

Package ‘paws.security.identity’

October 14, 2022

Title 'Amazon Web Services' Security, Identity, & Compliance Services

Version 0.1.12

Description Interface to 'Amazon Web Services' security, identity, and compliance services, including the 'Identity & Access Management' (IAM) service for managing access to services and resources, and more <<https://aws.amazon.com/>>.

License Apache License (>= 2.0)

URL <https://github.com/paws-r/paws>

BugReports <https://github.com/paws-r/paws/issues>

Imports paws.common (>= 0.3.0)

Suggests testthat

Encoding UTF-8

RoxygenNote 7.1.1

Collate 'acm_service.R' 'acm_interfaces.R' 'acm_operations.R'
'acmpca_service.R' 'acmpca_interfaces.R' 'acmpca_operations.R'
'clouddirectory_service.R' 'clouddirectory_interfaces.R'
'clouddirectory_operations.R' 'cloudhsm_service.R'
'cloudhsm_interfaces.R' 'cloudhsm_operations.R'
'cloudhsmv2_service.R' 'cloudhsmv2_interfaces.R'
'cloudhsmv2_operations.R' 'cognitoidentity_service.R'
'cognitoidentity_interfaces.R' 'cognitoidentity_operations.R'
'cognitoidentityprovider_service.R'
'cognitoidentityprovider_interfaces.R'
'cognitoidentityprovider_operations.R' 'cognitosync_service.R'
'cognitosync_interfaces.R' 'cognitosync_operations.R'
'directoryservice_service.R' 'directoryservice_interfaces.R'
'directoryservice_operations.R' 'fms_service.R'
'fms_interfaces.R' 'fms_operations.R' 'guardduty_service.R'
'guardduty_interfaces.R' 'guardduty_operations.R'
'iam_service.R' 'iam_interfaces.R' 'iam_operations.R'
'inspector_service.R' 'inspector_interfaces.R'
'inspector_operations.R' 'kms_service.R' 'kms_interfaces.R'

'kms_operations.R' 'macie_service.R' 'macie_interfaces.R'
 'macie_operations.R' 'ram_service.R' 'ram_interfaces.R'
 'ram_operations.R' 'secretsmanager_service.R'
 'secretsmanager_interfaces.R' 'secretsmanager_operations.R'
 'securityhub_service.R' 'securityhub_interfaces.R'
 'securityhub_operations.R' 'shield_service.R'
 'shield_interfaces.R' 'shield_operations.R' 'sts_service.R'
 'sts_interfaces.R' 'sts_operations.R' 'waf_service.R'
 'waf_interfaces.R' 'waf_operations.R' 'wafregional_service.R'
 'wafregional_interfaces.R' 'wafregional_operations.R'

NeedsCompilation no

Author David Kretch [aut, cre],
 Adam Banker [aut],
 Amazon.com, Inc. [cph]

Maintainer David Kretch <david.kretch@gmail.com>

Repository CRAN

Date/Publication 2021-08-23 07:10:06 UTC

R topics documented:

| | |
|-------------------------|----|
| acm | 3 |
| acmpca | 4 |
| clouddirectory | 6 |
| cloudhsm | 8 |
| cloudhsmv2 | 10 |
| cognitoidentity | 12 |
| cognitoidentityprovider | 13 |
| cognitosync | 17 |
| directoryservice | 18 |
| fms | 21 |
| guardduty | 23 |
| iam | 25 |
| inspector | 30 |
| kms | 32 |
| macie | 35 |
| ram | 36 |
| secretsmanager | 38 |
| securityhub | 41 |
| shield | 43 |
| sts | 45 |
| waf | 47 |
| wafregional | 50 |

Index

54

Description

Welcome to the AWS Certificate Manager (ACM) API documentation.

You can use ACM to manage SSL/TLS certificates for your AWS-based websites and applications. For general information about using ACM, see the *[AWS Certificate Manager User Guide](#)*.

Usage

```
acm(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- acm(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

| | |
|---|---|
| add_tags_to_certificate | Adds one or more tags to an ACM certificate |
| delete_certificate | Deletes a certificate and its associated private key |
| describe_certificate | Returns detailed metadata about the specified ACM certificate |
| export_certificate | Exports a private certificate issued by a private certificate authority (CA) for use anywhere |
| get_certificate | Retrieves an Amazon-issued certificate and its certificate chain |

| | |
|--|---|
| import_certificate | Imports a certificate into AWS Certificate Manager (ACM) to use with services that are integr |
| list_certificates | Retrieves a list of certificate ARNs and domain names |
| list_tags_for_certificate | Lists the tags that have been applied to the ACM certificate |
| remove_tags_from_certificate | Remove one or more tags from an ACM certificate |
| renew_certificate | Renews an eligible ACM certificate |
| request_certificate | Requests an ACM certificate for use with other AWS services |
| resend_validation_email | Resends the email that requests domain ownership validation |
| update_certificate_options | Updates a certificate |

Examples

```
## Not run:
svc <- acm()
svc$add_tags_to_certificate(
  Foo = 123
)

## End(Not run)
```

acmpca

AWS Certificate Manager Private Certificate Authority

Description

This is the *ACM Private CA API Reference*. It provides descriptions, syntax, and usage examples for each of the actions and data types involved in creating and managing private certificate authorities (CA) for your organization.

The documentation for each action shows the Query API request parameters and the XML response. Alternatively, you can use one of the AWS SDKs to access an API that's tailored to the programming language or platform that you're using. For more information, see [AWS SDKs](#).

Each ACM Private CA API action has a quota that determines the number of times the action can be called per second. For more information, see [API Rate Quotas in ACM Private CA](#) in the ACM Private CA user guide.

Usage

```
acmpca(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- acmpca(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

| | |
|---|---|
| create_certificate_authority | Creates a root or subordinate private certificate authority (CA) |
| create_certificate_authority_audit_report | Creates an audit report that lists every time that your CA private key is used |
| create_permission | Grants one or more permissions on a private CA to the AWS Certificate Manager (ACM) |
| delete_certificate_authority | Deletes a private certificate authority (CA) |
| delete_permission | Revokes permissions on a private CA granted to the AWS Certificate Manager (ACM) |
| delete_policy | Deletes the resource-based policy attached to a private CA |
| describe_certificate_authority | Lists information about your private certificate authority (CA) or one that has been shared with you |
| describe_certificate_authority_audit_report | Lists information about a specific audit report created by calling the <code>CreateCertificateAuthorityAuditReport</code> operation |
| get_certificate | Retrieves a certificate from your private CA or one that has been shared with you |
| get_certificate_authority_certificate | Retrieves the certificate and certificate chain for your private certificate authority (CA) |
| get_certificate_authority_csr | Retrieves the certificate signing request (CSR) for your private certificate authority (CA) |
| get_policy | Retrieves the resource-based policy attached to a private CA |
| import_certificate_authority_certificate | Imports a signed private CA certificate into ACM Private CA |
| issue_certificate | Uses your private certificate authority (CA), or one that has been shared with you, to issue a certificate |
| list_certificate_authorities | Lists the private certificate authorities that you created by using the <code>CreateCertificateAuthority</code> operation |
| list_permissions | List all permissions on a private CA, if any, granted to the AWS Certificate Manager (ACM) |
| list_tags | Lists the tags, if any, that are associated with your private CA or one that has been shared with you |
| put_policy | Attaches a resource-based policy to a private CA |
| restore_certificate_authority | Restores a certificate authority (CA) that is in the DELETED state |
| revoke_certificate | Revokes a certificate that was issued inside ACM Private CA |
| tag_certificate_authority | Adds one or more tags to your private CA |
| untag_certificate_authority | Remove one or more tags from your private CA |
| update_certificate_authority | Updates the status or configuration of a private certificate authority (CA) |

Examples

```
## Not run:
svc <- acmpca()
svc$create_certificate_authority(
  Foo = 123
)

## End(Not run)
```

clouddirectory

Amazon CloudDirectory

Description

Amazon Cloud Directory

Amazon Cloud Directory is a component of the AWS Directory Service that simplifies the development and management of cloud-scale web, mobile, and IoT applications. This guide describes the Cloud Directory operations that you can call programmatically and includes detailed information on data types and errors. For information about Cloud Directory features, see [AWS Directory Service](#) and the [Amazon Cloud Directory Developer Guide](#).

Usage

```
clouddirectory(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- clouddirectory(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
```

```

    ),
    profile = "string"
  ),
  endpoint = "string",
  region = "string"
)
)

```

Operations

| | |
|--|---|
| add_facet_to_object | Adds a new Facet to an object |
| apply_schema | Copies the input published schema, at the specified version, into the Directory with the sa |
| attach_object | Attaches an existing object to another object |
| attach_policy | Attaches a policy object to a regular object |
| attach_to_index | Attaches the specified object to the specified index |
| attach_typed_link | Attaches a typed link to a specified source and target object |
| batch_read | Performs all the read operations in a batch |
| batch_write | Performs all the write operations in a batch |
| create_directory | Creates a Directory by copying the published schema into the directory |
| create_facet | Creates a new Facet in a schema |
| create_index | Creates an index object |
| create_object | Creates an object in a Directory |
| create_schema | Creates a new schema in a development state |
| create_typed_link_facet | Creates a TypedLinkFacet |
| delete_directory | Deletes a directory |
| delete_facet | Deletes a given Facet |
| delete_object | Deletes an object and its associated attributes |
| delete_schema | Deletes a given schema |
| delete_typed_link_facet | Deletes a TypedLinkFacet |
| detach_from_index | Detaches the specified object from the specified index |
| detach_object | Detaches a given object from the parent object |
| detach_policy | Detaches a policy from an object |
| detach_typed_link | Detaches a typed link from a specified source and target object |
| disable_directory | Disables the specified directory |
| enable_directory | Enables the specified directory |
| get_applied_schema_version | Returns current applied schema version ARN, including the minor version in use |
| get_directory | Retrieves metadata about a directory |
| get_facet | Gets details of the Facet, such as facet name, attributes, Rules, or ObjectType |
| get_link_attributes | Retrieves attributes that are associated with a typed link |
| get_object_attributes | Retrieves attributes within a facet that are associated with an object |
| get_object_information | Retrieves metadata about an object |
| get_schema_as_json | Retrieves a JSON representation of the schema |
| get_typed_link_facet_information | Returns the identity attribute order for a specific TypedLinkFacet |
| list_applied_schema_arns | Lists schema major versions applied to a directory |
| list_attached_indices | Lists indices attached to the specified object |
| list_development_schema_arns | Retrieves each Amazon Resource Name (ARN) of schemas in the development state |
| list_directories | Lists directories created within an account |
| list_facet_attributes | Retrieves attributes attached to the facet |

| | |
|---|---|
| <code>list_facet_names</code> | Retrieves the names of facets that exist in a schema |
| <code>list_incoming_typed_links</code> | Returns a paginated list of all the incoming TypedLinkSpecifier information for an object |
| <code>list_index</code> | Lists objects attached to the specified index |
| <code>list_managed_schema_arns</code> | Lists the major version families of each managed schema |
| <code>list_object_attributes</code> | Lists all attributes that are associated with an object |
| <code>list_object_children</code> | Returns a paginated list of child objects that are associated with a given object |
| <code>list_object_parent_paths</code> | Retrieves all available parent paths for any object type such as node, leaf node, policy node |
| <code>list_object_parents</code> | Lists parent objects that are associated with a given object in pagination fashion |
| <code>list_object_policies</code> | Returns policies attached to an object in pagination fashion |
| <code>list_outgoing_typed_links</code> | Returns a paginated list of all the outgoing TypedLinkSpecifier information for an object |
| <code>list_policy_attachments</code> | Returns all of the ObjectIdentifiers to which a given policy is attached |
| <code>list_published_schema_arns</code> | Lists the major version families of each published schema |
| <code>list_tags_for_resource</code> | Returns tags for a resource |
| <code>list_typed_link_facet_attributes</code> | Returns a paginated list of all attribute definitions for a particular TypedLinkFacet |
| <code>list_typed_link_facet_names</code> | Returns a paginated list of TypedLink facet names for a particular schema |
| <code>lookup_policy</code> | Lists all policies from the root of the Directory to the object specified |
| <code>publish_schema</code> | Publishes a development schema with a major version and a recommended minor version |
| <code>put_schema_from_json</code> | Allows a schema to be updated using JSON upload |
| <code>remove_facet_from_object</code> | Removes the specified facet from the specified object |
| <code>tag_resource</code> | An API operation for adding tags to a resource |
| <code>untag_resource</code> | An API operation for removing tags from a resource |
| <code>update_facet</code> | Does the following: |
| <code>update_link_attributes</code> | Updates a given typed link's attributes |
| <code>update_object_attributes</code> | Updates a given object's attributes |
| <code>update_schema</code> | Updates the schema name with a new name |
| <code>update_typed_link_facet</code> | Updates a TypedLinkFacet |
| <code>upgrade_applied_schema</code> | Upgrades a single directory in-place using the PublishedSchemaArn with schema updates |
| <code>upgrade_published_schema</code> | Upgrades a published schema under a new minor version revision using the current content |

Examples

```
## Not run:
svc <- clouddirectory()
svc$add_facet_to_object(
  Foo = 123
)

## End(Not run)
```


Description

AWS CloudHSM Service

This is documentation for **AWS CloudHSM Classic**. For more information, see [AWS CloudHSM Classic FAQs](#), the [AWS CloudHSM Classic User Guide](#), and the [AWS CloudHSM Classic API Reference](#).

For information about the current version of AWS CloudHSM, see [AWS CloudHSM](#), the [AWS CloudHSM User Guide](#), and the [AWS CloudHSM API Reference](#).

Usage

```
cloudhsm(config = list())
```

Arguments

config Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- cloudhsm(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

| | |
|--------------------------------------|--|
| add_tags_to_resource | This is documentation for AWS CloudHSM Classic |
| create_hapg | This is documentation for AWS CloudHSM Classic |
| create_hsm | This is documentation for AWS CloudHSM Classic |
| create_luna_client | This is documentation for AWS CloudHSM Classic |
| delete_hapg | This is documentation for AWS CloudHSM Classic |
| delete_hsm | This is documentation for AWS CloudHSM Classic |
| delete_luna_client | This is documentation for AWS CloudHSM Classic |

| | |
|---|--|
| describe_hapg | This is documentation for AWS CloudHSM Classic |
| describe_hsm | This is documentation for AWS CloudHSM Classic |
| describe_luna_client | This is documentation for AWS CloudHSM Classic |
| get_config | This is documentation for AWS CloudHSM Classic |
| list_available_zones | This is documentation for AWS CloudHSM Classic |
| list_hapgs | This is documentation for AWS CloudHSM Classic |
| list_hsms | This is documentation for AWS CloudHSM Classic |
| list_luna_clients | This is documentation for AWS CloudHSM Classic |
| list_tags_for_resource | This is documentation for AWS CloudHSM Classic |
| modify_hapg | This is documentation for AWS CloudHSM Classic |
| modify_hsm | This is documentation for AWS CloudHSM Classic |
| modify_luna_client | This is documentation for AWS CloudHSM Classic |
| remove_tags_from_resource | This is documentation for AWS CloudHSM Classic |

Examples

```
## Not run:
svc <- cloudhsm()
svc$add_tags_to_resource(
  Foo = 123
)

## End(Not run)
```

cloudhsmv2

AWS CloudHSM V2

Description

For more information about AWS CloudHSM, see [AWS CloudHSM](#) and the [AWS CloudHSM User Guide](#).

