Manuals+ — User Manuals Simplified.

JUNIPER
NETWORKS

Juniper NETWORKS 4.4 Paragon Active Assurance Upgrade Instructions

Juniper NETWORKS 4.4 Paragon Active Assurance Upgrade Instructions

Contents

General

Upgrade Paths
If you are upgrading from an old Net rounds version, the following steps are ;ss;n█-VĹ

- Upgrading from version 2.34 to replace Ubuntu 16.04 with Ubuntu 18.04.
- Upgrading to version 4.0 to start using a Juniper license.

The following upgrade paths are recommended:

Source version	Target version	Note
< 2.28.99	2.28.99	For these upgrades, please contact Juniper support (see below).
2.28.99	2.29.2	
2.29.2	2.34.4	
2.30.x	2.34.4	
2.31.x	2.34.4	–
2.32.0	2.34.4	
2.33.x	2.34.4	
2.34.x	2.35.6	See *Upgrading Control Center from Version 2.34*.

Continued

Source version	Target version	Note
2.35.x	4.3.0	
2.36.x	4.3.0	
3.0.x	4.3.0	
3.1.x	4.3.0	
3.2.x	4.3.0	See **"Special Procedures for Upgrade to 3.0 or Later" on page 3** .If you are upgrading from Release 4. 1.X or earlier releases to Release 4.3, you need to upgrade the Ubuntu version to 22.04. See *Alternative Upgrade Procedure*.
3.3.x	4.3.0	
3.4.x	4.3.0	
4.0.x	4.3.0	
4.1.x	4.3.0	
4.2.x	4.3.0	

To contact Juniper technical support,at **support.juniper.net/support/requesting-support.** .

Please also contact technical support whenever you want to upgrade from a version or between versions that are EoS.

Release Notes

Before starting the upgrade, please always read the Release Notes for the version you are upgrading to. These notes describe new features and also inform you of important under-the-hood changes such as new configuration files.

If you are upgrading across multiple versions, please read the Release Notes for all intermediate versions.

Special Upgrade Procedures

Special Procedures for Upgrade to 4.3

When upgrading to version 4.3, you need to follow the document Upgrading Control Center to 4.3 rather than the present generic upgrade guide.

Special Procedures for Upgrade to 3.0 or Later

Obtaining a License
On upgrading to version 3.0 or later, you need a new license from Juniper Networks to be able to use the product.

To prevent Control Center 7own in conn cn with the upgrade, we recommend that you obtain the new license before doing the upgrade. To get the license from the Juniper EMS Portal, you need to provide the UUID of the system where Control Center is installed.

- Run this command on the Control Center machine:

  ncc license license-request

  The output includes a UUID in plain-text format.
- Log in to the Juniper EMS Portal at l**icense.juniper.net/licensemanage/** with the credentials you have received from Juniper.
- In the **My Product Licenses** view, click the **Activate** button for the relevant license.
- In the dialog that appears, under SW Version, leave the default choice 3.0 and Above.
- Under Universal Unique ID (UUID), enter the UUID string you generated with the ncc license license- request command.
- Click the Activate button at the bottom of the screen.
- A license key will now be generated. Download it and save it as a plain-text file cc_license.txt.
- Perform the Paragon Active Assurance upgrade according to the present document.
- Finally, activate the license in Control Center using the command

  ncc license activate cc_license.txt

Plugin Configuration File
This version introduces a new configuration file **/etc/netrounds/plugin.yaml**. During installation, this file needs to be updated with the correct database connection details if the latter have been changed from the default.

Special Procedure for Upgrade from

The upgrade from 2.34 to any release up to 3.3 involves an Ubuntu upgrade from version 16.04 to version 18.04. It is covered in the document Upgrading Control Center from Version 2.34.

Finding Out Your Paragon Active Assurance Software Version

To find out what version of Paragon Active Assurance you currently have installed, you can use this command:
dpkg -l | grep paa

Upgrade Procedure

⚠️ **WARNING**: If you are upgrading from 2.34, please make sure you use the special upgrade procedure described in the document Upgrading Net rounds Control Center from Version 2.34.

If you have previously upgraded from 2.34 and are now going to upgrade to 3.0 or later, you must begin by undoing a step performed in the 2.34 upgrade. Run this command:

sudo apt-mark unhold python-django python-django-common

You can then follow the instruction below.

Below are general instructions for upgrading Control Center. Note that for specific releases, additional actions may be required; separate instructions are then given in each case in what follows.

Be sure to refer to the current Installation Guide.

