aiospamc Documentation

Release 0.5.0

Michael Caley

Sep 20, 2019

CONTENTS:

aiospamc is an asyncio-based library to interact with SpamAssassin's SPAMD service.

CHAPTER

ONE

CONTENTS

1.1 User Guide

1.1.1 Requirements

- Python 3.5 or later is required to use the new async/await syntax provided by the asyncio library.
- SpamAssassin running as a service.

1.1.2 Install

With PIP

```
pip install aiospamc
```

With GIT

```
git clone https://github.com/mjcaley/aiospamc.git
python3 aiospamc/setup.py install
```

1.1.3 How to use aiospamc

Instantiating the *aiospamc.client.Client* class will be the primary way to interact with aiospamc.

Parameters are available to specify how to connect to the SpamAssassin SPAMD service including host, port, and whether SSL is enabled. They default to `localhost`, `783`, and SSL being disabled. Additional optional parameters are the username that requests will be sent as (no user by default) and whether to compress the request body (disabled by default).

A coroutine method is available for each type of request that can be sent to SpamAssassin.

An example using the *aiospamc.client.Client.check()* method:

```
import asyncio
import aiospamc

example_message = ('From: John Doe <jdoe@machine.example>'
                   'To: Mary Smith <mary@example.net>'
                   'Subject: Saying Hello'
```

(continues on next page)

(continued from previous page)

```
                    'Date: Fri, 21 Nov 1997 09:55:06 -0600'
                    'Message-ID: <1234@local.machine.example>'
                    ''
                    'This is a message just to say hello.'
                    'So, "Hello".').encode('ascii')

loop = asyncio.get_event_loop()
client = aiospamc.Client()
response = loop.run_until_complete(client.check(example_message))
print(response)
```

Other requests can be seen in the *aiospamc.client.Client* class.

1.1.4 Making your own requests

If a request that isn't built into aiospamc is needed a new request can be created and sent.

A new request can be made by instantiating the *aiospamc.requests.Request* class. The `aiospamc.requests.Request.verb` defines the method/verb of the request.

Standard headers or the *aiospamc.headers.XHeader* extension header are available in the *aiospamc.headers* module. The *aiospamc.requests.Request* class provides a headers attribute that has a dictionary-like interface.

Once a request is composed, it can be sent through the *aiospamc.client.Client.send()* method as-is. The method will automatically add the *aiospamc.headers.User* and *aiospamc.headers.Compress* headers if required.

For example:

```
import asyncio

import aiospamc
from aiospamc import Client
from aiospamc.exceptions import ResponseException
from aiospamc.requests import Request

example_message = ('From: John Doe <jdoe@machine.example>'
                   'To: Mary Smith <mary@example.net>'
                   'Subject: Saying Hello'
                   'Date: Fri, 21 Nov 1997 09:55:06 -0600'
                   'Message-ID: <1234@local.machine.example>'
                   ''
                   'This is a message just to say hello.'
                   'So, "Hello".').encode('ascii')

loop = asyncio.get_event_loop()
client = aiospamc.Client(host='localhost')

async def is_spam(message):
    request = Request(verb='CHECK', body=message.encode())
    try:
        response = await client.send(request)
        return response.get_header('Spam').value
    except aiospamc.ResponseException:
        raise
```

(continues on next page)

(continued from previous page)

```
spam_result = loop.run_until_complete(is_spam(example_message))
print('Example message is spam:', spam_result)
```

1.1.5 Interpreting results

Responses are encapsulated in the *aiospamc.responses.Response* class. It includes the status code, headers and body.

1.2 aiospamc

1.2.1 aiospamc package

Subpackages

aiospamc.connections package

Submodules

aiospamc.connections.tcp_connection module

TCP socket connection and manager.

class aiospamc.connections.tcp_connection.**TcpConnection**(*host: str*, *port: int*, *ssl: bool*, *loop: asyncio.events.AbstractEventLoop = None*)

Bases: *aiospamc.connections.Connection*

Manages a TCP connection.

property connection_string
String representation of the connection.

async open() → Tuple[asyncio.streams.StreamReader, asyncio.streams.StreamWriter]
Opens a connection.

Raises ***AIOSpamcConnectionFailed*** –

class aiospamc.connections.tcp_connection.**TcpConnectionManager**(*host: str*, *port: int*, *ssl: bool = False*, *loop: asyncio.events.AbstractEventLoop = None*)

Bases: *aiospamc.connections.ConnectionManager*

Creates new connections based on host and port provided.

new_connection() → aiospamc.connections.tcp_connection.TcpConnection
Creates a new TCP connection.

