

Baselines (Extended Info)

- [Introduction](#)
 - [Software](#)
 - [Netstat Ports](#)
 - [Users](#)
- [Baseline Creation](#)

DEPRECATED AT AT v2. See [Baselines](#).

Introduction

Starting in Open-Audit 1.10 we are introducing a new feature - Baselines.

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.

Our initial release (in 1.10) is functional but not yet complete. You can create a baseline, run it against a group of devices and view the results. We plan to add scheduled execution (done in 1.12), more tables for comparison (currently only software, netstat ports and users are enabled), in place baseline editing, archiving of results and more.

Terms:

Baseline - the overarching document that contains the baseline definition and the individual policy tests.

Policies - The individual tests contained within a Baseline. Each test is for a specific item. An example would be testing for SSH version 1.2.3.

Read on to learn how to create and execute a Baseline!

NOTE - Clicking an image will show a full size version of it.

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

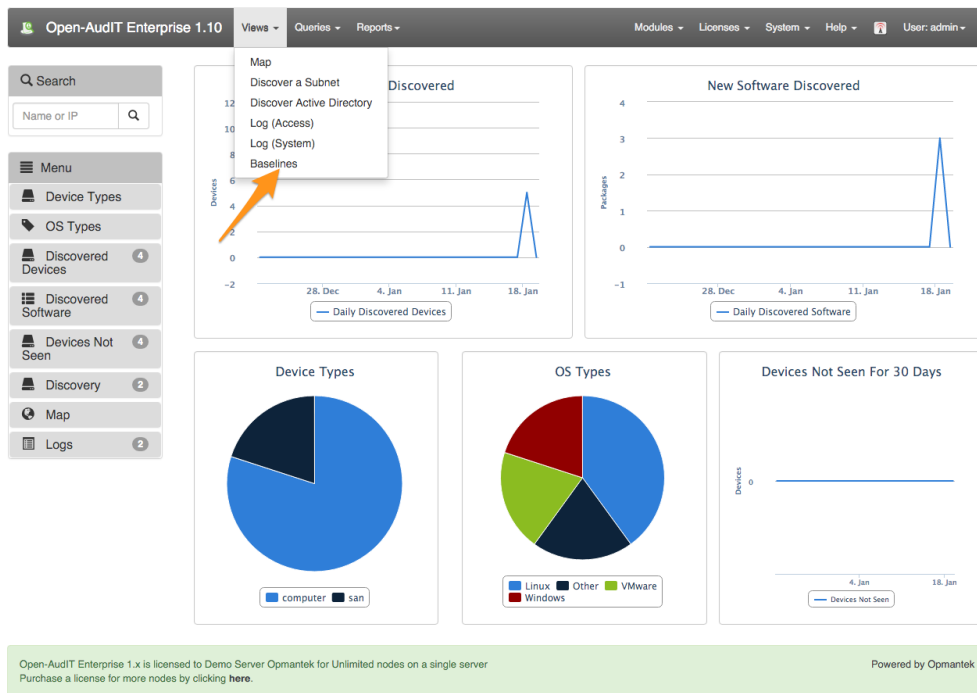
Netstat Ports use a combination of port number, protocol and program. If all are present the policy passes.

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.

Baseline Creation

Initially you will need to create a baseline definition. You can reach the GUI for this in Open-Audit Enterprise by clicking on menu -> Views -> Baselines.



This will bring you to a listing of all your currently defined Baselines.

The screenshot shows the 'Baselines' page in Open-AuditIT Enterprise 1.10. It features a 'Current Baselines' section with a 'Create' button and a search bar. Below is a table with one entry: 'Test Baseline for RH6 software'. The table has columns for 'ID', 'Name', and 'Actions'. The 'Actions' column contains buttons for 'View', 'Edit', 'Delete', 'Results', and 'Execute'. The page also includes a 'records per page' selector set to 10 and pagination controls at the bottom. The footer indicates the software is powered by Opmantek.

| ID | Name | Actions |
|----|--------------------------------|--|
| 1 | Test Baseline for RH6 software | View Edit Delete Results Execute |

Clicking the Create button on the right side will send you to the Create Baseline screen.

Open-AuditIT Enterprise 1.10

Views ▾Queries ▾Reports ▾

Modules ▾Licenses ▾System ▾Help ▾

User: admin ▾

Baselines

Baseline Details

ID

?

Name

The baseline name (required)

?

Description

The baseline description

?

Notes

Priority

5

?

Documentation

Add a New Policy

Add Policies From Device

Submit

Open-AuditIT 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

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

Open-AuditIT Enterprise 1.10

Views ▾Queries ▾Reports ▾

Modules ▾Licenses ▾System ▾Help ▾

User: admin ▾

Baselines

Baseline Details

ID

?

Name

Test Baseline for RH6 software

?

Description

The baseline description

?

