Baselines

- Introduction
- How Does it Work?
- Details
    - Software
    - Netstat Ports
    - Users
- Creating a Baseline Definition
- Executing a Baseline Definition
- Database Schema
- 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

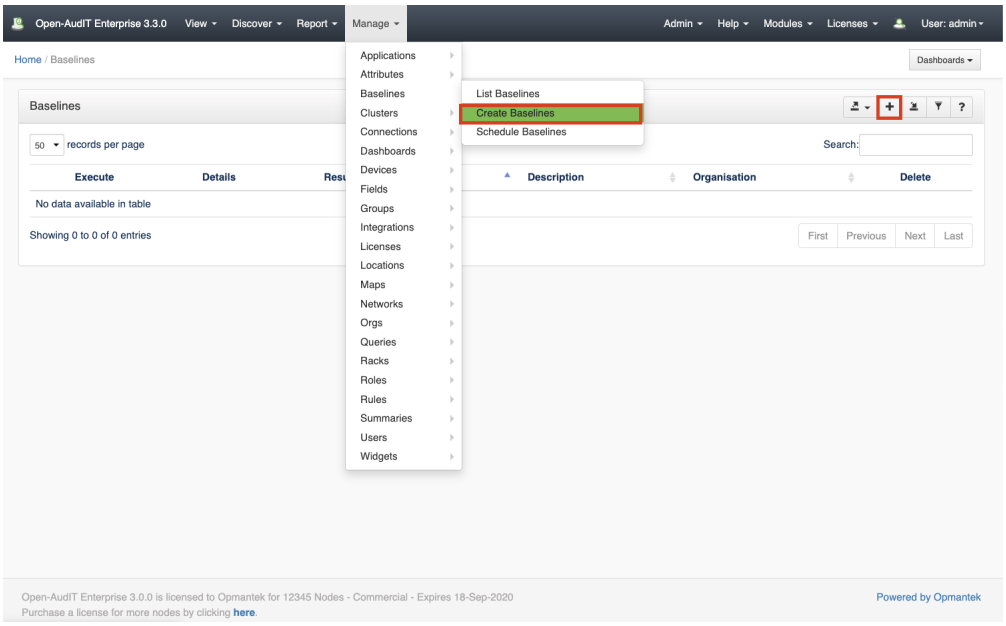
Netstat Ports use a combination of port number, protocol and program. If all are present the policy passes.

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.



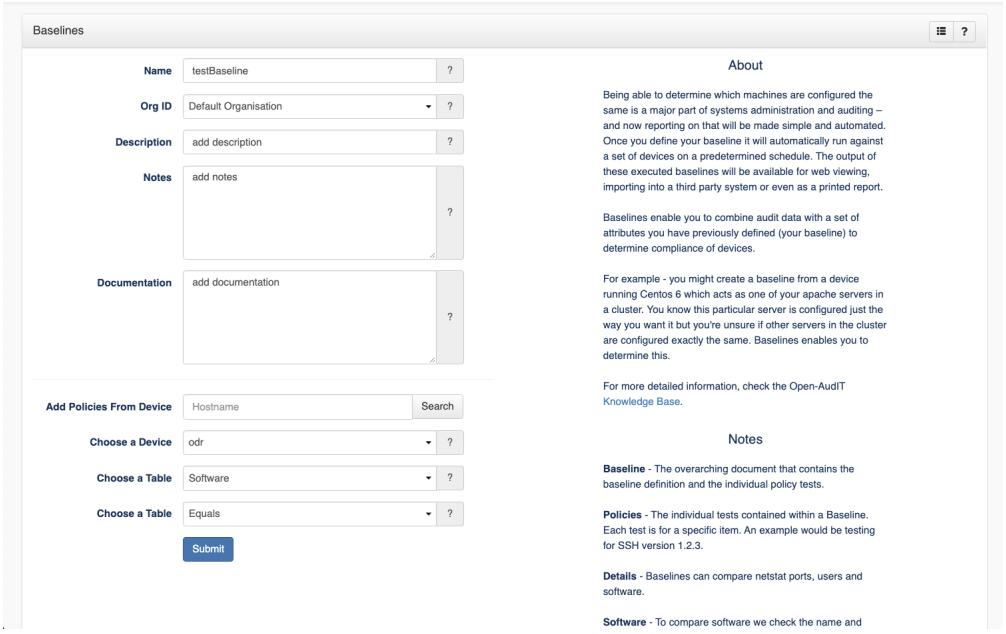
You must enter a (preferably unique) name.