Raises ***AIOSpamcConnectionFailed*** –

aiospamc.connections.unix_connection module

Unix domain socket connection and manager.

class aiospamc.connections.unix_connection.**UnixConnection**(*path: str*, *loop: asyncio.events.AbstractEventLoop = None*)

Bases: *aiospamc.connections.Connection*

Manages a Unix domain socket connection.

property connection_string
String representation of the connection.

async open() → Tuple[asyncio.streams.StreamReader, asyncio.streams.StreamWriter]
Opens a connection.

Raises ***AIOSpamcConnectionFailed*** –

class aiospamc.connections.unix_connection.**UnixConnectionManager**(*path: str*, *loop: asyncio.events.AbstractEventLoop = None*)

Bases: *aiospamc.connections.ConnectionManager*

Creates new connections based on Unix domain socket path provided.

new_connection() → aiospamc.connections.unix_connection.UnixConnection
Creates a new Unix domain socket connection.

Raises ***AIOSpamcConnectionFailed*** –

Module contents

Connection and ConnectionManager base classes.

class aiospamc.connections.**Connection**(*loop: asyncio.events.AbstractEventLoop = None*)

Bases: object

Base class for connection objects.

close() → None
Closes the connection.

property connection_string
String representation of the connection.

async open() → Tuple[asyncio.streams.StreamReader, asyncio.streams.StreamWriter]
Connect to a service.

Raises ***AIOSpamcConnectionFailed*** –

async receive() → bytes
Receives data from the connection.

async send(*data: Union[bytes, SupportsBytes]*) → None
Sends data through the connection.

class aiospamc.connections.**ConnectionManager**(*loop: asyncio.events.AbstractEventLoop = None*)

Bases: object

Stores connection parameters and creates connections.

new_connection() → aiospamc.connections.Connection
Creates a connection object.

Submodules

aiospamc.client module

Contains the Client class that is used to interact with SPAMD.

class aiospamc.client.**Client**(*socket_path: str = '/var/run/spamassassin/spamd.sock'*, *host: str = None*, *port: int = 783*, *user: str = None*, *compress: bool = False*, *ssl: bool = False*, *loop: asyncio.events.AbstractEventLoop = None*)

Bases: object

Client object for interacting with SPAMD.

async check(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response
Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async headers(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response
Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain the modified headers of the message.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async ping() → aiospamc.responses.Response
Sends a ping request to the SPAMD service and will receive a response if the service is alive.

Returns Response message will contain 'PONG' if successful.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.

- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async process(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response

Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a modified version of the message.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.

- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async report(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response
Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a report composed by the SPAMD service.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async report_if_spam(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response
Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a report composed by the SPAMD service only if the message is marked as being spam.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async send(*request: aiospamc.requests.Request*) → aiospamc.responses.Response

Sends a request to the SPAMD service.

If the SPAMD service gives a temporary failure response, then its retried.

Parameters **request** – Request object to send.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.

- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async symbols(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response

Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a comma separated list of all the rule names.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.

- ***TimeoutException*** – Timeout during connection.

async tell(*message_class: aiospamc.options.MessageClassOption, message: Union[bytes, SupportsBytes], remove_action: aiospamc.options.ActionOption = None, set_action: aiospamc.options.ActionOption = None*)

Instruct the SPAMD service to to mark the message

Parameters

- **message_class** – An enumeration to classify the message as 'spam' or 'ham.'
- **message** – A byte string containing the contents of the message to be scanned.

  SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.
- **remove_action** – Remove message class for message in database.
- **set_action** – Set message class for message in database.

Returns

Will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a report composed by the SPAMD service only if message is marked as being spam.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

aiospamc.common module

Common classes for the project.

class aiospamc.common.**SpamcBody**
Bases: object

Provides a descriptor for a bytes-like object.

class aiospamc.common.**SpamcHeaders**(*, *headers: Iterator[aiospamc.headers.Header] = None*, **_)
Bases: collections.abc.Mapping

Provides a dictionary-like interface for headers.

items() → a set-like object providing a view on D's items

keys() → a set-like object providing a view on D's keys

values() → an object providing a view on D's values

aiospamc.exceptions module

Collection of exceptions.

exception aiospamc.exceptions.**AIOSpamcConnectionException**
Bases: Exception

Base class for exceptions from the connection.

