AWS Identity and Access Management

API Reference

API Version 2010-05-08

AWS Identity and Access Management: API Reference

Table of Contents

Welcome to the IAM API Reference

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.

Programmatic Access to IAM

We recommend that you use the AWS SDKs to make programmatic API calls to IAM. The AWS SDKs consist of libraries and sample code for various programming languages and platforms (for example, Java, Ruby, .NET, iOS, and Android). The SDKs provide a convenient way to create programmatic access to IAM and AWS. For example, the SDKs take care of tasks such as cryptographically signing requests, managing errors, and retrying requests automatically. For more information, see Tools to Build on AWS.

Alternatively, you can also use the IAM Query API to make direct calls to the IAM service. For more information about calling the IAM Query API, see Making Query Requests in the *AWS Identity and Access Management User Guide*. IAM supports GET and POST requests for all actions. That is, the API does not 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.

Signing Requests

Requests must be signed using an access key ID and a secret access key. We strongly recommend that you do not use your AWS account access key ID and secret access key for everyday work with IAM. You can use the access key ID and secret access key for an IAM user or you can use the AWS Security Token Service to generate temporary security credentials and use those to sign requests.

To sign requests, we recommend that you use Signature Version 4. If you have an existing application that uses Signature Version 2, you do not have to update it to use Signature Version 4. However, some operations now require Signature Version 4. The documentation for operations that require version 4 indicate this requirement.

Additional Resources

- AWS Security Credentials. This topic provides general information about the types of credentials used for accessing AWS.
- IAM Best Practices. This topic presents a list of suggestions for using the IAM service to help secure your AWS resources.
- Signing AWS API Requests. This set of topics walk you through the process of signing a request using an access key ID and secret access key.

Actions

The following actions are supported:

AddClientIDToOpenIDConnectProvider

Adds a new client ID (also known as audience) to the list of client IDs already registered for the specified IAM OpenID Connect (OIDC) provider resource.

This operation is idempotent; it does not fail or return an error if you add an existing client ID to the provider.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ClientID

The client ID (also known as audience) to add to the IAM OpenID Connect provider resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the IAM OpenID Connect (OIDC) provider resource to add the client ID to. You can get a list of OIDC provider ARNs by using the ListOpenIDConnectProviders (p. 260) operation.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of AddClientIDToOpenIDConnectProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=AddClientIDToOpenIDConnectProvider
&ClientID=my-application-ID
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AddClientIDToOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>e4bdcdae-4f66-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</AddClientIDToOpenIDConnectProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AddRoleToInstanceProfile

Adds the specified IAM role to the specified instance profile. An instance profile can contain only one role, and this limit cannot be increased. You can remove the existing role and then add a different role to an instance profile. You must then wait for the change to appear across all of AWS because of eventual consistency. To force the change, you must disassociate the instance profile and then associate the instance profile, or you can stop your instance and then restart it.

> **Note**
> The caller of this API must be granted the `PassRole` permission on the IAM role by a permissions policy.

For more information about roles, go to Working with Roles. For more information about instance profiles, go to About Instance Profiles.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

InstanceProfileName

The name of the instance profile to update.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

RoleName

The name of the role to add.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of AddRoleToInstanceProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=AddRoleToInstanceProfile
&InstanceProfileName=Webserver
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AddRoleToInstanceProfileResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>12657608-99f2-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</AddRoleToInstanceProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AddUserToGroup

Adds the specified user to the specified group.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name of the group to update.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

UserName

The name of the user to add.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of AddUserToGroup.

Sample Request

```
https://iam.amazonaws.com/?Action=AddUserToGroup
&GroupName=Managers
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AddUserToGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</AddUserToGroupResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AttachGroupPolicy

Attaches the specified managed policy to the specified IAM group.

You use this API to attach a managed policy to a group. To embed an inline policy in a group, use PutGroupPolicy (p. 308).

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name (friendly name, not ARN) of the group to attach the policy to.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to attach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PolicyNotAttachable

The request failed because AWS service role policies can only be attached to the service-linked role for that service.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of AttachGroupPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=AttachGroupPolicy
&GroupName=Finance
&PolicyArn=arn:aws:iam::aws:policy/ReadOnlyAccess
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AttachGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>f8a7b7b9-3d01-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</AttachGroupPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

AttachRolePolicy

Attaches the specified managed policy to the specified IAM role. When you attach a managed policy to a role, the managed policy becomes part of the role's permission (access) policy.

> **Note**
> You cannot use a managed policy as the role's trust policy. The role's trust policy is created at the same time as the role, using CreateRole (p. 50). You can update a role's trust policy using UpdateAssumeRolePolicy (p. 376).

Use this API to attach a *managed* policy to a role. To embed an inline policy in a role, use PutRolePolicy (p. 313). For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to attach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

RoleName

The name (friendly name, not ARN) of the role to attach the policy to.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PolicyNotAttachable

The request failed because AWS service role policies can only be attached to the service-linked role for that service.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of AttachRolePolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=AttachRolePolicy
&PolicyArn=arn:aws:iam::aws:policy/ReadOnlyAccess
&RoleName=ReadOnlyRole
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AttachRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>37a87673-3d07-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</AttachRolePolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AttachUserPolicy

Attaches the specified managed policy to the specified user.

You use this API to attach a *managed* policy to a user. To embed an inline policy in a user, use PutUserPolicy (p. 318).

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to attach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

UserName

The name (friendly name, not ARN) of the IAM user to attach the policy to.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PolicyNotAttachable

The request failed because AWS service role policies can only be attached to the service-linked role for that service.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of AttachUserPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=AttachUserPolicy
&PolicyArn=arn:aws:iam::aws:policy/AdministratorAccess
&UserName=Alice
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<AttachUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>ed7e72d3-3d07-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</AttachUserPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

ChangePassword

Changes the password of the IAM user who is calling this operation. The AWS account root user password is not affected by this operation.

To change the password for a different user, see UpdateLoginProfile (p. 382). For more information about modifying passwords, see Managing Passwords in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

NewPassword

The new password. The new password must conform to the AWS account's password policy, if one exists.

The regex pattern that is used to validate this parameter is a string of characters. That string can include almost any printable ASCII character from the space (`\u0020`) through the end of the ASCII character range (`\u00FF`). You can also include the tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`) characters. Any of these characters are valid in a password. However, many tools, such as the AWS Management Console, might restrict the ability to type certain characters because they have special meaning within that tool.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

OldPassword

The IAM user's current password.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

InvalidUserType

The request was rejected because the type of user for the transaction was incorrect.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PasswordPolicyViolation

The request was rejected because the provided password did not meet the requirements imposed by the account password policy.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ChangePassword.

Sample Request

```
https://iam.amazonaws.com/?Action=ChangePassword
&OldPassword=U79}kgds4?
&NewPassword=Lb0*1(9xpN
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ChangePasswordResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ChangePasswordResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateAccessKey

Creates a new AWS secret access key and corresponding AWS access key ID for the specified user. The default status for new keys is `Active`.

If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID signing the request. This operation works for access keys under the AWS account. Consequently, you can use this operation to manage AWS account root user credentials. This is true even if the AWS account has no associated users.

For information about limits on the number of keys you can create, see Limitations on IAM Entities in the *IAM User Guide*.

> **Important**
> To ensure the security of your AWS account, the secret access key is accessible only during key and user creation. You must save the key (for example, in a text file) if you want to be able to access it again. If a secret key is lost, you can delete the access keys for the associated user and then create new keys.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

UserName

The name of the IAM user that the new key will belong to.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following element is returned by the service.

AccessKey

A structure with details about the access key.

Type: AccessKey (p. 423) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateAccessKey.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateAccessKey
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateAccessKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateAccessKeyResult>
    <AccessKey>
      <UserName>Bob</UserName>
      <AccessKeyId>AKIAIOSFODNN7EXAMPLE</AccessKeyId>
      <Status>Active</Status>
      <SecretAccessKey>wJalrXUtnFEMI/K7MDENG/bPxRfiCYzEXAMPLEKEY
      </SecretAccessKey>
    </AccessKey>
  </CreateAccessKeyResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateAccessKeyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateAccountAlias

Creates an alias for your AWS account. For information about using an AWS account alias, see Using an Alias for Your AWS Account ID in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AccountAlias

The account alias to create.

This parameter allows (through its regex pattern) a string of characters consisting of lowercase letters, digits, and dashes. You cannot start or finish with a dash, nor can you have two dashes in a row.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 63.

Pattern: `^[a-z0-9](([a-z0-9]|-(?!-))*[a-z0-9])?$`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateAccountAlias.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateAccountAlias
&AccountAlias=example-corporation
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateAccountAliasResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>36b5db08-f1b0-11df-8fbe-45274EXAMPLE</RequestId>
  </ResponseMetadata>
</CreateAccountAliasResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateGroup

Creates a new group.

For information about the number of groups you can create, see Limitations on IAM Entities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name of the group to create. Do not include the path in this value.

IAM user, group, role, and policy names must be unique within the account. Names are not distinguished by case. For example, you cannot create resources named both "MyResource" and "myresource".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Path

The path to the group. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

Response Elements

The following element is returned by the service.

Group

A structure containing details about the new group.

Type: Group (p. 440) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateGroup.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateGroup
&GroupName=Admins
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateGroupResult>
    <Group>
      <Path>/</Path>
      <GroupName>Admins</GroupName>
      <GroupId>AGPACKCEVSQ6C2EXAMPLE</GroupId>
      <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
    </Group>
  </CreateGroupResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateGroupResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateInstanceProfile

Creates a new instance profile. For information about instance profiles, go to About Instance Profiles.

For information about the number of instance profiles you can create, see Limitations on IAM Entities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

InstanceProfileName

The name of the instance profile to create.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Path

The path to the instance profile. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

Response Elements

The following element is returned by the service.

InstanceProfile

A structure containing details about the new instance profile.

Type: InstanceProfile (p. 444) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateInstanceProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateInstanceProfile
&InstanceProfileName=Webserver
&Path=/application_abc/component_xyz/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateInstanceProfileResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateInstanceProfileResult>
    <InstanceProfile>
      <InstanceProfileId>AIPAD5ARO2C5EXAMPLE3G</InstanceProfileId>
      <Roles/>
      <InstanceProfileName>Webserver</InstanceProfileName>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/component_xyz/
Webserver</Arn>
      <CreateDate>2012-05-09T16:11:10.222Z</CreateDate>
    </InstanceProfile>
  </CreateInstanceProfileResult>
  <ResponseMetadata>
    <RequestId>974142ee-99f1-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</CreateInstanceProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateLoginProfile

Creates a password for the specified user, giving the user the ability to access AWS services through the AWS Management Console. For more information about managing passwords, see Managing Passwords in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Password

The new password for the user.

The regex pattern that is used to validate this parameter is a string of characters. That string can include almost any printable ASCII character from the space (`\u0020`) through the end of the ASCII character range (`\u00FF`). You can also include the tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`) characters. Any of these characters are valid in a password. However, many tools, such as the AWS Management Console, might restrict the ability to type certain characters because they have special meaning within that tool.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PasswordResetRequired

Specifies whether the user is required to set a new password on next sign-in.

Type: Boolean

Required: No

UserName

The name of the IAM user to create a password for. The user must already exist.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

LoginProfile

A structure containing the user name and password create date.

Type: LoginProfile (p. 447) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PasswordPolicyViolation

The request was rejected because the provided password did not meet the requirements imposed by the account password policy.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateLoginProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateLoginProfile
&UserName=Bob
&Password=h]6EszR}vJ*m
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateLoginProfileResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
```

```
  <CreateLoginProfileResult>
    <LoginProfile>
      <PasswordResetRequired>false</PasswordResetRequired>
      <UserName>Bob</UserName>
      <CreateDate>2015-03-25T20:48:52.558Z</CreateDate>
    </LoginProfile>
  </CreateLoginProfileResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateLoginProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateOpenIDConnectProvider

Creates an IAM entity to describe an identity provider (IdP) that supports OpenID Connect (OIDC).

The OIDC provider that you create with this operation can be used as a principal in a role's trust policy. Such a policy establishes a trust relationship between AWS and the OIDC provider.

When you create the IAM OIDC provider, you specify the following:

- The URL of the OIDC identity provider (IdP) to trust
- A list of client IDs (also known as audiences) that identify the application or applications that are allowed to authenticate using the OIDC provider
- A list of thumbprints of one or more server certificates that the IdP uses

You get all of this information from the OIDC IdP that you want to use to access AWS.

> **Note**
> The trust for the OIDC provider is derived from the IAM provider that this operation creates. Therefore, it is best to limit access to the CreateOpenIDConnectProvider (p. 39) operation to highly privileged users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ClientIDList.member.N

A list of client IDs (also known as audiences). When a mobile or web app registers with an OpenID Connect provider, they establish a value that identifies the application. (This is the value that's sent as the `client_id` parameter on OAuth requests.)

You can register multiple client IDs with the same provider. For example, you might have multiple applications that use the same OIDC provider. You cannot register more than 100 client IDs with a single IAM OIDC provider.

