Package 'aws.signature'

June 1, 2020

Type Package

Title Amazon Web Services Request Signatures

Version 0.6.0

Date 2020-06-01

Description Generates version 2 and version 4 request signatures for Amazon Web Services ('AWS') <https://aws.amazon.com/> Application Programming Interfaces ('APIs') and provides a mechanism for retrieving credentials from environment variables, 'AWS' credentials files, and 'EC2' instance metadata. For use on 'EC2' instances, users will need to install the suggested package 'aws.ec2metadata' <https://cran.r-project.org/package=aws.ec2metadata>.

License GPL (>= 2)

Imports digest, base64enc

Suggests testthat (>= 2.1.0), aws.ec2metadata (>= 0.1.6)

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

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

RoxygenNote 7.1.0

NeedsCompilation no

Author Thomas J. Leeper [aut] (<https://orcid.org/0000-0003-4097-6326>),
Jonathan Stott [cre, aut],
Mike Kaminsky [ctb]

Maintainer Jonathan Stott <jonathan.stott@magairports.com>

Repository CRAN

Date/Publication 2020-06-01 10:10:02 UTC

R topics documented:

`aws.signature-package` *Amazon Web Services Request Signatures*

Description

Generates Amazon Web Services (AWS) request signatures for RESTful APIs.

Details

This package contains functions mostly intended for developers to use in building API client packages for Amazon Web Services APIs.

The main function of interest is `signature_v4_auth`, which wraps the other internal functions and returns a named list of elements to be used in authenticating an API request using AWS Signature Version 4. Another function, `signature_v2_auth` implements the older, mostly deprecated Version 2 algorithm.

Recent versions of the package (>= 0.2.8) identify credentials by walking through a tree of possible sources of values (described in `locate_credentials`), with optional verbosity, in a manner similar to the Python boto 3 library.

A lower-level function that may be of use to end users is `use_credentials`, which sets the environment variables used by this package based upon values specified in a '`.aws/credentials`' file. That function is called by default during package load, if no environment variables are set.

To use this (and any cloudyr package) on AWS EC2 instances or ECS tasks, users will also need to install the aws.ec2metadata package, which allows `locate_credentials` to know it is running in an instance and check for relevant values.

Author(s)

Thomas J. Leeper <thosjleeper@gmail.com>

See Also

`signature_v4_auth`, `signature_v2_auth`, `locate_credentials`, `use_credentials`

canonical_request *Construct a Canonical Request*

Description

Construct a Canonical Request from request elements

Usage

```
canonical_request(
  verb,
  canonical_uri = "",
  query_args = list(),
  canonical_headers,
  request_body = "",
  signed_body = FALSE
)
```

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.
signed_body	Sign the body request and add the correct header (x-amz-content-sha256) to the list of headers

Details

This function creates a "Canonical Request", which is part of the Signature Version 4. Users probably only need to use the signature_v4_auth function to generate signatures.

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 = Sys.getenv("AWS_SHARED_CREDENTIALS_FILE", default_credentials_file()),
```

```
  profile = NULL,
  default_region = getOption("cloudyr.aws.default_region", "us-east-1"),
  verbose = getOption("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 centralized '.aws/credentials' file.
profile	A character string specifying which profile to use from the file. By default, the profile named in AWS_PROFILE is used, otherwise 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. user-supplied values passed to the function
2. environment variables (AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY, AWS_DEFAULT_REGION, and AWS_SESSION_TOKEN)
3. an instance role (on the running ECS task from which this function is called) as identified by metadata, if the aws.ec2metadata package is installed
4. an IAM instance role (on the running EC2 instance from which this function is called) as identified by metadata, if the aws.ec2metadata package is installed
5. a profile in a local credentials dot file in the current working directory, using the profile specified by AWS_PROFILE
6. the default profile in that local credentials file
7. a profile in a global credentials dot file in a location set by AWS_SHARED_CREDENTIALS_FILE or defaulting typically to '~/.aws/credentials' (or another OS-specific location), using the profile specified by AWS_PROFILE
8. the default profile in that global credentials file

If AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY environment variables are not present when the package is loaded, then use_credentials is invoked using the file specified in AWS_SHARED_CREDENTIALS_FILE (or another default location) and the profile specified in AWS_PROFILE (or, if missing, the "default" profile).