exception aiospamc.exceptions.**AIOSpamcConnectionFailed**
Bases: *aiospamc.exceptions.AIOSpamcConnectionException*

Connection failed.

exception aiospamc.exceptions.**BadRequest**
Bases: *aiospamc.exceptions.ClientException*

Request is not in the expected format.

exception aiospamc.exceptions.**BadResponse**
Bases: *aiospamc.exceptions.ClientException*

Response is not in the expected format.

exception aiospamc.exceptions.**CantCreateException**
Bases: *aiospamc.exceptions.ResponseException*

Can't create (user) output file.

code = 73

exception aiospamc.exceptions.**ClientException**
Bases: Exception

Base class for exceptions raised from the client.

exception aiospamc.exceptions.**ConfigException**
Bases: *aiospamc.exceptions.ResponseException*

Configuration error.

code = 78

exception aiospamc.exceptions.**DataErrorException**
Bases: *aiospamc.exceptions.ResponseException*

Data format error.

code = 65

exception aiospamc.exceptions.**IOErrorException**
Bases: *aiospamc.exceptions.ResponseException*

Input/output error.

code = 74

exception aiospamc.exceptions.**InternalSoftwareException**
Bases: *aiospamc.exceptions.ResponseException*

Internal software error.

code = 70

exception aiospamc.exceptions.**NoHostException**
Bases: *aiospamc.exceptions.ResponseException*

Hostname unknown.

code = 68

exception aiospamc.exceptions.**NoInputException**
Bases: *aiospamc.exceptions.ResponseException*

Cannot open input.

code = 66

exception aiospamc.exceptions.**NoPermissionException**
Bases: *aiospamc.exceptions.ResponseException*

Permission denied.

code = 77

exception aiospamc.exceptions.**NoUserException**
Bases: *aiospamc.exceptions.ResponseException*

Addressee unknown.

code = 67

exception aiospamc.exceptions.**OSErrorException**
Bases: *aiospamc.exceptions.ResponseException*

System error (e.g. can't fork the process).

code = 71

exception aiospamc.exceptions.**OSFileException**
Bases: *aiospamc.exceptions.ResponseException*

Critical operating system file missing.

code = 72

exception aiospamc.exceptions.**ProtocolException**
Bases: *aiospamc.exceptions.ResponseException*

Remote error in protocol.

code = 76

exception aiospamc.exceptions.**ResponseException**
Bases: Exception

Base class for exceptions raised from a response.

exception aiospamc.exceptions.**TemporaryFailureException**
Bases: *aiospamc.exceptions.ResponseException*

Temporary failure, user is invited to try again.

code = 75

exception aiospamc.exceptions.**TimeoutException**
Bases: *aiospamc.exceptions.ResponseException*

Read timeout.

code = 79

exception aiospamc.exceptions.**UnavailableException**
Bases: *aiospamc.exceptions.ResponseException*

Service unavailable.

code = 69

exception aiospamc.exceptions.**UsageException**
Bases: *aiospamc.exceptions.ResponseException*

Command line usage error.

code = 64

aiospamc.headers module

Collection of request and response headers.

class aiospamc.headers.**Compress**
Bases: *aiospamc.headers.Header*

Compress header. Specifies what encryption scheme to use. So far only 'zlib' is supported.

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**ContentLength**(*length: int = 0*)
Bases: *aiospamc.headers.Header*

ContentLength header. Indicates the length of the body in bytes.

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**DidRemove**(*action: aiospamc.options.ActionOption = None*)
Bases: aiospamc.headers._SetRemoveBase

DidRemove header. Used by SPAMD to indicate if a message was removed from either a local or remote database in response to a TELL request.

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**DidSet**(*action: aiospamc.options.ActionOption = None*)
Bases: aiospamc.headers._SetRemoveBase

DidRemove header. Used by SPAMD to indicate if a message was added to either a local or remote database in response to a TELL request.

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**Header**
Bases: object

Header base class.

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**MessageClass**(*value: aiospamc.options.MessageClassOption = None*)
Bases: *aiospamc.headers.Header*

MessageClass header. Used to specify whether a message is 'spam' or 'ham.'

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**Remove**(*action: aiospamc.options.ActionOption = None*)
Bases: aiospamc.headers._SetRemoveBase

Remove header. Used in a TELL request to ask the SPAMD service remove a message from a local or remote database. The SPAMD service must have the –allow-tells switch in order for this to do anything.

field_name()
Returns the the field name for the header.

class aiospamc.headers.**Set**(*action: aiospamc.options.ActionOption = None*)
Bases: aiospamc.headers._SetRemoveBase

Set header. Used in a TELL request to ask the SPAMD service add a message from a local or remote database. The SPAMD service must have the –allow-tells switch in order for this to do anything.