Usage

```
cloudhsmv2(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```

svc <- cloudhsmv2(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

| | |
|--|--|
| copy_backup_to_region | Copy an AWS CloudHSM cluster backup to a different region |
| create_cluster | Creates a new AWS CloudHSM cluster |
| create_hsm | Creates a new hardware security module (HSM) in the specified AWS CloudHSM cluster |
| delete_backup | Deletes a specified AWS CloudHSM backup |
| delete_cluster | Deletes the specified AWS CloudHSM cluster |
| delete_hsm | Deletes the specified HSM |
| describe_backups | Gets information about backups of AWS CloudHSM clusters |
| describe_clusters | Gets information about AWS CloudHSM clusters |
| initialize_cluster | Claims an AWS CloudHSM cluster by submitting the cluster certificate issued by your issuing cert authority |
| list_tags | Gets a list of tags for the specified AWS CloudHSM cluster |
| modify_backup_attributes | Modifies attributes for AWS CloudHSM backup |
| modify_cluster | Modifies AWS CloudHSM cluster |
| restore_backup | Restores a specified AWS CloudHSM backup that is in the PENDING_DELETION state |
| tag_resource | Adds or overwrites one or more tags for the specified AWS CloudHSM cluster |
| untag_resource | Removes the specified tag or tags from the specified AWS CloudHSM cluster |

Examples

```

## Not run:
svc <- cloudhsmv2()
svc$copy_backup_to_region(
  Foo = 123
)

## End(Not run)

```

| | |
|-----------------|--------------------------------|
| cognitoidentity | <i>Amazon Cognito Identity</i> |
|-----------------|--------------------------------|

Description

Amazon Cognito Federated Identities

Amazon Cognito Federated Identities is a web service that delivers scoped temporary credentials to mobile devices and other untrusted environments. It uniquely identifies a device and supplies the user with a consistent identity over the lifetime of an application.

Using Amazon Cognito Federated Identities, you can enable authentication with one or more third-party identity providers (Facebook, Google, or Login with Amazon) or an Amazon Cognito user pool, and you can also choose to support unauthenticated access from your app. Cognito delivers a unique identifier for each user and acts as an OpenID token provider trusted by AWS Security Token Service (STS) to access temporary, limited-privilege AWS credentials.

For a description of the authentication flow from the Amazon Cognito Developer Guide see [Authentication Flow](#).

For more information see [Amazon Cognito Federated Identities](#).

Usage

```
cognitoidentity(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- cognitoidentity(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
```

```
)
)
```

Operations

| | |
|--|--|
| create_identity_pool | Creates a new identity pool |
| delete_identities | Deletes identities from an identity pool |
| delete_identity_pool | Deletes an identity pool |
| describe_identity | Returns metadata related to the given identity, including when the identity was created |
| describe_identity_pool | Gets details about a particular identity pool, including the pool name, ID description, and creation date |
| get_credentials_for_identity | Returns credentials for the provided identity ID |
| get_id | Generates (or retrieves) a Cognito ID |
| get_identity_pool_roles | Gets the roles for an identity pool |
| get_open_id_token | Gets an OpenID token, using a known Cognito ID |
| get_open_id_token_for_developer_identity | Registers (or retrieves) a Cognito IdentityId and an OpenID Connect token for a DeveloperUserIdentifier |
| list_identities | Lists the identities in an identity pool |
| list_identity_pools | Lists all of the Cognito identity pools registered for your account |
| list_tags_for_resource | Lists the tags that are assigned to an Amazon Cognito identity pool |
| lookup_developer_identity | Retrieves the IdentityID associated with a DeveloperUserIdentifier or the list of DeveloperUserIdentifiers associated with a particular IdentityID |
| merge_developer_identities | Merges two users having different IdentityIDs, existing in the same identity pool |
| set_identity_pool_roles | Sets the roles for an identity pool |
| tag_resource | Assigns a set of tags to an Amazon Cognito identity pool |
| unlink_developer_identity | Unlinks a DeveloperUserIdentifier from an existing identity |
| unlink_identity | Unlinks a federated identity from an existing account |
| untag_resource | Removes the specified tags from an Amazon Cognito identity pool |
| update_identity_pool | Updates an identity pool |

Examples

```
## Not run:
svc <- cognitoidentity()
svc$create_identity_pool(
  Foo = 123
)

## End(Not run)
```

Description

Using the Amazon Cognito User Pools API, you can create a user pool to manage directories and users. You can authenticate a user to obtain tokens related to user identity and access policies.

This API reference provides information about user pools in Amazon Cognito User Pools.

For more information, see the Amazon Cognito Documentation.

Usage

```
cognitoidentityprovider(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- cognitoidentityprovider(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

| | |
|---|---|
| add_custom_attributes | Adds additional user attributes to the user pool schema |
| admin_add_user_to_group | Adds the specified user to the specified group |
| admin_confirm_sign_up | Confirms user registration as an admin without using a confirmation code |
| admin_create_user | Creates a new user in the specified user pool |
| admin_delete_user | Deletes a user as an administrator |
| admin_delete_user_attributes | Deletes the user attributes in a user pool as an administrator |
| admin_disable_provider_for_user | Disables the user from signing in with the specified external (SAML or social) identity |
| admin_disable_user | Disables the specified user |
| admin_enable_user | Enables the specified user as an administrator |

| | |
|--|--|
| admin_forget_device | Forgets the device, as an administrator |
| admin_get_device | Gets the device, as an administrator |
| admin_get_user | Gets the specified user by user name in a user pool as an administrator |
| admin_initiate_auth | Initiates the authentication flow, as an administrator |
| admin_link_provider_for_user | Links an existing user account in a user pool (DestinationUser) to an identity from an e |
| admin_list_devices | Lists devices, as an administrator |
| admin_list_groups_for_user | Lists the groups that the user belongs to |
| admin_list_user_auth_events | Lists a history of user activity and any risks detected as part of Amazon Cognito advan |
| admin_remove_user_from_group | Removes the specified user from the specified group |
| admin_reset_user_password | Resets the specified user's password in a user pool as an administrator |
| admin_respond_to_auth_challenge | Responds to an authentication challenge, as an administrator |
| admin_set_user_mfa_preference | Sets the user's multi-factor authentication (MFA) preference, including which MFA op |
| admin_set_user_password | Sets the specified user's password in a user pool as an administrator |
| admin_set_user_settings | This action is no longer supported |
| admin_update_auth_event_feedback | Provides feedback for an authentication event as to whether it was from a valid user |
| admin_update_device_status | Updates the device status as an administrator |
| admin_update_user_attributes | Updates the specified user's attributes, including developer attributes, as an administrat |
| admin_user_global_sign_out | Signs out users from all devices, as an administrator |
| associate_software_token | Returns a unique generated shared secret key code for the user account |
| change_password | Changes the password for a specified user in a user pool |
| confirm_device | Confirms tracking of the device |
| confirm_forgot_password | Allows a user to enter a confirmation code to reset a forgotten password |
| confirm_sign_up | Confirms registration of a user and handles the existing alias from a previous user |
| create_group | Creates a new group in the specified user pool |
| create_identity_provider | Creates an identity provider for a user pool |
| create_resource_server | Creates a new OAuth2 |
| create_user_import_job | Creates the user import job |
| create_user_pool | Creates a new Amazon Cognito user pool and sets the password policy for the pool |
| create_user_pool_client | Creates the user pool client |
| create_user_pool_domain | Creates a new domain for a user pool |
| delete_group | Deletes a group |
| delete_identity_provider | Deletes an identity provider for a user pool |
| delete_resource_server | Deletes a resource server |
| delete_user | Allows a user to delete himself or herself |
| delete_user_attributes | Deletes the attributes for a user |
| delete_user_pool | Deletes the specified Amazon Cognito user pool |
| delete_user_pool_client | Allows the developer to delete the user pool client |
| delete_user_pool_domain | Deletes a domain for a user pool |
| describe_identity_provider | Gets information about a specific identity provider |
| describe_resource_server | Describes a resource server |
| describe_risk_configuration | Describes the risk configuration |
| describe_user_import_job | Describes the user import job |
| describe_user_pool | Returns the configuration information and metadata of the specified user pool |
| describe_user_pool_client | Client method for returning the configuration information and metadata of the specifie |
| describe_user_pool_domain | Gets information about a domain |
| forget_device | Forgets the specified device |
| forgot_password | Calling this API causes a message to be sent to the end user with a confirmation code t |
| get_csv_header | Gets the header information for the |

| | |
|---|--|
| <code>get_device</code> | Gets the device |
| <code>get_group</code> | Gets a group |
| <code>get_identity_provider_by_identifier</code> | Gets the specified identity provider |
| <code>get_signing_certificate</code> | This method takes a user pool ID, and returns the signing certificate |
| <code>get_ui_customization</code> | Gets the UI Customization information for a particular app client's app UI, if there is s |
| <code>get_user</code> | Gets the user attributes and metadata for a user |
| <code>get_user_attribute_verification_code</code> | Gets the user attribute verification code for the specified attribute name |
| <code>get_user_pool_mfa_config</code> | Gets the user pool multi-factor authentication (MFA) configuration |
| <code>global_sign_out</code> | Signs out users from all devices |
| <code>initiate_auth</code> | Initiates the authentication flow |
| <code>list_devices</code> | Lists the devices |
| <code>list_groups</code> | Lists the groups associated with a user pool |
| <code>list_identity_providers</code> | Lists information about all identity providers for a user pool |
| <code>list_resource_servers</code> | Lists the resource servers for a user pool |
| <code>list_tags_for_resource</code> | Lists the tags that are assigned to an Amazon Cognito user pool |
| <code>list_user_import_jobs</code> | Lists the user import jobs |
| <code>list_user_pool_clients</code> | Lists the clients that have been created for the specified user pool |
| <code>list_user_pools</code> | Lists the user pools associated with an AWS account |
| <code>list_users</code> | Lists the users in the Amazon Cognito user pool |
| <code>list_users_in_group</code> | Lists the users in the specified group |
| <code>resend_confirmation_code</code> | Resends the confirmation (for confirmation of registration) to a specific user in the user |
| <code>respond_to_auth_challenge</code> | Responds to the authentication challenge |
| <code>set_risk_configuration</code> | Configures actions on detected risks |
| <code>set_ui_customization</code> | Sets the UI customization information for a user pool's built-in app UI |
| <code>set_user_mfa_preference</code> | Set the user's multi-factor authentication (MFA) method preference, including which M |
| <code>set_user_pool_mfa_config</code> | Set the user pool multi-factor authentication (MFA) configuration |
| <code>set_user_settings</code> | This action is no longer supported |
| <code>sign_up</code> | Registers the user in the specified user pool and creates a user name, password, and use |
| <code>start_user_import_job</code> | Starts the user import |
| <code>stop_user_import_job</code> | Stops the user import job |
| <code>tag_resource</code> | Assigns a set of tags to an Amazon Cognito user pool |
| <code>untag_resource</code> | Removes the specified tags from an Amazon Cognito user pool |
| <code>update_auth_event_feedback</code> | Provides the feedback for an authentication event whether it was from a valid user or n |
| <code>update_device_status</code> | Updates the device status |
| <code>update_group</code> | Updates the specified group with the specified attributes |
| <code>update_identity_provider</code> | Updates identity provider information for a user pool |
| <code>update_resource_server</code> | Updates the name and scopes of resource server |
| <code>update_user_attributes</code> | Allows a user to update a specific attribute (one at a time) |
| <code>update_user_pool</code> | Updates the specified user pool with the specified attributes |
| <code>update_user_pool_client</code> | Updates the specified user pool app client with the specified attributes |
| <code>update_user_pool_domain</code> | Updates the Secure Sockets Layer (SSL) certificate for the custom domain for your use |
| <code>verify_software_token</code> | Use this API to register a user's entered TOTP code and mark the user's software token |
| <code>verify_user_attribute</code> | Verifies the specified user attributes in the user pool |

Examples

```
## Not run:
```



```
svc <- cognitoidentityprovider()
svc$add_custom_attributes(
  Foo = 123
)

## End(Not run)
```

cognitosync

Amazon Cognito Sync

Description

Amazon Cognito Sync provides an AWS service and client library that enable cross-device syncing of application-related user data. High-level client libraries are available for both iOS and Android. You can use these libraries to persist data locally so that it's available even if the device is offline. Developer credentials don't need to be stored on the mobile device to access the service. You can use Amazon Cognito to obtain a normalized user ID and credentials. User data is persisted in a dataset that can store up to 1 MB of key-value pairs, and you can have up to 20 datasets per user identity.

With Amazon Cognito Sync, the data stored for each identity is accessible only to credentials assigned to that identity. In order to use the Cognito Sync service, you need to make API calls using credentials retrieved with [Amazon Cognito Identity service](#).

If you want to use Cognito Sync in an Android or iOS application, you will probably want to make API calls via the AWS Mobile SDK. To learn more, see the [Developer Guide for Android](#) and the [Developer Guide for iOS](#).

Usage

```
cognitosync(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- cognitosync(
  config = list(
    credentials = list(
      creds = list(
```

```

        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
    ),
    profile = "string"
),
endpoint = "string",
region = "string"
)
)

```

Operations

| | |
|---|---|
| bulk_publish | Initiates a bulk publish of all existing datasets for an Identity Pool to the configured stream |
| delete_dataset | Deletes the specific dataset |
| describe_dataset | Gets meta data about a dataset by identity and dataset name |
| describe_identity_pool_usage | Gets usage details (for example, data storage) about a particular identity pool |
| describe_identity_usage | Gets usage information for an identity, including number of datasets and data usage |
| get_bulk_publish_details | Get the status of the last BulkPublish operation for an identity pool |
| get_cognito_events | Gets the events and the corresponding Lambda functions associated with an identity pool |
| get_identity_pool_configuration | Gets the configuration settings of an identity pool |
| list_datasets | Lists datasets for an identity |
| list_identity_pool_usage | Gets a list of identity pools registered with Cognito |
| list_records | Gets paginated records, optionally changed after a particular sync count for a dataset and id |
| register_device | Registers a device to receive push sync notifications |
| set_cognito_events | Sets the AWS Lambda function for a given event type for an identity pool |
| set_identity_pool_configuration | Sets the necessary configuration for push sync |
| subscribe_to_dataset | Subscribes to receive notifications when a dataset is modified by another device |
| unsubscribe_from_dataset | Unsubscribes from receiving notifications when a dataset is modified by another device |
| update_records | Posts updates to records and adds and deletes records for a dataset and user |

Examples

```

## Not run:
svc <- cognitosync()
svc$bulk_publish(
  Foo = 123
)

## End(Not run)

```

Description

AWS Directory Service is a web service that makes it easy for you to setup and run directories in the AWS cloud, or connect your AWS resources with an existing on-premises Microsoft Active Directory. This guide provides detailed information about AWS Directory Service operations, data types, parameters, and errors. For information about AWS Directory Services features, see [AWS Directory Service](#) and the [AWS Directory Service Administration Guide](#).

AWS provides SDKs that consist of libraries and sample code for various programming languages and platforms (Java, Ruby, .Net, iOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to AWS Directory Service and other AWS services. For more information about the AWS SDKs, including how to download and install them, see [Tools for Amazon Web Services](#).