There is no defined format for a client ID. The `CreateOpenIDConnectProviderRequest` operation accepts client IDs up to 255 characters long.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: No

ThumbprintList.member.N

A list of server certificate thumbprints for the OpenID Connect (OIDC) identity provider's server certificates. Typically this list includes only one entry. However, IAM lets you have up to five thumbprints for an OIDC provider. This lets you maintain multiple thumbprints if the identity provider is rotating certificates.

The server certificate thumbprint is the hex-encoded SHA-1 hash value of the X.509 certificate used by the domain where the OpenID Connect provider makes its keys available. It is always a 40-character string.

You must provide at least one thumbprint when creating an IAM OIDC provider. For example, assume that the OIDC provider is `server.example.com` and the provider stores its keys at https://

keys.server.example.com/openid-connect. In that case, the thumbprint string would be the hex-encoded SHA-1 hash value of the certificate used by https://keys.server.example.com.

For more information about obtaining the OIDC provider's thumbprint, see Obtaining the Thumbprint for an OpenID Connect Provider in the *IAM User Guide*.

Type: Array of strings

Length Constraints: Fixed length of 40.

Required: Yes

Url

The URL of the identity provider. The URL must begin with `https://` and should correspond to the `iss` claim in the provider's OpenID Connect ID tokens. Per the OIDC standard, path components are allowed but query parameters are not. Typically the URL consists of only a hostname, like `https://server.example.org` or `https://example.com`.

You cannot register the same provider multiple times in a single AWS account. If you try to submit a URL that has already been used for an OpenID Connect provider in the AWS account, you will get an error.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

Response Elements

The following element is returned by the service.

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the new IAM OpenID Connect provider that is created. For more information, see OpenIDConnectProviderListEntry (p. 452).

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateOpenIDConnectProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateOpenIDConnectProvider
&ThumbprintList.list.1=c3768084dfb3d2b68b7897bf5f565da8eEXAMPLE
&ClientIDList.list.1=my-application-ID
&Url=https://server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateOpenIDConnectProviderResult>
    <OpenIDConnectProviderArn>
      arn:aws:iam::123456789012:oidc-provider/server.example.com
    </OpenIDConnectProviderArn>
  </CreateOpenIDConnectProviderResult>
  <ResponseMetadata>
    <RequestId>f248366a-4f64-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateOpenIDConnectProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreatePolicy

Creates a new managed policy for your AWS account.

This operation creates a policy version with a version identifier of `v1` and sets v1 as the policy's default version. For more information about policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

For more information about managed policies in general, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Description

A friendly description of the policy.

Typically used to store information about the permissions defined in the policy. For example, "Grants access to production DynamoDB tables."

The policy description is immutable. After a value is assigned, it cannot be changed.

Type: String

Length Constraints: Maximum length of 1000.

Required: No

Path

The path for the policy.

For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

PolicyDocument

The JSON policy document that you want to use as the content for the new policy.

You must provide policies in JSON format in IAM. However, for AWS CloudFormation templates formatted in YAML, you can provide the policy in JSON or YAML format. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (\u0020) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through \u00FF)
- The special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: [\u0009\u000A\u000D\u0020-\u00FF]+

Required: Yes

PolicyName

The friendly name of the policy.

IAM user, group, role, and policy names must be unique within the account. Names are not distinguished by case. For example, you cannot create resources named both "MyResource" and "myresource".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: [\w+=,.@-]+

Required: Yes

Response Elements

The following element is returned by the service.

Policy

A structure containing details about the new policy.

Type: Policy (p. 457) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreatePolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=CreatePolicy
&PolicyDocument={"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Action":"s3:ListAllMyBuckets",
"Resource":"arn:aws:s3:::*"},{"Effect":"Allow","Action":["s3:Get*","s3:List*"],"Resource":
["arn:aws:s3:::EXAMPLE-BUCKET","arn:aws:s3:::EXAMPLE-BUCKET/*"]}]}
&PolicyName=S3-read-only-example-bucket
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreatePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreatePolicyResult>
    <Policy>
      <PolicyName>S3-read-only-example-bucket</PolicyName>
      <DefaultVersionId>v1</DefaultVersionId>
      <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
      <Path>/</Path>
      <Arn>arn:aws:iam::123456789012:policy/S3-read-only-example-bucket</Arn>
      <AttachmentCount>0</AttachmentCount>
      <CreateDate>2014-09-15T17:36:14.673Z</CreateDate>
      <UpdateDate>2014-09-15T17:36:14.673Z</UpdateDate>
    </Policy>
  </CreatePolicyResult>
  <ResponseMetadata>
    <RequestId>ca64c9e1-3cfe-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</CreatePolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreatePolicyVersion

Creates a new version of the specified managed policy. To update a managed policy, you create a new policy version. A managed policy can have up to five versions. If the policy has five versions, you must delete an existing version using DeletePolicyVersion (p. 91) before you create a new version.

Optionally, you can set the new version as the policy's default version. The default version is the version that is in effect for the IAM users, groups, and roles to which the policy is attached.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy to which you want to add a new version.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

PolicyDocument

The JSON policy document that you want to use as the content for this new version of the policy.

You must provide policies in JSON format in IAM. However, for AWS CloudFormation templates formatted in YAML, you can provide the policy in JSON or YAML format. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

SetAsDefault

Specifies whether to set this version as the policy's default version.

When this parameter is `true`, the new policy version becomes the operative version. That is, it becomes the version that is in effect for the IAM users, groups, and roles that the policy is attached to.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: Boolean

Required: No

Response Elements

The following element is returned by the service.

PolicyVersion

A structure containing details about the new policy version.

Type: PolicyVersion (p. 466) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreatePolicyVersion.

Sample Request

```
https://iam.amazonaws.com/?Action=CreatePolicyVersion
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&PolicyDocument={"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Action":"s3:ListAllMyBuckets",
"Resource":"arn:aws:s3:::*"},{"Effect":"Allow","Action":["s3:Get*","s3:List*"],"Resource":
["arn:aws:s3:::EXAMPLE-BUCKET","arn:aws:s3:::EXAMPLE-BUCKET/*"]},
{"Effect":"Deny","Action":"s3:*",
"Resource":["arn:aws:s3:::EXAMPLE-BUCKET","arn:aws:s3:::EXAMPLE-BUCKET/*"],"Condition":
{"StringLike":
{"s3:prefix":["SENSITIVE-FILES*"]}}}]}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreatePolicyVersionResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreatePolicyVersionResult>
    <PolicyVersion>
      <IsDefaultVersion>false</IsDefaultVersion>
      <VersionId>v2</VersionId>
      <CreateDate>2014-09-15T19:58:59.430Z</CreateDate>
    </PolicyVersion>
  </CreatePolicyVersionResult>
  <ResponseMetadata>
    <RequestId>bb551b92-3d12-11e4-bfad-8d1c6EXAMPLE</RequestId>
  </ResponseMetadata>
</CreatePolicyVersionResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateRole

Creates a new role for your AWS account. For more information about roles, go to IAM Roles. For information about limitations on role names and the number of roles you can create, go to Limitations on IAM Entities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AssumeRolePolicyDocument

The trust relationship policy document that grants an entity permission to assume the role.

In IAM, you must provide a JSON policy that has been converted to a string. However, for AWS CloudFormation templates formatted in YAML, you can provide the policy in JSON or YAML format. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Upon success, the response includes the same trust policy in JSON format.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

Description

A description of the role.

Type: String

Length Constraints: Maximum length of 1000.

Pattern: `[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}]*`

Required: No

MaxSessionDuration

The maximum session duration (in seconds) that you want to set for the specified role. If you do not specify a value for this setting, the default maximum of one hour is applied. This setting can have a value from 1 hour to 12 hours.

Anyone who assumes the role from the AWS CLI or API can use the `DurationSeconds` API parameter or the `duration-seconds` CLI parameter to request a longer session. The `MaxSessionDuration` setting determines the maximum duration that can be requested using

the `DurationSeconds` parameter. If users don't specify a value for the `DurationSeconds` parameter, their security credentials are valid for one hour by default. This applies when you use the `AssumeRole*` API operations or the `assume-role*` CLI operations but does not apply when you use those operations to create a console URL. For more information, see Using IAM Roles in the *IAM User Guide*.

Type: Integer

Valid Range: Minimum value of 3600. Maximum value of 43200.

Required: No

Path

The path to the role. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

PermissionsBoundary

The ARN of the policy that is used to set the permissions boundary for the role.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

RoleName

The name of the role to create.

IAM user, group, role, and policy names must be unique within the account. Names are not distinguished by case. For example, you cannot create resources named both "MyResource" and "myresource".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Tags.member.N

A list of tags that you want to attach to the newly created role. Each tag consists of a key name and an associated value. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Note
If any one of the tags is invalid or if you exceed the allowed number of tags per role, then the entire request fails and the role is not created.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Required: No

Response Elements

The following element is returned by the service.

Role

A structure containing details about the new role.

Type: Role (p. 471) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateRole.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateRole
&RoleName=S3Access
&Path=/application_abc/component_xyz/
&AssumeRolePolicyDocument={"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"Service":["ec2.amazonaws.com"]},"Action":
["sts:AssumeRole"]}]}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateRoleResult>
    <Role>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/S3Access</Arn>
      <RoleName>S3Access</RoleName>
      <AssumeRolePolicyDocument>
        {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
        "Principal":{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
      </AssumeRolePolicyDocument>
      <CreateDate>2012-05-08T23:34:01.495Z</CreateDate>
      <RoleId>AROADBQP57FF2AEXAMPLE</RoleId>
    </Role>
  </CreateRoleResult>
  <ResponseMetadata>
    <RequestId>4a93ceee-9966-11e1-b624-b1aEXAMPLE7c</RequestId>
  </ResponseMetadata>
</CreateRoleResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateSAMLProvider

Creates an IAM resource that describes an identity provider (IdP) that supports SAML 2.0.

The SAML provider resource that you create with this operation can be used as a principal in an IAM role's trust policy. Such a policy can enable federated users who sign in using the SAML IdP to assume the role. You can create an IAM role that supports Web-based single sign-on (SSO) to the AWS Management Console or one that supports API access to AWS.

When you create the SAML provider resource, you upload a SAML metadata document that you get from your IdP. That document includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that the IdP sends. You must generate the metadata document using the identity management software that is used as your organization's IdP.

Note
This operation requires Signature Version 4.

For more information, see Enabling SAML 2.0 Federated Users to Access the AWS Management Console and About SAML 2.0-based Federation in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Name

The name of the provider to create.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w._-]+`

Required: Yes

SAMLMetadataDocument

An XML document generated by an identity provider (IdP) that supports SAML 2.0. The document includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that are received from the IdP. You must generate the metadata document using the identity management software that is used as your organization's IdP.

For more information, see About SAML 2.0-based Federation in the *IAM User Guide*

Type: String

Length Constraints: Minimum length of 1000. Maximum length of 10000000.

Required: Yes

Response Elements

The following element is returned by the service.

SAMLProviderArn

The Amazon Resource Name (ARN) of the new SAML provider resource in IAM.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateSAMLProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateSAMLProvider
&Name=MyUniversity
&SAMLProviderDocument=VGhpcyBpcyB3aGVyZSB5b3UgcHV0IHRoZSBTQU1MIHByb3ZpZGVyIG1ldGFkYXRhIGRvY3VtZW50
LCBCYXNlNjQtZW5jb2RlZCBpbnRvIGEgYmlnIHN0cmluZy4=
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateSAMLProviderResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateSAMLProviderResult>
    <SAMLProviderArn>arn:aws:iam::123456789012:saml-provider/MyUniversity</SAMLProviderArn>
```

```
  </CreateSAMLProviderResult>
  <ResponseMetadata>
    <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</CreateSAMLProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateServiceLinkedRole

Creates an IAM role that is linked to a specific AWS service. The service controls the attached policies and when the role can be deleted. This helps ensure that the service is not broken by an unexpectedly changed or deleted role, which could put your AWS resources into an unknown state. Allowing the service to control the role helps improve service stability and proper cleanup when a service and its role are no longer needed. For more information, see Using Service-Linked Roles in the *IAM User Guide*.

To attach a policy to this service-linked role, you must make the request using the AWS service that depends on this role.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AWSServiceName

The service principal for the AWS service to which this role is attached. You use a string similar to a URL but without the http:// in front. For example: `elasticbeanstalk.amazonaws.com`.

Service principals are unique and case-sensitive. To find the exact service principal for your service-linked role, see AWS Services That Work with IAM in the *IAM User Guide*. Look for the services that have **Yes** in the **Service-Linked Role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

CustomSuffix

A string that you provide, which is combined with the service-provided prefix to form the complete role name. If you make multiple requests for the same service, then you must supply a different `CustomSuffix` for each request. Otherwise the request fails with a duplicate role name error. For example, you could add `-1` or `-debug` to the suffix.

Some services do not support the `CustomSuffix` parameter. If you provide an optional suffix and the operation fails, try the operation again without the suffix.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

Description

The description of the role.

Type: String

Length Constraints: Maximum length of 1000.

Pattern: `[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}]*`

Required: No

Response Elements

The following element is returned by the service.

Role

A Role (p. 471) object that contains details about the newly created role.

Type: Role (p. 471) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

CreateServiceSpecificCredential

Generates a set of credentials consisting of a user name and password that can be used to access the service specified in the request. These credentials are generated by IAM, and can be used only for the specified service.

You can have a maximum of two sets of service-specific credentials for each supported service per user.

The only supported service at this time is AWS CodeCommit.

You can reset the password to a new service-generated value by calling ResetServiceSpecificCredential (p. 328).

For more information about service-specific credentials, see Using IAM with AWS CodeCommit: Git Credentials, SSH Keys, and AWS Access Keys in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ServiceName

The name of the AWS service that is to be associated with the credentials. The service you specify here is the only service that can be accessed using these credentials.

Type: String

Required: Yes

UserName

The name of the IAM user that is to be associated with the credentials. The new service-specific credentials have the same permissions as the associated user except that they can be used only to access the specified service.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

ServiceSpecificCredential

A structure that contains information about the newly created service-specific credential.

Important
This is the only time that the password for this credential set is available. It cannot be recovered later. Instead, you must reset the password with ResetServiceSpecificCredential (p. 328).

Type: ServiceSpecificCredential (p. 485) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

NotSupportedService

The specified service does not support service-specific credentials.

HTTP Status Code: 404

Examples

Example

In the following example, the caller creates service-specific credentials for the IAM user named `Anika` in account `123456789012`. The credentials can be used only with the AWS service associated with the service endpoint at `codecommit.amazonaws.com` .

Sample Request