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**Spam**(*value: bool = False*, *score: float = 0.0*, *threshold: float = 0.0*)
Bases: *aiospamc.headers.Header*

Spam header. Used by the SPAMD service to report on if the submitted message was spam and the score/threshold that it used.

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**User**(*name: str = None*)
Bases: *aiospamc.headers.Header*

User header. Used to specify which user the SPAMD service should use when loading configuration files.

field_name() → str
Returns the the field name for the header.

class aiospamc.headers.**XHeader**(*name: str*, *value: str*)
Bases: *aiospamc.headers.Header*

Extension header. Used to specify a header that's not supported natively by the SPAMD service.

field_name() → str
Returns the the field name for the header.

aiospamc.options module

Data structures used for function parameters.

class aiospamc.options.**ActionOption**(*local*, *remote*)
Bases: tuple

Option to be used in the DidRemove, DidSet, Set, and Remove headers.

local [bool] An action will be performed on the SPAMD service's local database.

remote [bool] An action will be performed on the SPAMD service's remote database.

property local
Alias for field number 0

property remote
Alias for field number 1

class aiospamc.options.**MessageClassOption**
Bases: enum.IntEnum

Option to be used for the MessageClass header.

ham = 2

spam = 1

aiospamc.parser module

Parser object for SPAMC/SPAMD requests and responses.

exception aiospamc.parser.**ParseError**(*index: int*, *message: str*)
Bases: Exception

An exception occurring when parsing.

class aiospamc.parser.**Parser**(*string: bytes = None*)
Bases: object

Parser object for requests and responses.

advance(*by: int*) → None
Advance the current index by number of bytes.

Parameters **by** – Number of bytes in the stream to advance.

body() → bytes
Consumes the rest of the message and returns the contents.

compress_value() → str
Consumes the Compression header value.

consume(*pattern: bytes*) → Match[bytes]
If the pattern matches, advances the index the length of the match. Returns the regular expression match.

Parameters **pattern** – Regular expression pattern.

Raises ***ParseError*** –

content_length_value() → int
Consumes the Content-length header value.

current() → bytes
The remainder of the string that hasn't been parsed.

end() → bool
Whether the parser has parsed the entire string.

header() → aiospamc.headers.Header
Consumes the string and returns an instance of *aiospamc.headers.Header*.

headers() → List[aiospamc.headers.Header]
Consumes all headers.

match(*pattern: bytes*) → Optional[Match[bytes]]
Returns the regular expression matches string at the current index.

Parameters **pattern** – Regular expression pattern.

message() → str
Consumes a string until it matches a newline.

message_class_value() → aiospamc.options.MessageClassOption
Consumes the Message-class header value.

method() → str
Consumes the method name in a request.

newline() → None
Consumes a newline sequence (carriage return and line feed).

request() → aiospamc.requests.Request
Consumes a SPAMC request.

response() → aiospamc.responses.Response
Consumes a SPAMD response.

set_remove_value() → aiospamc.options.ActionOption
Consumes the value for the DidRemove, DidSet, Remove and Set headers.

static skip(*func: Callable*) → None
Makes the parser function optional by ignore whether it raises a *aiospamc.parser.ParseError* exception or not.

Parameters **func** – Function to execute.

spam_value() → Mapping[str, Union[bool, float]]
Consumes the Spam header value.

spamc_protocol() → str
Consumes the string "SPAMC".

spamd_protocol() → str
Consumes the string "SPAMD".

status_code() → int
Consumes the status code.

user_value() → str
Consumes the User header value.

version() → str
Consumes a version pattern. For example, "1.5".

whitespace() → None
Consumes spaces or tabs.

aiospamc.parser.**checkpoint**(*func*) → Callable
A decorator to restore the index if an exception occurred.

aiospamc.parser.**parse**(*string*) → Union[aiospamc.requests.Request, aiospamc.responses.Response]
Parses a request or response.

aiospamc.requests module

Contains all requests that can be made to the SPAMD service.

class aiospamc.requests.**Request**(*verb: str*, *version: str = '1.5'*, *headers: Iterator[aiospamc.headers.Header] = None*, *body: Union[bytes, SupportsBytes] = None*)
Bases: object

SPAMC request object.

body
Provides a descriptor for a bytes-like object.

aiospamc.responses module

Contains classes used for responses.

class aiospamc.responses.**Response**(*version: str*, *status_code: aiospamc.responses.Status*, *message: str*, *headers: Iterator[aiospamc.headers.Header] = None*, *body=None*)
Bases: object

Class to encapsulate response.

body
Provides a descriptor for a bytes-like object.

raise_for_status() → None

class aiospamc.responses.**Status**
Bases: enum.IntEnum

Enumeration of status codes that the SPAMD will accompany with a response.