Usage

```
directoryservice(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- directoryservice(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

[accept_shared_directory](#)
[add_ip_routes](#)
[add_region](#)

Accepts a directory sharing request that was sent from the directory owner account
 If the DNS server for your on-premises domain uses a publicly addressable IP address
 Adds two domain controllers in the specified Region for the specified directory

| | |
|--|---|
| <code>add_tags_to_resource</code> | Adds or overwrites one or more tags for the specified directory |
| <code>cancel_schema_extension</code> | Cancels an in-progress schema extension to a Microsoft AD directory |
| <code>connect_directory</code> | Creates an AD Connector to connect to an on-premises directory |
| <code>create_alias</code> | Creates an alias for a directory and assigns the alias to the directory |
| <code>create_computer</code> | Creates an Active Directory computer object in the specified directory |
| <code>create_conditional_forwarder</code> | Creates a conditional forwarder associated with your AWS directory |
| <code>create_directory</code> | Creates a Simple AD directory |
| <code>create_log_subscription</code> | Creates a subscription to forward real-time Directory Service domain controller security events |
| <code>create_microsoft_ad</code> | Creates a Microsoft AD directory in the AWS Cloud |
| <code>create_snapshot</code> | Creates a snapshot of a Simple AD or Microsoft AD directory in the AWS cloud |
| <code>create_trust</code> | AWS Directory Service for Microsoft Active Directory allows you to configure trust relationships between your AWS Managed Microsoft AD directory and other Microsoft AD directories |
| <code>delete_conditional_forwarder</code> | Deletes a conditional forwarder that has been set up for your AWS directory |
| <code>delete_directory</code> | Deletes an AWS Directory Service directory |
| <code>delete_log_subscription</code> | Deletes the specified log subscription |
| <code>delete_snapshot</code> | Deletes a directory snapshot |
| <code>delete_trust</code> | Deletes an existing trust relationship between your AWS Managed Microsoft AD directory and another Microsoft AD directory |
| <code>deregister_certificate</code> | Deletes from the system the certificate that was registered for secure LDAP or client certificate authentication |
| <code>deregister_event_topic</code> | Removes the specified directory as a publisher to the specified SNS topic |
| <code>describe_certificate</code> | Displays information about the certificate registered for secure LDAP or client certificate authentication |
| <code>describe_conditional_forwarders</code> | Obtains information about the conditional forwarders for this account |
| <code>describe_directories</code> | Obtains information about the directories that belong to this account |
| <code>describe_domain_controllers</code> | Provides information about any domain controllers in your directory |
| <code>describe_event_topics</code> | Obtains information about which SNS topics receive status messages from the specified directory |
| <code>describe_ldaps_settings</code> | Describes the status of LDAP security for the specified directory |
| <code>describe_regions</code> | Provides information about the Regions that are configured for multi-Region replication |
| <code>describe_shared_directories</code> | Returns the shared directories in your account |
| <code>describe_snapshots</code> | Obtains information about the directory snapshots that belong to this account |
| <code>describe_trusts</code> | Obtains information about the trust relationships for this account |
| <code>disable_client_authentication</code> | Disables alternative client authentication methods for the specified directory |
| <code>disable_ldaps</code> | Deactivates LDAP secure calls for the specified directory |
| <code>disable_radius</code> | Disables multi-factor authentication (MFA) with the Remote Authentication Dial In User Service (RADIUS) protocol |
| <code>disable_sso</code> | Disables single-sign on for a directory |
| <code>enable_client_authentication</code> | Enables alternative client authentication methods for the specified directory |
| <code>enable_ldaps</code> | Activates the switch for the specific directory to always use LDAP secure calls |
| <code>enable_radius</code> | Enables multi-factor authentication (MFA) with the Remote Authentication Dial In User Service (RADIUS) protocol |
| <code>enable_sso</code> | Enables single sign-on for a directory |
| <code>get_directory_limits</code> | Obtains directory limit information for the current Region |
| <code>get_snapshot_limits</code> | Obtains the manual snapshot limits for a directory |
| <code>list_certificates</code> | For the specified directory, lists all the certificates registered for a secure LDAP or client certificate authentication |
| <code>list_ip_routes</code> | Lists the address blocks that you have added to a directory |
| <code>list_log_subscriptions</code> | Lists the active log subscriptions for the AWS account |
| <code>list_schema_extensions</code> | Lists all schema extensions applied to a Microsoft AD Directory |
| <code>list_tags_for_resource</code> | Lists all tags on a directory |
| <code>register_certificate</code> | Registers a certificate for a secure LDAP or client certificate authentication |
| <code>register_event_topic</code> | Associates a directory with an SNS topic |
| <code>reject_shared_directory</code> | Rejects a directory sharing request that was sent from the directory owner account |
| <code>remove_ip_routes</code> | Removes IP address blocks from a directory |
| <code>remove_region</code> | Stops all replication and removes the domain controllers from the specified Region |

| | |
|---|--|
| remove_tags_from_resource | Removes tags from a directory |
| reset_user_password | Resets the password for any user in your AWS Managed Microsoft AD or Simple A |
| restore_from_snapshot | Restores a directory using an existing directory snapshot |
| share_directory | Shares a specified directory (DirectoryId) in your AWS account (directory owner) w |
| start_schema_extension | Applies a schema extension to a Microsoft AD directory |
| unshare_directory | Stops the directory sharing between the directory owner and consumer accounts |
| update_conditional_forwarder | Updates a conditional forwarder that has been set up for your AWS directory |
| update_number_of_domain_controllers | Adds or removes domain controllers to or from the directory |
| update_radius | Updates the Remote Authentication Dial In User Service (RADIUS) server informa |
| update_trust | Updates the trust that has been set up between your AWS Managed Microsoft AD d |
| verify_trust | AWS Directory Service for Microsoft Active Directory allows you to configure and |

Examples

```
## Not run:
svc <- directoryservice()
svc$accept_shared_directory(
  Foo = 123
)

## End(Not run)
```

fms

Firewall Management Service

Description

AWS Firewall Manager

This is the *AWS Firewall Manager API Reference*. This guide is for developers who need detailed information about the AWS Firewall Manager API actions, data types, and errors. For detailed information about AWS Firewall Manager features, see the [AWS Firewall Manager Developer Guide](#).

Some API actions require explicit resource permissions. For information, see the developer guide topic [Firewall Manager required permissions for API actions](#).

Usage

```
fms(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- fms(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

| | |
|---|--|
| associate_admin_account | Sets the AWS Firewall Manager administrator account |
| delete_apps_list | Permanently deletes an AWS Firewall Manager applications list |
| delete_notification_channel | Deletes an AWS Firewall Manager association with the IAM role and the Amazon Simple Notification Service (SNS) topic |
| delete_policy | Permanently deletes an AWS Firewall Manager policy |
| delete_protocols_list | Permanently deletes an AWS Firewall Manager protocols list |
| disassociate_admin_account | Disassociates the account that has been set as the AWS Firewall Manager administrator account |
| get_admin_account | Returns the AWS Organizations master account that is associated with AWS Firewall Manager |
| get_apps_list | Returns information about the specified AWS Firewall Manager applications list |
| get_compliance_detail | Returns detailed compliance information about the specified member account |
| get_notification_channel | Information about the Amazon Simple Notification Service (SNS) topic that is used to record AWS Firewall Manager events |
| get_policy | Returns information about the specified AWS Firewall Manager policy |
| get_protection_status | If you created a Shield Advanced policy, returns policy-level attack summary information in the specified region |
| get_protocols_list | Returns information about the specified AWS Firewall Manager protocols list |
| get_violation_details | Retrieves violations for a resource based on the specified AWS Firewall Manager policy and AWS resource |
| list_apps_lists | Returns an array of AppsListDataSummary objects |
| list_compliance_status | Returns an array of PolicyComplianceStatus objects |
| list_member_accounts | Returns a MemberAccounts object that lists the member accounts in the administrator's AWS account |
| list_policies | Returns an array of PolicySummary objects |
| list_protocols_lists | Returns an array of ProtocolsListDataSummary objects |
| list_tags_for_resource | Retrieves the list of tags for the specified AWS resource |
| put_apps_list | Creates an AWS Firewall Manager applications list |
| put_notification_channel | Designates the IAM role and Amazon Simple Notification Service (SNS) topic that AWS Firewall Manager uses to record events |
| put_policy | Creates an AWS Firewall Manager policy |
| put_protocols_list | Creates an AWS Firewall Manager protocols list |

| | |
|--------------------------------|---|
| tag_resource | Adds one or more tags to an AWS resource |
| untag_resource | Removes one or more tags from an AWS resource |

Examples

```
## Not run:
svc <- fms()
svc$associate_admin_account(
  Foo = 123
)

## End(Not run)
```

guardduty

Amazon GuardDuty

Description

Amazon GuardDuty is a continuous security monitoring service that analyzes and processes the following data sources: VPC Flow Logs, AWS CloudTrail event logs, and DNS logs. It uses threat intelligence feeds (such as lists of malicious IPs and domains) and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IPs, URLs, or domains. For example, GuardDuty can detect compromised EC2 instances that serve malware or mine bitcoin.

GuardDuty also monitors AWS account access behavior for signs of compromise. Some examples of this are unauthorized infrastructure deployments such as EC2 instances deployed in a Region that has never been used, or unusual API calls like a password policy change to reduce password strength.

GuardDuty informs you of the status of your AWS environment by producing security findings that you can view in the GuardDuty console or through Amazon CloudWatch events. For more information, see the [Amazon GuardDuty User Guide](#).

Usage

```
guardduty(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```

svc <- guardduty(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

| | |
|---|--|
| accept_invitation | Accepts the invitation to be monitored by a GuardDuty administrator account |
| archive_findings | Archives GuardDuty findings that are specified by the list of finding IDs |
| create_detector | Creates a single Amazon GuardDuty detector |
| create_filter | Creates a filter using the specified finding criteria |
| create_ip_set | Creates a new IPSet, which is called a trusted IP list in the console user interface |
| create_members | Creates member accounts of the current AWS account by specifying a list of AWS accounts |
| create_publishing_destination | Creates a publishing destination to export findings to |
| create_sample_findings | Generates example findings of types specified by the list of finding types |
| create_threat_intel_set | Creates a new ThreatIntelSet |
| decline_invitations | Declines invitations sent to the current member account by AWS accounts specified by the list of AWS account IDs |
| delete_detector | Deletes an Amazon GuardDuty detector that is specified by the detector ID |
| delete_filter | Deletes the filter specified by the filter name |
| delete_invitations | Deletes invitations sent to the current member account by AWS accounts specified by the list of AWS account IDs |
| delete_ip_set | Deletes the IPSet specified by the ipSetId |
| delete_members | Deletes GuardDuty member accounts (to the current GuardDuty administrator account) |
| delete_publishing_destination | Deletes the publishing definition with the specified destinationId |
| delete_threat_intel_set | Deletes the ThreatIntelSet specified by the ThreatIntelSet ID |
| describe_organization_configuration | Returns information about the account selected as the delegated administrator for GuardDuty |
| describe_publishing_destination | Returns information about the publishing destination specified by the provided destinationId |
| disable_organization_admin_account | Disables an AWS account within the Organization as the GuardDuty delegated administrator |
| disassociate_from_master_account | Disassociates the current GuardDuty member account from its administrator account |
| disassociate_members | Disassociates GuardDuty member accounts (to the current GuardDuty administrator account) |
| enable_organization_admin_account | Enables an AWS account within the organization as the GuardDuty delegated administrator |
| get_detector | Retrieves an Amazon GuardDuty detector specified by the detectorId |
| get_filter | Returns the details of the filter specified by the filter name |
| get_findings | Describes Amazon GuardDuty findings specified by finding IDs |
| get_findings_statistics | Lists Amazon GuardDuty findings statistics for the specified detector ID |
| get_invitations_count | Returns the count of all GuardDuty membership invitations that were sent to the current member account |
| get_ip_set | Retrieves the IPSet specified by the ipSetId |
| get_master_account | Provides the details for the GuardDuty administrator account associated with the current member account |

| | |
|---|---|
| get_member_detectors | Describes which data sources are enabled for the member account's detector |
| get_members | Retrieves GuardDuty member accounts (of the current GuardDuty administrator account) |
| get_threat_intel_set | Retrieves the ThreatIntelSet that is specified by the ThreatIntelSet ID |
| get_usage_statistics | Lists Amazon GuardDuty usage statistics over the last 30 days for the specified detector |
| invite_members | Invites other AWS accounts (created as members of the current AWS account by CreateAccount) |
| list_detectors | Lists detectorIds of all the existing Amazon GuardDuty detector resources |
| list_filters | Returns a paginated list of the current filters |
| list_findings | Lists Amazon GuardDuty findings for the specified detector ID |
| list_invitations | Lists all GuardDuty membership invitations that were sent to the current AWS account |
| list_ip_sets | Lists the IPSets of the GuardDuty service specified by the detector ID |
| list_members | Lists details about all member accounts for the current GuardDuty administrator account |
| list_organization_admin_accounts | Lists the accounts configured as GuardDuty delegated administrators |
| list_publishing_destinations | Returns a list of publishing destinations associated with the specified detectorId |
| list_tags_for_resource | Lists tags for a resource |
| list_threat_intel_sets | Lists the ThreatIntelSets of the GuardDuty service specified by the detector ID |
| start_monitoring_members | Turns on GuardDuty monitoring of the specified member accounts |
| stop_monitoring_members | Stops GuardDuty monitoring for the specified member accounts |
| tag_resource | Adds tags to a resource |
| unarchive_findings | Unarchives GuardDuty findings specified by the findingIds |
| untag_resource | Removes tags from a resource |
| update_detector | Updates the Amazon GuardDuty detector specified by the detectorId |
| update_filter | Updates the filter specified by the filter name |
| update_findings_feedback | Marks the specified GuardDuty findings as useful or not useful |
| update_ip_set | Updates the IPSet specified by the IPSet ID |
| update_member_detectors | Contains information on member accounts to be updated |
| update_organization_configuration | Updates the delegated administrator account with the values provided |
| update_publishing_destination | Updates information about the publishing destination specified by the destinationId |
| update_threat_intel_set | Updates the ThreatIntelSet specified by the ThreatIntelSet ID |

Examples

```
## Not run:
svc <- guardduty()
svc$accept_invitation(
  Foo = 123
)

## End(Not run)
```

Description

AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access. For more information about IAM, see [AWS Identity and Access Management \(IAM\)](#) and the [AWS Identity and Access Management User Guide](#).

Usage

```
iam(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- iam(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

[add_client_id_to_open_id_connect_provider](#)
[add_role_to_instance_profile](#)
[add_user_to_group](#)
[attach_group_policy](#)
[attach_role_policy](#)
[attach_user_policy](#)
[change_password](#)
[create_access_key](#)

Adds a new client ID (also known as audience) to the list of client IDs a
 Adds the specified IAM role to the specified instance profile
 Adds the specified user to the specified group
 Attaches the specified managed policy to the specified IAM group
 Attaches the specified managed policy to the specified IAM role
 Attaches the specified managed policy to the specified user
 Changes the password of the IAM user who is calling this operation
 Creates a new AWS secret access key and corresponding AWS access k

| | |
|---|---|
| <code>create_account_alias</code> | Creates an alias for your AWS account |
| <code>create_group</code> | Creates a new group |
| <code>create_instance_profile</code> | Creates a new instance profile |
| <code>create_login_profile</code> | Creates a password for the specified user, giving the user the ability to a |
| <code>create_open_id_connect_provider</code> | Creates an IAM entity to describe an identity provider (IdP) that support |
| <code>create_policy</code> | Creates a new managed policy for your AWS account |
| <code>create_policy_version</code> | Creates a new version of the specified managed policy |
| <code>create_role</code> | Creates a new role for your AWS account |
| <code>create_saml_provider</code> | Creates an IAM resource that describes an identity provider (IdP) that s |
| <code>create_service_linked_role</code> | Creates an IAM role that is linked to a specific AWS service |
| <code>create_service_specific_credential</code> | Generates a set of credentials consisting of a user name and password th |
| <code>create_user</code> | Creates a new IAM user for your AWS account |
| <code>create_virtual_mfa_device</code> | Creates a new virtual MFA device for the AWS account |
| <code>deactivate_mfa_device</code> | Deactivates the specified MFA device and removes it from association w |
| <code>delete_access_key</code> | Deletes the access key pair associated with the specified IAM user |
| <code>delete_account_alias</code> | Deletes the specified AWS account alias |
| <code>delete_account_password_policy</code> | Deletes the password policy for the AWS account |
| <code>delete_group</code> | Deletes the specified IAM group |
| <code>delete_group_policy</code> | Deletes the specified inline policy that is embedded in the specified IAM |
| <code>delete_instance_profile</code> | Deletes the specified instance profile |
| <code>delete_login_profile</code> | Deletes the password for the specified IAM user, which terminates the u |
| <code>delete_open_id_connect_provider</code> | Deletes an OpenID Connect identity provider (IdP) resource object in IA |
| <code>delete_policy</code> | Deletes the specified managed policy |
| <code>delete_policy_version</code> | Deletes the specified version from the specified managed policy |
| <code>delete_role</code> | Deletes the specified role |
| <code>delete_role_permissions_boundary</code> | Deletes the permissions boundary for the specified IAM role |
| <code>delete_role_policy</code> | Deletes the specified inline policy that is embedded in the specified IAM |
| <code>delete_saml_provider</code> | Deletes a SAML provider resource in IAM |
| <code>delete_server_certificate</code> | Deletes the specified server certificate |
| <code>delete_service_linked_role</code> | Submits a service-linked role deletion request and returns a DeletionTas |
| <code>delete_service_specific_credential</code> | Deletes the specified service-specific credential |
| <code>delete_signing_certificate</code> | Deletes a signing certificate associated with the specified IAM user |
| <code>delete_ssh_public_key</code> | Deletes the specified SSH public key |
| <code>delete_user</code> | Deletes the specified IAM user |
| <code>delete_user_permissions_boundary</code> | Deletes the permissions boundary for the specified IAM user |
| <code>delete_user_policy</code> | Deletes the specified inline policy that is embedded in the specified IAM |
| <code>delete_virtual_mfa_device</code> | Deletes a virtual MFA device |
| <code>detach_group_policy</code> | Removes the specified managed policy from the specified IAM group |
| <code>detach_role_policy</code> | Removes the specified managed policy from the specified role |
| <code>detach_user_policy</code> | Removes the specified managed policy from the specified user |
| <code>enable_mfa_device</code> | Enables the specified MFA device and associates it with the specified IA |
| <code>generate_credential_report</code> | Generates a credential report for the AWS account |
| <code>generate_organizations_access_report</code> | Generates a report for service last accessed data for AWS Organizations |
| <code>generate_service_last_accessed_details</code> | Generates a report that includes details about when an IAM resource (us |
| <code>get_access_key_last_used</code> | Retrieves information about when the specified access key was last used |
| <code>get_account_authorization_details</code> | Retrieves information about all IAM users, groups, roles, and policies in |
| <code>get_account_password_policy</code> | Retrieves the password policy for the AWS account |
| <code>get_account_summary</code> | Retrieves information about IAM entity usage and IAM quotas in the A |

