HP VAN SDN Controller 2.3 Installation Guide

Abstract

HP VAN SDN Controller This guide describes the steps for installing the HP VAN SDN (Virtual Area Network Software-Defined Networking) Controller software on a system running Ubuntu version 12.04 LTS 64-bit server. The intended audience is administrators who are familiar with installing and using the Ubuntu server, experienced in using and configuring the OpenStack Keystone authentication software, and familiar with configuring an OpenFlow network to operate with a controller or team of controllers.

Acknowledgments

UNIX is a registered trademark of the Open Group.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

OpenFlow is a trademark of the Open Networking Foundation. Open Source is a trademark of the Open Source Initiative. Linux is a trademark of Linus Torvalds. Ubuntu is a trademark of Canonical Group Limited.

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*.

For information on acquiring the open source code for the HP VAN SDN Controller, send an email to **HPN-Open-Source-Query@lists.hp.com**.

Contents

1 Overview

The HP VAN SDN Controller provides an extensive platform for developing and running SDN applications. It features:

- A base controller platform for Linux/Java/OSGi, OpenFlow 1.0/1.3, built-in services, and a device driver framework
- Operation with either a local or a remote Keystone server
- Controller teaming for distributed platform for High Availability (HA) and scalability
- Embedded Java applications, an extensible REST API and UI, and an IMC management interface

As an HP VAN SDN Controller administrator, you should be familiar with OpenFlow, and have OpenFlow configured and enabled on the network switches to be managed by the controller.

1.1 Before installing the controller

- See the *HP VAN SDN Controller and Applications Support Matrix* for hardware and software requirements, supported OpenFlow versions and network switches, and other controller support information.
- Ensure that NTP (Network Time Protocol) is installed and configured on your system.
- See Figure 1 (page 5) for an overview of the controller installation process.

NOTE: The controller supports v2.0 of the Keystone REST API.

Figure 1 HP VAN SDN Controller installation overview
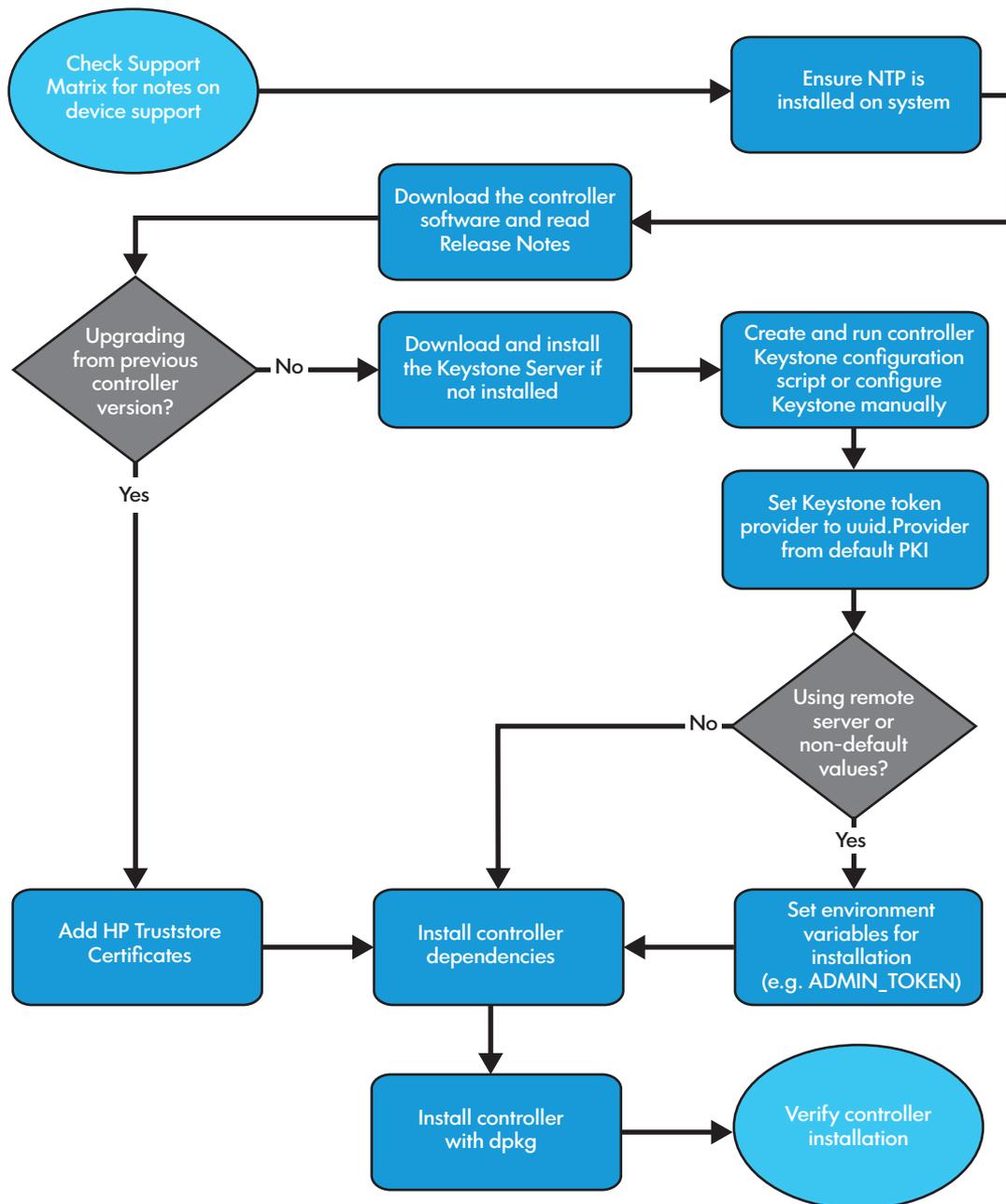
1.2 Downloading the controller software