Reference: https://svn.apache.org/repos/asf/spamassassin/trunk/spamd/spamd.raw Look for the %resphash variable.

EX_CANTCREAT = 73

EX_CONFIG = 78

EX_DATAERR = 65

EX_IOERR = 74

EX_NOHOST = 68

EX_NOINPUT = 66

EX_NOPERM = 77

EX_NOUSER = 67

EX_OK = 0

EX_OSERR = 71

EX_OSFILE = 72

EX_PROTOCOL = 76

EX_SOFTWARE = 70

EX_TEMPFAIL = 75

EX_TIMEOUT = 79

EX_UNAVAILABLE = 69

EX_USAGE = 64

Module contents

aiospamc package.

An asyncio-based library to communicate with SpamAssassin's SPAMD service.

class aiospamc.**Client**(*socket_path: str = '/var/run/spamassassin/spamd.sock'*, *host: str = None*, *port: int = 783*, *user: str = None*, *compress: bool = False*, *ssl: bool = False*, *loop: asyncio.events.AbstractEventLoop = None*)

Bases: object

Client object for interacting with SPAMD.

async check(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response

Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.

- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async headers(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response

Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain the modified headers of the message.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async ping() → aiospamc.responses.Response

Sends a ping request to the SPAMD service and will receive a response if the service is alive.

Returns Response message will contain 'PONG' if successful.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async process(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response

Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a modified version of the message.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.

- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async report(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response

Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a report composed by the SPAMD service.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.

- ***TimeoutException*** – Timeout during connection.

async report_if_spam(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response
Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a report composed by the SPAMD service only if the message is marked as being spam.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async send(*request: aiospamc.requests.Request*) → aiospamc.responses.Response
Sends a request to the SPAMD service.

If the SPAMD service gives a temporary failure response, then its retried.

Parameters **request** – Request object to send.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.

- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async symbols(*message: Union[bytes, SupportsBytes]*) → aiospamc.responses.Response

Request the SPAMD service to check a message with a HEADERS request.

Parameters **message** – A byte string containing the contents of the message to be scanned.

SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.

Returns

The response will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a comma separated list of all the rule names.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.

- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.
- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

async tell(*message_class: aiospamc.options.MessageClassOption, message: Union[bytes, SupportsBytes], remove_action: aiospamc.options.ActionOption = None, set_action: aiospamc.options.ActionOption = None*)

Instruct the SPAMD service to to mark the message

Parameters

- **message_class** – An enumeration to classify the message as 'spam' or 'ham.'
- **message** – A byte string containing the contents of the message to be scanned.

  SPAMD will perform a scan on the included message. SPAMD expects an RFC 822 or RFC 2822 formatted email.
- **remove_action** – Remove message class for message in database.
- **set_action** – Set message class for message in database.

Returns

Will contain a 'Spam' header if the message is marked as spam as well as the score and threshold.

The body will contain a report composed by the SPAMD service only if message is marked as being spam.

Raises

- ***BadResponse*** – If the response from SPAMD is ill-formed this exception will be raised.
- ***AIOSpamcConnectionFailed*** – Raised if an error occurred when trying to connect.
- ***UsageException*** – Error in command line usage.
- ***DataErrorException*** – Error with data format.
- ***NoInputException*** – Cannot open input.
- ***NoUserException*** – Addressee unknown.
- ***NoHostException*** – Hostname unknown.
- ***UnavailableException*** – Service unavailable.
- ***InternalSoftwareException*** – Internal software error.
- ***OSErrorException*** – System error.
- ***OSFileException*** – Operating system file missing.
- ***CantCreateException*** – Cannot create output file.
- ***IOErrorException*** – Input/output error.
- ***TemporaryFailureException*** – Temporary failure, may reattempt.
- ***ProtocolException*** – Error in the protocol.