| | |
|---|--|
| get_context_keys_for_custom_policy | Gets a list of all of the context keys referenced in the input policies |
| get_context_keys_for_principal_policy | Gets a list of all of the context keys referenced in all the IAM policies that are attached to the specified principal |
| get_credential_report | Retrieves a credential report for the AWS account |
| get_group | Returns a list of IAM users that are in the specified IAM group |
| get_group_policy | Retrieves the specified inline policy document that is embedded in the specified IAM group |
| get_instance_profile | Retrieves information about the specified instance profile, including the instance profile's path |
| get_login_profile | Retrieves the user name and password-creation date for the specified IAM user |
| get_open_id_connect_provider | Returns information about the specified OpenID Connect (OIDC) provider |
| get_organizations_access_report | Retrieves the service last accessed data report for AWS Organizations that was created using the GenerateServiceLastAccessedDetails API |
| get_policy | Retrieves information about the specified managed policy, including the policy's path |
| get_policy_version | Retrieves information about the specified version of the specified managed policy |
| get_role | Retrieves information about the specified role, including the role's path |
| get_role_policy | Retrieves the specified inline policy document that is embedded with the specified IAM role |
| get_saml_provider | Returns the SAML provider metadocument that was uploaded when the specified SAML provider was created |
| get_server_certificate | Retrieves information about the specified server certificate stored in IAM |
| get_service_last_accessed_details | Retrieves a service last accessed report that was created using the GenerateServiceLastAccessedDetails API |
| get_service_last_accessed_details_with_entities | After you generate a group or policy report using the GenerateServiceLastAccessedDetails API, this API returns the status of your service-linked role deletion |
| get_service_linked_role_deletion_status | Retrieves the status of your service-linked role deletion |
| get_ssh_public_key | Retrieves the specified SSH public key, including metadata about the key |
| get_user | Retrieves information about the specified IAM user, including the user's path |
| get_user_policy | Retrieves the specified inline policy document that is embedded in the specified IAM user |
| list_access_keys | Returns information about the access key IDs associated with the specified IAM user |
| list_account_aliases | Lists the account alias associated with the AWS account (Note: you can only have one account alias) |
| list_attached_group_policies | Lists all managed policies that are attached to the specified IAM group |
| list_attached_role_policies | Lists all managed policies that are attached to the specified IAM role |
| list_attached_user_policies | Lists all managed policies that are attached to the specified IAM user |
| list_entities_for_policy | Lists all IAM users, groups, and roles that the specified managed policy is attached to |
| list_group_policies | Lists the names of the inline policies that are embedded in the specified IAM group |
| list_groups | Lists the IAM groups that have the specified path prefix |
| list_groups_for_user | Lists the IAM groups that the specified IAM user belongs to |
| list_instance_profiles | Lists the instance profiles that have the specified path prefix |
| list_instance_profiles_for_role | Lists the instance profiles that have the specified associated IAM role |
| list_mfa_devices | Lists the MFA devices for an IAM user |
| list_open_id_connect_providers | Lists information about the IAM OpenID Connect (OIDC) provider resource objects defined in IAM in the account |
| list_policies | Lists all the managed policies that are available in your AWS account, including the policy's path |
| list_policies_granting_service_access | Retrieves a list of policies that the IAM identity (user, group, or role) can use to access the specified AWS service |
| list_policy_versions | Lists information about the versions of the specified managed policy, including the policy's path |
| list_role_policies | Lists the names of the inline policies that are embedded in the specified IAM role |
| list_roles | Lists the IAM roles that have the specified path prefix |
| list_role_tags | Lists the tags that are attached to the specified role |
| list_saml_providers | Lists the SAML provider resource objects defined in IAM in the account |
| list_server_certificates | Lists the server certificates stored in IAM that have the specified path prefix |
| list_service_specific_credentials | Returns information about the service-specific credentials associated with the specified IAM user |
| list_signing_certificates | Returns information about the signing certificates associated with the specified IAM user |
| list_ssh_public_keys | Returns information about the SSH public keys associated with the specified IAM user |
| list_user_policies | Lists the names of the inline policies embedded in the specified IAM user |
| list_users | Lists the IAM users that have the specified path prefix |
| list_user_tags | Lists the tags that are attached to the specified user |

| | |
|---|--|
| <code>list_virtual_mfa_devices</code> | Lists the virtual MFA devices defined in the AWS account by assignment |
| <code>put_group_policy</code> | Adds or updates an inline policy document that is embedded in the spec |
| <code>put_role_permissions_boundary</code> | Adds or updates the policy that is specified as the IAM role's permission |
| <code>put_role_policy</code> | Adds or updates an inline policy document that is embedded in the spec |
| <code>put_user_permissions_boundary</code> | Adds or updates the policy that is specified as the IAM user's permission |
| <code>put_user_policy</code> | Adds or updates an inline policy document that is embedded in the spec |
| <code>remove_client_id_from_open_id_connect_provider</code> | Removes the specified client ID (also known as audience) from the list o |
| <code>remove_role_from_instance_profile</code> | Removes the specified IAM role from the specified EC2 instance profile |
| <code>remove_user_from_group</code> | Removes the specified user from the specified group |
| <code>reset_service_specific_credential</code> | Resets the password for a service-specific credential |
| <code>resync_mfa_device</code> | Synchronizes the specified MFA device with its IAM resource object on |
| <code>set_default_policy_version</code> | Sets the specified version of the specified policy as the policy's default (|
| <code>set_security_token_service_preferences</code> | Sets the specified version of the global endpoint token as the token versi |
| <code>simulate_custom_policy</code> | Simulate how a set of IAM policies and optionally a resource-based pol |
| <code>simulate_principal_policy</code> | Simulate how a set of IAM policies attached to an IAM entity works wi |
| <code>tag_role</code> | Adds one or more tags to an IAM role |
| <code>tag_user</code> | Adds one or more tags to an IAM user |
| <code>untag_role</code> | Removes the specified tags from the role |
| <code>untag_user</code> | Removes the specified tags from the user |
| <code>update_access_key</code> | Changes the status of the specified access key from Active to Inactive, o |
| <code>update_account_password_policy</code> | Updates the password policy settings for the AWS account |
| <code>update_assume_role_policy</code> | Updates the policy that grants an IAM entity permission to assume a rol |
| <code>update_group</code> | Updates the name and/or the path of the specified IAM group |
| <code>update_login_profile</code> | Changes the password for the specified IAM user |
| <code>update_open_id_connect_provider_thumbprint</code> | Replaces the existing list of server certificate thumbprints associated wi |
| <code>update_role</code> | Updates the description or maximum session duration setting of a role |
| <code>update_role_description</code> | Use UpdateRole instead |
| <code>update_saml_provider</code> | Updates the metadata document for an existing SAML provider resourc |
| <code>update_server_certificate</code> | Updates the name and/or the path of the specified server certificate stor |
| <code>update_service_specific_credential</code> | Sets the status of a service-specific credential to Active or Inactive |
| <code>update_signing_certificate</code> | Changes the status of the specified user signing certificate from active to |
| <code>update_ssh_public_key</code> | Sets the status of an IAM user's SSH public key to active or inactive |
| <code>update_user</code> | Updates the name and/or the path of the specified IAM user |
| <code>upload_server_certificate</code> | Uploads a server certificate entity for the AWS account |
| <code>upload_signing_certificate</code> | Uploads an X |
| <code>upload_ssh_public_key</code> | Uploads an SSH public key and associates it with the specified IAM use |

Examples

```
## Not run:
svc <- iam()
# The following add-client-id-to-open-id-connect-provider command adds the
# client ID my-application-ID to the OIDC provider named
# server.example.com:
svc$add_client_id_to_open_id_connect_provider(
  ClientID = "my-application-ID",
  OpenIDConnectProviderArn = "arn:aws:iam::123456789012:oidc-provider/server.example.com"
```

```
)
## End(Not run)
```

inspector

Amazon Inspector

Description

Amazon Inspector enables you to analyze the behavior of your AWS resources and to identify potential security issues. For more information, see [Amazon Inspector User Guide](#).

Usage

```
inspector(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- inspector(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

| | |
|--|--|
| add_attributes_to_findings | Assigns attributes (key and value pairs) to the findings that are specified by the ARNs of the findings. |
| create_assessment_target | Creates a new assessment target using the ARN of the resource group that is generated by the <code>create_resource_group</code> operation. |
| create_assessment_template | Creates an assessment template for the assessment target that is specified by the ARN of the assessment target. |
| create_exclusions_preview | Starts the generation of an exclusions preview for the specified assessment template. |
| create_resource_group | Creates a resource group using the specified set of tags (key and value pairs) that are used to identify the resource group. |
| delete_assessment_run | Deletes the assessment run that is specified by the ARN of the assessment run. |
| delete_assessment_target | Deletes the assessment target that is specified by the ARN of the assessment target. |
| delete_assessment_template | Deletes the assessment template that is specified by the ARN of the assessment template. |
| describe_assessment_runs | Describes the assessment runs that are specified by the ARNs of the assessment runs. |
| describe_assessment_targets | Describes the assessment targets that are specified by the ARNs of the assessment targets. |
| describe_assessment_templates | Describes the assessment templates that are specified by the ARNs of the assessment templates. |
| describe_cross_account_access_role | Describes the IAM role that enables Amazon Inspector to access your AWS account. |
| describe_exclusions | Describes the exclusions that are specified by the exclusions' ARNs. |
| describe_findings | Describes the findings that are specified by the ARNs of the findings. |
| describe_resource_groups | Describes the resource groups that are specified by the ARNs of the resource groups. |
| describe_rules_packages | Describes the rules packages that are specified by the ARNs of the rules packages. |
| get_assessment_report | Produces an assessment report that includes detailed and comprehensive results of a scan. |
| get_exclusions_preview | Retrieves the exclusions preview (a list of <code>ExclusionPreview</code> objects) specified by the ARN of the assessment template. |
| get_telemetry_metadata | Information about the data that is collected for the specified assessment run. |
| list_assessment_run_agents | Lists the agents of the assessment runs that are specified by the ARNs of the assessment runs. |
| list_assessment_runs | Lists the assessment runs that correspond to the assessment templates that are specified by the ARNs of the assessment templates. |
| list_assessment_targets | Lists the ARNs of the assessment targets within this AWS account. |
| list_assessment_templates | Lists the assessment templates that correspond to the assessment targets that are specified by the ARNs of the assessment targets. |
| list_event_subscriptions | Lists all the event subscriptions for the assessment template that is specified by the ARN of the assessment template. |
| list_exclusions | List exclusions that are generated by the assessment run. |
| list_findings | Lists findings that are generated by the assessment runs that are specified by the ARNs of the assessment runs. |
| list_rules_packages | Lists all available Amazon Inspector rules packages. |
| list_tags_for_resource | Lists all tags associated with an assessment template. |
| preview_agents | Previews the agents installed on the EC2 instances that are part of the specified assessment run. |
| register_cross_account_access_role | Registers the IAM role that grants Amazon Inspector access to AWS Services needed to perform the assessment. |
| remove_attributes_from_findings | Removes entire attributes (key and value pairs) from the findings that are specified by the ARNs of the findings. |
| set_tags_for_resource | Sets tags (key and value pairs) to the assessment template that is specified by the ARN of the assessment template. |
| start_assessment_run | Starts the assessment run specified by the ARN of the assessment template. |
| stop_assessment_run | Stops the assessment run that is specified by the ARN of the assessment run. |
| subscribe_to_event | Enables the process of sending Amazon Simple Notification Service (SNS) notifications for the specified assessment run. |
| unsubscribe_from_event | Disables the process of sending Amazon Simple Notification Service (SNS) notifications for the specified assessment run. |
| update_assessment_target | Updates the assessment target that is specified by the ARN of the assessment target. |

Examples

```
## Not run:
svc <- inspector()
# Assigns attributes (key and value pairs) to the findings that are
# specified by the ARNs of the findings.
svc$add_attributes_to_findings(
```



```
attributes = list(  
  list(  
    key = "Example",  
    value = "example"  
  )  
)  
findingArns = list(  
  "arn:aws:inspector:us-west-2:123456789012:target/0-0kFIPusq/template/0-..."  
)  
)  
  
## End(Not run)
```

kms

AWS Key Management Service

Description

AWS Key Management Service (AWS KMS) is an encryption and key management web service. This guide describes the AWS KMS operations that you can call programmatically. For general information about AWS KMS, see the [AWS Key Management Service Developer Guide](#).

AWS provides SDKs that consist of libraries and sample code for various programming languages and platforms (Java, Ruby, .Net, macOS, Android, etc.). The SDKs provide a convenient way to create programmatic access to AWS KMS and other AWS services. For example, the SDKs take care of tasks such as signing requests (see below), managing errors, and retrying requests automatically. For more information about the AWS SDKs, including how to download and install them, see [Tools for Amazon Web Services](#).

We recommend that you use the AWS SDKs to make programmatic API calls to AWS KMS.

Clients must support TLS (Transport Layer Security) 1.0. We recommend TLS 1.2. Clients must also support cipher suites with Perfect Forward Secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Signing Requests

Requests must be signed by using an access key ID and a secret access key. We strongly recommend that you *do not* use your AWS account (root) access key ID and secret key for everyday work with AWS KMS. Instead, use the access key ID and secret access key for an IAM user. You can also use the AWS Security Token Service to generate temporary security credentials that you can use to sign requests.

All AWS KMS operations require [Signature Version 4](#).

Logging API Requests

AWS KMS supports AWS CloudTrail, a service that logs AWS API calls and related events for your AWS account and delivers them to an Amazon S3 bucket that you specify. By using the information collected by CloudTrail, you can determine what requests were made to AWS KMS, who made the

request, when it was made, and so on. To learn more about CloudTrail, including how to turn it on and find your log files, see the [AWS CloudTrail User Guide](#).

Additional Resources

For more information about credentials and request signing, see the following:

- [AWS Security Credentials](#) - This topic provides general information about the types of credentials used for accessing AWS.
- [Temporary Security Credentials](#) - This section of the *IAM User Guide* describes how to create and use temporary security credentials.
- [Signature Version 4 Signing Process](#) - This set of topics walks you through the process of signing a request using an access key ID and a secret access key.

Commonly Used API Operations

Of the API operations discussed in this guide, the following will prove the most useful for most applications. You will likely perform operations other than these, such as creating keys and assigning policies, by using the console.

- [encrypt](#)
- [decrypt](#)
- [generate_data_key](#)
- [generate_data_key_without_plaintext](#)

Usage

```
kms(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- kms(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
  ),
```