To use this (and any cloudyr package) on AWS EC2 instances, users will also need to install the aws.ec2metadata package, which allows locate_credentials to know it is running in an instance and check for relevant values. If this package is not installed, instance metadata is not checked.

Because region is often handled slightly differently from credentials and is required for most requests (whereas some services allow anonymous requests without specifying credentials), the value of region is searched for in the same order as the above but lacking a value there fails safe with the following preference ranking of possible region values (regardless of location of other credentials):

1. a user-supplied value
2. the AWS_DEFAULT_REGION environment variable
3. (only on EC2 instances) a region declared in the instance metadata
4. (if a credentials file is being used) the value specified therein
5. the default value specified in default_region (i.e., "us-east-1" - this can be overriden with the option "cloudyr.aws.default_region")

As such, user-supplied values of region always trump any other value.

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 = Sys.getenv("AWS_SHARED_CREDENTIALS_FILE", default_credentials_file())
)

use_credentials(
  profile = Sys.getenv("AWS_PROFILE", "default"),
  file = Sys.getenv("AWS_SHARED_CREDENTIALS_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 given by AWS_SHARED_CREDENTIALS_FILE is used, otherwise an assumed default location is assumed. For use_credentials, this can also be an object of class "aws_credentials" (as returned by use_credentials).
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. It is called by default during package load if the AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY environment variables are not set.

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:
# read and parse a credentials file
read_credentials()

# set environment variables from a profile
use_credentials()

## End(Not run)
```

---

signature_v2_auth *Signature Version 2*

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,
  region = NULL,
  force_credentials = FALSE,
```

```
  verbose = getOption("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.
region	A character string containing the AWS region for the request. If missing, "us-east-1" is assumed.
force_credentials	A logical indicating whether to force use of user-supplied credentials. If FALSE (the default), locate_credentials is used to find credentials. If TRUE, user-supplied values are used regardless of their validity.
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. Version 2 is mostly deprecated and in most cases users should rely on signature_v4_auth for Version 4 signatures instead.

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

```
## Not run:
# 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\
"&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)

## End(Not run)
```

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 = getOption("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 missing, "us-east-1" is assumed.
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 from its pre-formatted components. Users probably only need to use the signature_v4_auth function to generate signatures.

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_v4_auth, signature_v2_auth, use_credentials

Examples

```
## Not run:
# 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")

## End(Not run)
```

---

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,
  signed_body = FALSE,
  key = NULL,
  secret = NULL,
  session_token = NULL,
  query = FALSE,
  algorithm = "AWS4-HMAC-SHA256",
  force_credentials = FALSE,
  verbose = getOption("verbose", FALSE)
)
```

Arguments

datetime	A character string containing a datetime in the form of "YYYYMMDDTHHMMSSZ". If missing, it is generated automatically using Sys.time.
region	A character string containing the AWS region for the request. If missing, "us-east-1" is assumed.
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.
signed_body	Should the body be signed
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.
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".
force_credentials	A logical indicating whether to force use of user-supplied credentials. If FALSE (the default), locate_credentials is used to find credentials. If TRUE, user-supplied values are used regardless of their validity.
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.
`Body`	The value passed to `request_body`.
`BodyHash`	A character string containing a SHA256 hash of the request body.
`Verb`	The value passed to `verb`.
`Query`	The value passed to `query_args`.
`Service`	The value passed to `service`.
`Action`	The value passed to `action`.
`CanonicalRequest`	A character string containing the canonical request.
`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.
`AccessKeyId`	A character string containing the access key id identified by `locate_credentials`.
`SecretAccessKey`	A character string containing the secret access key identified by `locate_credentials`.
`SessionToken`	A character string containing the session token identified by `locate_credentials`.
`Region`	A character string containing the region identified by `locate_credentials`.

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)

Add the Signing Information to the Request

See Also

signature_v2_auth, locate_credentials

---

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 "YYYYMMDDTHHMMSSZ".
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 is a mostly internal function that creates a "String To Sign", which is part of the Signature Version 4. Users probably only need to use the signature_v4_auth function to generate signatures.

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