- ***NoPermissionException*** – Permission denied.
- ***ConfigException*** – Error in configuration.
- ***TimeoutException*** – Timeout during connection.

class aiospamc.**MessageClassOption**
Bases: enum.IntEnum

Option to be used for the MessageClass header.

ham = 2

spam = 1

class aiospamc.**ActionOption**(*local*, *remote*)
Bases: tuple

Option to be used in the DidRemove, DidSet, Set, and Remove headers.

local [bool] An action will be performed on the SPAMD service's local database.

remote [bool] An action will be performed on the SPAMD service's remote database.

property local
Alias for field number 0

property remote
Alias for field number 1

1.3 SPAMC/SPAMD Protocol As Implemented by SpamAssassin

1.3.1 Requests and Responses

The structure of a request is similar to an HTTP request.[1] The method/verb, protocol name and version are listed followed by headers separated by newline characters (carriage return and linefeed or \r\n). Following the headers is a blank line with a newline (\r\n). If there is a message body it will be added after all headers.

The current requests are *CHECK*, *HEADERS*, *PING*, *PROCESS*, *REPORT*, *REPORT_IFSPAM*, *SKIP*, *SYMBOLS*, and *TELL*:

```
METHOD SPAMC/1.5\r\n
HEADER_NAME1 : HEADER_VALUE1\r\n
HEADER_NAME2 : HEADER_VALUE2\r\n
...
\r\n
REQUEST_BODY
```

The structure of responses are also similar to HTTP responses. The protocol name, version, status code, and message are listed on the first line. Any headers are also listed and all are separated by newline characters. Following the headers is a newline. If there is a message body it's included after all headers:

```
SPAMD/1.5 STATUS_CODE MESSAGE\r\n
HEADER_NAME1 : HEADER_VALUE1\r\n
HEADER_NAME2 : HEADER_VALUE2\r\n
...
\r\n
RESPONSE_BODY
```

[1] https://svn.apache.org/viewvc/spamassassin/branches/3.4/spamd/PROTOCOL?revision=1676616&view=co

The following are descriptions of the requests that can be sent and examples of the responses that you can expect to receive.

CHECK

Instruct SpamAssassin to process the included message.

Request

Required Headers

- *Content-length*

Optional Headers

- *Compress*
- *User*

Required body

An email based on the **RFC 5322** standard.

Response

Will include a Spam header with a "True" or "False" value, followed by the score and threshold. Example:

```
SPAMD/1.1 0 EX_OK
Spam: True ; 1000.0 / 5.0
```

HEADERS

Process the included message and return only the modified headers.

Request

Required Headers

- *Content-length*

Optional Headers

- *Compress*
- *User*

Required Body

An email based on the **RFC 5322** standard.

Response

Will return the modified headers of the message in the body. The *Spam* header is also included.

```
SPAMD/1.1 0 EX_OK
Spam: True ; 1000.0 / 5.0
Content-length: 654

Received: from localhost by debian
    with SpamAssassin (version 3.4.0);
    Tue, 10 Jan 2017 11:09:26 -0500
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Subject: Test spam mail (GTUBE)
Date: Wed, 23 Jul 2003 23:30:00 +0200
Message-Id: <GTUBE1.1010101@example.net>
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on debian
X-Spam-Flag: YES
X-Spam-Level: **********************************************
X-Spam-Status: Yes, score=1000.0 required=5.0 tests=GTUBE,NO_RECEIVED,
    NO_RELAYS autolearn=no autolearn_force=no version=3.4.0
MIME-Version: 1.0Content-Type: multipart/mixed; boundary="----------=_58750736.
↪8D9F70BC"
```

PING

Send a request to test if the server is alive.

Request

Required Headers

None.

Optional Headers

None.

Response

Example:

```
SPAMD/1.5 0 PONG
```

PROCESS

Instruct SpamAssassin to process the message and return the modified message.

Request

Required Headers

- *Content-length*

Optional Headers

- *Compress*
- *User*

Required Body

An email based on the **RFC 5322** standard.