Notes

Priority

5

?

Documentation

Add a New Policy

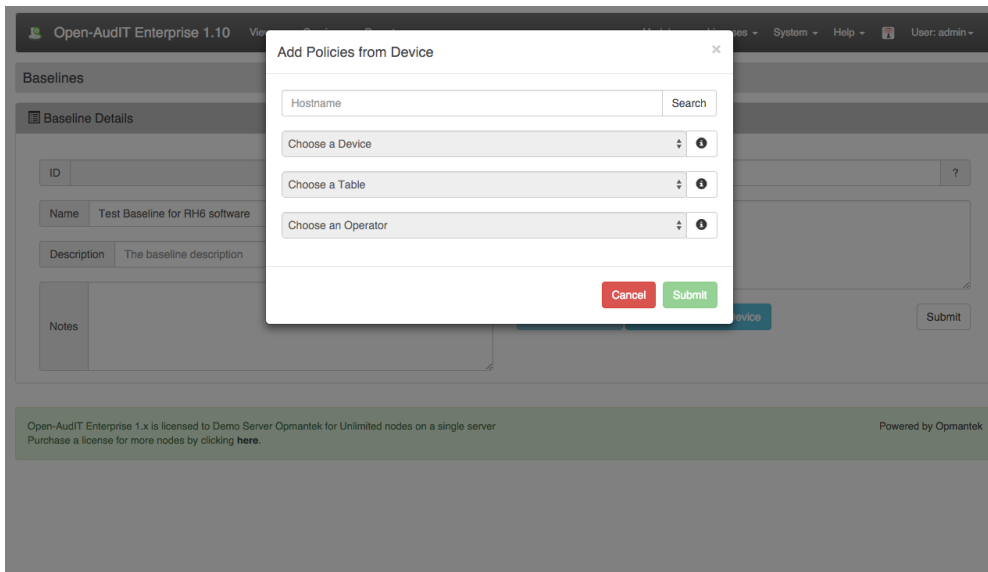
Add Policies From Device

Submit

Open-AuditIT 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

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.

We plan to enable individual policy editing in a soon to be release version (post 1.10).

Open-Audit Enterprise 1.10
Views
Queries
Reports
Modules
Licenses
System
Help
User: admin

Baselines

Baseline Details

ID
1
?

Name
Test Baseline for RH6 software
?

Description
This is a test
?

Notes
If we want notes, put them here

Priority
5
?

Documentation
links to documentation (for example) go here

Add a New Policy
Add Policies From Device
Submit

Baseline Policies

Software
Netstat
User

10 records per page
Search:

| | | Name | Documentation | Notes |
|--------|--------|---|---------------|-------|
| Update | Delete | software, perl-Compress-Zlib = 2.021-141.el6 | | |
| Update | Delete | software, plymouth = 0.8.3-27.el6.centos.1 | | |
| Update | Delete | software, basesystem = 10.0-4.el6 | | |
| Update | Delete | software, pinentry = 0.7.6-8.el6 | | |
| Update | Delete | software, xorg-x11-fonts-Type1 = 7.2-11.el6 | | |
| Update | Delete | software, cryptsetup-luks = 1.2.0-11.el6 | | |
| Update | Delete | software, dejavu-lgc-serif-fonts = 2.33-1.el6 | | |
| Update | Delete | software, info = 4.13a-8.el6 | | |
| Update | Delete | software, dummy-package = 1.10 | | |
| Update | Delete | software, perl-Compress-Zlib = 2.003-141.el6 | | |

Showing 1 to 10 of 20 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

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.

Open-Audit Enterprise 1.10
Views
Modules
Licenses
System
Help
User: admin

Baselines

Execute Baseline

Baseline
Test Baseline for RH6 software

Baseline ID
1

Group
CentOS Linux Systems

Submit

Powered by Opmantek

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.

Open-AuditIT Enterprise 1.10

ViewsQueriesReports

ModulesLicensesSystemHelpUser: admin

Baselines

Baseline Results for Test Baseline for RH6 software

10 records per page

Search:

| Timestamp | Group | Devices | Pass | Fail | | |
|---------------------|----------------------|---------|------|------|---------|--------|
| 2016-01-19 14:30:01 | CentOS Linux Systems | 2 | 17 | 71 | Results | Delete |

Showing 1 to 1 of 1 entries

FirstPreviousNextLast

Powered by Opmantek

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

Open-AuditIT Enterprise 1.10

ViewsQueriesReports

ModulesLicensesSystemHelpUser: admin

Baselines

Baseline Result for Test Baseline for RH6 software run on 2016-01-19 14:30:01

NameTest Baseline for RH6 software?

DescriptionThis is a test?

Timestamp2016-01-19 14:30:01?

GroupCentOS Linux Systems?

Device Count2?

Priority5?