To download the HP VAN SDN Controller software:

1. Go to the HP Networking support site at www.hp.com/networking/support.
2. Enter the HP VAN SDN base product number **J9863AAE** in the **Auto Search** field, as shown in Figure 2.

Figure 2 HPN Networking support site
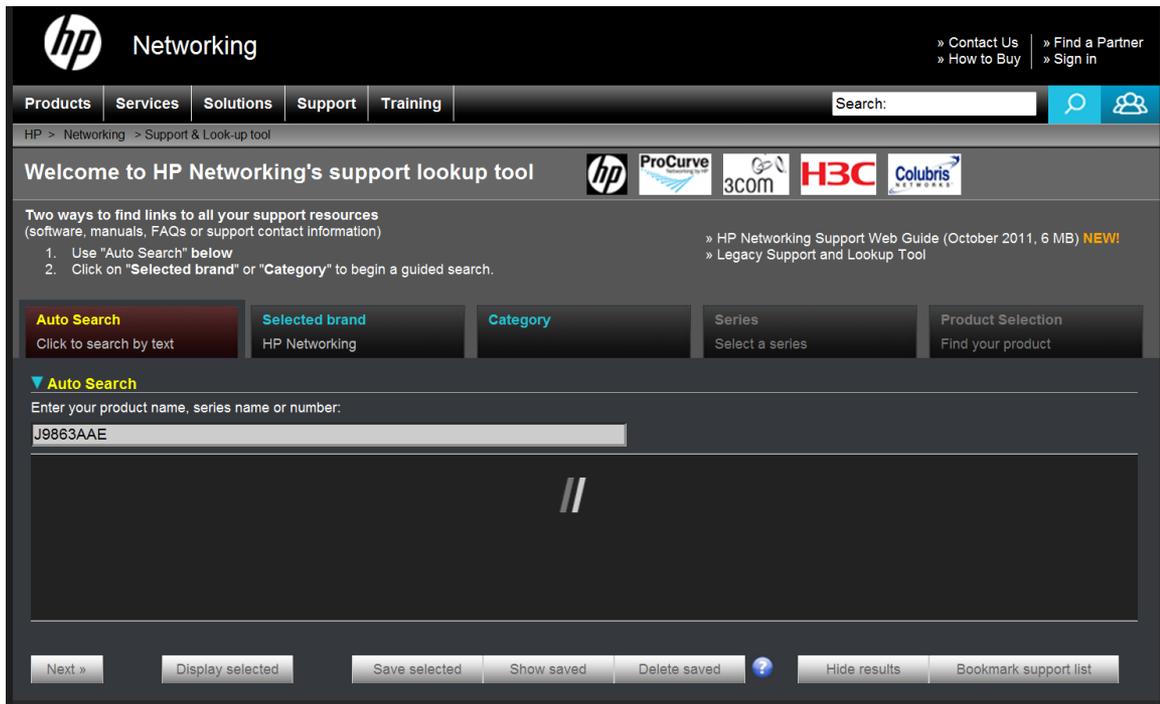
3. Select the check box next to the HP VAN SDN Controller product, and then click **Display selected**.
4. In the lower right quadrant of the product display screen, click **Software downloads**, as shown in Figure 3.