- Disable the apache 2 and netrounds-executioner services completely:

   sudo systemctl disable apache2

   sudo systemctl disable netrounds-callexecuter
- Stop all Paragon Active Assurance services:

   sudo systemctl stop "netrounds-*" apache2 openvpn@netrounds
- Make backups according to the Operations Guide, chapter Backing Up Product Data, starting with the section "Backing Up the PostgreSQL Database".
- **Verify the integrity** of the tarball containing the new Control Center version:

   # Compute the checksum for the tar file and verify that it is equal to the SHA256

   # checksum provided on the download page

   export CC_BUILD=4.4.0.12

   sha256sum paa-control-center_${CC_BUILD}.tar.gz
- **Unpack the Control Center tarball:**

   tar -xzf paa-control-center_${CC_BUILD}.tar.gz
- Install new Control Center packages.

   In the CV; /etc/netrounds/netrounds.conf you can optionally configure the SPEEDIEST_ADDRESS s;■n] (if you're going to use Speedtest). This can either point to the same IP address that SITE_URL resolves to, or it can have a host name of its own.

⚠️ **WARNING:** You will now be prompted about overwriting existing configuration files. Before proceeding, please read all the information about settings below.

📶 **NOTE:**

- We highly recommend that you first inspect the difference between your old configuration and the new one using the "D" choice. In most cases you will then want to keep your old settings by pressing "N" (do not

overwrite).

- New optional and updated settings may be available in the example configuration files provided in the packages. We recommend that you review these and add new options as appropriate for your installation.

⚠ **WARNING:** For the Apache configuration files found in
/etc/apache2/sites-available/

you need to press "Y", which is the "package maintainer's version".

If you have installed proper SSL certificates (as recommended) instead of the default snake oil ones, you will have to modify the file again to point to the correct path in the SSL Certificate File and SSL Certificate Key File settings after the Debian package installation has completed. See the Installation Guide, chapter Service Configuration, section "SSL Certificate Configuration".
sudo apt-get update
sudo apt-get install ./paa-control-center_${CC_BUILD}/.deb*

- Run the database Migration

  ⚠ **WARNING:** If you have changed the database password from the default, make sure you also change this in the db-password setting in the **/etc/netrounds/plugin.yaml** file before running ncc migrate. Otherwise, the command will fail.

  NOTE:
    - This is a sensitive command, and care should be taken when executing it on a remote machine. In such a scenario it is strongly recommended that you use a program like screen (generally installed by default on popular Linux distributions) or tmux (run sudo apt-get install tmux to install) so that the migrate command will continue running even if the ssh session breaks.
    - This command takes considerable time to execute.
      sudo ncc migrate
- **Restart** all Paragon Active Assurance services:
  sudo ncc services restart
- **Install the new Test Agent repository and plugins**
  The plugins are used by Test Agent Applications
  TA_APPLIANCE_BUILD=4.4.0.12
  TA_APPLICATION_BUILD=4.4.0.12
  PLUGIN_BUILD=4.4.0.24# Compute checksum for the repositories and verify that they match the
  # SHA256 checksum provided on the download page
  sha256sum paa-test-agent_${TA_APPLIANCE_BUILD}_all.deb
  sha256sum paa-test-agent-application_${TA_APPLICATION_BUILD}_all.deb
  sha256sum paa-test-agent-plugins_${PLUGIN_BUILD}_all.deb# Start the installation
  sudo apt-get install ./paa-test-agent_${TA_APPLIANCE_BUILD}_all.deb
  sudo apt-get install ./paa-test-agent-application_${TA_APPLICATION_BUILD}_all.deb
  sudo apt-get install ./paa-test-agent-plugins_${PLUGIN_BUILD}_all.deb
- **Enable** services as follows:
  sudo ncc services enable apache2
  sudo ncc services enable kafka
  sudo ncc services enable callexecuter

- Restart all Paragon Active Assurance services:

  NOTE: You must do this to get the services up and running again after the upgrade.

  sudo ncc services restart
- To activate the new configuration, you also need to run:

  sudo systemctl reload apache2
- Check that the system is up and running with the commands

  ncc status

  sudo systemctl status "netrounds-"*
- Run the following script to enable the latest version of all plugins in all accounts:

  export PORT=49900

  while true; do

  if netstat -lnt | grep ":$PORT " > /dev/null; then

  echo "$(date): Plugin service is listening on port $PORT"

  echo "Enabling latest plugins for all accounts"

  sudo ncc plugins edit enabled-version –all-plugins –latest-version –all-accounts —

  exit-on-failure=false –verbose

  break

  fi

  echo "Waiting for plugin service listening on $PORT"

  sleep 3

  done

  If you encounter the following error after you run the script, create a support case by attaching the script output in order to troubleshoot the error.

  2023-11-17T09:22:46Z ERR ../../app/api/handlers/update_plugin.go: 246 > Failed to change enabled plugin version error="unknown account short name account_name" host-ip-10-0-0-11 service-plugin-service short_name=account_name src=core

  For more information on how to manage plugins using the Control Center CLI, see the in-app help under "Plugins".
- Log in to the Control Center GUI and go to the Test Agents view. Next to each Test Agent for which an upgrade is available, an up-arrow icon appears. Click that icon to go ahead with the upgrade.