Response

Will return a modified message in the body. The *Spam* header is also included. Example:

```
SPAMD/1.1 0 EX_OK
Spam: True ; 1000.0 / 5.0
Content-length: 2948

Received: from localhost by debian
    with SpamAssassin (version 3.4.0);
    Tue, 10 Jan 2017 10:57:02 -0500
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Subject: Test spam mail (GTUBE)
Date: Wed, 23 Jul 2003 23:30:00 +0200
Message-Id: <GTUBE1.1010101@example.net>
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on debian
X-Spam-Flag: YES
X-Spam-Level: **************************************************
X-Spam-Status: Yes, score=1000.0 required=5.0 tests=GTUBE,NO_RECEIVED,
    NO_RELAYS autolearn=no autolearn_force=no version=3.4.0
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----------=_5875044E.D4EFFFD7"

This is a multi-part message in MIME format.

------------=_5875044E.D4EFFFD7
Content-Type: text/plain; charset=iso-8859-1
Content-Disposition: inline
Content-Transfer-Encoding: 8bit

Spam detection software, running on the system "debian",
```

(continues on next page)

(continued from previous page)

```
has identified this incoming email as possible spam.  The original
message has been attached to this so you can view it or label
similar future email.  If you have any questions, see
@@CONTACT_ADDRESS@@ for details.

Content preview:  This is the GTUBE, the Generic Test for Unsolicited Bulk Email
If your spam filter supports it, the GTUBE provides a test by which you can
verify that the filter is installed correctly and is detecting incoming spam.
You can send yourself a test mail containing the following string of characters
(in upper case and with no white spaces and line breaks): [...]

Content analysis details:   (1000.0 points, 5.0 required)

pts rule name              description
---- ---------------------- --------------------------------------------------
1000 GTUBE                   BODY: Generic Test for Unsolicited Bulk Email
-0.0 NO_RELAYS               Informational: message was not relayed via SMTP
-0.0 NO_RECEIVED             Informational: message has no Received headers



------------=_5875044E.D4EFFFD7
Content-Type: message/rfc822; x-spam-type=original
Content-Description: original message before SpamAssassin
Content-Disposition: inline
Content-Transfer-Encoding: 8bit

Subject: Test spam mail (GTUBE)
Message-ID: <GTUBE1.1010101@example.net>
Date: Wed, 23 Jul 2003 23:30:00 +0200
From: Sender <sender@example.net>
To: Recipient <recipient@example.net>
Precedence: junk
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

This is the GTUBE, the
    Generic
    Test for
    Unsolicited
    Bulk
    Email

If your spam filter supports it, the GTUBE provides a test by which you
can verify that the filter is installed correctly and is detecting incoming
spam. You can send yourself a test mail containing the following string of
characters (in upper case and with no white spaces and line breaks):

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

You should send this test mail from an account outside of your network.


------------=_5875044E.D4EFFFD7--
```

REPORT

Send a request to process a message and return a report.

Request

Required Headers

- *Content-length*

Optional Headers

- *Compress*
- *User*

Required body

An email based on the **RFC 5322** standard.

Response

Response returns the *Spam* header and the body containing a report of the message scanned.

Example:

```
SPAMD/1.1 0 EX_OK
Content-length: 1071
Spam: True ; 1000.0 / 5.0

Spam detection software, running on the system "debian",
has identified this incoming email as possible spam.  The original
message has been attached to this so you can view it or label
similar future email.  If you have any questions, see
@@CONTACT_ADDRESS@@ for details.

Content preview:  This is the GTUBE, the Generic Test for Unsolicited Bulk Email
   If your spam filter supports it, the GTUBE provides a test by which you can
   verify that the filter is installed correctly and is detecting incoming spam.
   You can send yourself a test mail containing the following string of characters
   (in upper case and with no white spaces and line breaks): [...]

Content analysis details:   (1000.0 points, 5.0 required)

 pts rule name              description
---- ---------------------- --------------------------------------------------
1000 GTUBE                  BODY: Generic Test for Unsolicited Bulk Email
-0.0 NO_RELAYS              Informational: message was not relayed via SMTP
-0.0 NO_RECEIVED            Informational: message has no Received headers
```

REPORT_IFSPAM

Matches the *REPORT* request, with the exception a report will not be generated if the message is not spam.

SKIP

Sent when a connection is made in error. The SPAMD service will immediately close the connection.

Request

Required Headers

None.

Optional Headers

None.

SYMBOLS

Instruct SpamAssassin to process the message and return the rules that were matched.

Request

Required Headers

- *Content-length*

Optional Headers

- *Compress*
- *User*

Required body

An email based on the **RFC 5322** standard.

Response

Response includes the *Spam* header. The body contains the SpamAssassin rules that were matched. Example:

```
SPAMD/1.1 0 EX_OK
Content-length: 27
Spam: True ; 1000.0 / 5.0

GTUBE,NO_RECEIVED,NO_RELAYS
```

TELL

Send a request to classify a message and add or remove it from a database. The message type is defined by the *Message-class*. The *Remove* and *Set* headers are used to choose the location ("local" or "remote") to add or remove it. SpamAssassin will return an error if a request tries to apply a conflicting change (e.g. both setting and removing to the same location).