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

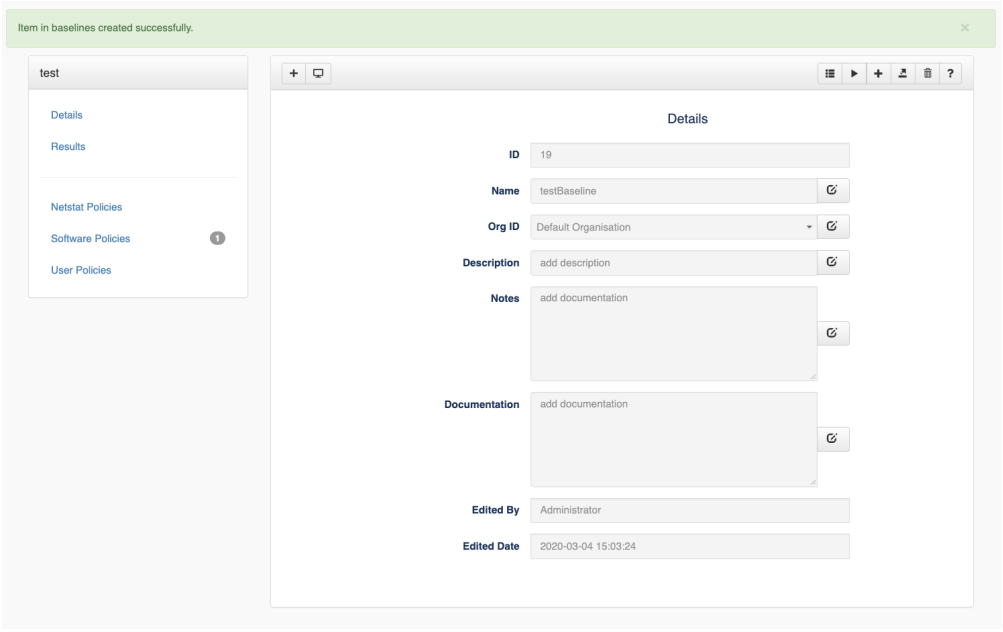
Choose a device from the drop down, a table from the dropdown and a comparison operator.

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.



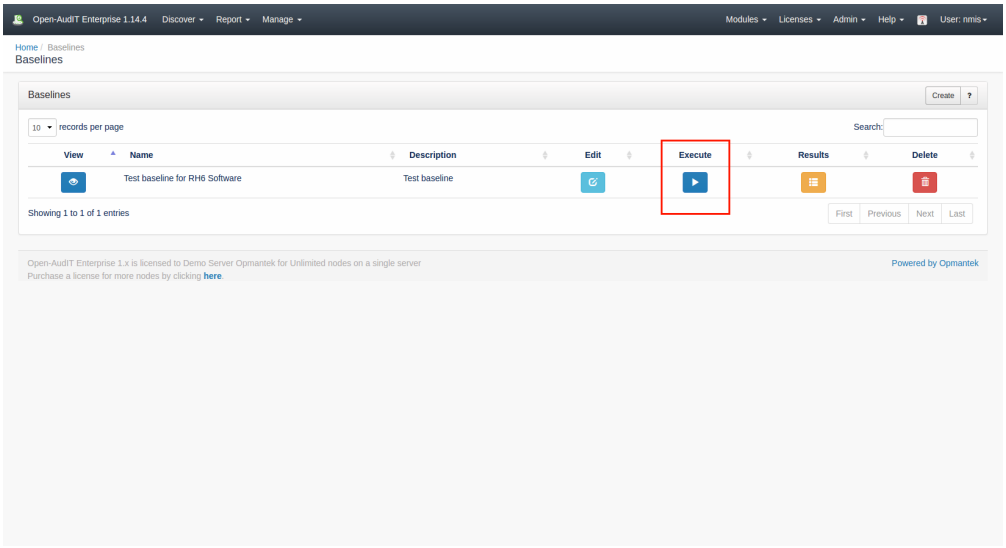
Once you click Submit, the baseline will be created and the policies will be added. You will then be sent to the Edit Baseline screen where you can add further policies from a device if required.