```

        endpoint = "string",
        region = "string"
    )
)

```

Operations

| | |
|--|---|
| cancel_key_deletion | Cancels the deletion of a customer master key (CMK) |
| connect_custom_key_store | Connects or reconnects a custom key store to its associated AWS CloudHSM cluster |
| create_alias | Creates a friendly name for a customer master key (CMK) |
| create_custom_key_store | Creates a custom key store that is associated with an AWS CloudHSM cluster |
| create_grant | Adds a grant to a customer master key (CMK) |
| create_key | Creates a unique customer managed customer master key (CMK) in your AWS account |
| decrypt | Decrypts ciphertext that was encrypted by a AWS KMS customer master key (CMK) |
| delete_alias | Deletes the specified alias |
| delete_custom_key_store | Deletes a custom key store |
| delete_imported_key_material | Deletes key material that you previously imported |
| describe_custom_key_stores | Gets information about custom key stores in the account and region |
| describe_key | Provides detailed information about a customer master key (CMK) |
| disable_key | Sets the state of a customer master key (CMK) to disabled |
| disable_key_rotation | Disables automatic rotation of the key material for the specified symmetric customer master key (CMK) |
| disconnect_custom_key_store | Disconnects the custom key store from its associated AWS CloudHSM cluster |
| enable_key | Sets the key state of a customer master key (CMK) to enabled |
| enable_key_rotation | Enables automatic rotation of the key material for the specified symmetric customer master key (CMK) |
| encrypt | Encrypts plaintext into ciphertext by using a customer master key (CMK) |
| generate_data_key | Generates a unique symmetric data key for client-side encryption |
| generate_data_key_pair | Generates a unique asymmetric data key pair |
| generate_data_key_pair_without_plaintext | Generates a unique asymmetric data key pair |
| generate_data_key_without_plaintext | Generates a unique symmetric data key |
| generate_random | Returns a random byte string that is cryptographically secure |
| get_key_policy | Gets a key policy attached to the specified customer master key (CMK) |
| get_key_rotation_status | Gets a Boolean value that indicates whether automatic rotation of the key material is enabled |
| get_parameters_for_import | Returns the items you need to import key material into a symmetric, customer managed key store |
| get_public_key | Returns the public key of an asymmetric CMK |
| import_key_material | Imports key material into an existing symmetric AWS KMS customer master key (CMK) |
| list_aliases | Gets a list of aliases in the caller's AWS account and region |
| list_grants | Gets a list of all grants for the specified customer master key (CMK) |
| list_key_policies | Gets the names of the key policies that are attached to a customer master key (CMK) |
| list_keys | Gets a list of all customer master keys (CMKs) in the caller's AWS account and region |
| list_resource_tags | Returns all tags on the specified customer master key (CMK) |
| list_retirable_grants | Returns all grants in which the specified principal is the RetiringPrincipal in the caller's AWS account |
| put_key_policy | Attaches a key policy to the specified customer master key (CMK) |
| re_encrypt | Decrypts ciphertext and then reencrypts it entirely within AWS KMS |
| retire_grant | Retires a grant |
| revoke_grant | Revokes the specified grant for the specified customer master key (CMK) |
| schedule_key_deletion | Schedules the deletion of a customer master key (CMK) |
| sign | Creates a digital signature for a message or message digest by using the private key of a customer master key (CMK) |
| tag_resource | Adds or edits tags on a customer managed CMK |

| | |
|---|---|
| untag_resource | Deletes tags from a customer managed CMK |
| update_alias | Associates an existing AWS KMS alias with a different customer master key (CMK) |
| update_custom_key_store | Changes the properties of a custom key store |
| update_key_description | Updates the description of a customer master key (CMK) |
| verify | Verifies a digital signature that was generated by the Sign operation |

Examples

```
## Not run:
svc <- kms()
# The following example cancels deletion of the specified CMK.
svc$cancel_key_deletion(
  KeyId = "1234abcd-12ab-34cd-56ef-1234567890ab"
)

## End(Not run)
```

macie

Amazon Macie

Description

Amazon Macie Classic

Amazon Macie Classic is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Macie Classic recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides you with dashboards and alerts that give visibility into how this data is being accessed or moved. For more information, see the [Amazon Macie Classic User Guide](#).

A new Amazon Macie is now available with significant design improvements and additional features, at a lower price and in most AWS Regions. We encourage you to explore and use the new and improved features, and benefit from the reduced cost. To learn about features and pricing for the new Amazon Macie, see [Amazon Macie](#).

Usage

```
macie(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```

svc <- macie(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

| | |
|---|---|
| associate_member_account | Associates a specified AWS account with Amazon Macie Classic as a member account |
| associate_s3_resources | Associates specified S3 resources with Amazon Macie Classic for monitoring and data classification |
| disassociate_member_account | Removes the specified member account from Amazon Macie Classic |
| disassociate_s3_resources | Removes specified S3 resources from being monitored by Amazon Macie Classic |
| list_member_accounts | Lists all Amazon Macie Classic member accounts for the current Amazon Macie Classic managed account |
| list_s3_resources | Lists all the S3 resources associated with Amazon Macie Classic |
| update_s3_resources | Updates the classification types for the specified S3 resources |

Examples

```

## Not run:
svc <- macie()
svc$associate_member_account(
  Foo = 123
)

## End(Not run)

```

Description

Use AWS Resource Access Manager to share AWS resources between AWS accounts. To share a resource, you create a resource share, associate the resource with the resource share, and specify the principals that can access the resources associated with the resource share. The following

principals are supported: AWS accounts, organizational units (OU) from AWS Organizations, and organizations from AWS Organizations.

For more information, see the [AWS Resource Access Manager User Guide](#).

Usage

```
ram(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- ram(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

| | |
|--|---|
| accept_resource_share_invitation | Accepts an invitation to a resource share from another AWS account |
| associate_resource_share | Associates the specified resource share with the specified principals and resources |
| associate_resource_share_permission | Associates a permission with a resource share |
| create_resource_share | Creates a resource share |
| delete_resource_share | Deletes the specified resource share |
| disassociate_resource_share | Disassociates the specified principals or resources from the specified resource share |
| disassociate_resource_share_permission | Disassociates an AWS RAM permission from a resource share |
| enable_sharing_with_aws_organization | Enables resource sharing within your AWS Organization |
| get_permission | Gets the contents of an AWS RAM permission in JSON format |
| get_resource_policies | Gets the policies for the specified resources that you own and have shared |
| get_resource_share_associations | Gets the resources or principals for the resource shares that you own |
| get_resource_share_invitations | Gets the invitations for resource sharing that you've received |

| | |
|--|--|
| get_resource_shares | Gets the resource shares that you own or the resource shares that are shared with you |
| list_pending_invitation_resources | Lists the resources in a resource share that is shared with you but that the invitation is still pending |
| list_permissions | Lists the AWS RAM permissions |
| list_principals | Lists the principals that you have shared resources with or that have shared resources with you |
| list_resources | Lists the resources that you added to a resource share or the resources that are shared with you |
| list_resource_share_permissions | Lists the AWS RAM permissions that are associated with a resource share |
| list_resource_types | Lists the shareable resource types supported by AWS RAM |
| promote_resource_share_created_from_policy | Resource shares that were created by attaching a policy to a resource are visible to all principals in the account |
| reject_resource_share_invitation | Rejects an invitation to a resource share from another AWS account |
| tag_resource | Adds the specified tags to the specified resource share that you own |
| untag_resource | Removes the specified tags from the specified resource share that you own |
| update_resource_share | Updates the specified resource share that you own |

Examples

```
## Not run:
svc <- ram()
svc$accept_resource_share_invitation(
  Foo = 123
)

## End(Not run)
```

secretsmanager

AWS Secrets Manager

Description

AWS Secrets Manager API Reference

AWS Secrets Manager provides a service to enable you to store, manage, and retrieve, secrets.

This guide provides descriptions of the Secrets Manager API. For more information about using this service, see the [AWS Secrets Manager User Guide](#).

API Version

This version of the Secrets Manager API Reference documents the Secrets Manager API version 2017-10-17.

As an alternative to using the API, you can use one of the AWS SDKs, which consist of libraries and sample code for various programming languages and platforms such as Java, Ruby, .NET, iOS, and Android. The SDKs provide a convenient way to create programmatic access to AWS Secrets Manager. For example, the SDKs provide cryptographically signing requests, managing errors, and retrying requests automatically. For more information about the AWS SDKs, including downloading and installing them, see [Tools for Amazon Web Services](#).

We recommend you use the AWS SDKs to make programmatic API calls to Secrets Manager. However, you also can use the Secrets Manager HTTP Query API to make direct calls to the Secrets

Manager web service. To learn more about the Secrets Manager HTTP Query API, see [Making Query Requests](#) in the *AWS Secrets Manager User Guide*.

Secrets Manager API supports GET and POST requests for all actions, and doesn't require you to use GET for some actions and POST for others. However, GET requests are subject to the limitation size of a URL. Therefore, for operations that require larger sizes, use a POST request.

Support and Feedback for AWS Secrets Manager

We welcome your feedback. Send your comments to awssecretsmanager-feedback@amazon.com, or post your feedback and questions in the [AWS Secrets Manager Discussion Forum](#). For more information about the AWS Discussion Forums, see [Forums Help](#).

How examples are presented

The JSON that AWS Secrets Manager expects as your request parameters and the service returns as a response to HTTP query requests contain single, long strings without line breaks or white space formatting. The JSON shown in the examples displays the code formatted with both line breaks and white space to improve readability. When example input parameters can also cause long strings extending beyond the screen, you can insert line breaks to enhance readability. You should always submit the input as a single JSON text string.

Logging API Requests

AWS Secrets Manager supports AWS CloudTrail, a service that records AWS API calls for your AWS account and delivers log files to an Amazon S3 bucket. By using information that's collected by AWS CloudTrail, you can determine the requests successfully made to Secrets Manager, who made the request, when it was made, and so on. For more about AWS Secrets Manager and support for AWS CloudTrail, see [Logging AWS Secrets Manager Events with AWS CloudTrail](#) in the *AWS Secrets Manager User Guide*. To learn more about CloudTrail, including enabling it and find your log files, see the [AWS CloudTrail User Guide](#).

Usage

```
secretsmanager(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the [Operations](#) section.

Service syntax

```
svc <- secretsmanager(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
```

```

        session_token = "string"
    ),
    profile = "string"
),
endpoint = "string",
region = "string"
)
)

```

Operations

| | |
|---|--|
| cancel_rotate_secret | Disables automatic scheduled rotation and cancels the rotation of a secret if currently in progress |
| create_secret | Creates a new secret |
| delete_resource_policy | Deletes the resource-based permission policy attached to the secret |
| delete_secret | Deletes an entire secret and all of its versions |
| describe_secret | Retrieves the details of a secret |
| get_random_password | Generates a random password of the specified complexity |
| get_resource_policy | Retrieves the JSON text of the resource-based policy document attached to the specified secret |
| get_secret_value | Retrieves the contents of the encrypted fields SecretString or SecretBinary from the specified version |
| list_secrets | Lists all of the secrets that are stored by Secrets Manager in the AWS account |
| list_secret_version_ids | Lists all of the versions attached to the specified secret |
| put_resource_policy | Attaches the contents of the specified resource-based permission policy to a secret |
| put_secret_value | Stores a new encrypted secret value in the specified secret |
| restore_secret | Cancels the scheduled deletion of a secret by removing the DeletedDate time stamp |
| rotate_secret | Configures and starts the asynchronous process of rotating this secret |
| tag_resource | Attaches one or more tags, each consisting of a key name and a value, to the specified secret |
| untag_resource | Removes one or more tags from the specified secret |
| update_secret | Modifies many of the details of the specified secret |
| update_secret_version_stage | Modifies the staging labels attached to a version of a secret |
| validate_resource_policy | Validates the JSON text of the resource-based policy document attached to the specified secret |

Examples

```

## Not run:
svc <- secretsmanager()
# The following example shows how to cancel rotation for a secret. The
# operation sets the RotationEnabled field to false and cancels all
# scheduled rotations. To resume scheduled rotations, you must re-enable
# rotation by calling the rotate-secret operation.
svc$cancel_rotate_secret(
  SecretId = "MyTestDatabaseSecret"
)

## End(Not run)

```

`securityhub`*AWS SecurityHub*

Description

Security Hub provides you with a comprehensive view of the security state of your AWS environment and resources. It also provides you with the readiness status of your environment based on controls from supported security standards. Security Hub collects security data from AWS accounts, services, and integrated third-party products and helps you analyze security trends in your environment to identify the highest priority security issues. For more information about Security Hub, see the *AWS Security Hub User Guide*.

When you use operations in the Security Hub API, the requests are executed only in the AWS Region that is currently active or in the specific AWS Region that you specify in your request. Any configuration or settings change that results from the operation is applied only to that Region. To make the same change in other Regions, execute the same command for each Region to apply the change to.

For example, if your Region is set to `us-west-2`, when you use `create_members` to add a member account to Security Hub, the association of the member account with the master account is created only in the `us-west-2` Region. Security Hub must be enabled for the member account in the same Region that the invitation was sent from.

The following throttling limits apply to using Security Hub API operations.

- `batch_enable_standards` - RateLimit of 1 request per second, BurstLimit of 1 request per second.
- `get_findings` - RateLimit of 3 requests per second. BurstLimit of 6 requests per second.
- `update_findings` - RateLimit of 1 request per second. BurstLimit of 5 requests per second.
- `update_standards_control` - RateLimit of 1 request per second, BurstLimit of 5 requests per second.
- All other operations - RateLimit of 10 requests per second. BurstLimit of 30 requests per second.

Usage

```
securityhub(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```

svc <- securityhub(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

| | |
|---|---|
| accept_invitation | Accepts the invitation to be a member account and be monitored by the Security Hub |
| batch_disable_standards | Disables the standards specified by the provided StandardsSubscriptionArns |
| batch_enable_standards | Enables the standards specified by the provided StandardsArn |
| batch_import_findings | Imports security findings generated from an integrated third-party product into Security Hub |
| batch_update_findings | Used by Security Hub customers to update information about their investigation into a finding |
| create_action_target | Creates a custom action target in Security Hub |
| create_insight | Creates a custom insight in Security Hub |
| create_members | Creates a member association in Security Hub between the specified accounts and the associated master account |
| decline_invitations | Declines invitations to become a member account |
| delete_action_target | Deletes a custom action target from Security Hub |
| delete_insight | Deletes the insight specified by the InsightArn |
| delete_invitations | Deletes invitations received by the AWS account to become a member account |
| delete_members | Deletes the specified member accounts from Security Hub |
| describe_action_targets | Returns a list of the custom action targets in Security Hub in your account |
| describe_hub | Returns details about the Hub resource in your account, including the HubArn and the Region |
| describe_organization_configuration | Returns information about the Organizations configuration for Security Hub |
| describe_products | Returns information about the available products that you can subscribe to and integrate with Security Hub |
| describe_standards | Returns a list of the available standards in Security Hub |
| describe_standards_controls | Returns a list of security standards controls |
| disable_import_findings_for_product | Disables the integration of the specified product with Security Hub |
| disable_organization_admin_account | Disables a Security Hub administrator account |
| disable_security_hub | Disables Security Hub in your account only in the current Region |
| disassociate_from_master_account | Disassociates the current Security Hub member account from the associated master account |
| disassociate_members | Disassociates the specified member accounts from the associated master account |
| enable_import_findings_for_product | Enables the integration of a partner product with Security Hub |
| enable_organization_admin_account | Designates the Security Hub administrator account for an organization |
| enable_security_hub | Enables Security Hub for your account in the current Region or the Region you specify |
| get_enabled_standards | Returns a list of the standards that are currently enabled |
| get_findings | Returns a list of findings that match the specified criteria |
| get_insight_results | Lists the results of the Security Hub insight specified by the insight ARN |

| | |
|---|--|
| get_insights | Lists and describes insights for the specified insight ARNs |
| get_invitations_count | Returns the count of all Security Hub membership invitations that were sent to the current AWS account |
| get_master_account | Provides the details for the Security Hub master account for the current member account |
| get_members | Returns the details for the Security Hub member accounts for the specified account ID |
| invite_members | Invites other AWS accounts to become member accounts for the Security Hub master account |
| list_enabled_products_for_import | Lists all findings-generating solutions (products) that you are subscribed to receive findings for |
| list_invitations | Lists all Security Hub membership invitations that were sent to the current AWS account |
| list_members | Lists details about all member accounts for the current Security Hub master account |
| list_organization_admin_accounts | Lists the Security Hub administrator accounts |
| list_tags_for_resource | Returns a list of tags associated with a resource |
| tag_resource | Adds one or more tags to a resource |
| untag_resource | Removes one or more tags from a resource |
| update_action_target | Updates the name and description of a custom action target in Security Hub |
| update_findings | UpdateFindings is deprecated |
| update_insight | Updates the Security Hub insight identified by the specified insight ARN |
| update_organization_configuration | Used to update the configuration related to Organizations |
| update_security_hub_configuration | Updates configuration options for Security Hub |
| update_standards_control | Used to control whether an individual security standard control is enabled or disabled |

Examples

```
## Not run:
svc <- securityhub()
svc$accept_invitation(
  Foo = 123
)

## End(Not run)
```

shield

AWS Shield

Description

AWS Shield Advanced

This is the *AWS Shield Advanced API Reference*. This guide is for developers who need detailed information about the AWS Shield Advanced API actions, data types, and errors. For detailed information about AWS WAF and AWS Shield Advanced features and an overview of how to use the AWS WAF and AWS Shield Advanced APIs, see the [AWS WAF and AWS Shield Developer Guide](#).

Usage