Note: The SpamAssassin daemon must have the `--allow-tell` option enabled to support this feature.

Request

Required Headers

- *Content-length*
- *Message-class*
- *Remove* and/or *Set*
- *User*

Optional Headers

- *Compress*

Required Body

An email based on the **RFC 5322** standard.

Response

If successful, the response will include the *DidRemove* and/or *DidSet* headers depending on the request.

Response from a request that sent a *Remove*:

```
SPAMD/1.1 0 EX_OK
DidRemove: local
Content-length: 2
```

Response from a request that sent a *Set*:

```
SPAMD/1.1 0 EX_OK
DidSet: local
Content-length: 2
```

1.3.2 Headers

Headers are structured very simply. They have a name and value which are separated by a colon (:). All headers are followed by a newline. The current headers include *Compress*, *Content-length*, *DidRemove*, *DidSet*, *Message-class*, *Remove*, *Set*, *Spam*, and *User*.

For example:

```
Content-length: 42\r\n
```

The following is a list of headers defined by SpamAssassin, although anything is allowable as a header. If an unrecognized header is included in the request or response it should be ignored.

Compress

Specifies that the body is compressed and what compression algorithm is used. Contains a string of the compression algorithm. Currently only `zlib` is supported.

Content-length

The length of the body in bytes. Contains an integer representing the body length.

DidRemove

Included in a response to a *TELL* request. Identifies which databases a message was removed from. Contains a string containing either `local`, `remote` or both seprated by a comma.

DidSet

Included in a response to a *TELL* request. Identifies which databases a message was set in. Contains a string containing either `local`, `remote` or both seprated by a comma.

Message-class

Classifies the message contained in the body. Contains a string containing either `local`, `remote` or both seprated by a comma.

Remove

Included in a *TELL* request to remove the message from the specified database. Contains a string containing either `local`, `remote` or both seprated by a comma.

Set

Included in a *TELL* request to remove the message from the specified database. Contains a string containing either `local`, `remote` or both seprated by a comma.

Spam

Identify whether the message submitted was spam or not including the score and threshold. Contains a string containing a boolean if the message is spam (either `True`, `False`, `Yes`, or `No`), followed by a `;`, a floating point number representing the score, followed by a `/`, and finally a floating point number representing the threshold of which to consider it spam.

For example:

```
Spam: True ; 1000.0 / 5.0
```

User

Specify which user the request will run under. SpamAssassin will use the configuration files for the user included in the header. Contains a string containing the name of the user.

1.3.3 Status Codes

A status code is an integer detailing whether the request was successful or if an error occurred.

The following status codes are defined in the SpamAssassin source repository[2].

EX_OK

Code: 0

Definition: No problems were found.

EX_USAGE

Code: 64

Definition: Command line usage error.

EX_DATAERR

Code: 65

Definition: Data format error.

EX_NOINPUT

Code: 66

Definition: Cannot open input.

EX_NOUSER

Code: 67

Definition: Addressee unknown.

EX_NOHOST

Code: 68

Definition: Hostname unknown.

[2] https://svn.apache.org/viewvc/spamassassin/branches/3.4/spamd/spamd.raw?revision=1749346&view=co

EX_UNAVAILABLE

Code: 69

Definition: Service unavailable.

EX_SOFTWARE

Code: 70

Definition: Internal software error.

EX_OSERR

Code: 71

Definition: System error (e.g. can't fork the process).

EX_OSFILE

Code: 72

Definition: Critical operating system file missing.

EX_CANTCREAT

Code: 73

Definition: Can't create (user) output file.

EX_IOERR

Code: 74

Definition: Input/output error.

EX_TEMPFAIL

Code: 75

Definition: Temporary failure, user is invited to retry.

EX_PROTOCOL

Code: 76

Definition: Remote error in protocol.

EX_NOPERM

Code: 77

Definition: Permission denied.

EX_CONFIG

Code: 78

Definition: Configuration error.

EX_TIMEOUT

Code: 79

Definition: Read timeout.

1.3.4 Body

SpamAssassin will generally want the body of a request to be in a supported RFC email format. The response body will differ depending on the type of request that was sent.

1.3.5 References

CHAPTER

TWO

INDICES AND TABLES

- genindex
- modindex
- search

PYTHON MODULE INDEX

a

INDEX