

asprom Firewall Compliance scanner

Generated by Doxygen 1.8.8

Tue Jan 6 2015 19:58:03

Contents

1	Namespace Index	1
1.1	Packages	1
2	Hierarchical Index	3
2.1	Class Hierarchy	3
3	Class Index	5
3.1	Class List	5
4	File Index	7
4.1	File List	7
5	Namespace Documentation	9
5.1	asprom Namespace Reference	9
5.2	asprom.aspromGUI Namespace Reference	9
5.2.1	Detailed Description	10
5.2.2	Function Documentation	10
5.2.2.1	before_request	10
5.2.2.2	returnjson	11
5.2.2.3	serve_addjob	11
5.2.2.4	serve_addjob_view	11
5.2.2.5	serve_alertsclosed	11
5.2.2.6	serve_alertsexposed	11
5.2.2.7	serve_approve	11
5.2.2.8	serve_changejob	12
5.2.2.9	serve_deleteJob	12
5.2.2.10	serve_editjob_view	12
5.2.2.11	serve_flipCrit	12
5.2.2.12	serve_forensic	13
5.2.2.13	serve_homepage	13
5.2.2.14	serve_log	13
5.2.2.15	serve_neatline	13
5.2.2.16	serve_remove	13

5.2.2.17	serve_rescanController	13
5.2.2.18	serve_rescanMachine	13
5.2.2.19	serve_rescanService	14
5.2.2.20	serve_schedule	14
5.2.2.21	static	14
5.2.3	Variable Documentation	14
5.2.3.1	localconf	14
5.2.3.2	M	14
5.2.3.3	SM	14
5.2.3.4	sr	14
5.3	asprom.aspromNagiosCheck Namespace Reference	14
5.3.1	Detailed Description	15
5.3.2	Function Documentation	15
5.3.2.1	genMessages	15
5.3.2.2	main	15
5.4	asprom.aspromScan Namespace Reference	15
5.4.1	Detailed Description	15
5.4.2	Function Documentation	15
5.4.2.1	main	15
5.5	asprom.inc Namespace Reference	16
5.6	asprom.inc.asprom Namespace Reference	16
5.6.1	Detailed Description	17
5.6.2	Function Documentation	17
5.6.2.1	closeDB	17
5.6.2.2	initDB	17
5.6.2.3	scan	17
6	Class Documentation	19
6.1	asprom.inc.asprom.AspromModel Class Reference	19
6.1.1	Detailed Description	20
6.1.2	Constructor & Destructor Documentation	20
6.1.2.1	__init__	20
6.1.3	Member Function Documentation	20
6.1.3.1	getAlertsClosed	20
6.1.3.2	getAlertsExposed	20
6.1.3.3	getForensic	21
6.1.3.4	getLastLog	21
6.1.3.5	getNeatline	21
6.1.3.6	tojson	21
6.2	asprom.inc.asprom.AspromScheduleModel Class Reference	21

6.2.1	Detailed Description	23
6.2.2	Constructor & Destructor Documentation	23
6.2.2.1	__init__	23
6.2.3	Member Function Documentation	23
6.2.3.1	addJob	23
6.2.3.2	changeJob	23
6.2.3.3	deleteJob	24
6.2.3.4	getJobByID	24
6.2.3.5	getSchedule	24
6.2.3.6	getScheduleEntryByID	24
6.2.3.7	promoteToIndex	24
6.2.3.8	read	25
6.2.4	Member Data Documentation	25
6.2.4.1	jobsByID	25
6.2.4.2	schedule	25
6.2.4.3	scheduleLog	25
6.3	asprom.inc.asprom.Cfg Class Reference	25
6.3.1	Detailed Description	26
6.3.2	Constructor & Destructor Documentation	26
6.3.2.1	__init__	26
6.3.3	Member Data Documentation	27
6.3.3.1	maindir	27
6.4	asprom.inc.asprom.Controller Class Reference	27
6.4.1	Detailed Description	28
6.4.2	Member Function Documentation	28
6.4.2.1	approve	28
6.4.2.2	flipCrit	28
6.4.2.3	remove	28
6.4.2.4	rescanJob	28
6.4.2.5	rescanMachine	28
6.4.2.6	rescanService	30
6.5	asprom.inc.asprom.Machine Class Reference	30
6.5.1	Detailed Description	31
6.5.2	Constructor & Destructor Documentation	31
6.5.2.1	__init__	31
6.5.3	Member Function Documentation	31
6.5.3.1	create	31
6.5.3.2	delete	32
6.5.3.3	getIPsInRange	32
6.5.3.4	getServices	32

6.5.3.5	inRange	32
6.5.4	Member Data Documentation	32
6.5.4.1	ffdate	32
6.5.4.2	hostname	33
6.5.4.3	id	33
6.5.4.4	ip	33
6.5.4.5	lsdate	33
6.6	asprom.inc.asprom.NoJoibIDException Class Reference	33
6.6.1	Detailed Description	34
6.6.2	Constructor & Destructor Documentation	34
6.6.2.1	__init__	34
6.6.3	Member Data Documentation	34
6.6.3.1	job	34
6.7	asprom.inc.asprom.Service Class Reference	34
6.7.1	Detailed Description	36
6.7.2	Constructor & Destructor Documentation	36
6.7.2.1	__init__	36
6.7.3	Member Function Documentation	36
6.7.3.1	approve	36
6.7.3.2	create	36
6.7.3.3	delete	37
6.7.3.4	flipCrit	37
6.7.3.5	getMachine	37
6.7.3.6	inRange	37
6.7.3.7	remove	37
6.7.4	Member Data Documentation	38
6.7.4.1	critClosed	38
6.7.4.2	critExposed	38
6.7.4.3	extrainfo	38
6.7.4.4	ffdate	38
6.7.4.5	id	38
6.7.4.6	lsdate	38
6.7.4.7	machine	38
6.7.4.8	port	38
6.7.4.9	product	38
6.7.4.10	version	38
7	File Documentation	39
7.1	__init__.py File Reference	39
7.2	aspromGUI.py File Reference	39

7.3	aspromNagiosCheck.py File Reference	40
7.4	aspromScan.py File Reference	41
7.5	inc/asprom.py File Reference	41
Index		42

