

Package ‘aws.signature’

July 1, 2017

Type Package

Title Amazon Web Services Request Signatures

Version 0.3.5

Date 2017-07-01

Description Generates version 2 and version 4 request signatures for Amazon Web Services ('AWS') <<https://aws.amazon.com/>> Application Programming Interfaces ('APIs').

License GPL (>= 2)

Imports digest, base64enc

Suggests testthat, aws.ec2metadata (>= 0.1.2)

URL <https://github.com/cloudyr/aws.signature>

BugReports <https://github.com/cloudyr/aws.signature/issues>

RoxygenNote 6.0.1

NeedsCompilation no

Author Thomas J. Leeper [aut, cre]

Maintainer Thomas J. Leeper <thosjleeper@gmail.com>

Repository CRAN

Date/Publication 2017-07-01 07:58:47 UTC

R topics documented:

aws.signature-package	2
canonical_request	2
locate_credentials	4
read_credentials	5
signature_v2_auth	6
signature_v4	8
signature_v4_auth	9
string_to_sign	11

Index	13
--------------	-----------

Arguments

verb	A character string containing the HTTP verb being used in the request.
canonical_uri	A character string containing the “canonical URI”, meaning the contents of the API request URI excluding the host and the query parameters.
query_args	A named list of character strings containing the query string values (if any) used in the API request.
canonical_headers	A named list of character strings containing the headers used in the request.
request_body	The body of the HTTP request, or a filename. If a filename, hashing is performed on the file without reading it into memory.

Details

This function creates a “Canonical Request”, which is part of the Signature Version 4.

Value

A list containing

Author(s)

Thomas J. Leeper <thosjleeper@gmail.com>

References

[Create a Canonical Request For Signature Version 4](#)

See Also

[signature_v4](#), [signature_v4_auth](#)
[link{signature_v4_aut}](#), [string_to_sign](#)

Examples

```
# From AWS documentation
# http://docs.aws.amazon.com/general/latest/gr/sigv4-create-canonical-request.html
fromDocs <- "POST
/

content-type:application/x-www-form-urlencoded; charset=utf-8
host:iam.amazonaws.com
x-amz-date:20110909T233600Z

content-type;host;x-amz-date
b6359072c78d70ebee1e81adcbab4f01bf2c23245fa365ef83fe8f1f955085e2"

hdrs <- list(`Content-Type` = "application/x-www-form-urlencoded; charset=utf-8",
            Host = "iam.amazonaws.com",
            `x-amz-date` = "20110909T233600Z")
```

```
r <- canonical_request(verb = "POST",
  canonical_uri = "/",
  query_args = list(),
  canonical_headers = hdrs,
  request_body = "Action=ListUsers&Version=2010-05-08")

identical(fromDocs, r$canonical)
```

locate_credentials *Locate AWS Credentials*

Description

Locate AWS credentials from likely sources

Usage

```
locate_credentials(key = NULL, secret = NULL, session_token = NULL,
  region = NULL, file = NULL, profile = "default",
  default_region = "us-east-1", verbose = FALSE)
```

Arguments

key	An AWS Access Key ID
secret	An AWS Secret Access Key
session_token	Optionally, an AWS Security Token Service (STS) temporary Session Token
region	A character string containing the AWS region for the request. If missing, "us-east-1" is assumed.
file	A character string containing a path to a '.aws/credentials' file.
profile	A character string specifying which profile to use from the file. By default, the "default" profile is used.
default_region	A character string specifying a default string to use of no user-supplied value is found.
verbose	A logical indicating whether to be verbose.

Details

These functions locate values of AWS credentials (access key, secret access key, session token, and region) from likely sources. The order in which these are searched is as follows:

1. values passed to the function
2. environment variables (AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY, AWS_SESSION_TOKEN, AWS_DEFAULT_REGION)
3. an IAM instance role (on the running EC2 instance from which this function is called) as identified by [metadata](#)

4. a specified profile in a local credentials dot file in the current working directory
5. the default profile in a local credentials dot file in the current working directory
6. a specified profile in a global credentials dot file in, typically in ‘~/ .aws/credentials’. See [use_credentials](#) for details
7. the default profile in a global credentials dot file in, typically in ‘~/ .aws/credentials’. See [use_credentials](#) for details

See Also

[signature_v4](#), [signature_v2_auth](#), [use_credentials](#)

read_credentials *Use Credentials from .aws/credentials File*

Description

Use a profile from a ‘.aws/credentials’ file

Usage

```
read_credentials(file = default_credentials_file())
```

```
use_credentials(profile = "default", file = default_credentials_file())
```

```
default_credentials_file()
```

Arguments

file	A character string containing a path to a ‘.aws/credentials’ file. By default, the standard/centralized file is used. For <code>use_credentials</code> , this can also be an object of class “aws_credentials” (as returned by <code>use_credentials</code>).
profile	A character string specifying which profile to use from the file. By default, the “default” profile is used.