Figure 3 Software downloads pane
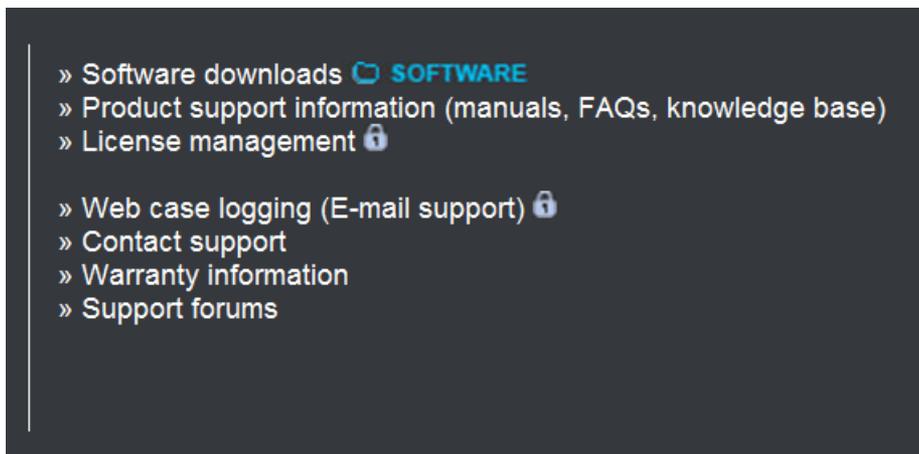
5. On the **My Networking Download software** screen, select and download the `VAN_SDN_Controller_v2.3.5` software package (`.zip` file) to your Ubuntu machine.
6. Unzip the software package.
7. Read the latest *HP VAN SDN Controller Release Notes* included with the software package.
8. If you are upgrading from an earlier version of the controller, see also the ReadMe file included in the software package.

2 Installing the HP VAN SDN Controller

2.1 Selecting a controller mode

Beginning with controller software release 2.3, the HP VAN SDN Controller supports both local and remote Keystone authentication servers. When upgrading from a previous controller version, the established local Keystone server is used. For a new controller installation, it is necessary to install and configure a Keystone server on either a local or remote machine.

You can configure controllers to operate in either standalone or team mode.

- **Standalone mode**—(Required) Creates a single, standalone controller as described in this guide. Using one standalone controller in a network does not provide high availability and automatic failover, leaving the network in an unmanaged state if the controller fails. Installing this mode on three controllers , however, enables you to operate in team mode.

- **Team mode**—Creates a team of three controllers with automatic failover, resulting in a continuously managed network in the event that one controller in the team goes down. This mode also provides centralized controller configuration and monitoring.

   To operate in team mode:
   1. Install the software on a single controller as described in this manual.
   2. Repeat the process to install two additional controllers on separate nodes in preparation for team operation.
   3. Configure the group of installed controllers to operate in a team, as described in the *HP VAN SDN Controller Administrator Guide*.

For software licensing and registration information for standalone and teamed controllers, see the chapter covering licensing in the *HP VAN SDN Controller Administrator Guide*.

2.2 Installing a new controller and Keystone server

For a first-time controller installation, do the following before installing the controller.
1. Install the Keystone server on a local or remote machine.
2. Configure a user on the Keystone server.

2.2.1 Installing a Keystone server

Skip this action and go to "Adding the HP TrustStore certificate for an upgrade to controller release 2.3" (page 9) if you are upgrading to controller release hp-sdn-ctl_2.3 from an earlier version. Otherwise install the latest Keystone server version on the local or remote device you want to manage Keystone authentication. Use this action if you are performing a first-time HP VAN SDN Controller installation.

NOTE: Although the HP VAN SDN Controller operates with the Folsom, Grizzly, Havana, or Icehouse releases of OpenStack Keystone, HP recommends that you use the Icehouse or later version with the controller.

```
~$ sudo apt-get install python-software-properties
ubuntu-cloud-keyring
~$ sudo add-apt-repository "deb
http://ubuntu-cloud.archive.canonical.com/ubuntu
precise-updates/version_name main"
sudo apt-get update
~$ sudo apt-get install keystone
```

Where: *version_name* is one of these OpenStack Keystone versions:

- folsom
- grizzly
- havana
- icehouse

For information on a specific Keystone version, visit http://docs.openstack.org/developer/keystone/ and see the documentation for the OpenStack Keystone version you are using.

NOTE: The scripts used to create users, passwords, roles, and tenants require that the configured keystone server is accessible and responsive to basic Keystone REST API queries.

The controller supports v2.0 of the Keystone REST API.