```
shield(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```
svc <- shield(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)
```

Operations

| | |
|--|--|
| associate_drt_log_bucket | Authorizes the DDoS Response Team (DRT) to access the specified Amazon S3 bucket |
| associate_drt_role | Authorizes the DDoS Response Team (DRT), using the specified role, to access your AWS account |
| associate_health_check | Adds health-based detection to the Shield Advanced protection for a resource |
| associate_proactive_engagement_details | Initializes proactive engagement and sets the list of contacts for the DDoS Response Team (DRT) |
| create_protection | Enables AWS Shield Advanced for a specific AWS resource |
| create_protection_group | Creates a grouping of protected resources so they can be handled as a collective |
| create_subscription | Activates AWS Shield Advanced for an account |
| delete_protection | Deletes an AWS Shield Advanced Protection |
| delete_protection_group | Removes the specified protection group |
| delete_subscription | Removes AWS Shield Advanced from an account |
| describe_attack | Describes the details of a DDoS attack |
| describe_attack_statistics | Provides information about the number and type of attacks AWS Shield has detected |
| describe_drt_access | Returns the current role and list of Amazon S3 log buckets used by the DDoS Response Team (DRT) |
| describe_emergency_contact_settings | A list of email addresses and phone numbers that the DDoS Response Team (DRT) can use to reach you |
| describe_protection | Lists the details of a Protection object |
| describe_protection_group | Returns the specification for the specified protection group |
| describe_subscription | Provides details about the AWS Shield Advanced subscription for an account |
| disable_proactive_engagement | Removes authorization from the DDoS Response Team (DRT) to notify contacts about attacks |
| disassociate_drt_log_bucket | Removes the DDoS Response Team's (DRT) access to the specified Amazon S3 bucket |
| disassociate_drt_role | Removes the DDoS Response Team's (DRT) access to your AWS account |

| | |
|--|---|
| disassociate_health_check | Removes health-based detection from the Shield Advanced protection for a resource |
| enable_proactive_engagement | Authorizes the DDoS Response Team (DRT) to use email and phone to notify contacts |
| get_subscription_state | Returns the SubscriptionState, either Active or Inactive |
| list_attacks | Returns all ongoing DDoS attacks or all DDoS attacks during a specified time period |
| list_protection_groups | Retrieves the ProtectionGroup objects for the account |
| list_protections | Lists all Protection objects for the account |
| list_resources_in_protection_group | Retrieves the resources that are included in the protection group |
| update_emergency_contact_settings | Updates the details of the list of email addresses and phone numbers that the DDoS Response Team (DRT) can use to contact you |
| update_protection_group | Updates an existing protection group |
| update_subscription | Updates the details of an existing subscription |

Examples

```
## Not run:
svc <- shield()
svc$associate_drt_log_bucket(
  Foo = 123
)

## End(Not run)
```

 sts

 AWS Security Token Service

Description

AWS Security Token Service (STS) enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users). This guide provides descriptions of the STS API. For more information about using this service, see [Temporary Security Credentials](#).

Usage

```
sts(config = list())
```

Arguments

config Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the [Operations](#) section.

Service syntax

```

svc <- sts(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

| | |
|---|---|
| assume_role | Returns a set of temporary security credentials that you can use to access AWS resources th |
| assume_role_with_saml | Returns a set of temporary security credentials for users who have been authenticated via a |
| assume_role_with_web_identity | Returns a set of temporary security credentials for users who have been authenticated in a n |
| decode_authorization_message | Decodes additional information about the authorization status of a request from an encode |
| get_access_key_info | Returns the account identifier for the specified access key ID |
| get_caller_identity | Returns details about the IAM user or role whose credentials are used to call the operation |
| get_federation_token | Returns a set of temporary security credentials (consisting of an access key ID, a secret acc |
| get_session_token | Returns a set of temporary credentials for an AWS account or IAM user |

Examples

```

## Not run:
svc <- sts()
#
svc$assume_role(
  ExternalId = "123ABC",
  Policy = "{\Version\": \"2012-10-17\", \"Statement\": [{\Sid\": \"Stmnt1\", \"Effect\": \"A...\",
  RoleArn = \"arn:aws:iam::123456789012:role/demo\",
  RoleSessionName = \"testAssumeRoleSession\",
  Tags = list(
    list(
      Key = \"Project\",
      Value = \"Unicorn\"
    ),
    list(
      Key = \"Team\",
      Value = \"Automation\"
    ),
    list(

```

```
        Key = "Cost-Center",
        Value = "12345"
    )
),
TransitiveTagKeys = list(
    "Project",
    "Cost-Center"
)
)

## End(Not run)
```

waf

AWS WAF

Description

This is **AWS WAF Classic** documentation. For more information, see [AWS WAF Classic](#) in the developer guide.

For the latest version of AWS WAF, use the AWS WAFV2 API and see the [AWS WAF Developer Guide](#). With the latest version, AWS WAF has a single set of endpoints for regional and global use.

This is the *AWS WAF Classic API Reference* for using AWS WAF Classic with Amazon CloudFront. The AWS WAF Classic actions and data types listed in the reference are available for protecting Amazon CloudFront distributions. You can use these actions and data types via the endpoint *waf.amazonaws.com*. This guide is for developers who need detailed information about the AWS WAF Classic API actions, data types, and errors. For detailed information about AWS WAF Classic features and an overview of how to use the AWS WAF Classic API, see the [AWS WAF Classic](#) in the developer guide.

Usage

```
waf(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the Operations section.

Service syntax

```

svc <- waf(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

| | |
|--|--|
| create_byte_match_set | This is AWS WAF Classic documentation |
| create_geo_match_set | This is AWS WAF Classic documentation |
| create_ip_set | This is AWS WAF Classic documentation |
| create_rate_based_rule | This is AWS WAF Classic documentation |
| create_regex_match_set | This is AWS WAF Classic documentation |
| create_regex_pattern_set | This is AWS WAF Classic documentation |
| create_rule | This is AWS WAF Classic documentation |
| create_rule_group | This is AWS WAF Classic documentation |
| create_size_constraint_set | This is AWS WAF Classic documentation |
| create_sql_injection_match_set | This is AWS WAF Classic documentation |
| create_web_acl | This is AWS WAF Classic documentation |
| create_web_acl_migration_stack | Creates an AWS CloudFormation WAFV2 template for the specified web ACL in the sp |
| create_xss_match_set | This is AWS WAF Classic documentation |
| delete_byte_match_set | This is AWS WAF Classic documentation |
| delete_geo_match_set | This is AWS WAF Classic documentation |
| delete_ip_set | This is AWS WAF Classic documentation |
| delete_logging_configuration | This is AWS WAF Classic documentation |
| delete_permission_policy | This is AWS WAF Classic documentation |
| delete_rate_based_rule | This is AWS WAF Classic documentation |
| delete_regex_match_set | This is AWS WAF Classic documentation |
| delete_regex_pattern_set | This is AWS WAF Classic documentation |
| delete_rule | This is AWS WAF Classic documentation |
| delete_rule_group | This is AWS WAF Classic documentation |
| delete_size_constraint_set | This is AWS WAF Classic documentation |
| delete_sql_injection_match_set | This is AWS WAF Classic documentation |
| delete_web_acl | This is AWS WAF Classic documentation |
| delete_xss_match_set | This is AWS WAF Classic documentation |
| get_byte_match_set | This is AWS WAF Classic documentation |
| get_change_token | This is AWS WAF Classic documentation |
| get_change_token_status | This is AWS WAF Classic documentation |

| | |
|--|---------------------------------------|
| get_geo_match_set | This is AWS WAF Classic documentation |
| get_ip_set | This is AWS WAF Classic documentation |
| get_logging_configuration | This is AWS WAF Classic documentation |
| get_permission_policy | This is AWS WAF Classic documentation |
| get_rate_based_rule | This is AWS WAF Classic documentation |
| get_rate_based_rule_managed_keys | This is AWS WAF Classic documentation |
| get_regex_match_set | This is AWS WAF Classic documentation |
| get_regex_pattern_set | This is AWS WAF Classic documentation |
| get_rule | This is AWS WAF Classic documentation |
| get_rule_group | This is AWS WAF Classic documentation |
| get_sampled_requests | This is AWS WAF Classic documentation |
| get_size_constraint_set | This is AWS WAF Classic documentation |
| get_sql_injection_match_set | This is AWS WAF Classic documentation |
| get_web_acl | This is AWS WAF Classic documentation |
| get_xss_match_set | This is AWS WAF Classic documentation |
| list_activated_rules_in_rule_group | This is AWS WAF Classic documentation |
| list_byte_match_sets | This is AWS WAF Classic documentation |
| list_geo_match_sets | This is AWS WAF Classic documentation |
| list_ip_sets | This is AWS WAF Classic documentation |
| list_logging_configurations | This is AWS WAF Classic documentation |
| list_rate_based_rules | This is AWS WAF Classic documentation |
| list_regex_match_sets | This is AWS WAF Classic documentation |
| list_regex_pattern_sets | This is AWS WAF Classic documentation |
| list_rule_groups | This is AWS WAF Classic documentation |
| list_rules | This is AWS WAF Classic documentation |
| list_size_constraint_sets | This is AWS WAF Classic documentation |
| list_sql_injection_match_sets | This is AWS WAF Classic documentation |
| list_subscribed_rule_groups | This is AWS WAF Classic documentation |
| list_tags_for_resource | This is AWS WAF Classic documentation |
| list_web_acl_ls | This is AWS WAF Classic documentation |
| list_xss_match_sets | This is AWS WAF Classic documentation |
| put_logging_configuration | This is AWS WAF Classic documentation |
| put_permission_policy | This is AWS WAF Classic documentation |
| tag_resource | This is AWS WAF Classic documentation |
| untag_resource | This is AWS WAF Classic documentation |
| update_byte_match_set | This is AWS WAF Classic documentation |
| update_geo_match_set | This is AWS WAF Classic documentation |
| update_ip_set | This is AWS WAF Classic documentation |
| update_rate_based_rule | This is AWS WAF Classic documentation |
| update_regex_match_set | This is AWS WAF Classic documentation |
| update_regex_pattern_set | This is AWS WAF Classic documentation |
| update_rule | This is AWS WAF Classic documentation |
| update_rule_group | This is AWS WAF Classic documentation |
| update_size_constraint_set | This is AWS WAF Classic documentation |
| update_sql_injection_match_set | This is AWS WAF Classic documentation |
| update_web_acl | This is AWS WAF Classic documentation |
| update_xss_match_set | This is AWS WAF Classic documentation |

Examples

```
## Not run:
svc <- waf()
# The following example creates an IP match set named MyIPSetFriendlyName.
svc$create_ip_set(
  ChangeToken = "abcd12f2-46da-4fdb-b8d5-fbd4c466928f",
  Name = "MyIPSetFriendlyName"
)

## End(Not run)
```

wafregional

AWS WAF Regional

Description

This is **AWS WAF Classic Regional** documentation. For more information, see [AWS WAF Classic](#) in the developer guide.

For the latest version of AWS WAF, use the AWS WAFV2 API and see the [AWS WAF Developer Guide](#). With the latest version, AWS WAF has a single set of endpoints for regional and global use.

This is the *AWS WAF Regional Classic API Reference* for using AWS WAF Classic with the AWS resources, Elastic Load Balancing (ELB) Application Load Balancers and API Gateway APIs. The AWS WAF Classic actions and data types listed in the reference are available for protecting Elastic Load Balancing (ELB) Application Load Balancers and API Gateway APIs. You can use these actions and data types by means of the endpoints listed in [AWS Regions and Endpoints](#). This guide is for developers who need detailed information about the AWS WAF Classic API actions, data types, and errors. For detailed information about AWS WAF Classic features and an overview of how to use the AWS WAF Classic API, see the [AWS WAF Classic](#) in the developer guide.

Usage

```
wafregional(config = list())
```

Arguments

`config` Optional configuration of credentials, endpoint, and/or region.

Value

A client for the service. You can call the service's operations using syntax like `svc$operation(...)`, where `svc` is the name you've assigned to the client. The available operations are listed in the [Operations](#) section.

Service syntax

```

svc <- wafregional(
  config = list(
    credentials = list(
      creds = list(
        access_key_id = "string",
        secret_access_key = "string",
        session_token = "string"
      ),
      profile = "string"
    ),
    endpoint = "string",
    region = "string"
  )
)

```

Operations

| | |
|--|--|
| associate_web_acl | This is AWS WAF Classic Regional documentation |
| create_byte_match_set | This is AWS WAF Classic documentation |
| create_geo_match_set | This is AWS WAF Classic documentation |
| create_ip_set | This is AWS WAF Classic documentation |
| create_rate_based_rule | This is AWS WAF Classic documentation |
| create_regex_match_set | This is AWS WAF Classic documentation |
| create_regex_pattern_set | This is AWS WAF Classic documentation |
| create_rule | This is AWS WAF Classic documentation |
| create_rule_group | This is AWS WAF Classic documentation |
| create_size_constraint_set | This is AWS WAF Classic documentation |
| create_sql_injection_match_set | This is AWS WAF Classic documentation |
| create_web_acl | This is AWS WAF Classic documentation |
| create_web_acl_migration_stack | Creates an AWS CloudFormation WAFV2 template for the specified web ACL in the sp |
| create_xss_match_set | This is AWS WAF Classic documentation |
| delete_byte_match_set | This is AWS WAF Classic documentation |
| delete_geo_match_set | This is AWS WAF Classic documentation |
| delete_ip_set | This is AWS WAF Classic documentation |
| delete_logging_configuration | This is AWS WAF Classic documentation |
| delete_permission_policy | This is AWS WAF Classic documentation |
| delete_rate_based_rule | This is AWS WAF Classic documentation |
| delete_regex_match_set | This is AWS WAF Classic documentation |
| delete_regex_pattern_set | This is AWS WAF Classic documentation |
| delete_rule | This is AWS WAF Classic documentation |
| delete_rule_group | This is AWS WAF Classic documentation |
| delete_size_constraint_set | This is AWS WAF Classic documentation |
| delete_sql_injection_match_set | This is AWS WAF Classic documentation |
| delete_web_acl | This is AWS WAF Classic documentation |
| delete_xss_match_set | This is AWS WAF Classic documentation |
| disassociate_web_acl | This is AWS WAF Classic Regional documentation |
| get_byte_match_set | This is AWS WAF Classic documentation |

| | |
|--|--|
| get_change_token | This is AWS WAF Classic documentation |
| get_change_token_status | This is AWS WAF Classic documentation |
| get_geo_match_set | This is AWS WAF Classic documentation |
| get_ip_set | This is AWS WAF Classic documentation |
| get_logging_configuration | This is AWS WAF Classic documentation |
| get_permission_policy | This is AWS WAF Classic documentation |
| get_rate_based_rule | This is AWS WAF Classic documentation |
| get_rate_based_rule_managed_keys | This is AWS WAF Classic documentation |
| get_regex_match_set | This is AWS WAF Classic documentation |
| get_regex_pattern_set | This is AWS WAF Classic documentation |
| get_rule | This is AWS WAF Classic documentation |
| get_rule_group | This is AWS WAF Classic documentation |
| get_sampled_requests | This is AWS WAF Classic documentation |
| get_size_constraint_set | This is AWS WAF Classic documentation |
| get_sql_injection_match_set | This is AWS WAF Classic documentation |
| get_web_acl | This is AWS WAF Classic documentation |
| get_web_acl_for_resource | This is AWS WAF Classic Regional documentation |
| get_xss_match_set | This is AWS WAF Classic documentation |
| list_activated_rules_in_rule_group | This is AWS WAF Classic documentation |
| list_byte_match_sets | This is AWS WAF Classic documentation |
| list_geo_match_sets | This is AWS WAF Classic documentation |
| list_ip_sets | This is AWS WAF Classic documentation |
| list_logging_configurations | This is AWS WAF Classic documentation |
| list_rate_based_rules | This is AWS WAF Classic documentation |
| list_regex_match_sets | This is AWS WAF Classic documentation |
| list_regex_pattern_sets | This is AWS WAF Classic documentation |
| list_resources_for_web_acl | This is AWS WAF Classic Regional documentation |
| list_rule_groups | This is AWS WAF Classic documentation |
| list_rules | This is AWS WAF Classic documentation |
| list_size_constraint_sets | This is AWS WAF Classic documentation |
| list_sql_injection_match_sets | This is AWS WAF Classic documentation |
| list_subscribed_rule_groups | This is AWS WAF Classic documentation |
| list_tags_for_resource | This is AWS WAF Classic documentation |
| list_web_acl_ls | This is AWS WAF Classic documentation |
| list_xss_match_sets | This is AWS WAF Classic documentation |
| put_logging_configuration | This is AWS WAF Classic documentation |
| put_permission_policy | This is AWS WAF Classic documentation |
| tag_resource | This is AWS WAF Classic documentation |
| untag_resource | This is AWS WAF Classic documentation |
| update_byte_match_set | This is AWS WAF Classic documentation |
| update_geo_match_set | This is AWS WAF Classic documentation |
| update_ip_set | This is AWS WAF Classic documentation |
| update_rate_based_rule | This is AWS WAF Classic documentation |
| update_regex_match_set | This is AWS WAF Classic documentation |
| update_regex_pattern_set | This is AWS WAF Classic documentation |
| update_rule | This is AWS WAF Classic documentation |
| update_rule_group | This is AWS WAF Classic documentation |
| update_size_constraint_set | This is AWS WAF Classic documentation |

| | |
|--|---------------------------------------|
| update_sql_injection_match_set | This is AWS WAF Classic documentation |
| update_web_acl | This is AWS WAF Classic documentation |
| update_xss_match_set | This is AWS WAF Classic documentation |

