

Baselines

- [Introduction](#)
- [How Does it Work?](#)
- [Details](#)
 - [Software](#)
 - [Netstat Ports](#)
 - [Users](#)
- [Creating a Baseline Definition](#)
- [Executing a Baseline Definition](#)
- [API / Web Access](#)

Introduction

Being able to determine which machines are configured in the same way is a major part of systems administration and auditing – and now reporting on that will be made simple and automated. Once you define your baseline it will automatically run against a set of devices on a predetermined schedule. The output of these executed baselines will be available for web viewing, importing into a third party system or even as a printed report.

How Does it Work?

Baselines enable you to combine audit data with a set of attributes you have previously defined (your baseline) to determine compliance of devices.

For example - you might create a baseline from a device running Centos 6 which acts as one of your Apache servers in a cluster. You know this particular server is configured just the way you want it but you're unsure if other servers in the cluster are configured exactly the same. Baselines enables you to determine this.

You can create a baseline, run it against a group of devices and view the results, add scheduled execution, add more tables for comparison (currently only software, netstat ports and users are enabled), in place baseline editing, archiving of results and more.

WARNING - When creating a baseline using software policies, at present Centos and RedHat package the kernel using the names 'kernel' and 'kernel-devel'. There can be multiple packages with this name and different versions concurrently installed. Debian based distributions use names like 'linux-image-3.13.0-24-generic', note the version number is included in the package name. Because RedHat based OS's use this format and subsequently have multiple identical package names with different versions we currently exclude 'kernel' and 'kernel-devel' from software policies. This may be addressed in a future update.

Details

Baselines can compare netstat ports, users and software.

Software

To compare software we check the name and version. Because version numbers are not all standardised in format, when we receive an audit result we create a new attribute called software_padded which we store in the database along with the rest of the software details for each package. For this reason, baselines using software policies will not work when run against a device that has not been audited by 1.10 (at least). Software policies can test against the version being "equal to", "greater than" or "equal to or greater than".

Netstat Ports

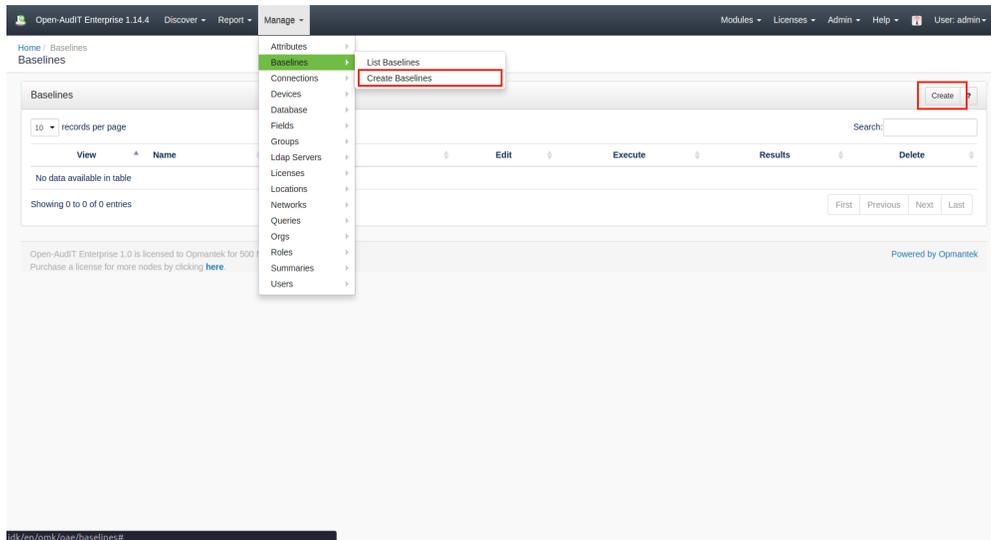
Netstat Ports use a combination of port number, protocol and program. If all are present the policy passes.

