` file in the "/opt/sdn/virgo/metrics" directory.

HP recommends deleting JVM metrics data older than seven days. Creating a cron job for this task can help with scheduled deletions.

- **The RSDoc interface of the VAN SDN controller is unavailable when the controller is implemented using CA signed certificates** (CR_172363): The controller URL reachable at `https://controller-IP-address:8443/api/` may only be used when the controller is configured to use self-signed certificates (the default).

  NOTE: This utility is designed for programmatic access only and is not intended for use in production deployments.

- **TLS v1.0 has known security vulnerabilities** (CR_178737): For details on these vulnerabilities, see publication HPSBPV03516 at the HP Support Center.
- **The SDN controller upgrade to release 2.5.20 causes applications such as Network Protector to produce large numbers of error log messages until the application itself is also upgraded** (CR_180609): You may observe a continual flow of application error messages logged during and after upgrading the controller to release 2.5.20. After upgrading the controller, upgrade the application itself to remedy this condition. For Network Protector, upgrade to release 1.3.53. For Network Optimizer, upgrade to release 1.3.41. For other applications, consult the appropriate release notes and then upgrade to the latest release supporting operation with controller release 2.5.20.
- **The controller support log lists a `Server Error – Invalid Data` message after upgrading to controller release 2.5.20** (CR_180728): This error occurs in the support logs immediately after the upgrade, and is usually caused by incompatible data in the log from the prior controller release. The `Invalid Data` will eventually scroll out of the log display. An alternative method to eliminate the Invalid Data messages is to select **Configurations** in the controller web interface, then select `com.hp.adm.log.impl.LogManager` and modify the `max.display.rows` value to a small number, such as 20.
- **Schema Disagreement Exception after trying to verify synch behavior during multiple backups of three-node team** (CR_180777): Occurs in instances where there is an attempt to restore a team of controllers using different restore points. Specifically, after restoring a controller, an application that has also been restored fails to contact the Cassandra API and generates the following message in the `/var/log/sdn/virgo/logs/log.log` file:

  ```
  SchemaDisagreementException: [host=127.0.0.1(127.0.0.1):9160,
  latency=2(2), attempts=1]Can't change schema due to pending schema agreement
  ```

  Workaround: If the above occurs, run the script "`npDbShutdown.sh`" in the directory `/opt/sdn/cassandra/bin/` and then run the restore operation again on only that node.

- **Data logged in a teamed controller disappears** (CR_176111): An application log may show errors or warnings similar to the following:

  ```
  2015-10-13 22:13:21.148 ERROR [http-bio-8443-exec-104] DNSDataDaoImpl : Exception in getRange() 2015-10-13
   22:13:21.162 WARN [http-bio-8443-exec-102] ParameterizedQuery : Error executing request (requestID=311)

  com.mycompany.astyanax.connectionpool.exceptions.OperationTimeoutException: OperationTimeoutException:
  [host=127.0.0.1(127.0.0.1):9160, latency=10004(10004), attempts=1]TimedOutException()
  ```

  The Cassandra database automatic synch-up supports a maximum down time for a teamed controller of no more than one hour. The data inconsistency can be detected by comparing the Web UI and REST API outputs from different nodes. Note that Cassandra is used only by applications, meaning that you should check the application Web UI and REST UI instead of the Controller UIs. In this case, the data flow from the affected controller remains out of synchronization, requiring the System Administrator to run nodetool repair to import data into the controller node and add the node back into the appropriate database in the Cassandra node cluster.

The Cassandra nodes must be online during the repair. (Installed applications can be running during the repair. No application restart is required.) To verify whether the Cassandra nodes are up, run the following `status` command on any controller node in the team:

```
$ /opt/sdn/cassandra/bin/nodetool status
```

You should then see an output similar to the following:

```
root@source-ubu14:/opt/sdn/cassandra/bin# ./nodetool status
Datacenter: datacenter1
=======================
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load      Tokens Owns (effective) Host
ID                          Rack
UN 192.17.4.142 1.23 GB   1      100.0%           4245b8ab-6c3c-4755-bb28-90850d3a4a24 rack1
UN 192.17.4.140 1.23 GB   1      100.0%           c172bbe2-799c-4adf-bd38-690dfa75ac79 rack1
UN 192.17.4.141 310.11 MB 1      100.0%           26999328-abec-4d80-a689-eb8b1f7f89d1  rack1
```