Examples

```
## Not run:
svc <- wafregional()
# The following example creates an IP match set named MyIPSetFriendlyName.
svc$create_ip_set(
  ChangeToken = "abcd12f2-46da-4fdb-b8d5-fbd4c466928f",
  Name = "MyIPSetFriendlyName"
)

## End(Not run)
```

Index

accept_invitation, [24, 42](#)
accept_resource_share_invitation, [37](#)
accept_shared_directory, [19](#)
acm, [3](#)
acmpca, [4](#)
add_attributes_to_findings, [31](#)
add_client_id_to_open_id_connect_provider, [26](#)
add_custom_attributes, [14](#)
add_facet_to_object, [7](#)
add_ip_routes, [19](#)
add_region, [19](#)
add_role_to_instance_profile, [26](#)
add_tags_to_certificate, [3](#)
add_tags_to_resource, [9, 20](#)
add_user_to_group, [26](#)
admin_add_user_to_group, [14](#)
admin_confirm_sign_up, [14](#)
admin_create_user, [14](#)
admin_delete_user, [14](#)
admin_delete_user_attributes, [14](#)
admin_disable_provider_for_user, [14](#)
admin_disable_user, [14](#)
admin_enable_user, [14](#)
admin_forget_device, [15](#)
admin_get_device, [15](#)
admin_get_user, [15](#)
admin_initiate_auth, [15](#)
admin_link_provider_for_user, [15](#)
admin_list_devices, [15](#)
admin_list_groups_for_user, [15](#)
admin_list_user_auth_events, [15](#)
admin_remove_user_from_group, [15](#)
admin_reset_user_password, [15](#)
admin_respond_to_auth_challenge, [15](#)
admin_set_user_mfa_preference, [15](#)
admin_set_user_password, [15](#)
admin_set_user_settings, [15](#)
admin_update_auth_event_feedback, [15](#)
admin_update_device_status, [15](#)
admin_update_user_attributes, [15](#)
admin_user_global_sign_out, [15](#)
apply_schema, [7](#)
archive_findings, [24](#)
associate_admin_account, [22](#)
associate_drt_log_bucket, [44](#)
associate_drt_role, [44](#)
associate_health_check, [44](#)
associate_member_account, [36](#)
associate_proactive_engagement_details, [44](#)
associate_resource_share, [37](#)
associate_resource_share_permission, [37](#)
associate_s3_resources, [36](#)
associate_software_token, [15](#)
associate_web_acl, [51](#)
assume_role, [46](#)
assume_role_with_saml, [46](#)
assume_role_with_web_identity, [46](#)
attach_group_policy, [26](#)
attach_object, [7](#)
attach_policy, [7](#)
attach_role_policy, [26](#)
attach_to_index, [7](#)
attach_typed_link, [7](#)
attach_user_policy, [26](#)
batch_disable_standards, [42](#)
batch_enable_standards, [41, 42](#)
batch_import_findings, [42](#)
batch_read, [7](#)
batch_update_findings, [42](#)
batch_write, [7](#)
bulk_publish, [18](#)
cancel_key_deletion, [34](#)
cancel_rotate_secret, [40](#)
cancel_schema_extension, [20](#)

- change_password, [15](#), [26](#)
- clouddirectory, [6](#)
- cloudhsm, [8](#)
- cloudhsmv2, [10](#)
- cognitoidentity, [12](#)
- cognitoidentityprovider, [13](#)
- cognitosync, [17](#)
- confirm_device, [15](#)
- confirm_forgot_password, [15](#)
- confirm_sign_up, [15](#)
- connect_custom_key_store, [34](#)
- connect_directory, [20](#)
- copy_backup_to_region, [11](#)
- create_access_key, [26](#)
- create_account_alias, [27](#)
- create_action_target, [42](#)
- create_alias, [20](#), [34](#)
- create_assessment_target, [31](#)
- create_assessment_template, [31](#)
- create_byte_match_set, [48](#), [51](#)
- create_certificate_authority, [5](#)
- create_certificate_authority_audit_report, [5](#)
- create_cluster, [11](#)
- create_computer, [20](#)
- create_conditional_forwarder, [20](#)
- create_custom_key_store, [34](#)
- create_detector, [24](#)
- create_directory, [7](#), [20](#)
- create_exclusions_preview, [31](#)
- create_facet, [7](#)
- create_filter, [24](#)
- create_geo_match_set, [48](#), [51](#)
- create_grant, [34](#)
- create_group, [15](#), [27](#)
- create_hapg, [9](#)
- create_hsm, [9](#), [11](#)
- create_identity_pool, [13](#)
- create_identity_provider, [15](#)
- create_index, [7](#)
- create_insight, [42](#)
- create_instance_profile, [27](#)
- create_ip_set, [24](#), [48](#), [51](#)
- create_key, [34](#)
- create_log_subscription, [20](#)
- create_login_profile, [27](#)
- create_luna_client, [9](#)
- create_members, [24](#), [41](#), [42](#)
- create_microsoft_ad, [20](#)
- create_object, [7](#)
- create_open_id_connect_provider, [27](#)
- create_permission, [5](#)
- create_policy, [27](#)
- create_policy_version, [27](#)
- create_protection, [44](#)
- create_protection_group, [44](#)
- create_publishing_destination, [24](#)
- create_rate_based_rule, [48](#), [51](#)
- create_regex_match_set, [48](#), [51](#)
- create_regex_pattern_set, [48](#), [51](#)
- create_resource_group, [31](#)
- create_resource_server, [15](#)
- create_resource_share, [37](#)
- create_role, [27](#)
- create_rule, [48](#), [51](#)
- create_rule_group, [48](#), [51](#)
- create_saml_provider, [27](#)
- create_sample_findings, [24](#)
- create_schema, [7](#)
- create_secret, [40](#)
- create_service_linked_role, [27](#)
- create_service_specific_credential, [27](#)
- create_size_constraint_set, [48](#), [51](#)
- create_snapshot, [20](#)
- create_sql_injection_match_set, [48](#), [51](#)
- create_subscription, [44](#)
- create_threat_intel_set, [24](#)
- create_trust, [20](#)
- create_typed_link_facet, [7](#)
- create_user, [27](#)
- create_user_import_job, [15](#)
- create_user_pool, [15](#)
- create_user_pool_client, [15](#)
- create_user_pool_domain, [15](#)
- create_virtual_mfa_device, [27](#)
- create_web_acl, [48](#), [51](#)
- create_web_acl_migration_stack, [48](#), [51](#)
- create_xss_match_set, [48](#), [51](#)
- deactivate_mfa_device, [27](#)
- decline_invitations, [24](#), [42](#)
- decode_authorization_message, [46](#)
- decrypt, [33](#), [34](#)
- delete_access_key, [27](#)
- delete_account_alias, [27](#)
- delete_account_password_policy, [27](#)
- delete_action_target, [42](#)

- delete_alias, [34](#)
- delete_apps_list, [22](#)
- delete_assessment_run, [31](#)
- delete_assessment_target, [31](#)
- delete_assessment_template, [31](#)
- delete_backup, [11](#)
- delete_byte_match_set, [48, 51](#)
- delete_certificate, [3](#)
- delete_certificate_authority, [5](#)
- delete_cluster, [11](#)
- delete_conditional_forwarder, [20](#)
- delete_custom_key_store, [34](#)
- delete_dataset, [18](#)
- delete_detector, [24](#)
- delete_directory, [7, 20](#)
- delete_facet, [7](#)
- delete_filter, [24](#)
- delete_geo_match_set, [48, 51](#)
- delete_group, [15, 27](#)
- delete_group_policy, [27](#)
- delete_hapg, [9](#)
- delete_hsm, [9, 11](#)
- delete_identities, [13](#)
- delete_identity_pool, [13](#)
- delete_identity_provider, [15](#)
- delete_imported_key_material, [34](#)
- delete_insight, [42](#)
- delete_instance_profile, [27](#)
- delete_invitations, [24, 42](#)
- delete_ip_set, [24, 48, 51](#)
- delete_log_subscription, [20](#)
- delete_logging_configuration, [48, 51](#)
- delete_login_profile, [27](#)
- delete_luna_client, [9](#)
- delete_members, [24, 42](#)
- delete_notification_channel, [22](#)
- delete_object, [7](#)
- delete_open_id_connect_provider, [27](#)
- delete_permission, [5](#)
- delete_permission_policy, [48, 51](#)
- delete_policy, [5, 22, 27](#)
- delete_policy_version, [27](#)
- delete_protection, [44](#)
- delete_protection_group, [44](#)
- delete_protocols_list, [22](#)
- delete_publishing_destination, [24](#)
- delete_rate_based_rule, [48, 51](#)
- delete_regex_match_set, [48, 51](#)
- delete_regex_pattern_set, [48, 51](#)
- delete_resource_policy, [40](#)
- delete_resource_server, [15](#)
- delete_resource_share, [37](#)
- delete_role, [27](#)
- delete_role_permissions_boundary, [27](#)
- delete_role_policy, [27](#)
- delete_rule, [48, 51](#)
- delete_rule_group, [48, 51](#)
- delete_saml_provider, [27](#)
- delete_schema, [7](#)
- delete_secret, [40](#)
- delete_server_certificate, [27](#)
- delete_service_linked_role, [27](#)
- delete_service_specific_credential, [27](#)
- delete_signing_certificate, [27](#)
- delete_size_constraint_set, [48, 51](#)
- delete_snapshot, [20](#)
- delete_sql_injection_match_set, [48, 51](#)
- delete_ssh_public_key, [27](#)
- delete_subscription, [44](#)
- delete_threat_intel_set, [24](#)
- delete_trust, [20](#)
- delete_typed_link_facet, [7](#)
- delete_user, [15, 27](#)
- delete_user_attributes, [15](#)
- delete_user_permissions_boundary, [27](#)
- delete_user_policy, [27](#)
- delete_user_pool, [15](#)
- delete_user_pool_client, [15](#)
- delete_user_pool_domain, [15](#)
- delete_virtual_mfa_device, [27](#)
- delete_web_acl, [48, 51](#)
- delete_xss_match_set, [48, 51](#)
- deregister_certificate, [20](#)
- deregister_event_topic, [20](#)
- describe_action_targets, [42](#)
- describe_assessment_runs, [31](#)
- describe_assessment_targets, [31](#)
- describe_assessment_templates, [31](#)
- describe_attack, [44](#)
- describe_attack_statistics, [44](#)
- describe_backups, [11](#)
- describe_certificate, [3, 20](#)
- describe_certificate_authority, [5](#)
- describe_certificate_authority_audit_report, [5](#)
- describe_clusters, [11](#)

- describe_conditional_forwarders, [20](#)
- describe_cross_account_access_role, [31](#)
- describe_custom_key_stores, [34](#)
- describe_dataset, [18](#)
- describe_directories, [20](#)
- describe_domain_controllers, [20](#)
- describe_drt_access, [44](#)
- describe_emergency_contact_settings, [44](#)
- describe_event_topics, [20](#)
- describe_exclusions, [31](#)
- describe_findings, [31](#)
- describe_hapg, [10](#)
- describe_hsm, [10](#)
- describe_hub, [42](#)
- describe_identity, [13](#)
- describe_identity_pool, [13](#)
- describe_identity_pool_usage, [18](#)
- describe_identity_provider, [15](#)
- describe_identity_usage, [18](#)
- describe_key, [34](#)
- describe_ldaps_settings, [20](#)
- describe_luna_client, [10](#)
- describe_organization_configuration, [24](#), [42](#)
- describe_products, [42](#)
- describe_protection, [44](#)
- describe_protection_group, [44](#)
- describe_publishing_destination, [24](#)
- describe_regions, [20](#)
- describe_resource_groups, [31](#)
- describe_resource_server, [15](#)
- describe_risk_configuration, [15](#)
- describe_rules_packages, [31](#)
- describe_secret, [40](#)
- describe_shared_directories, [20](#)
- describe_snapshots, [20](#)
- describe_standards, [42](#)
- describe_standards_controls, [42](#)
- describe_subscription, [44](#)
- describe_trusts, [20](#)
- describe_user_import_job, [15](#)
- describe_user_pool, [15](#)
- describe_user_pool_client, [15](#)
- describe_user_pool_domain, [15](#)
- detach_from_index, [7](#)
- detach_group_policy, [27](#)
- detach_object, [7](#)
- detach_policy, [7](#)
- detach_role_policy, [27](#)
- detach_typed_link, [7](#)
- detach_user_policy, [27](#)
- directoryservice, [18](#)
- disable_client_authentication, [20](#)
- disable_directory, [7](#)
- disable_import_findings_for_product, [42](#)
- disable_key, [34](#)
- disable_key_rotation, [34](#)
- disable_ldaps, [20](#)
- disable_organization_admin_account, [24](#), [42](#)
- disable_proactive_engagement, [44](#)
- disable_radius, [20](#)
- disable_security_hub, [42](#)
- disable_sso, [20](#)
- disassociate_admin_account, [22](#)
- disassociate_drt_log_bucket, [44](#)
- disassociate_drt_role, [44](#)
- disassociate_from_master_account, [24](#), [42](#)
- disassociate_health_check, [45](#)
- disassociate_member_account, [36](#)
- disassociate_members, [24](#), [42](#)
- disassociate_resource_share, [37](#)
- disassociate_resource_share_permission, [37](#)
- disassociate_s3_resources, [36](#)
- disassociate_web_acl, [51](#)
- disconnect_custom_key_store, [34](#)
- enable_client_authentication, [20](#)
- enable_directory, [7](#)
- enable_import_findings_for_product, [42](#)
- enable_key, [34](#)
- enable_key_rotation, [34](#)
- enable_ldaps, [20](#)
- enable_mfa_device, [27](#)
- enable_organization_admin_account, [24](#), [42](#)
- enable_proactive_engagement, [45](#)
- enable_radius, [20](#)
- enable_security_hub, [42](#)
- enable_sharing_with_aws_organization, [37](#)
- enable_sso, [20](#)
- encrypt, [33](#), [34](#)

- export_certificate, 3
- fms, 21
- forget_device, 15
- forgot_password, 15

- generate_credential_report, 27
- generate_data_key, 33, 34
- generate_data_key_pair, 34
- generate_data_key_pair_without_plaintext, 34
- generate_data_key_without_plaintext, 33, 34
- generate_organizations_access_report, 27
- generate_random, 34
- generate_service_last_accessed_details, 27

- get_access_key_info, 46
- get_access_key_last_used, 27
- get_account_authorization_details, 27
- get_account_password_policy, 27
- get_account_summary, 27
- get_admin_account, 22
- get_applied_schema_version, 7
- get_apps_list, 22
- get_assessment_report, 31
- get_bulk_publish_details, 18
- get_byte_match_set, 48, 51
- get_caller_identity, 46
- get_certificate, 3, 5
- get_certificate_authority_certificate, 5
- get_certificate_authority_csr, 5
- get_change_token, 48, 52
- get_change_token_status, 48, 52
- get_cognito_events, 18
- get_compliance_detail, 22
- get_config, 10
- get_context_keys_for_custom_policy, 28
- get_context_keys_for_principal_policy, 28
- get_credential_report, 28
- get_credentials_for_identity, 13
- get_csv_header, 15
- get_detector, 24
- get_device, 16
- get_directory, 7
- get_directory_limits, 20