Users

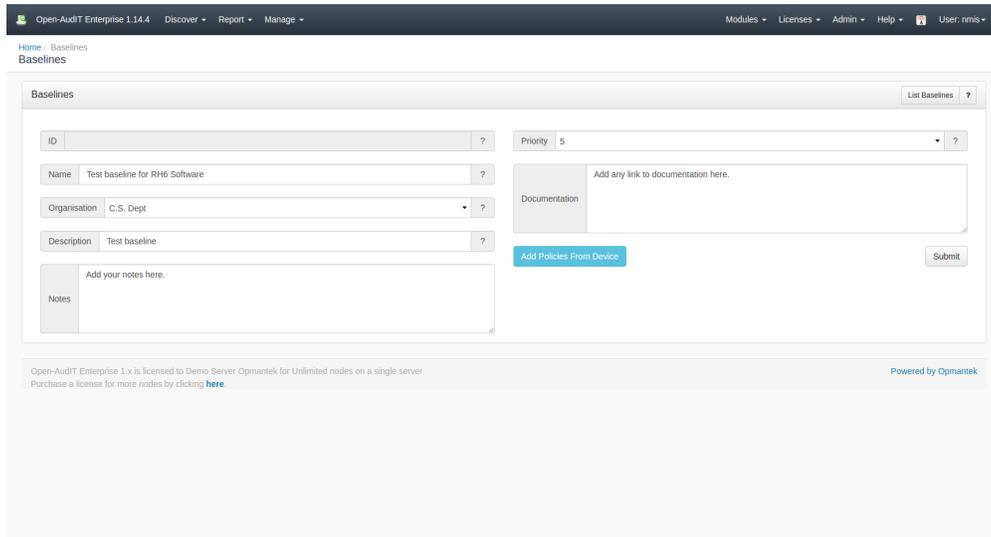
Users work similar to Netstat Ports. If a user exists with a matching name, status and password details (changeable, expires, required) then the policy passes.

Creating a Baseline Definition

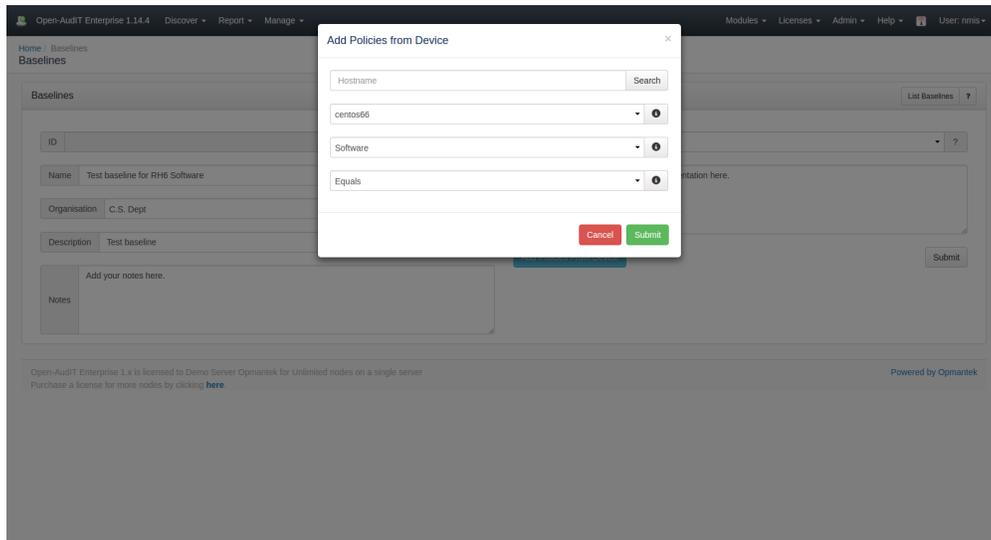
A baseline can be created using the web interface if a user has a role that contains the baselines::create permission. Go to menu: Manage -> Baselines -> Create Baselines. There is also a create button on the collection page.



You must enter a (preferably unique) name and then the "Add policy from device" button will be enabled.



Click this button and a modal will appear.