2.2.2 Configuring a user on the Keystone server

For a first-time HP VAN SDN Controller installation, do one of the following on the Keystone server:

- use the Keystone server CLI to configure a user. For more information, see the OpenStack Keystone documentation at http://docs.openstack.org/developer/keystone/.
- create and apply a script similar to the one shown under "Using a script to configure users, passwords, roles, and tenants" (page 15)

2.2.3 Setting the provider type to UUID on the Keystone server

UUID is the default provider type for the Folsom release of Keystone. However, if the machine supporting your Keystone server is running the Grizzly, Havana, or Icehouse version of Keystone (which all use the PKI provider type), do the following:

1. Edit the `/etc/keystone/keystone.conf` file with the following line to set UUID as the provider type:

    ```
    provider=keystone.token.providers.uuid.Provider
    ```

    For example, in the Icehouse version of Keystone, you would insert the above command in the [token] section of the file, as shown in the **boldface** entry, below:

    ```
    [token]

    #
    # Options defined in keystone
    #

    # External auth mechanisms that should add bind information to
    # token e.g. kerberos, x509. (list value)
    #bind=

    # Enforcement policy on tokens presented to keystone with bind
    # information. One of disabled, permissive, strict, required
    # or a specifically required bind mode e.g. kerberos or x509
    # to require binding to that authentication. (string value)
    #enforce_token_bind=permissive

    # Amount of time a token should remain valid (in seconds).
    # (integer value)
    #expiration=3600

    # Controls the token construction, validation, and revocation
    # operations. Core providers are
    # "keystone.token.providers.[pki|uuid].Provider". (string
    # value)
    provider=keystone.token.providers.uuid.Provider 1
    # Keystone Token persistence backend driver. (string value)
    #driver=keystone.token.backends.sql.Token

    # Toggle for token system cacheing. This has no effect unless
    # global caching is enabled. (boolean value)
    #caching=true

    . . .
    ```

    1   Adding this line sets
        the UUID provider
        type.

2. Restart the Keystone server.

NOTE: The PKI provider type is not currently supported on the HP VAN SDN Controller.

2.2.4 Adding the HP TrustStore certificate for an upgrade to controller release 2.3

Perform this step if you are upgrading the HP VAN SDN Controller to release 2.3 from an earlier version. This step adds a new HP certificate to the controller TrustStore by running the `update_truststore.sh` script provided in the software package (`.zip` file) you downloaded earlier from the HP Networking support site. For information on how to use the script, see the ReadMe file included in the software package.

NOTE: If you are upgrading from an earlier controller version and have third-party applications installed, running the script installs the new HP certificate and preserves the certificates for previously installed applications.

After completing this step, go to "Installing or upgrading the controller" (page 10).

2.3 Installing or upgrading the controller

NOTE: If you are using non-default Keystone authentication, go to "Configuring Keystone authentication" (page 14) before continuing here.

NOTE: Installed controller licenses, applications, and application licenses are preserved across an upgrade of an installed controller.

NOTE: Where a command in this procedure is shown with multiple lines, the line breaks are inserted at the points where a space occurs in the actual command.

Use this procedure for either upgrading an installed controller or performing a first-time controller installation.

To install the downloaded HP VAN SDN Controller software:

1. If you are upgrading a controller in an existing team, disband the team. (See the "Team Configuration" chapter in the latest *HP VAN SDN Controller Administrator Guide*.)
2. Ensure that you have root access on the Ubuntu system (`sudo`).
3. On the machine you will run the controller, execute the following command for installing software dependencies. When prompted, press **Y**.

    ```
    ~$ sudo apt-get install openjdk-7-jre-headless postgresql
    postgresql-client iptables unzip curl
    ```

4. Ensure that Java 7 is installed on your Ubuntu machine. (If, in addition to Java 7, there is an older version of Java installed, such as Java 6, the installation will automatically designate Java 7 as the default version.) Use the following command to determine the version(s) of Java installed.

    ```
    ~$ sudo update-java-alternatives -l
    ```

    An output with one or more lines appears, similar to the following:

    ```
    java-1.6.0-openjdk-amd64 1061 /usr/lib/jvm/java-1.6.0-openjdk-amd64
    java-1.7.0-openjdk-amd64 1051 /usr/lib/jvm/java-1.7.0-openjdk-amd64
    ```

    If Java 7 is listed, go to Step 5. If Java 7 is not listed, repeat Step 3.

5. Install the HP VAN SDN Controller from the directory in which the package is stored:

    ```
    ~$ sudo dpkg -i hp-sdn-ctl_version_amd64.deb
    ```
    (Replace `version` with the actual release version number of the controller.)

    *   If you are doing a first-time installation of the controller, the system prompt appears (`~$`). Go to "Verifying the controller installation" (page 11).
    *   If you are upgrading the controller from an earlier version, the prompt in Figure 4 (page 11) may appear. If the prompt does not appear, go to Step 7.