```
https://iam.amazonaws.com/?Action=CreateServiceSpecificCredential
&UserName=Anika
&ServiceName=codecommit.amazonaws.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateServiceSpecificCredentialResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateServiceSpecificCredentialResult>
    <ServiceSpecificCredential>
      <ServicePassword>xTBAr/czp+D3EXAMPLE47lrJ6/43r2zqGwR3EXAMPLE=</ServicePassword>
      <ServiceName>codecommit.amazonaws.com</ServiceName>
      <UserName>anika</UserName>
      <ServiceUserName>anika+1-at-123456789012</ServiceUserName>
      <ServiceSpecificCredentialId>ACCA12345ABCDEXAMPLE</ServiceSpecificCredentialId>
      <Status>Active</Status>
      <CreateDate>2016-11-01T17:47:22.382Z</CreateDate>
    </ServiceSpecificCredential>
  </CreateServiceSpecificCredentialResult>
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
```

```
  </ResponseMetadata>
</CreateServiceSpecificCredentialResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateUser

Creates a new IAM user for your AWS account.

For information about limitations on the number of IAM users you can create, see Limitations on IAM Entities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Path

The path for the user name. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

PermissionsBoundary

The ARN of the policy that is used to set the permissions boundary for the user.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

Tags.member.N

A list of tags that you want to attach to the newly created user. Each tag consists of a key name and an associated value. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

> **Note**
> If any one of the tags is invalid or if you exceed the allowed number of tags per user, then the entire request fails and the user is not created.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Required: No

UserName

The name of the user to create.

IAM user, group, role, and policy names must be unique within the account. Names are not distinguished by case. For example, you cannot create resources named both "MyResource" and "myresource".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

User

A structure with details about the new IAM user.

Type: User (p. 499) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateUser.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateUser
&Path=/division_abc/subdivision_xyz/
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateUserResult>
    <User>
      <Path>/division_abc/subdivision_xyz/</Path>
      <UserName>Bob</UserName>
      <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
      <Arn>arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/Bob</Arn>
    </User>
  </CreateUserResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateUserResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateVirtualMFADevice

Creates a new virtual MFA device for the AWS account. After creating the virtual MFA, use EnableMFADevice (p. 129) to attach the MFA device to an IAM user. For more information about creating and working with virtual MFA devices, go to Using a Virtual MFA Device in the *IAM User Guide*.

For information about limits on the number of MFA devices you can create, see Limitations on Entities in the *IAM User Guide*.

Important
The seed information contained in the QR code and the Base32 string should be treated like any other secret access information. In other words, protect the seed information as you would your AWS access keys or your passwords. After you provision your virtual device, you should ensure that the information is destroyed following secure procedures.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Path

The path for the virtual MFA device. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/).

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

VirtualMFADeviceName

The name of the virtual MFA device. Use with path to uniquely identify a virtual MFA device.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

VirtualMFADevice

A structure containing details about the new virtual MFA device.

Type: VirtualMFADevice (p. 504) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of CreateVirtualMFADevice.

Sample Request

```
https://iam.amazonaws.com/?Action=CreateVirtualMFADevice
&VirtualMFADeviceName=ExampleName
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<CreateVirtualMFADeviceResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <CreateVirtualMFADeviceResult>
    <VirtualMFADevice>
      <SerialNumber>arn:aws:iam::123456789012:mfa/ExampleName</SerialNumber>
      <Base32StringSeed>
        2K5K5XTLA7GGE75TQLYEXAMPLEEXAMPLEEXAMPLECHDFW4KJYZ6UFQ75LL7COCYKM
      </Base32StringSeed>
      <QRCodePNG>
        89504E470D0A1A0AASDFAHSDFKJKLJFKALSDFJASDF <!-- byte array of png file -->
      </QRCodePNG>
    </VirtualMFADevice>
  </CreateVirtualMFADeviceResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
```

```
  </ResponseMetadata>
</CreateVirtualMFADeviceResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeactivateMFADevice

Deactivates the specified MFA device and removes it from association with the user name for which it was originally enabled.

For more information about creating and working with virtual MFA devices, go to Enabling a Virtual Multi-factor Authentication (MFA) Device in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

SerialNumber

The serial number that uniquely identifies the MFA device. For virtual MFA devices, the serial number is the device ARN.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@:/-

Type: String

Length Constraints: Minimum length of 9. Maximum length of 256.

Pattern: `[\w+=/:,.@-]+`

Required: Yes

UserName

The name of the user whose MFA device you want to deactivate.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeactivateMFADevice.

Sample Request

```
https://iam.amazonaws.com/?Action=DeactivateMFADevice
&UserName=Bob
&SerialNumber=R1234
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeactivateMFADeviceResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeactivateMFADeviceResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteAccessKey

Deletes the access key pair associated with the specified IAM user.

If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID signing the request. This operation works for access keys under the AWS account. Consequently, you can use this operation to manage AWS account root user credentials even if the AWS account has no associated users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AccessKeyId

The access key ID for the access key ID and secret access key you want to delete.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the user whose access key pair you want to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteAccessKey.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteAccessKey
&UserName=Bob
&AccessKeyId=AKIAIOSFODNN7EXAMPLE
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteAccessKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteAccessKeyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteAccountAlias

Deletes the specified AWS account alias. For information about using an AWS account alias, see Using an Alias for Your AWS Account ID in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AccountAlias

The name of the account alias to delete.

This parameter allows (through its regex pattern) a string of characters consisting of lowercase letters, digits, and dashes. You cannot start or finish with a dash, nor can you have two dashes in a row.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 63.

Pattern: `^[a-z0-9](([a-z0-9]|-(?!-))*[a-z0-9])?$`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteAccountAlias.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteAccountAlias
&AccountAlias=ExampleCorp
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteAccountAliasResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteAccountAliasResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteAccountPasswordPolicy

Deletes the password policy for the AWS account. There are no parameters.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteAccountPasswordPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteAccountPasswordPolicy
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteAccountPasswordPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteAccountPasswordPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteGroup

Deletes the specified IAM group. The group must not contain any users or have any attached policies.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name of the IAM group to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteGroup.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteGroup
&GroupName=Test
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteGroupResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteGroupPolicy

Deletes the specified inline policy that is embedded in the specified IAM group.

A group can also have managed policies attached to it. To detach a managed policy from a group, use DetachGroupPolicy (p. 122). For more information about policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name (friendly name, not ARN) identifying the group that the policy is embedded in.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

PolicyName

The name identifying the policy document to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteGroupPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteGroupPolicy
&GroupName=Admins
&PolicyName=AdminFullAccess
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteGroupPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteInstanceProfile

Deletes the specified instance profile. The instance profile must not have an associated role.

> **Important**
> Make sure that you do not have any Amazon EC2 instances running with the instance profile you are about to delete. Deleting a role or instance profile that is associated with a running instance will break any applications running on the instance.

For more information about instance profiles, go to About Instance Profiles.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

InstanceProfileName

The name of the instance profile to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteInstanceProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteInstanceProfile
&InstanceProfileName=Webserver
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteInstanceProfileResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>90c18667-99f3-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</DeleteInstanceProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteLoginProfile

Deletes the password for the specified IAM user, which terminates the user's ability to access AWS services through the AWS Management Console.

Important
Deleting a user's password does not prevent a user from accessing AWS through the command line interface or the API. To prevent all user access, you must also either make any access keys inactive or delete them. For more information about making keys inactive or deleting them, see UpdateAccessKey (p. 369) and DeleteAccessKey (p. 72).

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

UserName

The name of the user whose password you want to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteLoginProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteLoginProfile
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteLoginProfileResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteLoginProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteOpenIDConnectProvider

Deletes an OpenID Connect identity provider (IdP) resource object in IAM.

Deleting an IAM OIDC provider resource does not update any roles that reference the provider as a principal in their trust policies. Any attempt to assume a role that references a deleted provider fails.

This operation is idempotent; it does not fail or return an error if you call the operation for a provider that does not exist.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the IAM OpenID Connect provider resource object to delete. You can get a list of OpenID Connect provider resource ARNs by using the ListOpenIDConnectProviders (p. 260) operation.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteOpenIDConnectProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteOpenIDConnectProvider
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>b5e49e29-4f64-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteOpenIDConnectProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeletePolicy

Deletes the specified managed policy.

Before you can delete a managed policy, you must first detach the policy from all users, groups, and roles that it is attached to. In addition, you must delete all the policy's versions. The following steps describe the process for deleting a managed policy:

- Detach the policy from all users, groups, and roles that the policy is attached to, using the DetachUserPolicy (p. 127), DetachGroupPolicy (p. 122), or DetachRolePolicy (p. 124) API operations. To list all the users, groups, and roles that a policy is attached to, use ListEntitiesForPolicy (p. 238).
- Delete all versions of the policy using DeletePolicyVersion (p. 91). To list the policy's versions, use ListPolicyVersions (p. 270). You cannot use DeletePolicyVersion (p. 91) to delete the version that is marked as the default version. You delete the policy's default version in the next step of the process.
- Delete the policy (this automatically deletes the policy's default version) using this API.

For information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to delete.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeletePolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=DeletePolicy
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeletePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>4706281b-3d19-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DeletePolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeletePolicyVersion

Deletes the specified version from the specified managed policy.

You cannot delete the default version from a policy using this API. To delete the default version from a policy, use DeletePolicy (p. 88). To find out which version of a policy is marked as the default version, use ListPolicyVersions (p. 270).

For information about versions for managed policies, see Versioning for Managed Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy from which you want to delete a version.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

VersionId

The policy version to delete.

This parameter allows (through its regex pattern) a string of characters that consists of the lowercase letter 'v' followed by one or two digits, and optionally followed by a period '.' and a string of letters and digits.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeletePolicyVersion.