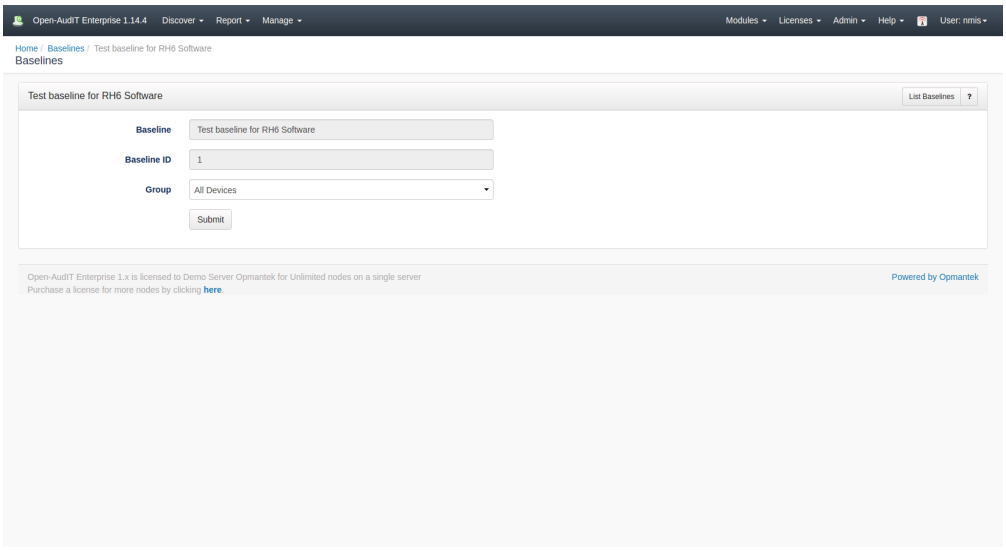


Executing a Baseline Definition

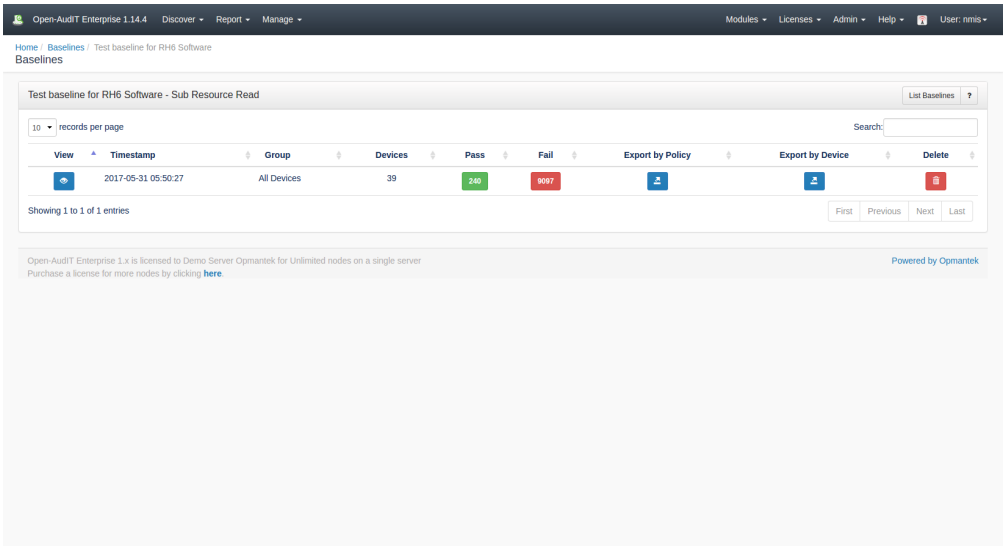
Once you have created your baseline and added some policies, you can execute it against a group of devices. When executing a baseline, bear in mind that baselines will only really provide useful information when the policies are matched to the specific operating system the baseline is executed against.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