The first column of output should display 'UN' (Up/Normal) for all nodes. However, if a node is down, the controller outputs one of the following responses:

- If Cassandra is down on the node on which you executed the above `status` command, a `Failed to connect` message similar to the following appears:

  ```
  Failed to connect to '127.0.0.1:7199': Connection refused
  ```

- If Cassandra is down on a different node than the one on which you executed the above `status` command, an output similar to the following appears, with `DN` (Down/Normal) appearing in the first column for the downed node:

  ```
  root@source-ubu14:/opt/sdn/cassandra/bin# ./nodetool status
  Datacenter: datacenter1
  =======================
  Status=Up/Down
  |/ State=Normal/Leaving/Joining/Moving
  -- Address      Load      Tokens Owns (effective) Host
  ID                          Rack
  UN 192.17.4.142 1.23 GB   1      100.0%           4245b8ab-6c3c-4755-bb28-90850d3a4a24 rack1
  UN 192.17.4.140 1.23 GB   1      100.0%           c172bbe2-799c-4adf-bd38-690dfa75ac79 rack1
  DN 192.17.4.141 310.11 MB 1      100.0%           26999328-abec-4d80-a689-eb8b1f7f89d1  rack1
  ```

If a node is down, close any instance of the web interface in which the controller is running, then restart the node by executing the following command in that node:

```
$ sudo service sdnc restart
```

NOTE: This command also restarts the Controller. A Cassandra-only restart is not supported. (You should always restart Cassandra by restarting the Controller.)

Run the following command on each controller node to complete the resynchronization process for the Cassandra database:

```
$ /opt/sdn/cassandra/bin/nodetool repair
```

- **Alert Notification: Team controller fails to push alerts to IMC ISDNM** (CR_176684): IMC SDNM registers as an Alert listener for specific controller alert topics. For controller teams, IMC registers using the team IP address. However, any member of the controller team can issue alerts. Because these alerts come from individual controller IP addresses instead of the team IP address, IMC rejects the alerts for security reasons. Because the team leader does not re-issue the alerts from the team IP address, IMC does not receive the alerts.
- **Master Controller to switch connectivity time during failover and fallback varies, based on the scale of deployment** (CR_182008): Controller fail-over and fail-back occur through a process of refreshing policies on a switch-by-switch basis. Fail-over and fail-back time can increase,

based on the switch deployment scale. That is, in either of the following cases, if a controller fails-over or fails-back, there is a delay while another controller takes over:

- One controller manages multiple switches, or
- One switch managed by a controller is configured with a large number of instances

Deprecated or changed features

The following features are deprecated as of controller version 2.5.14:

- SSLv3 support
- `sdn/v2.0/regions`
- `/sdn/v2.0/regions/{region_uid}/refresh`

The following features are changed as of software version 2.5.14:

- High Availability (HA)

Upgrade information

Prerequisites

See the latest version of the *HP VAN SDN Controller and Applications Support Matrix* at the SDN Networking Resources library.

Contacting HP

For additional information or assistance, contact HP Networking Support:

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

Before contacting HP, 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

HP 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 HP Support Center website at www.hp.com/go/hpsc.
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 HP Security Bulletin alerts via email, sign up at:

http://h41183.www4.hp.com/signup_alerts.php?jumpid=hpsc_secbulletins

Related information

Documents

To find related documents, see the HP Support Center website:

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

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Related documents

The following documents provide related information:

- *HP VAN SDN Controller Release Notes*
- *HP VAN SDN Controller and Applications Support Matrix*
- *HP VAN SDN Controller Installation Guide*
- *HP VAN SDN Controller Administrator Guide*
- *HP VAN SDN Controller Programming Guide*
- *HP VAN SDN Controller REST API Reference*
- *HPN SDN Controller Link Discovery* (a technical white paper)
- *HP VAN SDN Controller Open Source and Third-Party Software License Agreements*
- *HP VAN SDN Controller Troubleshooting Guide*

Websites

- Official HP Home page: http://www.hp.com
- HP Networking: http://www.hp.com/go/networking
- HP Enterprise Information Library: http://h17007.www1.hp.com/us/en/networking/library/index.aspx?cat=sdn#technical
- HP product manuals: http://www.hp.com/support/manuals
- HP download drivers and software: http://www.hp.com/support/downloads
- HP software depot: http://www.software.hp.com
- HP education services: http://www.hp.com/learn

Documentation feedback

HP 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@hp.com**). Include the document title and part number, version number, or the URL when submitting your feedback.