Sample Request

```
https://iam.amazonaws.com/?Action=DeletePolicyVersion
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&VersionId=v2
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeletePolicyVersionResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>268e1556-3d19-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DeletePolicyVersionResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRole

Deletes the specified role. The role must not have any policies attached. For more information about roles, go to Working with Roles.

Important
Make sure that you do not have any Amazon EC2 instances running with the role you are about to delete. Deleting a role or instance profile that is associated with a running instance will break any applications running on the instance.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

RoleName

The name of the role to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DeleteRole.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteRole
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>913e3f37-99ed-11e1-a4c3-270EXAMPLE04</RequestId>
  </ResponseMetadata>
</DeleteRoleResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRolePermissionsBoundary

Deletes the permissions boundary for the specified IAM role.

> **Important**
> Deleting the permissions boundary for a role might increase its permissions. For example, it might allow anyone who assumes the role to perform all the actions granted in its permissions policies.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

RoleName

The name (friendly name, not ARN) of the IAM role from which you want to remove the permissions boundary.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRolePolicy

Deletes the specified inline policy that is embedded in the specified IAM role.

A role can also have managed policies attached to it. To detach a managed policy from a role, use DetachRolePolicy (p. 124). For more information about policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyName

The name of the inline policy to delete from the specified IAM role.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

RoleName

The name (friendly name, not ARN) identifying the role that the policy is embedded in.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DeleteRolePolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteRolePolicy
&PolicyName=S3AccessPolicy
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>c749ee7f-99ef-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</DeleteRolePolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteSAMLProvider

Deletes a SAML provider resource in IAM.

Deleting the provider resource from IAM does not update any roles that reference the SAML provider resource's ARN as a principal in their trust policies. Any attempt to assume a role that references a non-existent provider resource ARN fails.

Note
This operation requires Signature Version 4.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

SAMLProviderArn

The Amazon Resource Name (ARN) of the SAML provider to delete.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteSAMLProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteSAMLProvider
&SAMLProviderArn=arn:aws:iam::123456789012:saml-provider/MyUniversity
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteSAMLProviderResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>c749ee7f-99ef-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</DeleteSAMLProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteServerCertificate

Deletes the specified server certificate.

For more information about working with server certificates, see Working with Server Certificates in the *IAM User Guide*. This topic also includes a list of AWS services that can use the server certificates that you manage with IAM.

> **Important**
> If you are using a server certificate with Elastic Load Balancing, deleting the certificate could have implications for your application. If Elastic Load Balancing doesn't detect the deletion of bound certificates, it may continue to use the certificates. This could cause Elastic Load Balancing to stop accepting traffic. We recommend that you remove the reference to the certificate from Elastic Load Balancing before using this command to delete the certificate. For more information, go to DeleteLoadBalancerListeners in the *Elastic Load Balancing API Reference*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ServerCertificateName

The name of the server certificate you want to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteServerCertificate.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteServerCertificate
&ServerCertificateName=ProdServerCert
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteServerCertificateResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteServerCertificateResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteServiceLinkedRole

Submits a service-linked role deletion request and returns a `DeletionTaskId`, which you can use to check the status of the deletion. Before you call this operation, confirm that the role has no active sessions and that any resources used by the role in the linked service are deleted. If you call this operation more than once for the same service-linked role and an earlier deletion task is not complete, then the `DeletionTaskId` of the earlier request is returned.

If you submit a deletion request for a service-linked role whose linked service is still accessing a resource, then the deletion task fails. If it fails, the GetServiceLinkedRoleDeletionStatus (p. 208) API operation returns the reason for the failure, usually including the resources that must be deleted. To delete the service-linked role, you must first remove those resources from the linked service and then submit the deletion request again. Resources are specific to the service that is linked to the role. For more information about removing resources from a service, see the AWS documentation for your service.

For more information about service-linked roles, see Roles Terms and Concepts: AWS Service-Linked Role in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

RoleName

The name of the service-linked role to be deleted.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

DeletionTaskId

The deletion task identifier that you can use to check the status of the deletion. This identifier is returned in the format `task/aws-service-role/<service-principal-name>/<role-name>/<task-uuid>`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

The following example shows how to submit the role named `AWSServiceRoleForLexBots` for deletion.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteServiceLinkedRole
&RoleName=AWSServiceRoleForLexBots
&Version=2010-05-08
```

Example

This example illustrates one usage of DeleteServiceLinkedRole.

Sample Response

```
<DeleteServiceLinkedRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <DeleteServiceLinkedRoleResult>
    <DeletionTaskId>task/aws-service-role/lex.amazonaws.com/AWSServiceRoleForLexBots/
ec720f7a-c0ba-4838-be33-f72e1873dd52</DeletionTaskId>
  </DeleteServiceLinkedRoleResult>
  <ResponseMetadata>
    <RequestId>4aff7ebf-8297-11e7-898c-4904717fb079</RequestId>
  </ResponseMetadata>
</DeleteServiceLinkedRoleResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteServiceSpecificCredential

Deletes the specified service-specific credential.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ServiceSpecificCredentialId

The unique identifier of the service-specific credential. You can get this value by calling ListServiceSpecificCredentials (p. 287).

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the IAM user associated with the service-specific credential. If this value is not specified, then the operation assumes the user whose credentials are used to call the operation.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

The following example shows how to delete a service-specific credential associated with the user named Juan. If Juan's IAM access keys are used to make the call, then he does not need to include the `UserName` parameter.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteServiceSpecificCredential
&ServiceSpecificCredentialId=ACCA12345ABCDEXAMPLE
&UserName=Juan
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteServiceSpecificCredentialResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteServiceSpecificCredentialResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteSigningCertificate

Deletes a signing certificate associated with the specified IAM user.

If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID signing the request. This operation works for access keys under the AWS account. Consequently, you can use this operation to manage AWS account root user credentials even if the AWS account has no associated IAM users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

CertificateId

The ID of the signing certificate to delete.

The format of this parameter, as described by its regex pattern, is a string of characters that can be upper- or lower-cased letters or digits.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the user the signing certificate belongs to.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteSigningCertificate.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteSigningCertificate
&UserName=Bob
&CertificateId=TA7SMP42TDN5Z26OBPJE7EXAMPLE
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteSigningCertificateResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteSigningCertificateResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteSSHPublicKey

Deletes the specified SSH public key.

The SSH public key deleted by this operation is used only for authenticating the associated IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

SSHPublicKeyId

The unique identifier for the SSH public key.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the IAM user associated with the SSH public key.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

This example illustrates one usage of DeleteSSHPublicKey.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteSSHPublicKey
&SSHPublicKeyId=APKAEIVFHP46CEXAMPLE
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteSSHPublicKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1a21282e-f36e-11e4-a53b-6b544EXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteSSHPublicKeyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteUser

Deletes the specified IAM user. Unlike the AWS Management Console, when you delete a user programmatically, you must delete the items attached to the user manually, or the deletion fails. For more information, see Deleting an IAM User. Before attempting to delete a user, remove the following items:

- Password (DeleteLoginProfile (p. 84))
- Access keys (DeleteAccessKey (p. 72))
- Signing certificate (DeleteSigningCertificate (p. 109))
- SSH public key (DeleteSSHPublicKey (p. 111))
- Git credentials (DeleteServiceSpecificCredential (p. 107))
- Multi-factor authentication (MFA) device (DeactivateMFADevice (p. 69), DeleteVirtualMFADevice (p. 120))
- Inline policies (DeleteUserPolicy (p. 118))
- Attached managed policies (DetachUserPolicy (p. 127))
- Group memberships (RemoveUserFromGroup (p. 326))

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

UserName

The name of the user to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteUser.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteUser
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteUserResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

DeleteUserPermissionsBoundary

Deletes the permissions boundary for the specified IAM user.

> **Important**
> Deleting the permissions boundary for a user might increase its permissions by allowing the user to perform all the actions granted in its permissions policies.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

UserName

The name (friendly name, not ARN) of the IAM user from which you want to remove the permissions boundary.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteUserPolicy

Deletes the specified inline policy that is embedded in the specified IAM user.

A user can also have managed policies attached to it. To detach a managed policy from a user, use DetachUserPolicy (p. 127). For more information about policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyName

The name identifying the policy document to delete.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

UserName

The name (friendly name, not ARN) identifying the user that the policy is embedded in.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteUserPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteUserPolicy
&UserName=Bob
&PolicyName=AllAccessPolicy
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteUserPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteVirtualMFADevice

Deletes a virtual MFA device.

> **Note**
> You must deactivate a user's virtual MFA device before you can delete it. For information about deactivating MFA devices, see DeactivateMFADevice (p. 69).

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

SerialNumber

The serial number that uniquely identifies the MFA device. For virtual MFA devices, the serial number is the same as the ARN.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@:/-

Type: String

Length Constraints: Minimum length of 9. Maximum length of 256.

Pattern: `[\w+=/:,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

DeleteConflict

The request was rejected because it attempted to delete a resource that has attached subordinate entities. The error message describes these entities.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DeleteVirtualMFADevice.

Sample Request

```
https://iam.amazonaws.com/?Action=DeleteVirtualMFADevice
&SerialNumber=arn:aws:iam::123456789012:mfa/ExampleName
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DeleteVirtualMFADeviceResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</DeleteVirtualMFADeviceResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DetachGroupPolicy

Removes the specified managed policy from the specified IAM group.

A group can also have inline policies embedded with it. To delete an inline policy, use the DeleteGroupPolicy (p. 80) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name (friendly name, not ARN) of the IAM group to detach the policy from.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to detach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DetachGroupPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=DetachGroupPolicy
&GroupName=Finance
&PolicyArn=arn:aws:iam::aws:policy/ReadOnlyAccess
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DetachGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>d4faa7aa-3d1d-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DetachGroupPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DetachRolePolicy

Removes the specified managed policy from the specified role.

A role can also have inline policies embedded with it. To delete an inline policy, use the DeleteRolePolicy (p. 98) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to detach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

RoleName

The name (friendly name, not ARN) of the IAM role to detach the policy from.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of DetachRolePolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=DetachRolePolicy
&PolicyArn=arn:aws:iam::aws:policy/ReadOnlyAccess
&RoleName=ReadOnlyRole
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DetachRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>4c80ccf4-3d1e-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DetachRolePolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

DetachUserPolicy

Removes the specified managed policy from the specified user.

A user can also have inline policies embedded with it. To delete an inline policy, use the DeleteUserPolicy (p. 118) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy you want to detach.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

UserName

The name (friendly name, not ARN) of the IAM user to detach the policy from.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of DetachUserPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=DetachUserPolicy
&PolicyArn=arn:aws:iam::aws:policy/AdministratorAccess
&UserName=Alice
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<DetachUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>85ba31fa-3d1f-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</DetachUserPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

EnableMFADevice

Enables the specified MFA device and associates it with the specified IAM user. When enabled, the MFA device is required for every subsequent login by the IAM user associated with the device.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AuthenticationCode1

An authentication code emitted by the device.

The format for this parameter is a string of six digits.

> **Important**
> Submit your request immediately after generating the authentication codes. If you generate the codes and then wait too long to submit the request, the MFA device successfully associates with the user but the MFA device becomes out of sync. This happens because time-based one-time passwords (TOTP) expire after a short period of time. If this happens, you can resync the device.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `[\d]+`

Required: Yes

AuthenticationCode2

A subsequent authentication code emitted by the device.

The format for this parameter is a string of six digits.

> **Important**
> Submit your request immediately after generating the authentication codes. If you generate the codes and then wait too long to submit the request, the MFA device successfully associates with the user but the MFA device becomes out of sync. This happens because time-based one-time passwords (TOTP) expire after a short period of time. If this happens, you can resync the device.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `[\d]+`

Required: Yes

SerialNumber

The serial number that uniquely identifies the MFA device. For virtual MFA devices, the serial number is the device ARN.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@:/-

Type: String

Length Constraints: Minimum length of 9. Maximum length of 256.

Pattern: `[\w+=/:,.@-]+`

Required: Yes

UserName

The name of the IAM user for whom you want to enable the MFA device.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

InvalidAuthenticationCode

The request was rejected because the authentication code was not recognized. The error message describes the specific error.

HTTP Status Code: 403

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of EnableMFADevice.

Sample Request

```
https://iam.amazonaws.com/?Action=EnableMFADevice
&UserName=Bob
&SerialNumber=R1234
&AuthenticationCode1=234567
&AuthenticationCode2=987654
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<EnableMFADeviceResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</EnableMFADeviceResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GenerateCredentialReport

Generates a credential report for the AWS account. For more information about the credential report, see Getting Credential Reports in the *IAM User Guide*.

Response Elements

The following elements are returned by the service.

Description

Information about the credential report.

Type: String

State

Information about the state of the credential report.

Type: String

Valid Values: `STARTED | INPROGRESS | COMPLETE`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GenerateCredentialReport.

Sample Request

```
https://iam.amazonaws.com/?Action=GenerateCredentialReport
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GenerateCredentialReportResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
```

```
  <GenerateCredentialReportResult>
    <Description>No report exists. Starting a new report generation task</Description>
    <State>STARTED</State>
  </GenerateCredentialReportResult>
  <ResponseMetadata>
    <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
  </ResponseMetadata>
</GenerateCredentialReportResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GenerateOrganizationsAccessReport

Generates a report for service last accessed data for AWS Organizations. You can generate a report for any entities (organization root, organizational unit, or account) or policies in your organization.

To call this operation, you must be signed in using your AWS Organizations master account credentials. You can use your long-term IAM user or root user credentials, or temporary credentials from assuming an IAM role. SCPs must be enabled for your organization root. You must have the required IAM and AWS Organizations permissions. For more information, see Refining Permissions Using Service Last Accessed Data in the *IAM User Guide*.

You can generate a service last accessed data report for entities by specifying only the entity's path. This data includes a list of services that are allowed by any service control policies (SCPs) that apply to the entity.

You can generate a service last accessed data report for a policy by specifying an entity's path and an optional AWS Organizations policy ID. This data includes a list of services that are allowed by the specified SCP.

For each service in both report types, the data includes the most recent account activity that the policy allows to account principals in the entity or the entity's children. For important information about the data, reporting period, permissions required, troubleshooting, and supported Regions see Reducing Permissions Using Service Last Accessed Data in the *IAM User Guide*.

> **Important**
> The data includes all attempts to access AWS, not just the successful ones. This includes all attempts that were made using the AWS Management Console, the AWS API through any of the SDKs, or any of the command line tools. An unexpected entry in the service last accessed data does not mean that an account has been compromised, because the request might have been denied. Refer to your CloudTrail logs as the authoritative source for information about all API calls and whether they were successful or denied access. For more information, see Logging IAM Events with CloudTrail in the *IAM User Guide*.