Chapter 1

Namespace Index

1.1 Packages

Here are the packages with brief descriptions (if available):

asprom	9
asprom.aspromGUI Created on Oct 19, 2014	9
asprom.aspromNagiosCheck Created on Oct 23, 2014	14
asprom.aspromScan Created on Oct 23, 2014	15
asprom.inc	16
asprom.inc.asprom Created on Oct 22, 2014	16

Chapter 2

Hierarchical Index

2.1 Class Hierarchy

This inheritance list is sorted roughly, but not completely, alphabetically:

Exception	
asprom.inc.asprom.NoJoibIDException	33
object	
asprom.inc.asprom.AspromModel	19
asprom.inc.asprom.Controller	27
asprom.inc.asprom.Machine	30
asprom.inc.asprom.Service	34
Config	
asprom.inc.asprom.Cfg	25
CronTab	
asprom.inc.asprom.AspromScheduleModel	21

Chapter 3

Class Index

3.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

asprom.inc.asprom.AspromModel	
This Model abstracts calls to the database	19
asprom.inc.asprom.AspromScheduleModel	
This model abstracts access to the schedule, which consists of the users crontab and log data in the mysql DB	21
asprom.inc.asprom.Cfg	
Configuration in dict form from the config file etc/asprom.cfg	25
asprom.inc.asprom.Controller	
The Controller defines all actions that are possible from within the GUI	27
asprom.inc.asprom.Machine	
Machine , that is a singular IP adress	30
asprom.inc.asprom.NoJoibIDException	
Exception raised for crontab entries not concerning asprom	33
asprom.inc.asprom.Service	
This class represents a single Service , that is a port on a machine	34

Chapter 4

File Index

4.1 File List

Here is a list of all files with brief descriptions:

__init__.py	39
aspromGUI.py	39
aspromNagiosCheck.py	40
aspromScan.py	41
inc/asprom.py	41

Chapter 5

Namespace Documentation

5.1 asprom Namespace Reference

Namespaces

- [aspromGUI](#)
Created on Oct 19, 2014.
- [aspromNagiosCheck](#)
Created on Oct 23, 2014.
- [aspromScan](#)
Created on Oct 23, 2014.
- [inc](#)

5.2 asprom.aspromGUI Namespace Reference

Created on Oct 19, 2014.

Functions

- def [before_request](#)
before each dynamic request, create DB connection and Model instances.
- def [serve_homepage](#)
HTTP Redirect to <http://alerts-exposed>.
- def [serve_alertsexposed](#)
Presents view: <http://alerts-exposed>.
- def [serve_alertsclosed](#)
Presents view: <http://alerts-closed>.
- def [serve_neatline](#)
Presents view: <http://neatline>.
- def [serve_forensic](#)
Presents view: <http://forensic>.
- def [serve_schedule](#)
Presents view: <http://schedule>.
- def [serve_log](#)
Presents view: <http://log>.
- def [serve_editjob_view](#)

- Presents view: `http:///dia/editjob`.
 - def `serve_addjob_view`
 - Presents view: `http:///dia/addjob`.
 - def `returnjson`
 - Presents all json views: `http:///json/*`.
 - def `serve_rescanController`
 - Activates controller: `http:///controller/rescanjob/<jobid>`.
 - def `serve_rescanMachine`
 - Activates controller: `http:///controller/rescanmachine/<hostid>[/<portid>]`.
 - def `serve_rescanService`
 - Activates controller: `http:///controller/rescanservice/<serviceid>`.
 - def `serve_deleteJob`
 - Activates controller: `http:///controller/deletejob/<jobid>`.
 - def `serve_flipCrit`
 - Activates controller: `http:///controller/flipcrit/<exposed|closed>/<serviceid>`.
 - def `serve_approve`
 - Activates controller: `http:///controller/approve`.
 - def `serve_remove`
 - Activates controller: `http:///controller/remove`.
 - def `serve_changejob`
 - Activates controller: `http:///controller/editjob/<jobid>`.
 - def `serve_addjob`
 - Activates controller: `http:///controller/addjob/<jobid>`.
 - def `static`
 - returns static files from the path defined by variable SR.

Variables

- string `sr` = `'static'`
 - relative path to static files
- `M` = None
 - main model
- `SM` = None
 - schedule model
- tuple `localconf` = `Cfg()`

5.2.1 Detailed Description

Created on Oct 19, 2014.

Author

stefankn

Main Script for the asprom GUI. This script presents a webserver socket to which client browsers can connect to. Also, it orchestrates URL calls between the model, view and controller classes.

5.2.2 Function Documentation

5.2.2.1 def asprom.aspromGUI.before_request ()

before each dynamic request, create DB connection and Model instances.

5.2.2.2 `def asprom.aspromGUI.returnjson (filename)`

Presents all json views: <http://json/>.*.

These are used by the tables embedded in the main html views. The data is aquired using ajax calls. The data is pulled from the model in dict format and then converted to json.

Parameters

<i>filename</i>	the json view to be shown. can be any of alerts-exposed, alerts-closed, neatline, forensic or schedule.
-----------------	---

5.2.2.3 `def asprom.aspromGUI.serve_addjob (jobid)`

Activates controller: <http://controller/addjob/<jobid>>.

This method tells the controller to set the parameters of the specified job and add it to crontab.

Parameters

<i>jobid</i>	the job to be edited.
--------------	-----------------------

The following arguments are to be passed by using the HTTP POST method.

Parameters

<i>cronval</i>	the cron schedule string.
<i>iprange</i>	a CIDR range, single IP or hostname.
<i>portrange</i>	a single port or port range in the format <startport>-<endport> to be scanned.
<i>extraparams</i>	extra command line parameters for nmap.

5.2.2.4 `def asprom.aspromGUI.serve_addjob_view ()`

Presents view: <http://dia/addjob>.

This is meant to be used as a dialog popup in the schedule view. On this dialog, the parameters of a new job can be entered.

5.2.2.5 `def asprom.aspromGUI.serve_alertsclosed ()`

Presents view: <http://alerts-closed>.

5.2.2.6 `def asprom.aspromGUI.serve_alertsexposed ()`

Presents view: <http://alerts-exposed>.