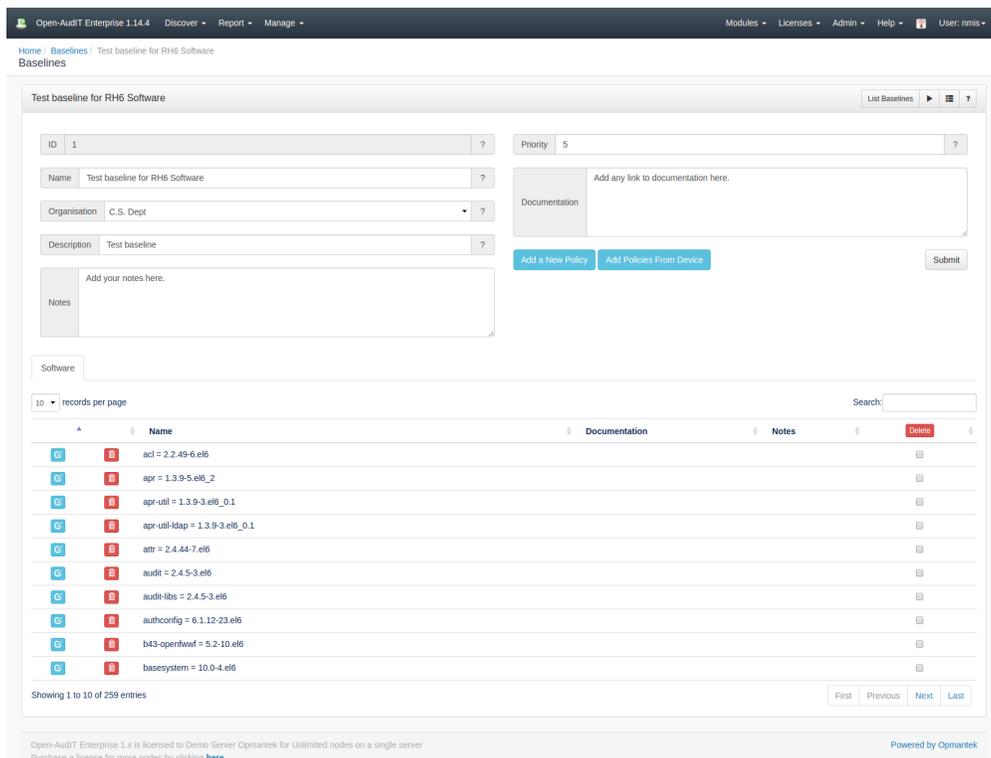
Type in a hostname and click Search to populate the dropdown to enable you to choose a device to extract policies from.

Choose a device from the drop down, a table from the dropdown and a comparison operator.

The comparison operator only really works for software at this stage. Both netstat ports and users work on the principle of it exists so it must match.

Software though compares the package name and version. If you would like the policy to test for SSH "at least" version 1.2.3, click the "Equals or Greater Than" comparison operator. Checking if a name and version match exactly, click the "Equals" operator.