Notes

If we want notes, put them here

Documentation

links to documentation (for example) go here

17 Passed and 71 Failed

Q Policies

10 records per page

Search:

| Type | Policy | Pass | Fail |
|-----------------------------|--|------|------|
| View Policy | software software, perl-Compress-Zlib = 2.021-141.el6 | 0 | 2 |
| View Policy | software software, plymouth = 0.8.3-27.el6.centos.1 | 1 | 1 |
| View Policy | software software, basesystem = 10.0-4.el6 | 1 | 1 |
| View Policy | software software, pinentry = 0.7.6-8.el6 | 2 | 0 |
| View Policy | software software, xorg-x11-fonts-Type1 = 7.2-11.el6 | 1 | 1 |
| View Policy | software software, cryptsetup-luks = 1.2.0-11.el6 | 2 | 0 |
| View Policy | software software, dejavu-lgc-serif-fonts = 2.33-1.el6 | 1 | 1 |
| View Policy | software software, info = 4.13a-8.el6 | 2 | 0 |
| View Policy | software software, dummy-package = 1.10 | 1 | 1 |
| View Policy | software software, perl-Compress-Zlib = 2.003-141.el6 | 0 | 2 |

Showing 1 to 10 of 44 entries

FirstPreviousNextLast

Devices

10 records per page

Search:

| Device | Pass | Fail |
|-----------------------------|-------|------|
| View Device | dummy | 935 |
| View Device | thor | 836 |

Showing 1 to 2 of 2 entries

FirstPreviousNextLast

Powered by Opmantek

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 1.10

ViewsQueriesReports

ModulesLicensesSystemHelp

User: admin

Baselines

Baseline Result for Test Baseline for RH6 software run on 2016-01-19 14:30:01

Name

Test Baseline for RH6 software

?

Description

This is a test

?

Timestamp

2016-01-19 14:30:01

?

Group

CentOS Linux Systems

?

Policy

software, plymouth = 0.8.3-27.el6.centos.1

?

Priority

5

?

Notes

If we want notes, put them here

Documentation

links to documentation (for example) go here

1

Passed and

1

Failed

Q Devices

10records per page

Search:

| | Device | Name | Version | Status |
|------------------------|--------|----------|-----------------------|----------------------|
| <div>View Device</div> | dummy | plymouth | 0.8.3-27.el6.centos.1 | <div>x</div> |
| <div>View Device</div> | thor | plymouth | 0.8.3-27.el6.centos.1 | <div>checkmark</div> |

Showing 1 to 2 of 2 entries

First

Previous

Next

Last

Powered by Opmantek

The device detailed result is below.

Open-Audit Enterprise 1.10

ViewsQueriesReports

ModulesLicensesSystemHelpUser: admin

Baselines

Baseline Result for Test Baseline for RH6 software run on 2016-01-19 14:30:01

Name

Test Baseline for RH6 software

?

Description

This is a test

?

Timestamp

2016-01-19 14:30:01

?

Group

CentOS Linux Systems

?

Device

dummy

?

Priority

5

?

Notes

If we want notes, put them here

Documentation

links to documentation (for example) go here

9

 Passed and

35

 Failed

Q Policies

10 records per page

Search:

| | Type | Policy | Result | Result | Status |
|-----------------------------|----------|---|------------------------|-----------------------|-------------|
| View Policy | software | software, perl-Compress-Zlib = 2.021-141.el6 | perl-Compress-Zlib | 2.021-141.el6 | <div></div> |
| View Policy | software | software, plymouth = 0.8.3-27.el6.centos.1 | plymouth | 0.8.3-27.el6.centos.1 | <div></div> |
| View Policy | software | software, basesystem = 10.0-4.el6 | basesystem | 10.0-4.el6 | <div></div> |
| View Policy | software | software, pinentry = 0.7.6-8.el6 | pinentry | 0.7.6-8.el6 | <div></div> |
| View Policy | software | software, xorg-x11-fonts-Type1 = 7.2-11.el6 | xorg-x11-fonts-Type1 | 7.2-11.el6 | <div></div> |
| View Policy | software | software, cryptsetup-luks = 1.2.0-11.el6 | cryptsetup-luks | 1.2.0-11.el6 | <div></div> |
| View Policy | software | software, dejavu-lgo-serif-fonts = 2.33-1.el6 | dejavu-lgo-serif-fonts | 2.33-1.el6 | <div></div> |
| View Policy | software | software, info = 4.13a-8.el6 | info | 4.13a-8.el6 | <div></div> |
| View Policy | software | software, dummy-package = 1.10 | dummy-package | 1.10 | <div></div> |
| View Policy | software | software, perl-Compress-Zlib = 2.003-141.el6 | perl-Compress-Zlib | 2.021-141.el6 | <div></div> |

Showing 1 to 10 of 44 entries

First

Previous

Next

Last

Powered by Opmantek