Troubleshooting

Password Authentication Failed For User
If the ncc migrate command fails with an error message

Failed to connect to database error="pq: password authentication failed for user \"netrounds\"" db-host=localhost db-name-paa-plugins db-port=5432 …

you must update the variable db-password in the /etc/netrounds/plugin.yaml file as explained in the "warning above" on page 7. Edit this file and then rerun ncc migrate.

Target WSGI Script Not Found
If you accidentally selected "N" for the Apache configuration files (see "this step above" on page 6) and got an error message like the one below

wsgi:error] [pid 29401:tid 140567451211520] [client 127.0.0.1:37172] Target WSGI script not found or unable to stat: /usr/lib/python2.7/dist-packages/netrounds/wsgi.py

run the following commands to get back on track:
export CC_BUILD=4.4.0.12
dpkg-deb –fsys-tarfile paa-webapp_${CC_BUILD}_all.deb | tar -x –wildcards ./etc/apache2/sitesavailable/.conf –strip-components 4*
sudo mv netrounds.conf /etc/apache2/sites-available/*
sudo chown -R root:root /etc/apache2/sites-available/
sudo systemctl reload apache2

This overwrites the old configuration with the new one in the updated package.

Again, if you have installed proper SSL certificates (as recommended) instead of the default snakeoil ones, you will have to modify the file again to point to the correct path in the SSL Certificate File and SSL Certificate Key File settings after the Debian package installation has completed. See the Installation Guide, chapter Service Configuration, section "SSL Certificate Configuration".

Same Origin Policy Disallows Reading the Remote Resource
This or some similar error may occur if you have set SITE_URL and SPEEDIEST_ADDRESS to different values in/etc/netrounds/netrounds.conf. You then need to change ALLOWED_ORIGINS in **/etc/netrounds/restol.conf to**

allow both of these values in the restol.conf file. The simplest way to achieve this is to delete any value previously assigned to ALLOWED_ORIGINS. That setting will then get a default value which allows SITE_URL and SPEEDIEST_ADDRESS as found in /etc/netrounds/netrounds.conf.

Test Agent Appliance Does Not Come Online After Control Center Upgrade
If you upgrade Control Center 3.1 or 3.2 to version 3.3 or later and you are using Test Agent Appliance 3.3, it may happen that a Test Agent Appliance on which a Test Agent Application is run (this is supported from version 3.3.1 onward) will not come online but remain gray in Control Center. This is because traffic on port 6800 is filtered by a DROP rule.

Resolve this issue by running the following command on the Control Center machine:
sudo iptables -I INPUT -i tun0 -p tcp –dport 6800 -j ACCEPT

Rollback in Case of Failed Upgrade

If a Control Center upgrade fails, here is how to return the system to its state immediately before the upgrade:

- Make a clean Ubuntu installation according to the Installation Guide, chapter Installing Required OS and Software.
- Install the version of Control Center that you were using before the upgrade. Again, follow the Installation Guide, chapter Installing Control Center and Related Tasks.
- Recover your data from backup as explained in the Operations Guide, chapter Restoring Product Data from Backup.

Applying Ubuntu Updates

NOTE: If you want to apply updates to Ubuntu 22.04, you first need to hold rrd packages with the command
.

sudo apt-mark hold librrd8 python3-rrdtool rrdtool

Then you can apply the updates with

sudo apt dist-upgrade

The hold command is necessary because the or;r-■n] system will by default remove Paragon Active Assurance packages:

(output from sudo apt dist-upgrade below)

The following packages will be REMOVED:
paa-callexecuter paa-common paa-license-daemon paa-test-agent-compact paa-test-agent-login paawebapp
The following packages will be upgraded:
librrd8 python3-rrdtool rrdtool
3 upgraded, 0 newly installed, 6 to remove and 0 not upgraded.

Note on Control Center YANG Models

Upgrading Control Center, and specifically the netrounds-confd_<version>_all.deb package, may replace the Control Center YANG model with a newer version. This is relevant for orchestration solutions which rely on that YANG model and on the NETCONF & YANG API. The Control Center YANG model
netrounds- ncc.yang is found under **/opt/netrounds-confd/.**

JUNIPER
NETWORKS

Documents / Resources

	Juniper NETWORKS 4.4 Paragon Active Assurance Upgrade [pdf] Instructions 4.4 Paragon Active Assurance Upgrade, 4.4 Paragon Active Assurance Upgrade, Active Assurance Upgrade, Assurance Upgrade, Upgrade

References

- 🌐 **license.juniper.net/licensemanage/**
- 🌐 **license.juniper.net/licensemanage/**
- **User Manual**