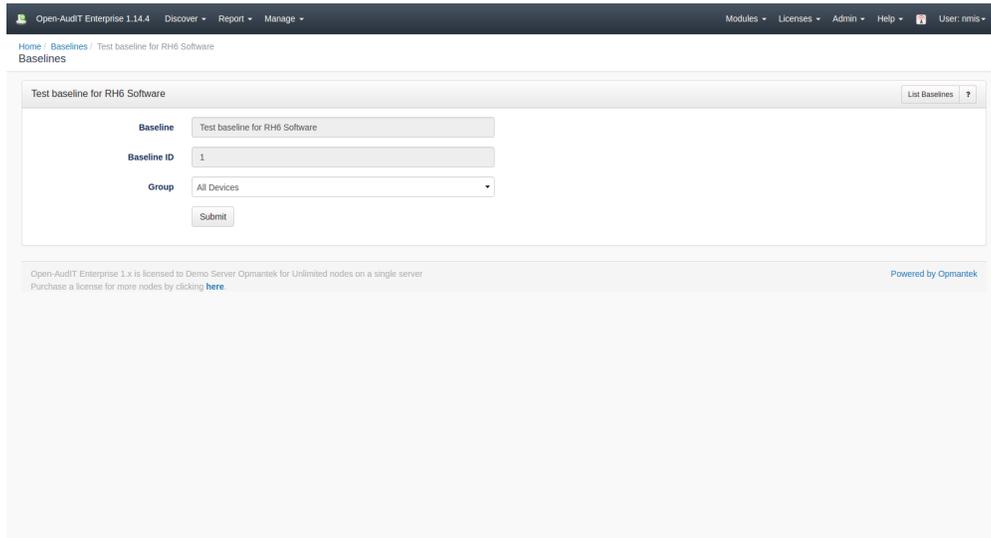
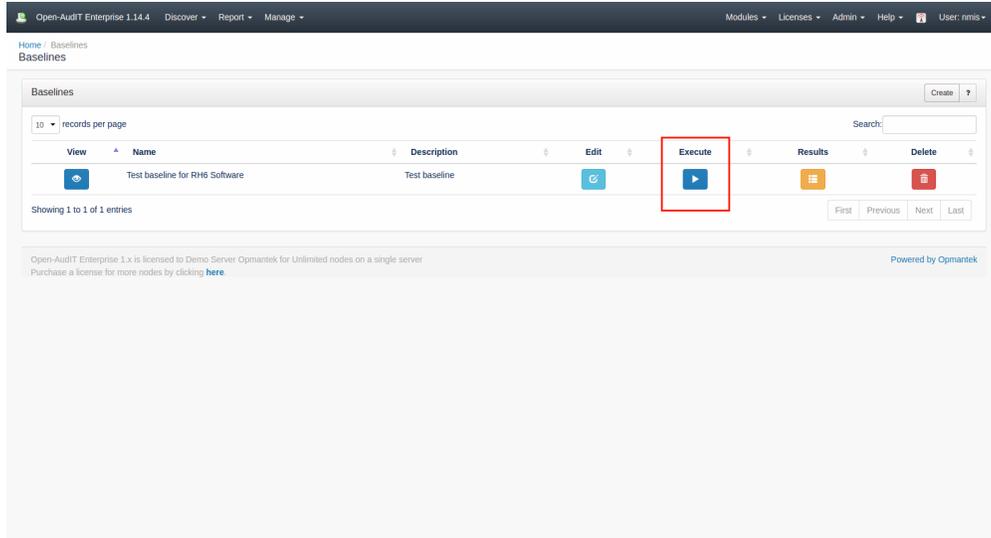
Once you click Submit, the baseline will be created and the policies will be added. You will then be sent to the Edit Baseline screen where you can add further policies from a device if required.