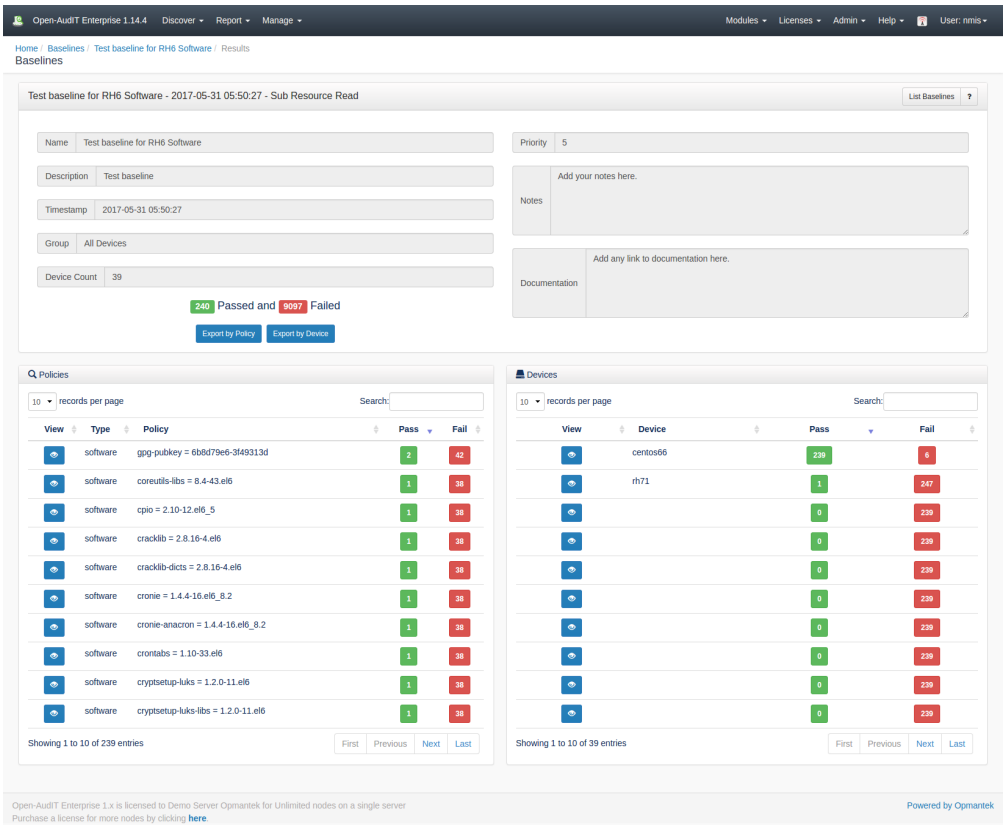




Once a baseline has been executed you will be directed to the baseline results page. This page lists all the results from any given baseline.

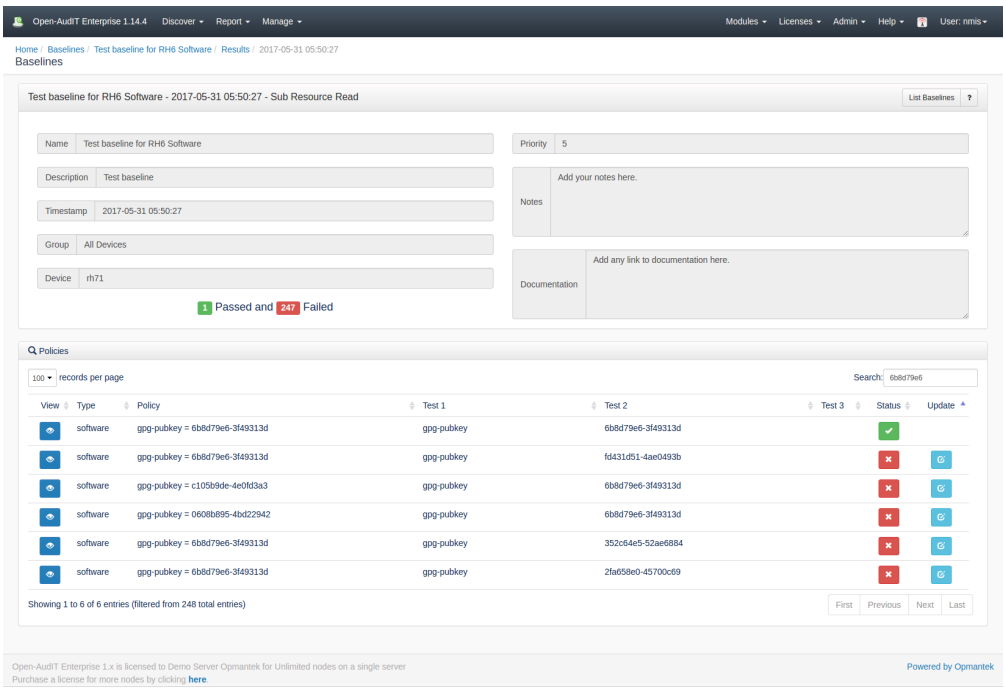


Clicking the Results button will show you the results from this particular baseline result.