Figure 4 Jar Signing TrustStore Prompt

```
Configuration file `/opt/sdn/admin/sdnjar_trust.jks'
 ==> File on system created by you or by a script.
 ==> File also in package provided by package maintainer.
   What would you like to do about it ?  Your options are:
     Y or I  : install the package maintainer's version
     N or O  : keep your currently-installed version
        D     : show the differences between the versions
        Z     : start a shell to examine the situation
 The default action is to keep your current version.
*** sdnjar_trust.jks (Y/I/N/O/D/Z) [default=N] ?
```

6. Press **N** to preserve HP and third-party certificates.
7. If the controller belongs in a team and the other controllers in the team are upgraded to release 2.3, then re-form the team. (See the "Team Configuration" chapter in the latest *HP VAN SDN Controller Administrator Guide*).

2.4 Verifying the controller installation

To verify the controller installation:

1. Using the Ubuntu command prompt, enter the following to check the installation state:

    ```
    ~$ dpkg -l hp-sdn-ctl
    ```

    If the HP HP VAN SDN Controller package is properly installed, output similar to the following appears:

    ```
    ii  hp-sdn-ctl     2.3.5.6499     HP VAN SDN Controller
    ```

2. In the command line window, verify that the sdnc service is started:

    ```
    ~$ service sdnc status
    ```
    The following output indicates that the sdnc service is started:

    ```
    ~$ sdnc start/running, process nnnn
    ```

    Where: *nnnn* is the process ID assigned to the main HP VAN SDN Controller process (sdnc).

2.5 Access a controller interface

This section describes the interfaces for operating the controller. (For information on supported web browsers, see the *HP VAN SDN Controller and Applications Support Matrix*.)

2.5.1 Using the controller console UI

1. Using a supported web browser, access the controller user interface:

   ```
   ~$ https://controller_ip_address:8443/sdn/ui/
   ```
   (Replace *controller_ip_address* with your controller IP address.)

   The **HP VAN SDN Controller** login screen appears, as shown in Figure 5.

   Figure 5 Logging in to the console
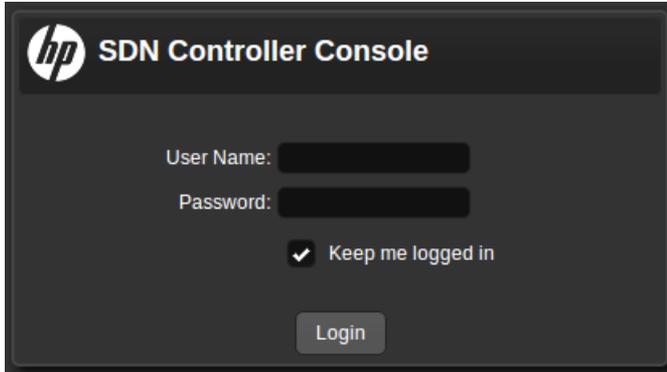
2. Enter your user name and Password, and then click **Login**.

   NOTE: The user name and password are set in the Keystone software prior to the HP VAN SDN Controller installation. Unless the Keystone configuration script is changed prior to installation, the default user name and password are used:

   - default user name: `sdn`.
   - default password: `skyline`.

If the controller is running, a display similar to Figure 6 appears:

Figure 6 Default controller console UI

2.6 Changing a user password

To change the user password:

NOTE: Where a command in this procedure is shown with multiple lines, the line breaks are inserted at the points where a space occurs in the actual command.

1. Determine the new SDN password you want to use for access to the controller. For this example, the new password is `mynewpassword`.
2. Determine whether the proxies for your shell session are removed. For example:

```
~$ env | grep -i proxy
http_proxy=http://web-proxy.lond.myco.com:8088/
https_proxy=https://web-proxy.lond.myco.com:8088/
```

If an output similar to the above appears, proxies are present that must be removed. Use the `unset` command to clear the indicated proxies:

```
~$ unset https_proxy http_proxy

~$ env | grep -i proxy
~$
```

3. Retrieve the `user-id`. For example, with only the default users enabled, use this command:

```
~$ curl -i http://localhost:35357/v2.0/users -H
"X-Auth-Token: ADMIN"
```

Output similar to Figure 7 appears.

Figure 7 Retrieving the user ID

{"users": [{"name": "sdn", "enabled": true, "email": null, "id":"6f8ca8ff92c94a87be8f679b73b923ed",
"tenantId": null}, {"name": "rsdoc", "enabled": true, "email": null, "id":
"156d211f437740608453bc29a432ac03", "tenantId": null}]}

4. Retrieve the SDN user ID (`6f8ca8ff92c94a87be8f679b73b923ed` in this example) and enter it in the following command, along with the new password, then execute the command.

```
curl -i http://localhost:35357/v2.0/users/6f8ca8ff92c94a87be8f679b73b923ed/OS-KSADM/password --request
PUT -H "Content-Type: application/json" -H "X-Auth-Token: ADMIN" -d '{"user":{"password": "mynewpassword",
 "id":"6f8ca8ff92c94a87be8f679b73b923ed"}}'
```