- get_enabled_standards, 42
- get_exclusions_preview, 31
- get_facet, 7
- get_federation_token, 46
- get_filter, 24
- get_findings, 24, 41, 42
- get_findings_statistics, 24
- get_geo_match_set, 49, 52
- get_group, 16, 28
- get_group_policy, 28
- get_id, 13
- get_identity_pool_configuration, 18
- get_identity_pool_roles, 13
- get_identity_provider_by_identifier, 16

- get_insight_results, 42
- get_insights, 43
- get_instance_profile, 28
- get_invitations_count, 24, 43
- get_ip_set, 24, 49, 52
- get_key_policy, 34
- get_key_rotation_status, 34
- get_link_attributes, 7
- get_logging_configuration, 49, 52
- get_login_profile, 28
- get_master_account, 24, 43
- get_member_detectors, 25
- get_members, 25, 43
- get_notification_channel, 22
- get_object_attributes, 7
- get_object_information, 7
- get_open_id_connect_provider, 28
- get_open_id_token, 13
- get_open_id_token_for_developer_identity, 13

- get_organizations_access_report, 28
- get_parameters_for_import, 34
- get_permission, 37
- get_permission_policy, 49, 52
- get_policy, 5, 22, 28
- get_policy_version, 28
- get_protection_status, 22
- get_protocols_list, 22
- get_public_key, 34
- get_random_password, 40
- get_rate_based_rule, 49, 52
- get_rate_based_rule_managed_keys, 49, 52

- get_regex_match_set, [49](#), [52](#)
- get_regex_pattern_set, [49](#), [52](#)
- get_resource_policies, [37](#)
- get_resource_policy, [40](#)
- get_resource_share_associations, [37](#)
- get_resource_share_invitations, [37](#)
- get_resource_shares, [38](#)
- get_role, [28](#)
- get_role_policy, [28](#)
- get_rule, [49](#), [52](#)
- get_rule_group, [49](#), [52](#)
- get_saml_provider, [28](#)
- get_sampled_requests, [49](#), [52](#)
- get_schema_as_json, [7](#)
- get_secret_value, [40](#)
- get_server_certificate, [28](#)
- get_service_last_accessed_details, [28](#)
- get_service_last_accessed_details_with_entities, [28](#)
- get_service_linked_role_deletion_status, [28](#)
- get_session_token, [46](#)
- get_signing_certificate, [16](#)
- get_size_constraint_set, [49](#), [52](#)
- get_snapshot_limits, [20](#)
- get_sql_injection_match_set, [49](#), [52](#)
- get_ssh_public_key, [28](#)
- get_subscription_state, [45](#)
- get_telemetry_metadata, [31](#)
- get_threat_intel_set, [25](#)
- get_typed_link_facet_information, [7](#)
- get_ui_customization, [16](#)
- get_usage_statistics, [25](#)
- get_user, [16](#), [28](#)
- get_user_attribute_verification_code, [16](#)
- get_user_policy, [28](#)
- get_user_pool_mfa_config, [16](#)
- get_violation_details, [22](#)
- get_web_acl, [49](#), [52](#)
- get_web_acl_for_resource, [52](#)
- get_xss_match_set, [49](#), [52](#)
- global_sign_out, [16](#)
- guardduty, [23](#)
- iam, [25](#)
- import_certificate, [4](#)
- import_certificate_authority_certificate, [5](#)
- import_key_material, [34](#)
- initialize_cluster, [11](#)
- initiate_auth, [16](#)
- inspector, [30](#)
- invite_members, [25](#), [43](#)
- issue_certificate, [5](#)
- kms, [32](#)
- list_access_keys, [28](#)
- list_account_aliases, [28](#)
- list_activated_rules_in_rule_group, [49](#), [52](#)
- list_aliases, [34](#)
- list_applied_schema_arns, [7](#)
- list_apps_lists, [22](#)
- list_assessment_run_agents, [31](#)
- list_assessment_runs, [31](#)
- list_assessment_targets, [31](#)
- list_assessment_templates, [31](#)
- list_attached_group_policies, [28](#)
- list_attached_indices, [7](#)
- list_attached_role_policies, [28](#)
- list_attached_user_policies, [28](#)
- list_attacks, [45](#)
- list_available_zones, [10](#)
- list_byte_match_sets, [49](#), [52](#)
- list_certificate_authorities, [5](#)
- list_certificates, [4](#), [20](#)
- list_compliance_status, [22](#)
- list_datasets, [18](#)
- list_detectors, [25](#)
- list_development_schema_arns, [7](#)
- list_devices, [16](#)
- list_directories, [7](#)
- list_enabled_products_for_import, [43](#)
- list_entities_for_policy, [28](#)
- list_event_subscriptions, [31](#)
- list_exclusions, [31](#)
- list_facet_attributes, [7](#)
- list_facet_names, [8](#)
- list_filters, [25](#)
- list_findings, [25](#), [31](#)
- list_geo_match_sets, [49](#), [52](#)
- list_grants, [34](#)
- list_group_policies, [28](#)
- list_groups, [16](#), [28](#)
- list_groups_for_user, [28](#)
- list_haps, [10](#)

- list_hsms, [10](#)
- list_identities, [13](#)
- list_identity_pool_usage, [18](#)
- list_identity_pools, [13](#)
- list_identity_providers, [16](#)
- list_incoming_typed_links, [8](#)
- list_index, [8](#)
- list_instance_profiles, [28](#)
- list_instance_profiles_for_role, [28](#)
- list_invitations, [25](#), [43](#)
- list_ip_routes, [20](#)
- list_ip_sets, [25](#), [49](#), [52](#)
- list_key_policies, [34](#)
- list_keys, [34](#)
- list_log_subscriptions, [20](#)
- list_logging_configurations, [49](#), [52](#)
- list_luna_clients, [10](#)
- list_managed_schema_arns, [8](#)
- list_member_accounts, [22](#), [36](#)
- list_members, [25](#), [43](#)
- list_mfa_devices, [28](#)
- list_object_attributes, [8](#)
- list_object_children, [8](#)
- list_object_parent_paths, [8](#)
- list_object_parents, [8](#)
- list_object_policies, [8](#)
- list_open_id_connect_providers, [28](#)
- list_organization_admin_accounts, [25](#),
[43](#)
- list_outgoing_typed_links, [8](#)
- list_pending_invitation_resources, [38](#)
- list_permissions, [5](#), [38](#)
- list_policies, [22](#), [28](#)
- list_policies_granting_service_access,
[28](#)
- list_policy_attachments, [8](#)
- list_policy_versions, [28](#)
- list_principals, [38](#)
- list_protection_groups, [45](#)
- list_protections, [45](#)
- list_protocols_lists, [22](#)
- list_published_schema_arns, [8](#)
- list_publishing_destinations, [25](#)
- list_rate_based_rules, [49](#), [52](#)
- list_records, [18](#)
- list_regex_match_sets, [49](#), [52](#)
- list_regex_pattern_sets, [49](#), [52](#)
- list_resource_servers, [16](#)
- list_resource_share_permissions, [38](#)
- list_resource_tags, [34](#)
- list_resource_types, [38](#)
- list_resources, [38](#)
- list_resources_for_web_acl, [52](#)
- list_resources_in_protection_group, [45](#)
- list_retirable_grants, [34](#)
- list_role_policies, [28](#)
- list_role_tags, [28](#)
- list_roles, [28](#)
- list_rule_groups, [49](#), [52](#)
- list_rules, [49](#), [52](#)
- list_rules_packages, [31](#)
- list_s3_resources, [36](#)
- list_saml_providers, [28](#)
- list_schema_extensions, [20](#)
- list_secret_version_ids, [40](#)
- list_secrets, [40](#)
- list_server_certificates, [28](#)
- list_service_specific_credentials, [28](#)
- list_signing_certificates, [28](#)
- list_size_constraint_sets, [49](#), [52](#)
- list_sql_injection_match_sets, [49](#), [52](#)
- list_ssh_public_keys, [28](#)
- list_subscribed_rule_groups, [49](#), [52](#)
- list_tags, [5](#), [11](#)
- list_tags_for_certificate, [4](#)
- list_tags_for_resource, [8](#), [10](#), [13](#), [16](#), [20](#),
[22](#), [25](#), [31](#), [43](#), [49](#), [52](#)
- list_threat_intel_sets, [25](#)
- list_typed_link_facet_attributes, [8](#)
- list_typed_link_facet_names, [8](#)
- list_user_import_jobs, [16](#)
- list_user_policies, [28](#)
- list_user_pool_clients, [16](#)
- list_user_pools, [16](#)
- list_user_tags, [28](#)
- list_users, [16](#), [28](#)
- list_users_in_group, [16](#)
- list_virtual_mfa_devices, [29](#)
- list_web_ac_ls, [49](#), [52](#)
- list_xss_match_sets, [49](#), [52](#)
- lookup_developer_identity, [13](#)
- lookup_policy, [8](#)
- macie, [35](#)
- merge_developer_identities, [13](#)
- modify_backup_attributes, [11](#)
- modify_cluster, [11](#)

- modify_hapg, [10](#)
- modify_hsm, [10](#)
- modify_luna_client, [10](#)
- preview_agents, [31](#)
- promote_resource_share_created_from_policy, [38](#)
- publish_schema, [8](#)
- put_apps_list, [22](#)
- put_group_policy, [29](#)
- put_key_policy, [34](#)
- put_logging_configuration, [49, 52](#)
- put_notification_channel, [22](#)
- put_permission_policy, [49, 52](#)
- put_policy, [5, 22](#)
- put_protocols_list, [22](#)
- put_resource_policy, [40](#)
- put_role_permissions_boundary, [29](#)
- put_role_policy, [29](#)
- put_schema_from_json, [8](#)
- put_secret_value, [40](#)
- put_user_permissions_boundary, [29](#)
- put_user_policy, [29](#)
- ram, [36](#)
- re_encrypt, [34](#)
- register_certificate, [20](#)
- register_cross_account_access_role, [31](#)
- register_device, [18](#)
- register_event_topic, [20](#)
- reject_resource_share_invitation, [38](#)
- reject_shared_directory, [20](#)
- remove_attributes_from_findings, [31](#)
- remove_client_id_from_open_id_connect_provider, [29](#)
- remove_facet_from_object, [8](#)
- remove_ip_routes, [20](#)
- remove_region, [20](#)
- remove_role_from_instance_profile, [29](#)
- remove_tags_from_certificate, [4](#)
- remove_tags_from_resource, [10, 21](#)
- remove_user_from_group, [29](#)
- renew_certificate, [4](#)
- request_certificate, [4](#)
- resend_confirmation_code, [16](#)
- resend_validation_email, [4](#)
- reset_service_specific_credential, [29](#)
- reset_user_password, [21](#)
- respond_to_auth_challenge, [16](#)
- restore_backup, [11](#)
- restore_certificate_authority, [5](#)
- restore_from_snapshot, [21](#)
- restore_secret, [40](#)
- resync_mfa_device, [29](#)
- retire_grant, [34](#)
- revoke_certificate, [5](#)
- revoke_grant, [34](#)
- rotate_secret, [40](#)
- schedule_key_deletion, [34](#)
- secretsmanager, [38](#)
- securityhub, [41](#)
- set_cognito_events, [18](#)
- set_default_policy_version, [29](#)
- set_identity_pool_configuration, [18](#)
- set_identity_pool_roles, [13](#)
- set_risk_configuration, [16](#)
- set_security_token_service_preferences, [29](#)
- set_tags_for_resource, [31](#)
- set_ui_customization, [16](#)
- set_user_mfa_preference, [16](#)
- set_user_pool_mfa_config, [16](#)
- set_user_settings, [16](#)
- share_directory, [21](#)
- shield, [43](#)
- sign, [34](#)
- sign_up, [16](#)
- simulate_custom_policy, [29](#)
- simulate_principal_policy, [29](#)
- start_assessment_run, [31](#)
- start_monitoring_members, [25](#)
- start_schema_extension, [21](#)
- start_user_import_job, [16](#)
- stop_assessment_run, [31](#)
- stop_monitoring_members, [25](#)
- stop_user_import_job, [16](#)
- sts, [45](#)
- subscribe_to_dataset, [18](#)
- subscribe_to_event, [31](#)
- tag_certificate_authority, [5](#)
- tag_resource, [8, 11, 13, 16, 23, 25, 34, 38, 40, 43, 49, 52](#)
- tag_role, [29](#)
- tag_user, [29](#)
- unarchive_findings, [25](#)

- unlink_developer_identity, [13](#)
- unlink_identity, [13](#)
- unshare_directory, [21](#)
- unsubscribe_from_dataset, [18](#)
- unsubscribe_from_event, [31](#)
- untag_certificate_authority, [5](#)
- untag_resource, [8](#), [11](#), [13](#), [16](#), [23](#), [25](#), [35](#), [38](#),
[40](#), [43](#), [49](#), [52](#)
- untag_role, [29](#)
- untag_user, [29](#)
- update_access_key, [29](#)
- update_account_password_policy, [29](#)
- update_action_target, [43](#)
- update_alias, [35](#)
- update_assessment_target, [31](#)
- update_assume_role_policy, [29](#)
- update_auth_event_feedback, [16](#)
- update_byte_match_set, [49](#), [52](#)
- update_certificate_authority, [5](#)
- update_certificate_options, [4](#)
- update_conditional_forwarder, [21](#)
- update_custom_key_store, [35](#)
- update_detector, [25](#)
- update_device_status, [16](#)
- update_emergency_contact_settings, [45](#)
- update_facet, [8](#)
- update_filter, [25](#)
- update_findings, [41](#), [43](#)
- update_findings_feedback, [25](#)
- update_geo_match_set, [49](#), [52](#)
- update_group, [16](#), [29](#)
- update_identity_pool, [13](#)
- update_identity_provider, [16](#)
- update_insight, [43](#)
- update_ip_set, [25](#), [49](#), [52](#)
- update_key_description, [35](#)
- update_link_attributes, [8](#)
- update_login_profile, [29](#)
- update_member_detectors, [25](#)
- update_number_of_domain_controllers,
[21](#)
- update_object_attributes, [8](#)
- update_open_id_connect_provider_thumbprint,
[29](#)
- update_organization_configuration, [25](#),
[43](#)
- update_protection_group, [45](#)
- update_publishing_destination, [25](#)
- update_radius, [21](#)
- update_rate_based_rule, [49](#), [52](#)
- update_records, [18](#)
- update_regex_match_set, [49](#), [52](#)
- update_regex_pattern_set, [49](#), [52](#)
- update_resource_server, [16](#)
- update_resource_share, [38](#)
- update_role, [29](#)
- update_role_description, [29](#)
- update_rule, [49](#), [52](#)
- update_rule_group, [49](#), [52](#)
- update_s3_resources, [36](#)
- update_saml_provider, [29](#)
- update_schema, [8](#)
- update_secret, [40](#)
- update_secret_version_stage, [40](#)
- update_security_hub_configuration, [43](#)
- update_server_certificate, [29](#)
- update_service_specific_credential, [29](#)
- update_signing_certificate, [29](#)
- update_size_constraint_set, [49](#), [52](#)
- update_sql_injection_match_set, [49](#), [53](#)
- update_ssh_public_key, [29](#)
- update_standards_control, [41](#), [43](#)
- update_subscription, [45](#)
- update_threat_intel_set, [25](#)
- update_trust, [21](#)
- update_typed_link_facet, [8](#)
- update_user, [29](#)
- update_user_attributes, [16](#)
- update_user_pool, [16](#)
- update_user_pool_client, [16](#)
- update_user_pool_domain, [16](#)
- update_web_acl, [49](#), [53](#)
- update_xss_match_set, [49](#), [53](#)
- upgrade_applied_schema, [8](#)
- upgrade_published_schema, [8](#)
- upload_server_certificate, [29](#)
- upload_signing_certificate, [29](#)
- upload_ssh_public_key, [29](#)
- validate_resource_policy, [40](#)
- verify, [35](#)
- verify_software_token, [16](#)
- verify_trust, [21](#)
- verify_user_attribute, [16](#)
- waf, [47](#)
- wafregional, [50](#)