This operation returns a `JobId`. Use this parameter in the `GetOrganizationsAccessReport (p. 178)` operation to check the status of the report generation. To check the status of this request, use the `JobId` parameter in the `GetOrganizationsAccessReport (p. 178)` operation and test the `JobStatus` response parameter. When the job is complete, you can retrieve the report.

To generate a service last accessed data report for entities, specify an entity path without specifying the optional AWS Organizations policy ID. The type of entity that you specify determines the data returned in the report.

- **Root** – When you specify the organizations root as the entity, the resulting report lists all of the services allowed by SCPs that are attached to your root. For each service, the report includes data for all accounts in your organization except the master account, because the master account is not limited by SCPs.
- **OU** – When you specify an organizational unit (OU) as the entity, the resulting report lists all of the services allowed by SCPs that are attached to the OU and its parents. For each service, the report includes data for all accounts in the OU or its children. This data excludes the master account, because the master account is not limited by SCPs.
- **Master account** – When you specify the master account, the resulting report lists all AWS services, because the master account is not limited by SCPs. For each service, the report includes data for only the master account.
- **Account** – When you specify another account as the entity, the resulting report lists all of the services allowed by SCPs that are attached to the account and its parents. For each service, the report includes data for only the specified account.

To generate a service last accessed data report for policies, specify an entity path and the optional AWS Organizations policy ID. The type of entity that you specify determines the data returned for each service.

- **Root** – When you specify the root entity and a policy ID, the resulting report lists all of the services that are allowed by the specified SCP. For each service, the report includes data for all accounts in your organization to which the SCP applies. This data excludes the master account, because the master account is not limited by SCPs. If the SCP is not attached to any entities in the organization, then the report will return a list of services with no data.
- **OU** – When you specify an OU entity and a policy ID, the resulting report lists all of the services that are allowed by the specified SCP. For each service, the report includes data for all accounts in the OU or its children to which the SCP applies. This means that other accounts outside the OU that are affected by the SCP might not be included in the data. This data excludes the master account, because the master account is not limited by SCPs. If the SCP is not attached to the OU or one of its children, the report will return a list of services with no data.
- **Master account** – When you specify the master account, the resulting report lists all AWS services, because the master account is not limited by SCPs. If you specify a policy ID in the CLI or API, the policy is ignored. For each service, the report includes data for only the master account.
- **Account** – When you specify another account entity and a policy ID, the resulting report lists all of the services that are allowed by the specified SCP. For each service, the report includes data for only the specified account. This means that other accounts in the organization that are affected by the SCP might not be included in the data. If the SCP is not attached to the account, the report will return a list of services with no data.

> **Note**
> Service last accessed data does not use other policy types when determining whether a principal could access a service. These other policy types include identity-based policies, resource-based policies, access control lists, IAM permissions boundaries, and STS assume role policies. It only applies SCP logic. For more about the evaluation of policy types, see Evaluating Policies in the *IAM User Guide*.

For more information about service last accessed data, see Reducing Policy Scope by Viewing User Activity in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

EntityPath

The path of the AWS Organizations entity (root, OU, or account). You can build an entity path using the known structure of your organization. For example, assume that your account ID is `123456789012` and its parent OU ID is `ou-rge0-awsabcde`. The organization root ID is `r-f6g7h8i9j0example` and your organization ID is `o-a1b2c3d4e5`. Your entity path is `o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-rge0-awsabcde/123456789012`.

Type: String

Length Constraints: Minimum length of 19. Maximum length of 427.

Pattern: `^o-[0-9a-z]{10,32}\/r-[0-9a-z]{4,32}[0-9a-z-\/]*`

Required: Yes

OrganizationsPolicyId

The identifier of the AWS Organizations service control policy (SCP). This parameter is optional.

This ID is used to generate information about when an account principal that is limited by the SCP attempted to access an AWS service.

Type: String

Pattern: `^p-[0-9a-zA-Z_]{8,128}$`

Required: No

Response Elements

The following element is returned by the service.

JobId

The job identifier that you can use in the GetOrganizationsAccessReport (p. 178) operation.

Type: String

Length Constraints: Fixed length of 36.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ReportGenerationLimitExceeded

The request failed because the maximum number of concurrent requests for this account are already running.

HTTP Status Code: 409

Examples

Example

This example illustrates one usage of GenerateOrganizationsAccessReport.

Sample Request

```
https://iam.amazonaws.com/?Action=GenerateOrganizationsAccessReport
&EntityPath=o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-1a2b3c-k9l8m7n6o5example
&OrganizationsPolicyId=p-9l89z4nw
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<JobId>examplea-1234-b567-cde8-90fg123abcd4</JobId>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GenerateServiceLastAccessedDetails

Generates a report that includes details about when an IAM resource (user, group, role, or policy) was last used in an attempt to access AWS services. Recent activity usually appears within four hours. IAM reports activity for the last 365 days, or less if your Region began supporting this feature within the last year. For more information, see Regions Where Data Is Tracked.

> **Important**
> The service last accessed data includes all attempts to access an AWS API, not just the successful ones. This includes all attempts that were made using the AWS Management Console, the AWS API through any of the SDKs, or any of the command line tools. An unexpected entry in the service last accessed data does not mean that your account has been compromised, because the request might have been denied. Refer to your CloudTrail logs as the authoritative source for information about all API calls and whether they were successful or denied access. For more information, see Logging IAM Events with CloudTrail in the *IAM User Guide*.

The `GenerateServiceLastAccessedDetails` operation returns a `JobId`. Use this parameter in the following operations to retrieve the following details from your report:

- GetServiceLastAccessedDetails (p. 199) – Use this operation for users, groups, roles, or policies to list every AWS service that the resource could access using permissions policies. For each service, the response includes information about the most recent access attempt.

  The `JobId` returned by `GenerateServiceLastAccessedDetail` must be used by the same role within a session, or by the same user when used to call `GetServiceLastAccessedDetail`.
- GetServiceLastAccessedDetailsWithEntities (p. 204) – Use this operation for groups and policies to list information about the associated entities (users or roles) that attempted to access a specific AWS service.

To check the status of the `GenerateServiceLastAccessedDetails` request, use the `JobId` parameter in the same operations and test the `JobStatus` response parameter.

For additional information about the permissions policies that allow an identity (user, group, or role) to access specific services, use the ListPoliciesGrantingServiceAccess (p. 266) operation.

> **Note**
> Service last accessed data does not use other policy types when determining whether a resource could access a service. These other policy types include resource-based policies, access control lists, AWS Organizations policies, IAM permissions boundaries, and AWS STS assume role policies. It only applies permissions policy logic. For more about the evaluation of policy types, see Evaluating Policies in the *IAM User Guide*.

For more information about service and action last accessed data, see Reducing Permissions Using Service Last Accessed Data in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Arn

The ARN of the IAM resource (user, group, role, or managed policy) used to generate information about when the resource was last used in an attempt to access an AWS service.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Granularity

The level of detail that you want to generate. You can specify whether you want to generate information about the last attempt to access services or actions. If you specify service-level granularity, this operation generates only service data. If you specify action-level granularity, it generates service and action data. If you don't include this optional parameter, the operation generates service data.

Type: String

Valid Values: `SERVICE_LEVEL | ACTION_LEVEL`

Required: No

Response Elements

The following element is returned by the service.

JobId

The `JobId` that you can use in the GetServiceLastAccessedDetails (p. 199) or GetServiceLastAccessedDetailsWithEntities (p. 204) operations. The `JobId` returned by `GenerateServiceLastAccessedDetail` must be used by the same role within a session, or by the same user when used to call `GetServiceLastAccessedDetail`.

Type: String

Length Constraints: Fixed length of 36.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

This example illustrates one usage of GenerateServiceLastAccessedDetails.

Sample Request

```
https://iam.amazonaws.com/?Action=GenerateServiceLastAccessedDetails
&Arn=arn:aws:iam::123456789012:policy/ExamplePolicy1
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<JobId>examplef-1305-c245-eba4-71fe298bcda7</JobId>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAccessKeyLastUsed

Retrieves information about when the specified access key was last used. The information includes the date and time of last use, along with the AWS service and Region that were specified in the last request made with that key.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AccessKeyId

The identifier of an access key.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Response Elements

The following elements are returned by the service.

AccessKeyLastUsed

Contains information about the last time the access key was used.

Type: AccessKeyLastUsed (p. 425) object

UserName

The name of the AWS IAM user that owns this access key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

Examples

Example

This example illustrates one usage of GetAccessKeyLastUsed.

Sample Request

```
https://iam.amazonaws.com/
?Action=GetAccessKeyLastUsed
&AccessKeyId=AKIAIOSFODNN7EXAMPLE
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetAccessKeyLastUsedResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetAccessKeyLastUsedResult>
    <AccessKeyLastUsed>
      <Region>us-west-2</Region>
      <LastUsedDate>2015-03-13T10:45:00Z</LastUsedDate>
      <ServiceName>s3</ServiceName>
    </AccessKeyLastUsed>
    <UserName>bob</UserName>
  </GetAccessKeyLastUsedResult>
  <ResponseMetadata>
    <RequestId>510a6abf-d022-11e4-abe8-9b0ebEXAMPLE</RequestId>
  </ResponseMetadata>
</GetAccessKeyLastUsedResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAccountAuthorizationDetails

Retrieves information about all IAM users, groups, roles, and policies in your AWS account, including their relationships to one another. Use this API to obtain a snapshot of the configuration of IAM permissions (users, groups, roles, and policies) in your account.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

You can optionally filter the results using the `Filter` parameter. You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Filter.member.N

A list of entity types used to filter the results. Only the entities that match the types you specify are included in the output. Use the value `LocalManagedPolicy` to include customer managed policies.

The format for this parameter is a comma-separated (if more than one) list of strings. Each string value in the list must be one of the valid values listed below.

Type: Array of strings

Valid Values: `User | Role | Group | LocalManagedPolicy | AWSManagedPolicy`

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

GroupDetailList.member.N

A list containing information about IAM groups.

Type: Array of GroupDetail (p. 442) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Policies.member.N

A list containing information about managed policies.

Type: Array of ManagedPolicyDetail (p. 448) objects

RoleDetailList.member.N

A list containing information about IAM roles.

Type: Array of RoleDetail (p. 474) objects

UserDetailList.member.N

A list containing information about IAM users.

Type: Array of UserDetail (p. 501) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetAccountAuthorizationDetails.

Sample Request

```
https://iam.amazonaws.com/?Action=GetAccountAuthorizationDetails
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetAccountAuthorizationDetailsResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetAccountAuthorizationDetailsResult>
    <IsTruncated>true</IsTruncated>
    <UserDetailList>
      <member>
        <GroupList>
          <member>Admins</member>
        </GroupList>
        <AttachedManagedPolicies/>
        <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
        <Path>/</Path>
        <UserName>Alice</UserName>
        <Arn>arn:aws:iam::123456789012:user/Alice</Arn>
        <CreateDate>2013-10-14T18:32:24Z</CreateDate>
      </member>
      <member>
        <GroupList>
          <member>Admins</member>
        </GroupList>
        <AttachedManagedPolicies/>
        <UserPolicyList>
          <member>
            <PolicyName>DenyBillingAndIAMPolicy</PolicyName>
            <PolicyDocument>
              {"Version":"2012-10-17","Statement":{"Effect":"Deny","Action":
              ["aws-portal:*","iam:*"],"Resource":"*"}}
            </PolicyDocument>
          </member>
        </UserPolicyList>
        <UserId>AIDACKCEVSQ6C3EXAMPLE</UserId>
        <Path>/</Path>
        <UserName>Bob</UserName>
        <Arn>arn:aws:iam::123456789012:user/Bob</Arn>
        <CreateDate>2013-10-14T18:32:25Z</CreateDate>
      </member>
      <member>
        <GroupList>
          <member>Dev</member>
        <AttachedManagedPolicies/>
        </GroupList>
        <UserId>AIDACKCEVSQ6C4EXAMPLE</UserId>
        <Path>/</Path>
        <UserName>Charlie</UserName>
        <Arn>arn:aws:iam::123456789012:user/Charlie</Arn>
        <CreateDate>2013-10-14T18:33:56Z</CreateDate>
      </member>
      <member>
```