A response similar to the following appears.

```
HTTP/1.1 200 OK
Vary: X-Auth-Token
Content-Type: application/json
Date: Sat, 14 Jun 2014 18:46:21 GMT
Transfer-Encoding: chunked
```

{"user": {"extra": {"password":
"6rounds=40000$SuDRFGlce64f5Lul$64fodORLelts.98s.1DrsdwScwiTc/gFLKj.hXK41iir0Kg/3MOzYGX3GXBxcs25t.SIkHBe8ODdxaggZTkq./",
 "enabled": true, "email": null, "tenantId": null}, "id": "6f8ca8ff92c94a87be8f679b73b923ed", "name":
"sdn"}}

The new SDN password is now set.

2.7 Obtaining a software license

To obtain a software license, see the licensing chapter in the *HP VAN SDN Controller Administrator Guide*.

To download the Administrator guide and other HP VAN SDN Controller documentation, go to the SDN Information Library. Click on the **Resources** tab, then scroll down to **Technical Guides**.

2.8 Installing a controller team

In a network managed by a single controller, the controller represents a single point of failure, and if the controller goes down, the network becomes unmanaged. Teaming three HP VAN SDN Controller instances together minimizes the impact of a controller failure by providing automatic failover from the current leader instance to another controller instance. To enable controller teaming, see the *HP VAN SDN Controller Administrator Guide*.

NOTE: The number of team members required for an HP VAN SDN Controller team is three.

3 Configuring Keystone authentication

3.1 Create a user on a non-default Keystone server

HP recommends creating a user on the Keystone server *before* installing the controller. For information on configuring a user on Keystone, see the OpenStack Keystone documentation http://docs.openstack.org/developer/keystone/. As an option for creating a user on the server, you can also design and use a script similar to the script shown under "Using a script to configure users, passwords, roles, and tenants" (page 15).

3.2 Installing a controller with non-default settings

The installer uses the following environmental variables to configure the HP VAN SDN Controller for communication with the Keystone server. Setting non-default environmental variables is needed only if your Keystone server is not using the default variables.

NOTE: Using this section requires an understanding of the authentication settings configured in your Keystone server. For more information on configuring Keystone, see the OpenStack Keystone documentation http://docs.openstack.org/developer/keystone/.

Table 1 Keystone server variables

Environmental variable	Default settings
ADMIN_TOKEN	ADMIN
AUTH_ENDPOINT	http://127.0.0.1:35357/v2.0
TRUSTSTORE_PASS	— *none* – User-defined. Used only for SSL.
TRUSTSTORE	— *n/a* –

1. Before installing the controller, set the environmental variables that you do not want to remain at their default settings.

   - ADMIN_TOKEN — Defines the token string to use for administrative configuration on the Keystone server. If not specified, defaults to `ADMIN`. Set the ADMIN_TOKEN environmental variable with the following `EXPORT` command using the new token string:

     `~$ export ADMIN_TOKEN=token_string`

   - AUTH_ENDPOINT — Defines the endpoint path to the Keystone server. The default is:
     `http://127.0.0.1:35357/v2.0`

     Execute the following `EXPORT` command on the system on which you are about to run the installation:

     `~$ export AUTH_ENDPOINT=http://keystone_server_ip:port_number/v2.0`

     NOTE: The following two EXPORT commands set the environmental variables for SSL communication with the keystone server.

     NOTE: If the https protocol is defined by the AUTH_ENDPOINT variable, then the TrustStore and TRUSTSTORE_PASS variables must also be defined in the installers environment. But if http is the defined protocol, these values are ignored.

   - TRUSTSTORE —Defines the location of the trust store file for use in one-way SSL communication with the Keystone server.

1. Use the following command to create a TrustStore on the controller.
   ```
   keytool -genkey -alias keystone -keyalg rsa -keysize 2048
   -keystore keystore-name
   ```

2. Import a signed root certificate into the TrustStore. See the section titled "Creating SDN Controller Keystore and Truststore" in the latest version of the *HP VAN SDN Controller Administrator Guide* for the certificate-related commands to perform this operation.

3. Set the TrustStore environmental variable with the following EXPORT command with the new location:

   ```
   ~$ export TRUSTSTORE=/truststore_location/keystore_name
   ```

- TRUSTSTORE_PASS —Defines the password used to access the contents of the Trust Store file. It must be provided in plain text, which is encrypted by the controller installer scripts when recorded for future use by the controller.If you change this setting, execute the following EXPORT command with the new password:

  ```
  ~$ export TRUSTSTORE_PASS=password
  ```

2. Return to to begin the installation.

3.3 Using a script to configure users, passwords, roles, and tenants

On the Keystone server, running a script similar to the sample script included in this section configures a user on the server, including the tenant, user, and role variables. The variables defined in the `/etc/keystone/keystone.conf` file, along with the desired tenant, user, and role variables, must be included in the script.