Details

`read_credentials` reads and parses a ‘.aws/credentials’ file into an object of class “aws_credentials”.
`use_credentials` uses credentials from a profile stored in a credentials file to set the environment variables used by this package.

Author(s)

Thomas J. Leeper <thosjleeper@gmail.com>

References

[Amazon blog post describing the format](#)

See Also

[signature_v2_auth](#), [locate_credentials](#)

Examples

```
## Not run:
# set environment variables from a profile
use_credentials()

# read and parse a file
read_credentials()

## End(Not run)
```

signature_v2_auth	<i>Signature Version 2</i>
-------------------	----------------------------

Description

Generates AWS Signature Version 2

Usage

```
signature_v2_auth(datetime = format(Sys.time(), "%Y-%M-%dT%H:%M:%S", tz
  = "UTC"), verb, service, path, query_args = list(), key = NULL,
  secret = NULL, verbose = FALSE)
```

Arguments

datetime	A character string containing a date in the form of “YYYY-MM-DDTH:M:S”. If missing, it is generated automatically using Sys.time .
verb	A character string specify an HTTP verb/method (e.g., “GET”).
service	A character string containing the full hostname of an AWS service (e.g., “iam.amazonaws.com”, etc.)
path	A character string specify the path to the API endpoint.
query_args	A list containing named query arguments.
key	An AWS Access Key ID. If NULL, it is retrieved using locate_credentials .
secret	An AWS Secret Access Key. If NULL, it is retrieved using locate_credentials .
verbose	A logical indicating whether to be verbose.

Details

This function generates an AWS Signature Version 2 for authorizing API requests. The function returns both an updated set of query string parameters, containing the required signature-related entries, as well as a Signature field containing the Signature string itself.

Value

A list.

Author(s)

Thomas J. Leeper <thosjleeper@gmail.com>

References

[AWS General Reference: Signature Version 2 Signing Process](#)

See Also

[signature_v4_auth](#), [use_credentials](#)

Examples

```
# examples from:
# http://docs.aws.amazon.com/general/latest/gr/signature-version-2.html

true_string <- paste0("GET\n",
  "elasticmapreduce.amazonaws.com\n",
  "/\n",
  "AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE",
  "&Action=DescribeJobFlows",
  "&SignatureMethod=HmacSHA256",
  "&SignatureVersion=2",
  "&Timestamp=2011-10-03T15:19:30",
  "&Version=2009-03-31", collapse = "")
true_sig <- "i91nKc4PWAt0JJIdXwz9HxZCJDdiy6cf/Mj6vPxyYIs="

q1 <-
list(Action = "DescribeJobFlows",
  Version = "2009-03-31",
  AWSAccessKeyId = "AKIAIOSFODNN7EXAMPLE",
  SignatureVersion = "2",
  SignatureMethod = "HmacSHA256",
  Timestamp = "2011-10-03T15:19:30")

sig1 <-
signature_v2_auth(datetime = "2011-10-03T15:19:30",
  service = "elasticmapreduce.amazonaws.com",
  verb = "GET",
  path = "/",
  query_args = q1,
  key = q1$AWSAccessKeyId,
  secret = "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY")
identical(true_string, sig1$CanonicalRequest)
identical(true_sig, sig1$Signature)

# leaving out some defaults
q2 <-
```

```
list(Action = "DescribeJobFlows",
      Version = "2009-03-31",
      Timestamp = "2011-10-03T15:19:30")
sig2 <-
signature_v2_auth(datetime = "2011-10-03T15:19:30",
                  service = "elasticmapreduce.amazonaws.com",
                  verb = "GET",
                  path = "/",
                  query_args = q2,
                  key = "AKIAIOSFODNN7EXAMPLE",
                  secret = "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY")
identical(true_string, sig2$CanonicalRequest)
identical(true_sig, sig2$Signature)
```

signature_v4

Signature Version 4

Description

Generates AWS Signature Version 4

Usage

```
signature_v4(secret = NULL, date = format(Sys.time(), "%Y%m%d"),
             region = NULL, service, string_to_sign, verbose = FALSE)
```