5.2.2.7 `def asprom.aspromGUI.serve_approve ()`

Activates controller: <http://controller/approve>.

The arguments are to be passed by using the HTTP POST method. Using this method, a service can be approved to the neatline.

Parameters

<i>pk</i>	The Service ID to be approved.
<i>value</i>	a business justification for the service to be approved.

5.2.2.8 def asprom.aspromGUI.serve_changejob (*jobid*)

Activates controller: <http://controller/editjob/<jobid>>.

This method tells the controller to set or change the parameters of the specified job.

Parameters

<i>jobid</i>	the job to be edited.
--------------	-----------------------

The following arguments are to be passed by using the HTTP POST method.

Parameters

<i>cronval</i>	the cron schedule string.
<i>iprange</i>	a CIDR range, single IP or hostname.
<i>portrange</i>	a single port or port range in the format <startport>--<endport> to be scanned.
<i>extraparams</i>	extra command line parameters for nmap.

5.2.2.9 def asprom.aspromGUI.serve_deleteJob (*jobid*)

Activates controller: <http://controller/deletejob/<jobid>>.

Instructs the controller to delete the job with id <jobid>.

Parameters

<i>jobid</i>	The Job ID to be scanned.
--------------	---------------------------

5.2.2.10 def asprom.aspromGUI.serve_editjob_view (*jobid*)

Presents view: <http://dia/editjob>.

This is meant to be used as a dialog popup in the schedule view. On this dialog, the parameters of an existing job can be edited.

Parameters

<i>jobid</i>	the job ID to be edited.
--------------	--------------------------

5.2.2.11 def asprom.aspromGUI.serve_flipCrit (*page*, *serviceid*)

Activates controller: <http://controller/flipcrit/<exposed|closed>/<serviceid>>.

Instructs the controller to flip the criticality of service <serviceid> on the alerts-<exposed|closed> view. Flipping sets the service criticality to WARNING if it was CRITICAL before and the other way round.

Parameters

<i>page</i>	Either "exposed" or "closed". Denominates the view on which the criticality of the service should be flipped.
-------------	---

<i>serviceid</i>	The Service whose criticality should be flipped.
------------------	--

5.2.2.12 `def asprom.aspromGUI.serve_forensic ()`

Presents view: <http://forensic>.

5.2.2.13 `def asprom.aspromGUI.serve_homepage ()`

HTTP Redirect to <http://alerts-exposed>.

5.2.2.14 `def asprom.aspromGUI.serve_log ()`

Presents view: <http://log>.

5.2.2.15 `def asprom.aspromGUI.serve_neatline ()`

Presents view: <http://neatline>.

5.2.2.16 `def asprom.aspromGUI.serve_remove ()`

Activates controller: <http://controller/remove>.

The arguments are to be passed by using the HTTP POST method. Using this method, a service can be removed from the neatline.

Parameters

<i>pk</i>	The Service ID to be removed.
<i>value</i>	a business justification for the service to be removed.

5.2.2.17 `def asprom.aspromGUI.serve_rescanController (jobid)`

Activates controller: <http://controller/rescanjob/<jobid>>.

Instructs the controller to perform a forensic rescan of the job with id <jobid> now.

Parameters

<i>jobid</i>	the job ID to be scanned.
--------------	---------------------------

5.2.2.18 `def asprom.aspromGUI.serve_rescanMachine (host, port=None)`

Activates controller: [http://controller/rescanmachine/<hostid>\[/<portid>\]](http://controller/rescanmachine/<hostid>[/<portid>]).

Instructs the controller to perform a forensic rescan of the machine with id <hostid> now. If <portid> is present, only this single port is being rescanned.

Parameters

<i>host</i>	the host ID to be scanned.
-------------	----------------------------

<i>port</i>	the port to be rescanned on the specified machine.
-------------	--

5.2.2.19 `def asprom.aspromGUI.serve_rescanService (serviceid)`

Activates controller: <http://controller/rescanservice/<serviceid>>.

Instructs the controller to perform a forensic rescan of the service with id <serviceid> now.

Parameters

<i>serviceid</i>	The Service ID to be scanned.
------------------	-------------------------------

5.2.2.20 `def asprom.aspromGUI.serve_schedule ()`

Presents view: <http://schedule>.

5.2.2.21 `def asprom.aspromGUI.static (filename)`

returns static files from the path defined by variable SR.

Parameters

<i>filename</i>	path to the static file relative to the SR directory.
-----------------	---

5.2.3 Variable Documentation

5.2.3.1 `tuple asprom.aspromGUI.localconf = Cfg()`

5.2.3.2 `asprom.aspromGUI.M = None`

main model

5.2.3.3 `asprom.aspromGUI.SM = None`

schedule model

5.2.3.4 `string asprom.aspromGUI.sr = 'static/'`

relative path to static files

5.3 asprom.aspromNagiosCheck Namespace Reference

Created on Oct 23, 2014.

Functions

- def [genMessages](#)
generates textual descriptions of profile discrepancies.
- def [main](#)

5.3.1 Detailed Description

Created on Oct 23, 2014.

Author

stefankn

This file is invoked from the CLI and can be directly used as a nagios plugin. if any of the services on the alerts-exposed or alerts-closed views are marked as critical, this script terminates with a return value of 2. if none are marked as critical, but at least one is marked as warning, this script terminates with a return value of 1. Else, it terminates with a value of 0 signalling everything is alright.

5.3.2 Function Documentation

5.3.2.1 `def asprom.aspromNagiosCheck.genMessages (exp)`

generates textual descriptions of profile discrepancies.

Parameters

<i>rowset</i>	a rowset as generated by <code>aspromModel.getAlertsExposed()</code> or <code>getAlertsClosed()</code>
---------------	--

Returns

a two-tuple containing a list of critical and a list of warning discrepancies

5.3.2.2 `def asprom.aspromNagiosCheck.main ()`

5.4 asprom.aspromScan Namespace Reference

Created on Oct 23, 2014.

Functions

- `def main`
parse arguments from command line.

5.4.1 Detailed Description

Created on Oct 23, 2014.

Author

stefankn

this file is invoked on the CLI as a wrapper script to nmap. when invoked from the command line, the `scan()` method is called.