```
      <GroupList>
        <member>Dev</member>
      </GroupList>
      <AttachedManagedPolicies/>
      <UserId>AIDACKCEVSQ6C5EXAMPLE</UserId>
      <Path>/</Path>
      <UserName>Danielle</UserName>
      <Arn>arn:aws:iam::123456789012:user/Danielle</Arn>
      <CreateDate>2013-10-14T18:33:56Z</CreateDate>
    </member>
    <member>
      <GroupList>
        <member>Finance</member>
      </GroupList>
      <AttachedManagedPolicies/>
      <UserId>AIDACKCEVSQ6C6EXAMPLE</UserId>
      <Path>/</Path>
      <UserName>Elaine</UserName>
      <Arn>arn:aws:iam::123456789012:user/Elaine</Arn>
      <CreateDate>2013-10-14T18:57:48Z</CreateDate>
    </member>
  </UserDetailList>
  <Marker>
    EXAMPLEkakv9BCuUNFDtxWSyfzetYwEx2ADc8dnzfvERF5S6YMvXKx41t6gCl/eeaCX3Jo94/
    bKqezEAg8TEVS99EKFLxm3jtbpl25FDWEXAMPLE
  </Marker>
  <GroupDetailList>
    <member>
      <GroupId>AIDACKCEVSQ6C7EXAMPLE</GroupId>
      <AttachedManagedPolicies>
        <member>
          <PolicyName>AdministratorAccess</PolicyName>
          <PolicyArn>arn:aws:iam::aws:policy/AdministratorAccess</PolicyArn>
        </member>
      </AttachedManagedPolicies>
      <GroupName>Admins</GroupName>
      <Path>/</Path>
      <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
      <CreateDate>2013-10-14T18:32:24Z</CreateDate>
      <GroupPolicyList/>
    </member>
    <member>
      <GroupId>AIDACKCEVSQ6C8EXAMPLE</GroupId>
      <AttachedManagedPolicies>
        <member>
          <PolicyName>PowerUserAccess</PolicyName>
          <PolicyArn>arn:aws:iam::aws:policy/PowerUserAccess</PolicyArn>
        </member>
      </AttachedManagedPolicies>
      <GroupName>Dev</GroupName>
      <Path>/</Path>
      <Arn>arn:aws:iam::123456789012:group/Dev</Arn>
      <CreateDate>2013-10-14T18:33:55Z</CreateDate>
      <GroupPolicyList/>
    </member>
    <member>
      <GroupId>AIDACKCEVSQ6C9EXAMPLE</GroupId>
      <AttachedManagedPolicies/>
      <GroupName>Finance</GroupName>
      <Path>/</Path>
      <Arn>arn:aws:iam::123456789012:group/Finance</Arn>
      <CreateDate>2013-10-14T18:57:48Z</CreateDate>
      <GroupPolicyList>
        <member>
          <PolicyName>policygen-201310141157</PolicyName>
          <PolicyDocument>
```

```
          {"Version":"2012-10-17","Statement":[{"Action":["aws-portal:*"],
          "Sid":"Stmt1381777017000","Resource":["*"],"Effect":"Allow"}]}
        </PolicyDocument>
      </member>
    </GroupPolicyList>
  </member>
</GroupDetailList>
<RoleDetailList>
  <member>
    <RolePolicyList/>
    <AttachedManagedPolicies>
      <member>
        <PolicyName>AmazonS3FullAccess</PolicyName>
        <PolicyArn>arn:aws:iam::aws:policy/AmazonS3FullAccess</PolicyArn>
      </member>
      <member>
        <PolicyName>AmazonDynamoDBFullAccess</PolicyName>
        <PolicyArn>arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess</PolicyArn>
      </member>
    </AttachedManagedPolicies>
    <InstanceProfileList>
      <member>
        <InstanceProfileName>EC2role</InstanceProfileName>
        <Roles>
          <member>
            <Path>/</Path>
            <Arn>arn:aws:iam::123456789012:role/EC2role</Arn>
            <RoleName>EC2role</RoleName>
            <AssumeRolePolicyDocument>
              {"Version":"2012-10-17","Statement":[{"Sid":"",
              "Effect":"Allow","Principal":{"Service":"ec2.amazonaws.com"},
              "Action":"sts:AssumeRole"}]}
            </AssumeRolePolicyDocument>
            <CreateDate>2014-07-30T17:09:20Z</CreateDate>
            <RoleId>AROAFP4BKI7Y7TEXAMPLE</RoleId>
            <RoleLastUsed>
              <LastUsedDate>2019-11-20T17:09:20Z</LastUsedDate>
              <Region>us-east-1</Region>
            </RoleLastUsed>
          </member>
        </Roles>
        <Path>/</Path>
        <Arn>arn:aws:iam::123456789012:instance-profile/EC2role</Arn>
        <InstanceProfileId>AIPAFFYRBHWXW2EXAMPLE</InstanceProfileId>
        <CreateDate>2014-07-30T17:09:20Z</CreateDate>
      </member>
    </InstanceProfileList>
    <Path>/</Path>
    <Arn>arn:aws:iam::123456789012:role/EC2role</Arn>
    <RoleName>EC2role</RoleName>
    <AssumeRolePolicyDocument>
      {"Version":"2012-10-17","Statement":[{"Sid":"","Effect":"Allow",
      "Principal":{"Service":"ec2.amazonaws.com"},
      "Action":"sts:AssumeRole"}]}
    </AssumeRolePolicyDocument>
    <CreateDate>2014-07-30T17:09:20Z</CreateDate>
    <RoleId>AROAFP4BKI7Y7TEXAMPLE</RoleId>      </member>
</RoleDetailList>
<Policies>
  <member>
    <PolicyName>create-update-delete-set-managed-policies</PolicyName>
    <DefaultVersionId>v1</DefaultVersionId>
    <PolicyId>ANPAJ2UCCR6DPCEXAMPLE</PolicyId>
    <Path>/</Path>
    <PolicyVersionList>
      <member>
```

```
        <Document>
          {"Version":"2012-10-17","Statement":{"Effect":"Allow",
          "Action":["iam:CreatePolicy","iam:CreatePolicyVersion",
          "iam:DeletePolicy","iam:DeletePolicyVersion","iam:GetPolicy",
          "iam:GetPolicyVersion","iam:ListPolicies",
          "iam:ListPolicyVersions","iam:SetDefaultPolicyVersion"],
          "Resource":"*"}}
        </Document>
        <IsDefaultVersion>true</IsDefaultVersion>
        <VersionId>v1</VersionId>
        <CreateDate>2015-02-06T19:58:34Z</CreateDate>
      </member>
    </PolicyVersionList>
    <Arn>
      arn:aws:iam::123456789012:policy/create-update-delete-set-managed-policies
    </Arn>
    <AttachmentCount>1</AttachmentCount>
    <CreateDate>2015-02-06T19:58:34Z</CreateDate>
    <IsAttachable>true</IsAttachable>
    <UpdateDate>2015-02-06T19:58:34Z</UpdateDate>
  </member>
  <member>
    <PolicyName>S3-read-only-specific-bucket</PolicyName>
    <DefaultVersionId>v1</DefaultVersionId>
    <PolicyId>ANPAJ4AE5446DAEXAMPLE</PolicyId>
    <Path>/</Path>
    <PolicyVersionList>
      <member>
        <Document>
          {"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
          ["s3:Get*","s3:List*"],"Resource":["arn:aws:s3:::example-bucket",
          "arn:aws:s3:::example-bucket/*"]}]}
        </Document>
        <IsDefaultVersion>true</IsDefaultVersion>
        <VersionId>v1</VersionId>
        <CreateDate>2015-01-21T21:39:41Z</CreateDate>
      </member>
    </PolicyVersionList>
    <Arn>arn:aws:iam::123456789012:policy/S3-read-only-specific-bucket</Arn>
    <AttachmentCount>1</AttachmentCount>
    <CreateDate>2015-01-21T21:39:41Z</CreateDate>
    <IsAttachable>true</IsAttachable>
    <UpdateDate>2015-01-21T23:39:41Z</UpdateDate>
  </member>
  <member>
    <PolicyName>AWSOpsWorksRole</PolicyName>
    <DefaultVersionId>v1</DefaultVersionId>
    <PolicyId>ANPAE376NQ77WV6KGJEBE</PolicyId>
    <Path>/service-role/</Path>
    <PolicyVersionList>
      <member>
        <Document>
          {"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
          ["cloudwatch:GetMetricStatistics","ec2:DescribeAccountAttributes",
          "ec2:DescribeAvailabilityZones","ec2:DescribeInstances",
          "ec2:DescribeKeyPairs","ec2:DescribeSecurityGroups","ec2:DescribeSubnets",
          "ec2:DescribeVpcs","elasticloadbalancing:DescribeInstanceHealth",
          "elasticloadbalancing:DescribeLoadBalancers","iam:GetRolePolicy",
          "iam:ListInstanceProfiles","iam:ListRoles","iam:ListUsers",
          "iam:PassRole","opsworks:*","rds:*"],"Resource":["*"]}]}
        </Document>
        <IsDefaultVersion>true</IsDefaultVersion>
        <VersionId>v1</VersionId>
        <CreateDate>2014-12-10T22:57:47Z</CreateDate>
      </member>
    </PolicyVersionList>
```

```
        <Arn>arn:aws:iam::aws:policy/service-role/AWSOpsWorksRole</Arn>
        <AttachmentCount>1</AttachmentCount>
        <CreateDate>2015-02-06T18:41:27Z</CreateDate>
        <IsAttachable>true</IsAttachable>
        <UpdateDate>2015-02-06T18:41:27Z</UpdateDate>
      </member>
      <member>
        <PolicyName>AmazonEC2FullAccess</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>ANPAE3QWE5YT46TQ34WLG</PolicyId>
        <Path>/</Path>
        <PolicyVersionList>
          <member>
            <Document>
              {"Version":"2012-10-17","Statement":[{"Action":"ec2:*",
              "Effect":"Allow","Resource":"*"},{"Effect":"Allow",
              "Action":"elasticloadbalancing:*","Resource":"*"},{"Effect":"Allow",
              "Action":"cloudwatch:*","Resource":"*"},{"Effect":"Allow",
              "Action":"autoscaling:*","Resource":"*"}]}
            </Document>
            <IsDefaultVersion>true</IsDefaultVersion>
            <VersionId>v1</VersionId>
            <CreateDate>2014-10-30T20:59:46Z</CreateDate>
          </member>
        </PolicyVersionList>
        <Arn>arn:aws:iam::aws:policy/AmazonEC2FullAccess</Arn>
        <AttachmentCount>1</AttachmentCount>
        <CreateDate>2015-02-06T18:40:15Z</CreateDate>
        <IsAttachable>true</IsAttachable>
        <UpdateDate>2015-02-06T18:40:15Z</UpdateDate>
      </member>
    </Policies>
  </GetAccountAuthorizationDetailsResult>
  <ResponseMetadata>
    <RequestId>92e79ae7-7399-11e4-8c85-4b53eEXAMPLE</RequestId>
  </ResponseMetadata>
</GetAccountAuthorizationDetailsResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAccountPasswordPolicy

Retrieves the password policy for the AWS account. For more information about using a password policy, go to Managing an IAM Password Policy.

Response Elements

The following element is returned by the service.

PasswordPolicy

A structure that contains details about the account's password policy.

Type: PasswordPolicy (p. 454) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetAccountPasswordPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=GetAccountPasswordPolicy
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetAccountPasswordPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetAccountPasswordPolicyResult>
    <PasswordPolicy>
      <AllowUsersToChangePassword>true</AllowUsersToChangePassword>
      <RequireUppercaseCharacters>true</RequireUppercaseCharacters>
      <RequireSymbols>true</RequireSymbols>
      <ExpirePasswords>false</ExpirePasswords>
      <PasswordReusePrevention>12</PasswordReusePrevention>
```

```
      <RequireLowercaseCharacters>true</RequireLowercaseCharacters>
      <MaxPasswordAge>90</MaxPasswordAge>
      <HardExpiry>false</HardExpiry>
      <RequireNumbers>true</RequireNumbers>
      <MinimumPasswordLength>12</MinimumPasswordLength>
    </PasswordPolicy>
  </GetAccountPasswordPolicyResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</GetAccountPasswordPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAccountSummary

Retrieves information about IAM entity usage and IAM quotas in the AWS account.

For information about limitations on IAM entities, see Limitations on IAM Entities in the *IAM User Guide*.

Response Elements

The following element is returned by the service.

SummaryMap , SummaryMap.entry.N.key (key), SummaryMap.entry.N.value (value)

A set of key–value pairs containing information about IAM entity usage and IAM quotas.

Type: String to integer map

Valid Keys: `Users | UsersQuota | Groups | GroupsQuota | ServerCertificates | ServerCertificatesQuota | UserPolicySizeQuota | GroupPolicySizeQuota | GroupsPerUserQuota | SigningCertificatesPerUserQuota | AccessKeysPerUserQuota | MFADevices | MFADevicesInUse | AccountMFAEnabled | AccountAccessKeysPresent | AccountSigningCertificatesPresent | AttachedPoliciesPerGroupQuota | AttachedPoliciesPerRoleQuota | AttachedPoliciesPerUserQuota | Policies | PoliciesQuota | PolicySizeQuota | PolicyVersionsInUse | PolicyVersionsInUseQuota | VersionsPerPolicyQuota | GlobalEndpointTokenVersion`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetAccountSummary.