Arguments

secret	An AWS Secret Access Key. If NULL, it is retrieved using locate_credentials .
date	A character string containing a date in the form of "YYMMDD". If missing, it is generated automatically using Sys.time .
region	A character string containing the AWS region for the request. If NULL, it is retrieved using locate_credentials or "us-east-1" is used.
service	A character string containing the AWS service (e.g., "iam", "host", "ec2").
string_to_sign	A character string containing the String To Sign, possibly returned by string_to_sign .
verbose	A logical indicating whether to be verbose.

Details

This function generates an AWS Signature Version 4 for authorizing API requests.

Author(s)

Thomas J. Leeper <thosjleeper@gmail.com>

References

- [AWS General Reference: Signature Version 4 Signing Process](#)
- [AWS General Reference: Examples of How to Derive a Version 4 Signing Key](#)
- [Amazon S3 API Reference: Authenticating Requests \(AWS Signature Version 4\)](#)

See Also

[signature_v2_auth](#), [use_credentials](#)

Examples

```
# From AWS documentation
# http://docs.aws.amazon.com/general/latest/gr/signature-v4-test-suite.html
StringToSign <- "AWS4-HMAC-SHA256
20110909T233600Z
20110909/us-east-1/host/aws4_request
e25f777ba161a0f1baf778a87faf057187cf5987f17953320e3ca399feb5f00d"

sig <-
signature_v4(secret = 'wJalrXUtnFEMI/K7MDENG+bPxRfiCYEXAMPLEKEY',
             date = '20110909',
             region = 'us-east-1',
             service = 'host',
             string_to_sign = StringToSign)
identical(sig, "be7148d34ebccdc6423b19085378aa0bee970bdc61d144bd1a8c48c33079ab09")

# http://docs.aws.amazon.com/general/latest/gr/sigv4-calculate-signature.html
StringToSign <- "AWS4-HMAC-SHA256
20110909T233600Z
20110909/us-east-1/iam/aws4_request
3511de7e95d28ecd39e9513b642aee07e54f4941150d8df8bf94b328ef7e55e2"

sig <-
signature_v4(secret = 'wJalrXUtnFEMI/K7MDENG+bPxRfiCYEXAMPLEKEY',
             date = '20110909',
             region = 'us-east-1',
             service = 'iam',
             string_to_sign = StringToSign)
identical(sig, "ced6826de92d2bdeed8f846f0bf508e8559e98e4b0199114b84c54174deb456c")
```

signature_v4_auth *Signature Version 4*

Description

AWS Signature Version 4 for use in query or header authorization

Usage

```
signature_v4_auth(datetime = format(Sys.time(), "%Y%M%dT%H%M%SZ", tz =
  "UTC"), region = NULL, service, verb, action, query_args = list(),
  canonical_headers, request_body, key = NULL, secret = NULL,
  session_token = NULL, query = FALSE, algorithm = "AWS4-HMAC-SHA256",
  verbose = FALSE)
```

Arguments

datetime	A character string containing a datetime in the form of “YYYYMMDDTHH-MMSSZ”. If missing, it is generated automatically using Sys.time .
region	A character string containing the AWS region for the request. See locate_credentials .
service	A character string containing the AWS service (e.g., “iam”, “host”, “ec2”).
verb	A character string containing the HTTP verb being used in the request.
action	A character string containing the API endpoint used in the request.
query_args	A named list of character strings containing the query string values (if any) used in the API request, passed to canonical_request .
canonical_headers	A named list of character strings containing the headers used in the request.
request_body	The body of the HTTP request.
key	An AWS Access Key ID. See locate_credentials .
secret	An AWS Secret Access Key. See locate_credentials .
session_token	Optionally, an AWS Security Token Service (STS) temporary Session Token. This is added automatically as a header to canonical_headers. See locate_credentials .
query	A logical. Currently ignored.
algorithm	A character string containing the hashing algorithm used in the request. Should only be “SHA256”.
verbose	A logical indicating whether to be verbose.