5.4.2 Function Documentation

5.4.2.1 `def asprom.aspromScan.main ()`

parse arguments from command line.

usage:

```
aspromScan.py [-h] [-o EXTRA_OPTIONS] [-s SENSOR] [-p PORT_RANGE]
               [-j JOB_ID] TARGET
```

Scans an IP Range for asprom. Needs nmap installed on the sensor host.

positional arguments:

TARGET the hostname/ip/ip range to be scanned

optional arguments:

```
-h, --help                    show this help message and exit
-o EXTRA_OPTIONS, --extra-options EXTRA_OPTIONS
                           extra options to be passed to nmap
-s SENSOR, --sensor SENSOR
                           start scanning on another sensor
-p PORT_RANGE, --port-range PORT_RANGE
                           set custom port range to be scanned
-j JOB_ID, --job-id JOB_ID
                           set arbitrary job id (used by aspromGUI and cron)
```

5.5 asprom.inc Namespace Reference

Namespaces

- [asprom](#)

Created on Oct 22, 2014.

5.6 asprom.inc.asprom Namespace Reference

Created on Oct 22, 2014.

Classes

- class [AspromModel](#)
This Model abstracts calls to the database.
- class [AspromScheduleModel](#)
This model abstracts access to the schedule, which consists of the users crontab and log data in the mysql DB.
- class [Cfg](#)
Configuration in dict form from the config file etc/asprom.cfg.
- class [Controller](#)
The [Controller](#) defines all actions that are possible from within the GUI.
- class [Machine](#)
represents a machine, that is a singular IP adress.
- class [NoJoiblDException](#)
Exception raised for crontab entries not concerning asprom.
- class [Service](#)
This class represents a single [Service](#), that is a port on a machine.

Functions

- def [scan](#)
Scans the port range on the target IP/IP Range with nmap.
- def [initDB](#)
inits the database into the bottle request scope.
- def [closeDB](#)
commit all open database cursors.

5.6.1 Detailed Description

Created on Oct 22, 2014.

Author

stefankn

Library for asprom Scripts.

5.6.2 Function Documentation

5.6.2.1 def asprom.inc.asprom.closeDB ()

commit all open database cursors.

close the connection.

5.6.2.2 def asprom.inc.asprom.initDB (*localconf*)

inits the database into the bottle request scope.

5.6.2.3 def asprom.inc.asprom.scan (*target*, *port_range*, *extra_options*, *job_id*, *sensor* = 'localhost')

Scans the port range on the target IP/IP Range with nmap.

extra_options are passed as CLI arguments to nmap. The *job_id* will be saved to the changelog entry in the database for reference to the actual job.

Parameters

<i>target</i>	CIDR Range, singular IP or hostname
<i>port_range</i>	range of ports to be scanned
<i>extra_options</i>	extra CLI arguments to be passed to nmap
<i>job_id</i>	job UUID as used by the schedule model
<i>sensor</i>	In future versions, you may specify a sensor to be used for scanning (not implemented yet).

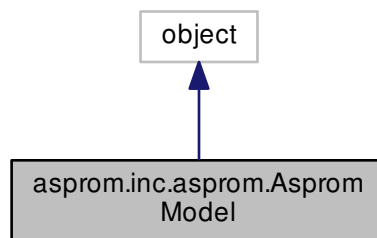
Chapter 6

Class Documentation

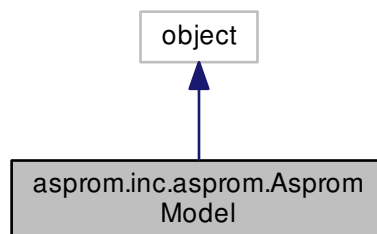
6.1 asprom.inc.asprom.AspromModel Class Reference

This Model abstracts calls to the database.

Inheritance diagram for asprom.inc.asprom.AspromModel:



Collaboration diagram for asprom.inc.asprom.AspromModel:



Public Member Functions

- def [__init__](#)
standard constructor
- def [getAlertsExposed](#)
returns row data for the alerts-exposed view.
- def [getAlertsClosed](#)
returns row data for the alerts-closed view.
- def [getNeatline](#)
returns row data for the neatline view.
- def [getForensic](#)
returns row data for the forensic view.
- def [getLastLog](#)
returns <count> last log entries from the changelog in html format.

Static Public Member Functions

- def [toJson](#)
converts row data to json format.

6.1.1 Detailed Description

This Model abstracts calls to the database.

It returns rows of data for the views in the GUI. Using the toJson static method, they can be easily converted to the json format used by bootstrap-table AJAX calls.

6.1.2 Constructor & Destructor Documentation

6.1.2.1 `def asprom.inc.asprom.AspromModel.__init__(self, args, kwargs)`

standard constructor

6.1.3 Member Function Documentation

6.1.3.1 `def asprom.inc.asprom.AspromModel.getAlertsClosed(self)`

returns row data for the alerts-closed view.

Returns

returns row data for the alerts-closed view.

6.1.3.2 `def asprom.inc.asprom.AspromModel.getAlertsExposed(self)`

returns row data for the alerts-exposed view.

Returns

row data for the alerts-exposed view.

6.1.3.3 def asprom.inc.asprom.AspromModel.getForensic (self)

returns row data for the forensic view.

Returns

returns row data for the forensic view.

6.1.3.4 def asprom.inc.asprom.AspromModel.getLastLog (self, count)

returns <count> last log entries from the changelog in html format.

Parameters

<i>count</i>	number of lines to return.
--------------	----------------------------

Returns

<count> last log entries from the changelog in html format.

6.1.3.5 def asprom.inc.asprom.AspromModel.getNeatline (self)

returns row data for the neatline view.

Returns

returns row data for the neatline view.

6.1.3.6 def asprom.inc.asprom.AspromModel.tojson (someDict) [static]

converts row data to json format.

Parameters

<i>someDict</i>	row data in dictionary format.
-----------------	--------------------------------

Returns

JSON String.