Sample Request

```
https://iam.amazonaws.com/?Action=GetAccountSummary
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetAccountSummaryResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetAccountSummaryResult>
    <SummaryMap>
```

```
<entry>
  <key>Users</key>
  <value>32</value>
</entry>
<entry>
  <key>GroupPolicySizeQuota</key>
  <value>10240</value>
</entry>
<entry>
  <key>PolicyVersionsInUseQuota</key>
  <value>10000</value>
</entry>
<entry>
  <key>ServerCertificatesQuota</key>
  <value>20</value>
</entry>
<entry>
  <key>AccountSigningCertificatesPresent</key>
  <value>0</value>
</entry>
<entry>
  <key>AccountAccessKeysPresent</key>
  <value>0</value>
</entry>
<entry>
  <key>Groups</key>
  <value>7</value>
</entry>
<entry>
  <key>UsersQuota</key>
  <value>150</value>
</entry>
<entry>
  <key>RolePolicySizeQuota</key>
  <value>2048</value>
</entry>
<entry>
  <key>UserPolicySizeQuota</key>
  <value>10240</value>
</entry>
<entry>
  <key>GroupsPerUserQuota</key>
  <value>10</value>
</entry>
<entry>
  <key>AssumeRolePolicySizeQuota</key>
  <value>2048</value>
</entry>
<entry>
  <key>AttachedPoliciesPerGroupQuota</key>
  <value>2</value>
</entry>
<entry>
  <key>Roles</key>
  <value>18</value>
</entry>
<entry>
  <key>VersionsPerPolicyQuota</key>
  <value>5</value>
</entry>
<entry>
  <key>GroupsQuota</key>
  <value>50</value>
</entry>
<entry>
  <key>PolicySizeQuota</key>
```

```
      <value>5120</value>
    </entry>
    <entry>
      <key>Policies</key>
      <value>22</value>
    </entry>
    <entry>
      <key>RolesQuota</key>
      <value>250</value>
    </entry>
    <entry>
      <key>ServerCertificates</key>
      <value>1</value>
    </entry>
    <entry>
      <key>AttachedPoliciesPerRoleQuota</key>
      <value>2</value>
    </entry>
    <entry>
      <key>MFADevicesInUse</key>
      <value>4</value>
    </entry>
    <entry>
      <key>PoliciesQuota</key>
      <value>1000</value>
    </entry>
    <entry>
      <key>AccountMFAEnabled</key>
      <value>1</value>
    </entry>
    <entry>
      <key>Providers</key>
      <value>3</value>
    </entry>
    <entry>
      <key>InstanceProfilesQuota</key>
      <value>100</value>
    </entry>
    <entry>
      <key>MFADevices</key>
      <value>4</value>
    </entry>
    <entry>
      <key>AccessKeysPerUserQuota</key>
      <value>2</value>
    </entry>
    <entry>
      <key>AttachedPoliciesPerUserQuota</key>
      <value>2</value>
    </entry>
    <entry>
      <key>SigningCertificatesPerUserQuota</key>
      <value>2</value>
    </entry>
    <entry>
      <key>PolicyVersionsInUse</key>
      <value>27</value>
    </entry>
    <entry>
      <key>InstanceProfiles</key>
      <value>12</value>
    </entry>
    <entry>
      <key>GlobalEndpointTokenVersion</key>
      <value>2</value>
    </entry>
```

```
    </SummaryMap>
  </GetAccountSummaryResult>
  <ResponseMetadata>
    <RequestId>85cb9b90-ac28-11e4-a88d-97964EXAMPLE</RequestId>
  </ResponseMetadata>
</GetAccountSummaryResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetContextKeysForCustomPolicy

Gets a list of all of the context keys referenced in the input policies. The policies are supplied as a list of one or more strings. To get the context keys from policies associated with an IAM user, group, or role, use GetContextKeysForPrincipalPolicy (p. 159).

Context keys are variables maintained by AWS and its services that provide details about the context of an API query request. Context keys can be evaluated by testing against a value specified in an IAM policy. Use `GetContextKeysForCustomPolicy` to understand what key names and values you must supply when you call SimulateCustomPolicy (p. 338). Note that all parameters are shown in unencoded form here for clarity but must be URL encoded to be included as a part of a real HTML request.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyInputList.member.N

A list of policies for which you want the list of context keys referenced in those policies. Each document is specified as a string containing the complete, valid JSON text of an IAM policy.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

Response Elements

The following element is returned by the service.

ContextKeyNames.member.N

The list of context keys that are referenced in the input policies.

Type: Array of strings

Length Constraints: Minimum length of 5. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

Examples

Example 1

In the following example, the request includes a policy as a string. The response shows that the policies use both `aws:CurrentTime` and `aws:username`.

Sample Request

```
https://iam.amazonaws.com/?Action=GetContextKeysForCustomPolicy
&PolicyInputList.member.1='{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-2:ACCOUNT-ID-WITHOUT-HYPHENS:table/
${aws:username}",
    "Condition":{"DateGreaterThan":{"aws:CurrentTime":"2015-08-16T12:00:00Z"}}
  }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetContextKeysForCustomPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetContextKeysForCustomPolicyResult>
    <ContextKeyNames>
      <member>aws:username</member>
      <member>aws:CurrentTime</member>
    </ContextKeyNames>
  </GetContextKeysForCustomPolicyResult>
  <ResponseMetadata>
    <RequestId>d6808605-4c06-11e5-b121-bd8c7EXAMPLE</RequestId>
  </ResponseMetadata>
</GetContextKeysForCustomPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetContextKeysForPrincipalPolicy

Gets a list of all of the context keys referenced in all the IAM policies that are attached to the specified IAM entity. The entity can be an IAM user, group, or role. If you specify a user, then the request also includes all of the policies attached to groups that the user is a member of.

You can optionally include a list of one or more additional policies, specified as strings. If you want to include *only* a list of policies by string, use GetContextKeysForCustomPolicy (p. 156) instead.

Note: This API discloses information about the permissions granted to other users. If you do not want users to see other user's permissions, then consider allowing them to use GetContextKeysForCustomPolicy (p. 156) instead.

Context keys are variables maintained by AWS and its services that provide details about the context of an API query request. Context keys can be evaluated by testing against a value in an IAM policy. Use GetContextKeysForPrincipalPolicy (p. 159) to understand what key names and values you must supply when you call SimulatePrincipalPolicy (p. 346).

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyInputList.member.N

An optional list of additional policies for which you want the list of context keys that are referenced.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

PolicySourceArn

The ARN of a user, group, or role whose policies contain the context keys that you want listed. If you specify a user, the list includes context keys that are found in all policies that are attached to the user. The list also includes all groups that the user is a member of. If you pick a group or a role, then it includes only those context keys that are found in policies attached to that entity. Note that all parameters are shown in unencoded form here for clarity, but must be URL encoded to be included as a part of a real HTML request.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following element is returned by the service.

ContextKeyNames.member.N

The list of context keys that are referenced in the input policies.

Type: Array of strings

Length Constraints: Minimum length of 5. Maximum length of 256.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example 1

In the following example, the request includes the ARN for a user named Dave, and includes one additional policy. This enables you to evaluate the impact that policy would have if you attached it to the user. The response includes five context keys, four from policies attached to the user and one from the added policy. Note that all parameters are shown in unencoded form here for clarity, but must be URL encoded to be included as a part of a real HTML request.

Sample Request

```
https://iam.amazonaws.com/?Action=GetContextKeysForPrincipalPolicy
&PolicySourceArn=arn:aws:iam::123456789012:user/Dave
&PolicyInputList.member.1='{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-2:ACCOUNT-ID-WITHOUT-HYPHENS:table/
${aws:username}",
    "Condition":{"DateGreaterThan":{"aws:CurrentTime":"2015-08-16T12:00:00Z"}}
  }
```

```
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetContextKeysForPrincipalPolicyResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetContextKeysForPrincipalPolicyResult>
    <ContextKeyNames>
      <member>aws:username</member>
      <member>aws:CurrentTime</member>
      <member>aws:username</member>
      <member>ec2:InstanceType</member>
      <member>aws:CurrentTime</member>
    </ContextKeyNames>
  </GetContextKeysForPrincipalPolicyResult>
  <ResponseMetadata>
    <RequestId>7ec754ab-4c08-11e5-b121-bd8c7EXAMPLE</RequestId>
  </ResponseMetadata>
</GetContextKeysForPrincipalPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetCredentialReport

Retrieves a credential report for the AWS account. For more information about the credential report, see Getting Credential Reports in the *IAM User Guide*.

Response Elements

The following elements are returned by the service.

Content

Contains the credential report. The report is Base64-encoded.

Type: Base64-encoded binary data object

GeneratedTime

The date and time when the credential report was created, in ISO 8601 date-time format.

Type: Timestamp

ReportFormat

The format (MIME type) of the credential report.

Type: String

Valid Values: `text/csv`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ReportExpired

The request was rejected because the most recent credential report has expired. To generate a new credential report, use GenerateCredentialReport (p. 132). For more information about credential report expiration, see Getting Credential Reports in the *IAM User Guide*.

HTTP Status Code: 410

ReportInProgress

The request was rejected because the credential report is still being generated.

HTTP Status Code: 404

ReportNotPresent

The request was rejected because the credential report does not exist. To generate a credential report, use GenerateCredentialReport (p. 132).

HTTP Status Code: 410

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetCredentialReport.

Sample Request

```
https://iam.amazonaws.com/?Action=GetCredentialReport
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetCredentialReportResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetCredentialReportResult>
  <Content>BASE-64 ENCODED FILE CONTENTS</Content>
  <ReportFormat>text/csv</ReportFormat>
  <GeneratedTime>2014-08-28T21:42:50Z</GeneratedTime>
</GetCredentialReportResult>
<ResponseMetadata>
  <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</GetCredentialReportResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetGroup

Returns a list of IAM users that are in the specified IAM group. You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name of the group.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

Group

A structure that contains details about the group.

Type: Group (p. 440) object

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Users.member.N

A list of users in the group.

Type: Array of User (p. 499) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetGroup.

Sample Request

```
https://iam.amazonaws.com/?Action=GetGroup
&GroupName=Admins
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <GetGroupResult>
    <Group>
       <Path>/</Path>
       <GroupName>Admins</GroupName>
       <GroupId>AGPACKCEVSQ6C2EXAMPLE</GroupId>
       <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
    </Group>
    <Users>
       <member>
          <Path>/division_abc/subdivision_xyz/</Path>
          <UserName>Bob</UserName>
          <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
          <Arn>
          arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/Bob
          </Arn>
       </member>
       <member>
          <Path>/division_abc/subdivision_xyz/</Path>
          <UserName>Susan</UserName>
          <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
          <Arn>
          arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/Susan
          </Arn>
       </member>
    </Users>
    <IsTruncated>false</IsTruncated>
 </GetGroupResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</GetGroupResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetGroupPolicy

Retrieves the specified inline policy document that is embedded in the specified IAM group.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

An IAM group can also have managed policies attached to it. To retrieve a managed policy document that is attached to a group, use GetPolicy (p. 182) to determine the policy's default version, then use GetPolicyVersion (p. 185) to retrieve the policy document.

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name of the group the policy is associated with.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

PolicyName

The name of the policy document to get.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

GroupName

The group the policy is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

PolicyDocument

The policy document.

IAM stores policies in JSON format. However, resources that were created using AWS CloudFormation templates can be formatted in YAML. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

PolicyName

The name of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetGroupPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=GetGroupPolicy
&GroupName=Admins
&PolicyName=AdminRoot
&AUTHPARAMS
```

Sample Response

```
<GetGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <GetGroupPolicyResult>
    <GroupName>Admins</GroupName>
    <PolicyName>AdminRoot</PolicyName>
    <PolicyDocument>
    {"Version":"2012-10-17","Statement":{"Effect":"Allow","Action":"*","Resource":"*"}}
    </PolicyDocument>
 </GetGroupPolicyResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</GetGroupPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetInstanceProfile

Retrieves information about the specified instance profile, including the instance profile's path, GUID, ARN, and role. For more information about instance profiles, see About Instance Profiles in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

InstanceProfileName

The name of the instance profile to get information about.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

InstanceProfile

A structure containing details about the instance profile.

Type: InstanceProfile (p. 444) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetInstanceProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=GetInstanceProfile
&InstanceProfileName=Webserver
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetInstanceProfileResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetInstanceProfileResult>
  <InstanceProfile>
    <InstanceProfileId>AIPAD5ARO2C5EXAMPLE3G</InstanceProfileId>
    <Roles>
      <member>
        <Path>/application_abc/component_xyz/</Path>
        <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/S3Access</Arn>
        <RoleName>S3Access</RoleName>
        <AssumeRolePolicyDocument>
          {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
          "Principal":{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
        </AssumeRolePolicyDocument>
        <CreateDate>2012-05-09T15:45:35Z</CreateDate>
        <RoleId>AROACVYKSVTSZFEXAMPLE</RoleId>
      </member>
    </Roles>
    <InstanceProfileName>Webserver</InstanceProfileName>
    <Path>/application_abc/component_xyz/</Path>
    <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/component_xyz/
Webserver</Arn>
    <CreateDate>2012-05-09T16:11:10Z</CreateDate>
  </InstanceProfile>
</GetInstanceProfileResult>
<ResponseMetadata>
  <RequestId>37289fda-99f2-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</GetInstanceProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

GetLoginProfile

Retrieves the user name and password-creation date for the specified IAM user. If the user has not been assigned a password, the operation returns a 404 (`NoSuchEntity`) error.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

UserName

The name of the user whose login profile you want to retrieve.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

LoginProfile

A structure containing the user name and password create date for the user.

Type: LoginProfile (p. 447) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetLoginProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=GetLoginProfile
&UserName=Bob
&AUTHPARAMS
```