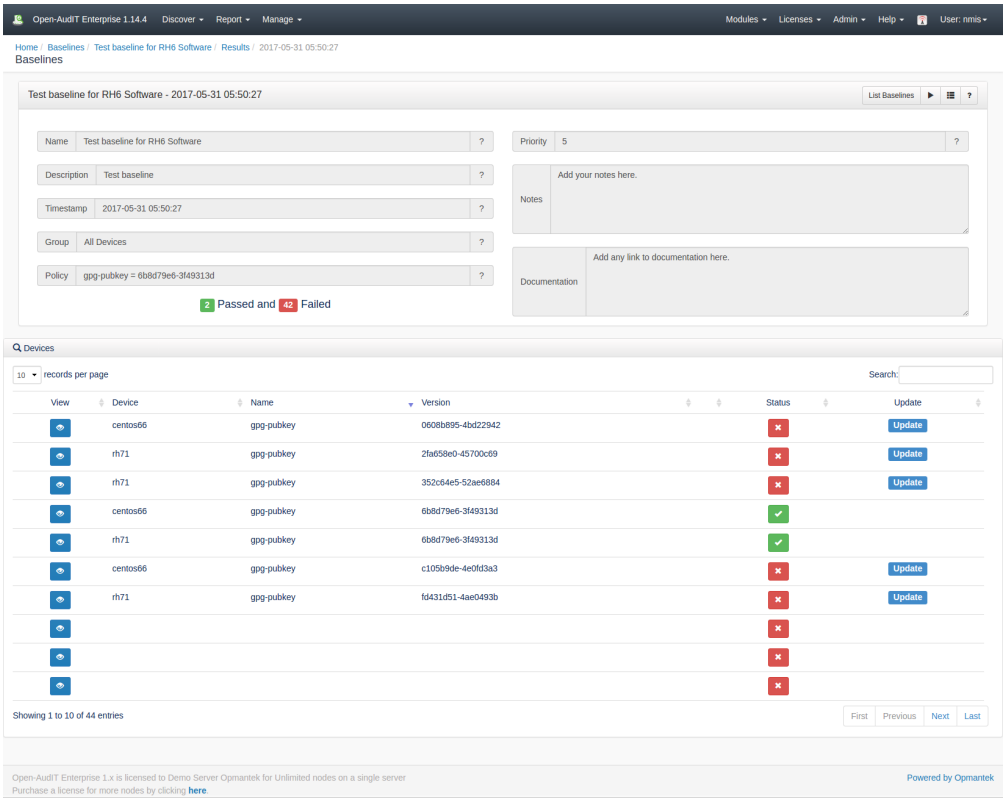


From the result page you can click an individual policy or device to view more details.

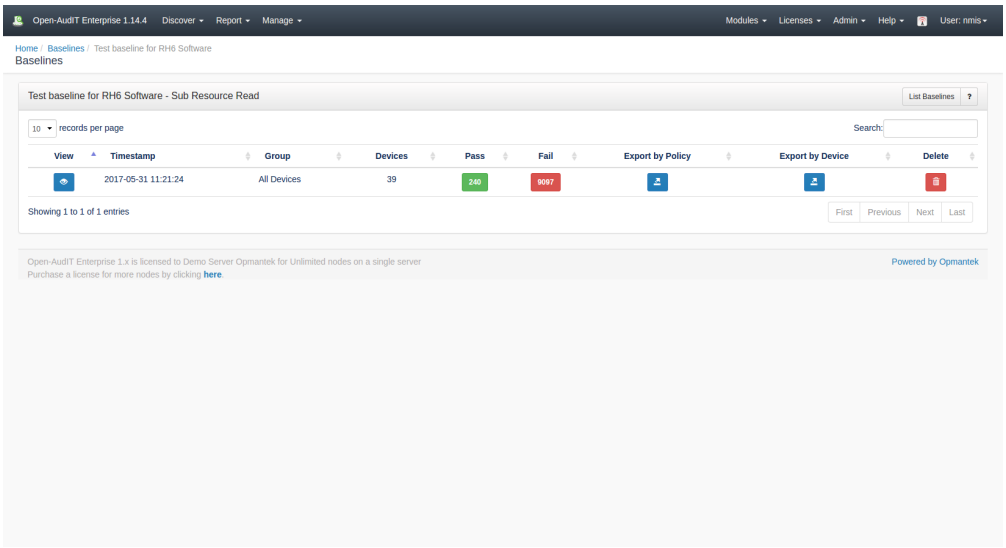
The policy detailed result is below.



The device detailed result is below.



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



Database Schema

The database schema can be found in the application is the user has database::read permission by going to menu: Admin -> Database -> List Tables, then clicking on the details button for the table.

API / Web Access

You can access the collection using the normal Open-AudIT JSON based API. Just like any other collection. Please see The Open-AudIT API documentation for further details.