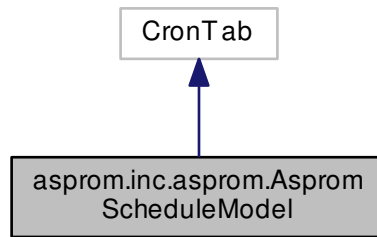
The documentation for this class was generated from the following file:

- [inc/asprom.py](#)

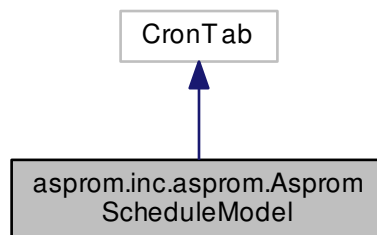
6.2 asprom.inc.asprom.AspromScheduleModel Class Reference

This model abstracts access to the schedule, which consists of the users crontab and log data in the mysql DB.

Inheritance diagram for asprom.inc.asprom.AspromScheduleModel:



Collaboration diagram for asprom.inc.asprom.AspromScheduleModel:



Public Member Functions

- def `__init__`
standard Constructor
- def `read`
override read method in CronTab.py.
- def `getJobByID`
returns the job with id <jobid>.
- def `changeJob`
changes the parameters of the Job with UUID <jobid> in the crontab.
- def `addJob`
adds a Job to the crontab.
- def `deleteJob`
deactivates the job with id <jobid> and refreshes the model.
- def `getScheduleEntryByID`
returns the job specifics for the job with id <jobid>.
- def `getSchedule`
returns the schedule (crontab) in flat (unindexed) form, e.g.

Static Public Member Functions

- def [promoteToIndex](#)
index the dic by valueKey.

Static Public Attributes

- [scheduleLog](#) = None
schedule log from database
- [schedule](#) = None
schedule data from crontab
- tuple [jobsByID](#) = dict()
dictionary of jobs indexed by id

6.2.1 Detailed Description

This model abstracts access to the schedule, which consists of the users crontab and log data in the mysql DB.

Both components are joined together using an UUID, the jobId.

requires CronTab.py, as this class inherits from that.

6.2.2 Constructor & Destructor Documentation

6.2.2.1 def asprom.inc.asprom.AspromScheduleModel.__init__(self, args, kwargs)

standard Constructor

6.2.3 Member Function Documentation

6.2.3.1 def asprom.inc.asprom.AspromScheduleModel.addJob(self, jobid, cronval, iprange, portrange, extraparams)

adds a Job to the crontab.

Parameters

<i>jobid</i>	the job id to be added.
<i>cronval</i>	the cron schedule string.
<i>iprange</i>	a CIDR range, single IP or hostname.
<i>portrange</i>	a single port or port range in the format <startport>-<endport> to be scanned.
<i>extraparams</i>	extra command line parameters for nmap.

6.2.3.2 def asprom.inc.asprom.AspromScheduleModel.changeJob(self, jobid, cronval, iprange, portrange, extraparams, job=None)

changes the parameters of the Job with UUID <jobid> in the crontab.

Parameters

<i>jobid</i>	the job to be edited.
<i>cronval</i>	the cron schedule string.

<i>iprange</i>	a CIDR range, single IP or hostname.
<i>portrange</i>	a single port or port range in the format <startport>--<endport> to be scanned.
<i>extraparams</i>	extra command line parameters for nmap.

6.2.3.3 `def asprom.inc.asprom.AspromScheduleModel.deleteJob (self, jobid)`

deactivates the job with id <jobid> and refreshes the model.

Parameters

<i>jobid</i>	the job's id.
--------------	---------------

6.2.3.4 `def asprom.inc.asprom.AspromScheduleModel.getJobByID (self, jobid)`

returns the job with id <jobid>.

Parameters

<i>jobid</i>	the job's id.
--------------	---------------

Returns

a job object.

6.2.3.5 `def asprom.inc.asprom.AspromScheduleModel.getSchedule (self)`

returns the schedule (crontab) in flat (unindexed) form, e.g.

for GUI table data.

6.2.3.6 `def asprom.inc.asprom.AspromScheduleModel.getScheduleEntryByID (self, jobid)`

returns the job specifics for the job with id <jobid>.

Parameters

<i>jobid</i>	the job's id.
--------------	---------------

Returns

a dictionary with job parameters.

6.2.3.7 `def asprom.inc.asprom.AspromScheduleModel.promoteToIndex (dici, valueKey) [static]`

index the dic by valueKey.

promotes the element on position <valueKey> from each sublist to an index in a dictionary.

Parameters

<i>dici</i>	a list of lists or a list of dictionaries, e.g. a database result set.
-------------	--

<i>valueKey</i>	position or name of the value to be promoted to an index.
-----------------	---

Returns

promoted dictionary.

example:

```
>>> d = [[1,2,3,4,5], [6,7], [8,9], [9,10]]
>>> e=AspromScheduleModel.promoteToIndex(d,1)
>>> print e
{9: [8], 2: [1, 3, 4, 5], 10: [9], 7: [6]}
```

6.2.3.8 `def asprom.inc.asprom.AspromScheduleModel.read (self, filename=None)`

override read method in CronTab.py.

Additionally fetches log information from the database and fills the properties schedule and scheduleLog.

6.2.4 Member Data Documentation

6.2.4.1 `tuple asprom.inc.asprom.AspromScheduleModel.jobsById = dict() [static]`

dictionary of jobs indexed by id

6.2.4.2 `asprom.inc.asprom.AspromScheduleModel.schedule = None [static]`

schedule data from crontab

6.2.4.3 `asprom.inc.asprom.AspromScheduleModel.scheduleLog = None [static]`

schedule log from database

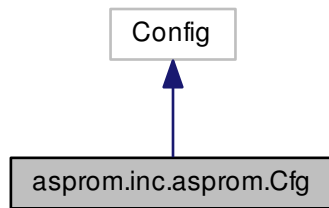
The documentation for this class was generated from the following file:

- [inc/asprom.py](#)

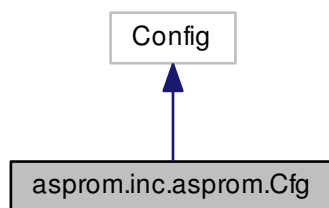
6.3 asprom.inc.asprom.Cfg Class Reference

Configuration in dict form from the config file etc/asprom.cfg.