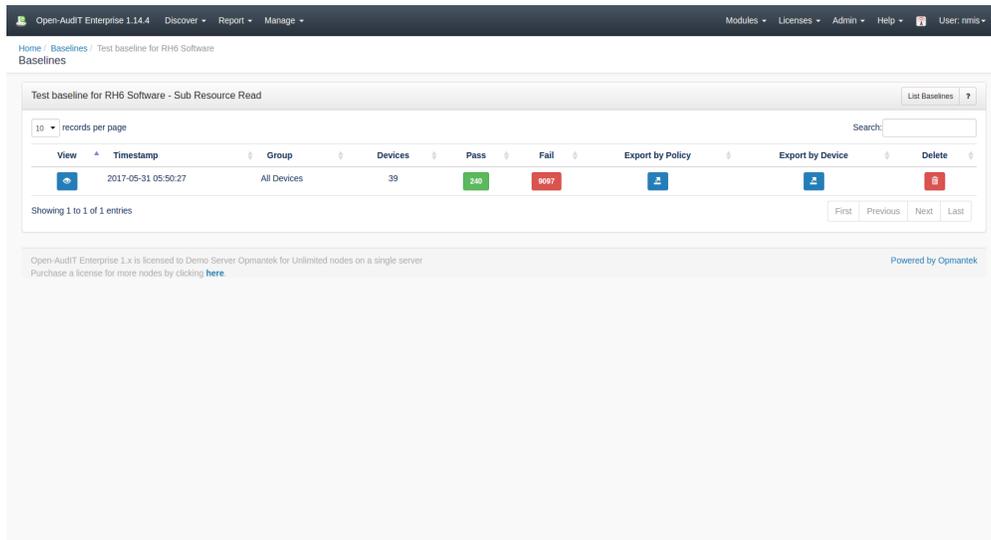
Executing a Baseline Definition

Once you have created your baseline and added some policies, you can execute it against a group of devices. When executing a baseline, bear in mind that baselines will only really provide useful information when the policies are matched to the specific operating system the baseline is executed against. IE - Don't create a baseline and add policies from a Windows Server and expect a group of devices containing Debian computers to match anything!

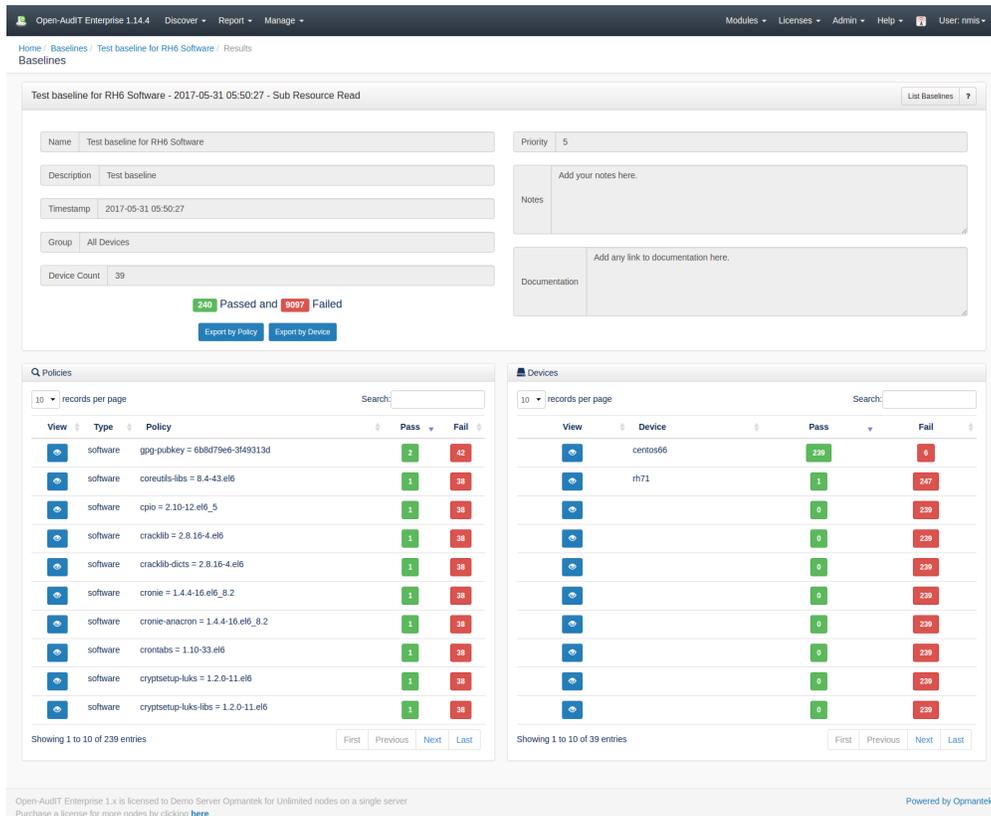
From the Baseline list page, click on the Execute button. The next screen will enable you to choose a group of devices to execute the baseline on.



Once a baseline has been executed you will be directed to the baseline results page. This page lists all the results from any given baseline.



Clicking the Results button will show you the results from this particular baseline result.



From the result page you can click an individual policy or device to view more details.

The policy detailed result is below.