Details

This function generates an AWS Signature Version 4 for authorizing API requests.

Value

A list of class “aws_signature_v4”, containing the information needed to sign an AWS API request using either query string authentication or request header authentication. Specifically, the list contains:

Algorithm	A character string containing the hashing algorithm used during the signing process (default is SHA256).
Credential	A character string containing an identifying credential “scoped” to the region, date, and service of the request.
Date	A character string containing a YYYYMMDD-formatted date.

SignedHeaders	A character string containing a semicolon-separated listing of request headers used in the signature.
BodyHash	A character string containing a SHA256 hash of the request body.
StringToSign	A character string containing the string to sign for the request.
Signature	A character string containing a request signature hash.
SignatureHeader	A character string containing a complete Authorization header value.
Region	A character string containing the region identified by <code>locate_credentials</code> .

These values can either be used as query parameters in a REST-style API request, or as request headers. If authentication is supplied via query string parameters, the query string should include the following:

```
Action=action &X-Amz-Algorithm=Algorithm &X-Amz-Credential=URLencode(Credentials)
&X-Amz-Date=Date &X-Amz-Expires=timeout &X-Amz-SignedHeaders=SignedHeaders
```

where `action` is the API endpoint being called and `timeout` is a numeric value indicating when the request should expire.

If signing a request using header-based authentication, the “Authorization” header in the request should be included with the request that looks as follows:

```
Authorization: Algorithm Credential=Credential, SignedHeaders=SignedHeaders, Signature=Signature
```

This is the value printed by default for all objects of class “aws_signature_v4”.

Author(s)

Thomas J. Leeper <thosjleeper@gmail.com>

References

[AWS General Reference: Signature Version 4 Signing Process](#)

[Amazon S3 API Reference: Authenticating Requests \(AWS Signature Version 4\)](#)

<http://docs.aws.amazon.com/general/latest/gr/sigv4-add-signature-to-request.html>

See Also

[signature_v4](#), [signature_v2_auth](#)

string_to_sign

Construct a String To Sign

Description

Construct a String to Sign from request elements

Usage

```
string_to_sign(algorithm = "AWS4-HMAC-SHA256", datetime, region, service,
              request_hash)
```

Arguments

algorithm	A character string containing the hashing algorithm used in signing process. Should only be "AWS4-HMAC-SHA256".
datetime	A character string containing a UTC date in the form of "YYYYMMDDTHH-MMSSZ".
region	A character string containing the AWS region for the request.
service	A character string containing the AWS service (e.g., "iam", "host", "ec2").
request_hash	A character string containing the hash of the canonical request, perhaps as returned by canonical_request .

Details

This function creates a "String To Sign", which is part of the Signature Version 4.

Author(s)

Thomas J. Leeper <thosjleeper@gmail.com>

References

[Create a String to Sign for Signature Version 4](#)

See Also

[signature_v4](#), [signature_v4_auth](#)

Examples

```
# From AWS documentation
rh <- "3511de7e95d28ecd39e9513b642aee07e54f4941150d8df8bf94b328ef7e55e2"
sts <-
string_to_sign(datetime = "20110909T233600Z",
              region = "us-east-1",
              service = "iam",
              request_hash = rh)
identical(sts, "AWS4-HMAC-SHA256
20110909T233600Z
20110909/us-east-1/iam/aws4_request
3511de7e95d28ecd39e9513b642aee07e54f4941150d8df8bf94b328ef7e55e2")
```

Index

*Topic **package**

- aws.signature-package, [2](#)
- aws.signature (aws.signature-package), [2](#)
- aws.signature-package, [2](#)
- canonical_request, [2](#), [10](#), [12](#)
- default_credentials_file
 - (read_credentials), [5](#)
- locate_credentials, [2](#), [4](#), [6](#), [8](#), [10](#), [11](#)
- metadata, [4](#)
- read_credentials, [5](#)
- signature_v2_auth, [2](#), [5](#), [6](#), [6](#), [9](#), [11](#)
- signature_v4, [3](#), [5](#), [8](#), [11](#), [12](#)
- signature_v4_auth, [2](#), [3](#), [7](#), [9](#), [12](#)
- string_to_sign, [3](#), [8](#), [11](#)
- Sys.time, [6](#), [8](#), [10](#)
- use_credentials, [2](#), [5](#), [7](#), [9](#)
- use_credentials (read_credentials), [5](#)