Inheritance diagram for asprom.inc.asprom.Cfg:



Collaboration diagram for asprom.inc.asprom.Cfg:



Public Member Functions

- `def __init__`

expanded constructor, calls the super constructor of Config with the path to asprom.cfg

Static Public Attributes

- `maindir = None`

6.3.1 Detailed Description

Configuration in dict form from the config file `etc/asprom.cfg`.

6.3.2 Constructor & Destructor Documentation

6.3.2.1 `def asprom.inc.asprom.Cfg.__init__(self)`

expanded constructor, calls the super constructor of Config with the path to asprom.cfg

6.3.3 Member Data Documentation

6.3.3.1 asprom.inc.asprom.Cfg.maindir = None [static]

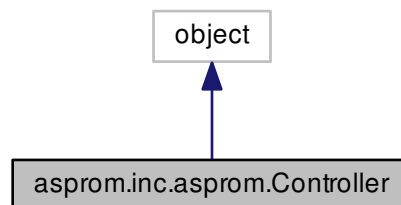
The documentation for this class was generated from the following file:

- inc/[asprom.py](#)

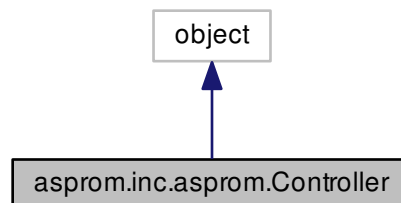
6.4 asprom.inc.asprom.Controller Class Reference

The [Controller](#) defines all actions that are possible from within the GUI.

Inheritance diagram for asprom.inc.asprom.Controller:



Collaboration diagram for asprom.inc.asprom.Controller:



Static Public Member Functions

- def [rescanJob](#)
run the scheduled job with id <jobid> right now.
- def [rescanMachine](#)
rescan the machine.
- def [rescanService](#)
rescans the service.
- def [flipCrit](#)

flips the criticality of the service.

- def [approve](#)

Using this method, a service can be approved to the neatline.

- def [remove](#)

Using this method, a service can be removed from the neatline.

6.4.1 Detailed Description

The [Controller](#) defines all actions that are possible from within the GUI.

6.4.2 Member Function Documentation

6.4.2.1 `def asprom.inc.asprom.Controller.approve (serviceid, justification) [static]`

Using this method, a service can be approved to the neatline.

Parameters

<i>serviceid</i>	The Service ID to be approved.
<i>justification</i>	a business justification for the service to be approved.

6.4.2.2 `def asprom.inc.asprom.Controller.flipCrit (serviceid, exposed = True) [static]`

flips the criticality of the service.

Flipping sets the service criticality to WARNING if it was CRITICAL before and the other way round.

Parameters

<i>serviceid</i>	The Service whose criticality should be flipped.
<i>page</i>	Denominates the view on which the criticality of the service should be flipped. If true, "alerts-exposed" is flipped. Else, "alerts-closed".

6.4.2.3 `def asprom.inc.asprom.Controller.remove (serviceid, justification) [static]`

Using this method, a service can be removed from the neatline.

Parameters

<i>serviceid</i>	The Service ID to be removed.
<i>justification</i>	a business justification for the service to be removed.

6.4.2.4 `def asprom.inc.asprom.Controller.rescanJob (jobid) [static]`

run the scheduled job with id <jobid> right now.

Parameters

<i>jobid</i>	the UUID of the job to be run
--------------	-------------------------------

6.4.2.5 `def asprom.inc.asprom.Controller.rescanMachine (machineid, port = None) [static]`

rescan the machine.

this method finds the task in the schedule to which the machine belongs and takes its additional arguments from there.

Parameters

<i>machineid</i>	ID of the machine to be rescanned.
<i>port</i>	port of the machine to be rescanned.

6.4.2.6 `def asprom.inc.asprom.Controller.rescanService (serviceid) [static]`

rescans the service.

Parameters

<i>serviceid</i>	ID of the service to be rescanned.
------------------	------------------------------------

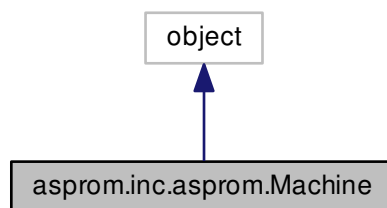
The documentation for this class was generated from the following file:

- [inc/asprom.py](#)

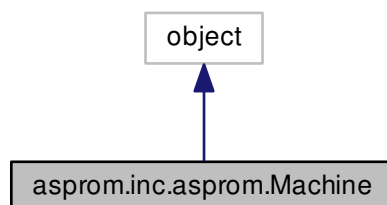
6.5 asprom.inc.asprom.Machine Class Reference

represents a machine, that is a singular IP adress.

Inheritance diagram for asprom.inc.asprom.Machine:



Collaboration diagram for asprom.inc.asprom.Machine:



Public Member Functions

- def `__init__`
Constructor Loads all information about the machine from the database.
- def `getServices`
return list of services associated with this machine.
- def `delete`
delete self.

Static Public Member Functions

- def `create`
create new [Machine](#) and return self.
- def `inRange`
returns true if ip is in range r, false otherwise.
- def `getIPsInRange`
return a dictionary of IPs to IDs for all known hosts in the defined range.

Static Public Attributes

- `id` = None
machines database id.
- `hostname` = None
hostname, if known.
- `ip` = None
ip address of the machine.
- `lsdate` = None
date when the machine was last seen by port scanner.
- `ffdate` = None
date when the machine was first found by the port scanner.

6.5.1 Detailed Description

represents a machine, that is a singular IP adress.

6.5.2 Constructor & Destructor Documentation

6.5.2.1 def asprom.inc.asprom.Machine.__init__(self, machineid)

Constructor Loads all information about the machine from the database.

Parameters

<code>machineid</code>	Database id of the machine.
------------------------	-----------------------------

6.5.3 Member Function Documentation

6.5.3.1 def asprom.inc.asprom.Machine.create(name, ip) [static]

create new [Machine](#) and return self.

Parameters

<i>name</i>	hostname
<i>ip</i>	ip address

Returns

self

6.5.3.2 `def asprom.inc.asprom.Machine.delete (self)`

delete self.

6.5.3.3 `def asprom.inc.asprom.Machine.getIPsInRange (r, exposedOnly=False) [static]`

return a dictionary of IPs to IDs for all known hosts in the defined range.