Open-Audit Enterprise 1.14.4 Discover Report Manage Modules Licenses Admin Help User: nmis

Home Baselines Test baseline for RH6 Software Results 2017-05-31 05:50:27

Baselines

Test baseline for RH6 Software - 2017-05-31 05:50:27 - Sub Resource Read List Baselines

Name: Test baseline for RH6 Software Priority: 5

Description: Test baseline

Timestamp: 2017-05-31 05:50:27

Group: All Devices

Device: rh71

Notes: Add your notes here.

Documentation: Add any link to documentation here.

1 Passed and 247 Failed

Q Policies

100 records per page Search: 6b8d79e6

View	Type	Policy	Test 1	Test 2	Test 3	Status	Update
	software	gpg-pubkey = 6b8d79e6-3f49313d	gpg-pubkey	6b8d79e6-3f49313d		✓	
	software	gpg-pubkey = 6b8d79e6-3f49313d	gpg-pubkey	f431d51-4ae0493b		✗	Update
	software	gpg-pubkey = c105b9de-4e0fd3a3	gpg-pubkey	6b8d79e6-3f49313d		✗	Update
	software	gpg-pubkey = 0608b895-4bd22942	gpg-pubkey	6b8d79e6-3f49313d		✗	Update
	software	gpg-pubkey = 6b8d79e6-3f49313d	gpg-pubkey	352c64e5-52ae6884		✗	Update
	software	gpg-pubkey = 6b8d79e6-3f49313d	gpg-pubkey	2fa658e0-45700c69		✗	Update

Showing 1 to 6 of 6 entries (filtered from 248 total entries)

Open-Audit Enterprise 1.x is licensed to Demo Server OpmanTek for Unlimited nodes on a single server. Purchase a license for more nodes by clicking [here](#). Powered by OpmanTek

The device detailed result is below.

Open-Audit Enterprise 1.14.4 Discover Report Manage Modules Licenses Admin Help User: nmis

Home Baselines Test baseline for RH6 Software Results 2017-05-31 05:50:27

Baselines

Test baseline for RH6 Software - 2017-05-31 05:50:27 List Baselines

Name: Test baseline for RH6 Software Priority: 5

Description: Test baseline

Timestamp: 2017-05-31 05:50:27

Group: All Devices

Policy: gpg-pubkey = 6b8d79e6-3f49313d

Notes: Add your notes here.

Documentation: Add any link to documentation here.

2 Passed and 42 Failed

Q Devices

10 records per page Search:

View	Device	Name	Version	Status	Update
	centos66	gpg-pubkey	0608b895-4bd22942	✗	Update
	rh71	gpg-pubkey	2fa658e0-45700c69	✗	Update
	rh71	gpg-pubkey	352c64e5-52ae6884	✗	Update
	centos66	gpg-pubkey	6b8d79e6-3f49313d	✓	
	rh71	gpg-pubkey	6b8d79e6-3f49313d	✓	
	centos66	gpg-pubkey	c105b9de-4e0fd3a3	✗	Update
	rh71	gpg-pubkey	f431d51-4ae0493b	✗	Update
				✗	
				✗	
				✗	

Showing 1 to 10 of 44 entries

Open-Audit Enterprise 1.x is licensed to Demo Server OpmanTek for Unlimited nodes on a single server. Purchase a license for more nodes by clicking [here](#). Powered by OpmanTek

The results can be exported by policy or by devices, a CSV file will be generated.

Open-Audit Enterprise 1.14.4 Discover Report Manage Modules Licenses Admin Help User: rnis

Home / Baselines / Test baseline for RH6 Software
Baselines

Test baseline for RH6 Software - Sub Resource Read List Baselines ?

10 records per page Search:

View	Timestamp	Group	Devices	Pass	Fail	Export by Policy	Export by Device	Delete
	2017-05-31 11:21:24	All Devices	39	240	9997			

Showing 1 to 1 of 1 entries First Previous Next Last

Open-Audit Enterprise 1.x is licensed to Demo Server Opmantek for Unlimited nodes on a single server
Purchase a license for more nodes by clicking [here](#) Powered by Opmantek

API / Web Access

Baselines do not at this time support the JSON API. This will be enabled in a future release.