NOTE: Proxy settings and other system factors require script content unique to your individual system. The following script is an example. If you use a script to create a user on a non-default Keystone server, you must design it for compatibility with your particular system.

For a local Keystone server, the installation script, by default, uses the following variables in the `keystone.conf` configuration:

- ADMIN_TOKEN: ADMIN
- AUTH_ENDPOINT: 127.0.0.1
- PORT: 35357

For a remote Keystone server, use the above variables described in Table 1 (page 14).

1. Copy the script into a file in a temporary directory on the machine where your Keystone service is running.
2. Populate the indicated variables by editing the variables listed at the top of the script as needed. The example script in this step uses the default settings listed in Table 1 (page 14).

NOTE: Where a command in this script is shown with multiple lines, the line breaks are inserted at the points where a space occurs in the actual command. Command string endpoints are indicated by the <CR> symbols, which should be removed before attempting to run a script built from this example.

```
#!/bin/bash
#---------------------------------------------------------------------
# Setup default keystone environment for the SDN controller
# Create a tenant "sdn"
# Create a user "sdn" with password "skyline"
# Create a role "sdn-admin"
# Create a role "sdn-user"
# Associates the user "sdn" with the create roles in the tenant "sdn"
#---------------------------------------------------------------------
ADMIN_TOKEN="ADMIN"<CR>
IP="127.0.0.1"<CR>
PORT="35357"<CR>
TENANT="sdn"<CR>
USER_NAME="sdn"<CR>
PASSWORD="skyline"<CR>
echo "Configure keystone server at $IP with admin token $ADMIN_TOKEN"<CR>
# Create the tenant
tenant_json="{\"tenant\":{\"name\":\"$TENANT\"}}"<CR>
tenant=$(curl --header "X-AUTH-Token:$ADMIN_TOKEN" --header "Content-Type:application/json" -ksS
--data-binary $tenant_json "http://$IP:$PORT/v2.0/tenants")<CR>
tenant_id=$(echo $tenant | sed 's/.*"id": "\([0-9a-z]*\)".*/\1/')<CR>
# Create the user
user_json="{\"user\":{\"name\":\"$USER_NAME\",\"enabled\":true,\"password\":\"$PASSWORD\"}}"
user=$(curl --header "X-AUTH-Token:$ADMIN_TOKEN" --header "Content-Type:application/json" -ksS --data-binary
 $user_json "http://$IP:$PORT/v2.0/users")<CR>
user_id=$(echo $user | sed 's/.*"id": "\([0-9a-z]*\)".*/\1/')<CR>
# Create the sdn-admin role
admin_role_json="{\"role\":{\"name\":\"sdn-admin\"}}"<CR>
admin_role=$(curl --header "X-AUTH-Token:$ADMIN_TOKEN" --header "Content-Type:application/json" -ksS
--data-binary $admin_role_json "http://$IP:$PORT/v2.0/OS-KSADM/roles")<CR>
admin_role_id=$(echo $admin_role | sed 's/.*"id": "\([0-9a-z]*\)".*/\1/')<CR>
# Create the sdn-user role
user_role_json="{\"role\":{\"name\":\"sdn-user\"}}"<CR>
user_role=$(curl --header "X-AUTH-Token:$ADMIN_TOKEN" --header "Content-Type:application/json" -ksS
--data-binary $user_role_json "http://$IP:$PORT/v2.0/OS-KSADM/roles")<CR>
user_role_id=$(echo $user_role | sed 's/.*"id": "\([0-9a-z]*\)".*/\1/')<CR>
# Associate user with admin role
admin_role_assoc=$(curl --header "X-AUTH-Token:$ADMIN_TOKEN" -ksS -X PUT
"http://$IP:$PORT/v2.0/tenants/$tenant_id/users/$user_id/roles/OS-KSADM/$admin_role_id")<CR>
# Associate user with user role
user_role_assoc=$(curl --header "X-AUTH-Token:$ADMIN_TOKEN" -ksS -X PUT
"http://$IP:$PORT/v2.0/tenants/$tenant_id/users/$user_id/roles/OS-KSADM/$user_role_id")<CR>
echo "Keystone configuration Complete"<CR>
```

3. Convert the script to an executable file:

   chmod +x *script_file_name*

4. Run the script file:

   ./*script_file_name*

4 Migrating the controller to another machine

⚠ **CAUTION:** Uninstalling either an application or the controller also erases any related licenses. For this reason, before you uninstall an application or the controller, you must first properly uninstall the related licenses so that they can be reinstalled on another machine.