Parameters

<i>r</i>	ip range
----------	----------

Returns

dictionary IPs/Machine IDs in that range

6.5.3.4 `def asprom.inc.asprom.Machine.getServices (self, exposedOnly=False)`

return list of services associated with this machine.

Parameters

<i>exposedOnly</i>	if true, only return currently exposed services.
--------------------	--

Returns

list of services.

6.5.3.5 `def asprom.inc.asprom.Machine.inRange (r, ip) [static]`

returns true if ip is in range r, false otherwise.

Parameters

<i>r</i>	range
<i>ip</i>	ip address

Returns

true if ip is in range r, false otherwise.

6.5.4 Member Data Documentation

6.5.4.1 `asprom.inc.asprom.Machine.fdate = None [static]`

date when the machine was first found by the port scanner.

6.5.4.2 asprom.inc.asprom.Machine.hostname = None [static]

hostname, if known.

6.5.4.3 asprom.inc.asprom.Machine.id = None [static]

machines database id.

6.5.4.4 asprom.inc.asprom.Machine.ip = None [static]

ip address of the machine.

6.5.4.5 asprom.inc.asprom.Machine.lsdte = None [static]

date when the machine was last seen by port scanner.

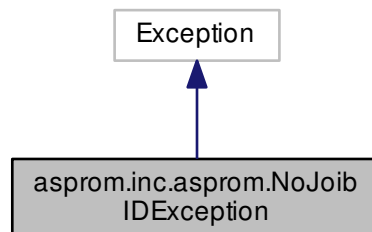
The documentation for this class was generated from the following file:

- [inc/asprom.py](#)

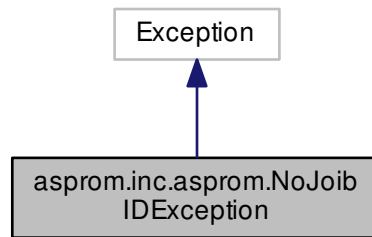
6.6 asprom.inc.asprom.NoJoibIDException Class Reference

Exception raised for crontab entries not concerning asprom.

Inheritance diagram for asprom.inc.asprom.NoJoibIDException:



Collaboration diagram for `asprom.inc.asprom.NoJoibIDException`:



Public Member Functions

- `def __init__`

Public Attributes

- `job`

6.6.1 Detailed Description

Exception raised for crontab entries not concerning asprom.

6.6.2 Constructor & Destructor Documentation

6.6.2.1 `def asprom.inc.asprom.NoJoibIDException.__init__(self, job)`

6.6.3 Member Data Documentation

6.6.3.1 `asprom.inc.asprom.NoJoibIDException.job`

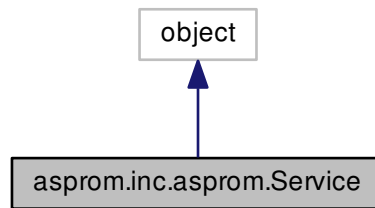
The documentation for this class was generated from the following file:

- `inc/asprom.py`

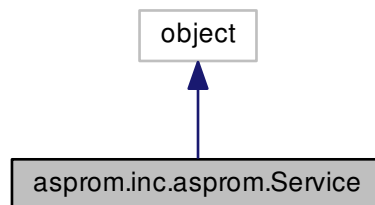
6.7 asprom.inc.asprom.Service Class Reference

This class represents a single [Service](#), that is a port on a machine.

Inheritance diagram for asprom.inc.asprom.Service:



Collaboration diagram for asprom.inc.asprom.Service:



Public Member Functions

- def `__init__`
Constructor.
- def `delete`
deletes this service.
- def `getMachine`
returns the machine object associated with this service.
- def `inRange`
tells if a service is in a specific port range.
- def `flipCrit`
Flip criticality of "exposed" view if exposed = true, else of the "closed" view.
- def `approve`
approve this service and add it to the neat line
- def `remove`
remove this service from the neat line.

Static Public Member Functions

- def `create`
create new service and return self

Static Public Attributes

- `id` = None
services database id
- `machine` = None
machine object to which this service is associated
- `port` = None
port number of this service
- `product` = None
additional product information gleaned by nmap
- `version` = None
additional version information gleaned by nmap
- `extrainfo` = None
additional extra information gleaned by nmap
- `lsdate` = None
datetime, when this service was last seen
- `ffdate` = None
datetime, when this service was first seen
- `critExposed` = True
- `critClosed` = False
flag: does this service raise a critical alert when closed and approved?

6.7.1 Detailed Description

This class represents a single [Service](#), that is a port on a machine.

6.7.2 Constructor & Destructor Documentation

6.7.2.1 `def asprom.inc.asprom.Service.__init__(self, serviceid)`

Constructor.

Loads all information about the service from the database.

Parameters

<i>serviceid</i>	Database id of the service.
------------------	-----------------------------

6.7.3 Member Function Documentation

6.7.3.1 `def asprom.inc.asprom.Service.approve (self, justification, neat = True)`

approve this service and add it to the neat line

Parameters

<i>justification</i>	a business justification.
<i>neat</i>	true for approval. if false, remove from neat line. this is used by the method remove() .

6.7.3.2 `def asprom.inc.asprom.Service.create (mach, portno, product = "", version = "", extrainfo = "") [static]`

create new service and return self

Parameters

<i>mach</i>	Machine object to which the service belongs
<i>portno</i>	Port number of this service
<i>product</i>	additional product information gleaned by nmap. if not defined, get generic information about port from /etc/services.
<i>version</i>	additional version information gleaned by nmap
<i>extrainfo</i>	additional extra information gleaned by nmap

Returns

self

6.7.3.3 `def asprom.inc.asprom.Service.delete (self)`

deletes this service.

6.7.3.4 `def asprom.inc.asprom.Service.flipCrit (self, exposed = True)`

Flip criticality of "exposed" view if exposed = true, else of the "closed" view.

Parameters

<i>exposed</i>	a boolean.
----------------	------------

6.7.3.5 `def asprom.inc.asprom.Service.getMachine (self)`

returns the machine object associated with this service.

Returns

a machine object.

6.7.3.6 `def asprom.inc.asprom.Service.inRange (self, r)`

tells if a service is in a specific port range.