- Note the Install ID for the controller from which you will uninstall a license.
- When you deactivate a license, the controller generates an Uninstall Key for that license, which you will need when you transfer the license. Be prepared to record the Uninstall Key for each license you deactivate.
- To uninstall application licenses, see the documentation provided for the specific application(s).
- To uninstall the controller license(s), see "Managing licenses" in the latest edition of the *HP VAN SDN Controller Administrator Guide* and perform the steps indicated in that section.

4.1 Applying the migration process

To move the controller and any installed applications from one machine to another, do the following:

1. Uninstall the licenses of any installed applications.
2. Uninstall the applications.
3. Uninstall the controller license(s).
4. Uninstall the controller itself.
5. On the new machine:
   a. Install the controller and related licenses.
   b. Install the applications and their related licenses.

4.2 Uninstalling the controller

NOTE: To uninstall a controller team, repeat this procedure on each controller in the team.

1. Uninstall any application licenses and applications, as outlined above. (See the documentation provided for the specific applications.)
2. Uninstall the controller licenses. (See "Managing licenses" in the latest edition of the *HP VAN SDN Controller Administrator Guide* and perform the steps indicated in that section.)
3. Enter the following command to uninstall the controller:
   ```
   ~$ sudo dpkg -P hp-sdn-ctl
   ```

5 Support and other resources

To learn how to contact HP, obtain software updates, submit feedback on documentation, and locate links to HP SDN websites and other related HP products, see the following topics.

5.1 Gather information before contacting an authorized support representative

If you need to contact an authorized HP support representative, be sure to have the following information available:

- If you have a Care Pack or other support contract, either your Service Agreement Identifier (SAID) or other proof of purchase of support for the controller and any HP SDN applications
- The HP VAN SDN Controller version and installed licenses
- The HP SDN application product names, versions, and installed licenses
- If you use a virtual machine for the operating system, the hypervisor virtualization platform and version
- Messages generated by the controller and applications
- Other HP or third-party software in use

5.2 How to contact HP

- See the Contact HP Worldwide website to obtain contact information for any country:

  http://www.hp.com/go/assistance
- See the contact information provided on the HP Support Center website:

  http://www.hp.com/go/hpsc
- In the United States, call +1 800 334 5144 to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.

5.3 Get connected to the HP SDN online user forum

The HP SDN community forum interactive online forum enables you to share your experiences and pose and answer questions related to using the HP VAN SDN Controller and SDN applications.

To join the discussion, see:

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

5.4 Software technical support and software updates

HP provides 90 days of limited technical support with the purchase of a base license for the HP VAN SDN Controller.

Some HP SDN applications have a trial period, during which limited technical support is provided for 90 days. Other HP SDN applications do not have a trial period and you must purchase a base license for the application to receive 90 days of limited support. Support for the controller and each HP SDN application is purchased separately, but you must have a base license for the controller to receive support for your licensed HP SDN application.

- For information about licenses for the controller, see the *HP VAN SDN Controller Administrator Guide*.
- For information about licenses for HP SDN applications, see the information about licensing in the administrator guide for the application.

5.4.1 Care Packs

To supplement the technical support provided with the purchase of a license, HP offers a wide variety of Care Packs that provide full technical support at 9x5 or 24x7 availability with annual or multi-year options. To purchase a Care Pack for an HP SDN application, you must have a license for that application and a license for the controller.

For a list of Care Packs available for the controller and HP SDN applications, see:

http://www.hp.com/go/cpc

Enter the SDN license product number to see a list of Care Packs offered.

Once registered, you receive a service contract in the mail containing the customer service phone number and your Service Agreement Identifier (SAID). You need the SAID when you phone for technical support.

To obtain full technical support prior to receiving the service contract in the mail, please call Technical Support with the proof of purchase of the Care Pack.

5.4.2 Obtaining software updates

The software for the HP VAN SDN Controller and HP SDN applications can be downloaded for free from the HP Networking support lookup tool:

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

This website also provides links for manuals, electronic case submission, and other support functions.

5.4.3 Warranty

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

5.5 Related information

Documentation

- HP SDN information library:
  http://www.hp.com/go/sdn/infolib

Product websites

- HP Software-Defined Networking website:

  ○ Primary website:
     http://www.hp.com/go/sdn

  ○ HP SDN Dev Center website:
     http://www.sdndevcenter.hp.com

  ○ HP SDN community discussion forum
     http://www.hp.com/networking/sdnforum

- HP Open Source Download Site:
  http://www.hp.com/software/opensource

- HP Networking services website:
  http://www.hp.com/networking/services

6 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.