Parameters

<i>r</i>	single port number or range, e.g. "1024-65535"
----------	--

Returns

boolean.

6.7.3.7 `def asprom.inc.asprom.Service.remove (self, justification)`

remove this service from the neat line.

Parameters

<i>justification</i>	a business justification.
----------------------	---------------------------

6.7.4 Member Data Documentation

6.7.4.1 `asprom.inc.asprom.Service.critClosed = False` `[static]`

flag: does this service raise a critical alert when closed and approved?

6.7.4.2 `asprom.inc.asprom.Service.critExposed = True` `[static]`

6.7.4.3 `asprom.inc.asprom.Service.extrainfo = None` `[static]`

additional extra information gleaned by nmap

6.7.4.4 `asprom.inc.asprom.Service.ffdate = None` `[static]`

datetime, when this service was first seen

6.7.4.5 `asprom.inc.asprom.Service.id = None` `[static]`

services database id

6.7.4.6 `asprom.inc.asprom.Service.lsddate = None` `[static]`

datetime, when this service was last seen

6.7.4.7 `asprom.inc.asprom.Service.machine = None` `[static]`

machine object to which this service is associated

6.7.4.8 `asprom.inc.asprom.Service.port = None` `[static]`

port number of this service

6.7.4.9 `asprom.inc.asprom.Service.product = None` `[static]`

additional product information gleaned by nmap

6.7.4.10 `asprom.inc.asprom.Service.version = None` `[static]`

additional version information gleaned by nmap

The documentation for this class was generated from the following file:

- [inc/asprom.py](#)

Chapter 7

File Documentation

7.1 `__init__.py` File Reference

Namespaces

- [asprom](#)

7.2 `aspromGUI.py` File Reference

Namespaces

- [asprom.aspromGUI](#)
Created on Oct 19, 2014.

Functions

- def [asprom.aspromGUI.before_request](#)
before each dynamic request, create DB connection and Model instances.
- def [asprom.aspromGUI.serve_homepage](#)
HTTP Redirect to <http://alerts-exposed>.
- def [asprom.aspromGUI.serve_alertsexposed](#)
Presents view: <http://alerts-exposed>.
- def [asprom.aspromGUI.serve_alertsclosed](#)
Presents view: <http://alerts-closed>.
- def [asprom.aspromGUI.serve_neatline](#)
Presents view: <http://neatline>.
- def [asprom.aspromGUI.serve_forensic](#)
Presents view: <http://forensic>.
- def [asprom.aspromGUI.serve_schedule](#)
Presents view: <http://schedule>.
- def [asprom.aspromGUI.serve_log](#)
Presents view: <http://log>.
- def [asprom.aspromGUI.serve_editjob_view](#)
Presents view: <http://dia/editjob>.
- def [asprom.aspromGUI.serve_addjob_view](#)
Presents view: <http://dia/addjob>.

- def `asprom.aspromGUI.returnjson`
Presents all json views: `http:///json/`.*
- def `asprom.aspromGUI.serve_rescanController`
Activates controller: `http:///controller/rescanjob/<jobid>`.
- def `asprom.aspromGUI.serve_rescanMachine`
Activates controller: `http:///controller/rescanmachine/<hostid>[/<portid>]`.
- def `asprom.aspromGUI.serve_rescanService`
Activates controller: `http:///controller/rescanservice/<serviceid>`.
- def `asprom.aspromGUI.serve_deleteJob`
Activates controller: `http:///controller/deletejob/<jobid>`.
- def `asprom.aspromGUI.serve_flipCrit`
Activates controller: `http:///controller/flipcrit/<exposed|closed>/<serviceid>`.
- def `asprom.aspromGUI.serve_approve`
Activates controller: `http:///controller/approve`.
- def `asprom.aspromGUI.serve_remove`
Activates controller: `http:///controller/remove`.
- def `asprom.aspromGUI.serve_changejob`
Activates controller: `http:///controller/editjob/<jobid>`.
- def `asprom.aspromGUI.serve_addjob`
Activates controller: `http:///controller/addjob/<jobid>`.
- def `asprom.aspromGUI.static`
returns static files from the path defined by variable SR.

Variables

- string `asprom.aspromGUI.sr` = 'static/'
relative path to static files
- `asprom.aspromGUI.M` = None
main model
- `asprom.aspromGUI.SM` = None
schedule model
- tuple `asprom.aspromGUI.localconf` = Cfg()

7.3 aspromNagiosCheck.py File Reference

Namespaces

- `asprom.aspromNagiosCheck`
Created on Oct 23, 2014.

Functions

- def `asprom.aspromNagiosCheck.genMessages`
generates textual descriptions of profile discrepancies.
- def `asprom.aspromNagiosCheck.main`

7.4 aspromScan.py File Reference

Namespaces

- [asprom.aspromScan](#)
Created on Oct 23, 2014.

Functions

- def [asprom.aspromScan.main](#)
parse arguments from command line.

7.5 inc/asprom.py File Reference

Classes

- class [asprom.inc.asprom.NoJoibIDException](#)
Exception raised for crontab entries not concerning asprom.
- class [asprom.inc.asprom.Cfg](#)
Configuration in dict form from the config file etc/asprom.cfg.
- class [asprom.inc.asprom.AspromModel](#)
This Model abstracts calls to the database.
- class [asprom.inc.asprom.AspromScheduleModel](#)
This model abstracts access to the schedule, which consists of the users crontab and log data in the mysql DB.
- class [asprom.inc.asprom.Controller](#)
The [Controller](#) defines all actions that are possible from within the GUI.
- class [asprom.inc.asprom.Service](#)
This class represents a single [Service](#), that is a port on a machine.
- class [asprom.inc.asprom.Machine](#)
represents a machine, that is a singular IP adress.

Namespaces

- [asprom.inc.asprom](#)
Created on Oct 22, 2014.

Functions

- def [asprom.inc.asprom.scan](#)
Scans the port range on the target IP/IP Range with nmap.
- def [asprom.inc.asprom.initDB](#)
inits the database into the bottle request scope.
- def [asprom.inc.asprom.closeDB](#)
commit all open database cursors.

Index

asprom, [9](#)