Sample Response

```
<GetLoginProfileResponse>
 <GetLoginProfileResult>
    <LoginProfile>
       <UserName>Bob</UserName>
       <CreateDate>2011-09-19T23:00:56Z</CreateDate>
    </LoginProfile>
 </GetLoginProfileResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</GetLoginProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetOpenIDConnectProvider

Returns information about the specified OpenID Connect (OIDC) provider resource object in IAM.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the OIDC provider resource object in IAM to get information for. You can get a list of OIDC provider resource ARNs by using the ListOpenIDConnectProviders (p. 260) operation.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following elements are returned by the service.

ClientIDList.member.N

A list of client IDs (also known as audiences) that are associated with the specified IAM OIDC provider resource object. For more information, see CreateOpenIDConnectProvider (p. 39).

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 255.

CreateDate

The date and time when the IAM OIDC provider resource object was created in the AWS account.

Type: Timestamp

ThumbprintList.member.N

A list of certificate thumbprints that are associated with the specified IAM OIDC provider resource object. For more information, see CreateOpenIDConnectProvider (p. 39).

Type: Array of strings

Length Constraints: Fixed length of 40.

Url

The URL that the IAM OIDC provider resource object is associated with. For more information, see CreateOpenIDConnectProvider (p. 39).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetOpenIDConnectProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=GetOpenIDConnectProvider
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetOpenIDConnectProviderResult>
    <ThumbprintList>
      <member>c3768084dfb3d2b68b7897bf5f565da8eEXAMPLE</member>
    </ThumbprintList>
    <CreateDate>2014-10-09T03:32:51.398Z</CreateDate>
    <ClientIDList>
      <member>my-application-ID</member>
    </ClientIDList>
    <Url>server.example.com</Url>
  </GetOpenIDConnectProviderResult>
  <ResponseMetadata>
    <RequestId>2c91531b-4f65-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</GetOpenIDConnectProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetOrganizationsAccessReport

Retrieves the service last accessed data report for AWS Organizations that was previously generated using the `GenerateOrganizationsAccessReport (p. 134)` operation. This operation retrieves the status of your report job and the report contents.

Depending on the parameters that you passed when you generated the report, the data returned could include different information. For details, see GenerateOrganizationsAccessReport (p. 134).

To call this operation, you must be signed in to the master account in your organization. SCPs must be enabled for your organization root. You must have permissions to perform this operation. For more information, see Refining Permissions Using Service Last Accessed Data in the *IAM User Guide*.

For each service that principals in an account (root users, IAM users, or IAM roles) could access using SCPs, the operation returns details about the most recent access attempt. If there was no attempt, the service is listed without details about the most recent attempt to access the service. If the operation fails, it returns the reason that it failed.

By default, the list is sorted by service namespace.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

JobId

The identifier of the request generated by the GenerateOrganizationsAccessReport (p. 134) operation.

Type: String

Length Constraints: Fixed length of 36.

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

SortKey

The key that is used to sort the results. If you choose the namespace key, the results are returned in alphabetical order. If you choose the time key, the results are sorted numerically by the date and time.

Type: String

Valid Values: `SERVICE_NAMESPACE_ASCENDING | SERVICE_NAMESPACE_DESCENDING | LAST_AUTHENTICATED_TIME_ASCENDING | LAST_AUTHENTICATED_TIME_DESCENDING`

Required: No

Response Elements

The following elements are returned by the service.

AccessDetails.member.N

An object that contains details about the most recent attempt to access the service.

Type: Array of AccessDetail (p. 421) objects

ErrorDetails

Contains information about the reason that the operation failed.

This data type is used as a response element in the GetOrganizationsAccessReport (p. 178), GetServiceLastAccessedDetails (p. 199), and GetServiceLastAccessedDetailsWithEntities (p. 204) operations.

Type: ErrorDetails (p. 436) object

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

JobCompletionDate

The date and time, in ISO 8601 date-time format, when the generated report job was completed or failed.

This field is null if the job is still in progress, as indicated by a job status value of `IN_PROGRESS`.

Type: Timestamp

JobCreationDate

The date and time, in ISO 8601 date-time format, when the report job was created.

Type: Timestamp

JobStatus

The status of the job.

Type: String

Valid Values: `IN_PROGRESS | COMPLETED | FAILED`

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `[\u0020-\u00FF]+`

NumberOfServicesAccessible

The number of services that the applicable SCPs allow account principals to access.

Type: Integer

NumberOfServicesNotAccessed

The number of services that account principals are allowed but did not attempt to access.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

This example illustrates one usage of GetOrganizationsAccessReport.

Sample Request

```
https://iam.amazonaws.com/?Action=GetOrganizationsAccessReport
&JobId=examplea-1234-b567-cde8-90fg123abcd4
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<IsTruncated>false</IsTruncated>
```

```
<JobCompletionDate>2019-06-18T19:47:35.241Z</JobCompletionDate>
<JobCreationDate>2019-06-18T19:47:31.466Z</JobCreationDate>
<JobStatus>COMPLETED</JobStatus>
<NumberOfServicesAccessible>3</NumberOfServicesAccessible>
<NumberOfServicesNotAccessed>1</NumberOfServicesNotAccessed>
<AccessDetails>
    <member>
        <EntityPath>o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-1a2b3c-
k9l8m7n6o5example/111122223333</EntityPath>
        <LastAuthenticatedTime>2019-05-25T16:29:52Z</LastAuthenticatedTime>
        <Region>us-west-2</Region>
        <ServiceName>Amazon DynamoDB</ServiceName>
        <ServiceNamespace>dynamodb</ServiceNamespace>
        <TotalAuthenticatedEntities>2</TotalAuthenticatedEntities>
    </member>
    <member>
        <EntityPath>o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-1a2b3c-
k9l8m7n6o5example/123456789012</EntityPath>
        <LastAuthenticatedTime>2019-06-15T13:12:06Z</LastAuthenticatedTime>
        <Region>us-east-1</Region>
        <ServiceName>AWS Identity and Access Management</ServiceName>
        <ServiceNamespace>iam</ServiceNamespace>
        <TotalAuthenticatedEntities>5</TotalAuthenticatedEntities>
    </member>
    <member>
        <ServiceName>Amazon Simple Storage Service</ServiceName>
        <ServiceNamespace>s3</ServiceNamespace>
        <TotalAuthenticatedEntities>0</TotalAuthenticatedEntities>
    </member>
</AccessDetails>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetPolicy

Retrieves information about the specified managed policy, including the policy's default version and the total number of IAM users, groups, and roles to which the policy is attached. To retrieve the list of the specific users, groups, and roles that the policy is attached to, use the ListEntitiesForPolicy (p. 238) API. This API returns metadata about the policy. To retrieve the actual policy document for a specific version of the policy, use GetPolicyVersion (p. 185).

This API retrieves information about managed policies. To retrieve information about an inline policy that is embedded with an IAM user, group, or role, use the GetUserPolicy (p. 217), GetGroupPolicy (p. 167), or GetRolePolicy (p. 190) API.

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the managed policy that you want information about.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following element is returned by the service.

Policy

A structure containing details about the policy.

Type: Policy (p. 457) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=GetPolicy
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetPolicyResult>
    <Policy>
      <PolicyName>S3-read-only-example-bucket</PolicyName>
      <Description>Allows read-only access to the example bucket</Description>
      <DefaultVersionId>v1</DefaultVersionId>
      <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
      <Path>/</Path>
      <Arn>arn:aws:iam::123456789012:policy/S3-read-only-example-bucket</Arn>
      <AttachmentCount>9</AttachmentCount>
      <CreateDate>2014-09-15T17:36:14Z</CreateDate>
      <UpdateDate>2014-09-15T20:31:47Z</UpdateDate>
    </Policy>
  </GetPolicyResult>
  <ResponseMetadata>
    <RequestId>684f0917-3d22-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</GetPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetPolicyVersion

Retrieves information about the specified version of the specified managed policy, including the policy document.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

To list the available versions for a policy, use ListPolicyVersions (p. 270).

This API retrieves information about managed policies. To retrieve information about an inline policy that is embedded in a user, group, or role, use the GetUserPolicy (p. 217), GetGroupPolicy (p. 167), or GetRolePolicy (p. 190) API.

For more information about the types of policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the managed policy that you want information about.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

VersionId

Identifies the policy version to retrieve.

This parameter allows (through its regex pattern) a string of characters that consists of the lowercase letter 'v' followed by one or two digits, and optionally followed by a period '.' and a string of letters and digits.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: Yes

Response Elements

The following element is returned by the service.

PolicyVersion

A structure containing details about the policy version.

Type: PolicyVersion (p. 466) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetPolicyVersion.

Sample Request

```
https://iam.amazonaws.com/?Action=GetPolicyVersion
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&VersionId=v1
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetPolicyVersionResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetPolicyVersionResult>
    <PolicyVersion>
      <Document>
      {"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["s3:Get*","s3:List*"],
      "Resource":["arn:aws:s3:::EXAMPLE-BUCKET","arn:aws:s3:::EXAMPLE-BUCKET/*"]}]}
      </Document>
      <IsDefaultVersion>true</IsDefaultVersion>
      <VersionId>v1</VersionId>
      <CreateDate>2014-09-15T20:31:47Z</CreateDate>
    </PolicyVersion>
```

```
  </GetPolicyVersionResult>
  <ResponseMetadata>
    <RequestId>d472f28e-3d23-11e4-a4a0-cffb9EXAMPLE</RequestId>
  </ResponseMetadata>
</GetPolicyVersionResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRole

Retrieves information about the specified role, including the role's path, GUID, ARN, and the role's trust policy that grants permission to assume the role. For more information about roles, see Working with Roles.

Note
Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

RoleName

The name of the IAM role to get information about.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

Role

A structure containing details about the IAM role.

Type: Role (p. 471) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetRole.

Sample Request

```
https://iam.amazonaws.com/?Action=GetRole
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetRoleResult>
  <Role>
    <Path>/application_abc/component_xyz/</Path>
    <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/S3Access</Arn>
    <RoleName>S3Access</RoleName>
    <AssumeRolePolicyDocument>
      {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
      "Principal":{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
    </AssumeRolePolicyDocument>
    <CreateDate>2012-05-08T23:34:01Z</CreateDate>
    <RoleId>AROADBQP57FF2AEXAMPLE</RoleId>
    <RoleLastUsed>
      <LastUsedDate>2019-11-20T17:09:20Z</LastUsedDate>
      <Region>us-east-1</Region>
    </RoleLastUsed>
  </Role>
</GetRoleResult>
<ResponseMetadata>
  <RequestId>df37e965-9967-11e1-a4c3-270EXAMPLE04</RequestId>
</ResponseMetadata>
</GetRoleResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetRolePolicy

Retrieves the specified inline policy document that is embedded with the specified IAM role.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

An IAM role can also have managed policies attached to it. To retrieve a managed policy document that is attached to a role, use GetPolicy (p. 182) to determine the policy's default version, then use GetPolicyVersion (p. 185) to retrieve the policy document.

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For more information about roles, see Using Roles to Delegate Permissions and Federate Identities.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyName

The name of the policy document to get.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

RoleName

The name of the role associated with the policy.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

PolicyDocument

The policy document.

IAM stores policies in JSON format. However, resources that were created using AWS CloudFormation templates can be formatted in YAML. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

PolicyName

The name of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

RoleName

The role the policy is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetRolePolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=GetRolePolicy
```

```
&PolicyName=S3AccessPolicy
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetRolePolicyResult>
  <PolicyName>S3AccessPolicy</PolicyName>
  <RoleName>S3Access</RoleName>
  <PolicyDocument>
  {"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":["s3:*"],"Resource":
["*"]}]}
  </PolicyDocument>
</GetRolePolicyResult>
<ResponseMetadata>
  <RequestId>7e7cd8bc-99ef-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</GetRolePolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetSAMLProvider

Returns the SAML provider metadocument that was uploaded when the IAM SAML provider resource object was created or updated.

Note
This operation requires Signature Version 4.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

SAMLProviderArn

The Amazon Resource Name (ARN) of the SAML provider resource object in IAM to get information about.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following elements are returned by the service.

CreateDate

The date and time when the SAML provider was created.

Type: Timestamp

SAMLMetadataDocument

The XML metadata document that includes information about an identity provider.

Type: String

Length Constraints: Minimum length of 1000. Maximum length of 10000000.

ValidUntil

The expiration date and time for the SAML provider.

Type: Timestamp

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetSAMLProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=GetSAMLProvider
&Name=arn:aws:iam::123456789012:saml-provider/MyUniversity
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetSAMLProviderResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetSAMLProviderResult>
  <CreateDate>2012-05-09T16:27:11Z</CreateDate>
  <ValidUntil>2015-12-31T211:59:59Z</ValidUntil>
  <SAMLMetadataDocument>Pd9fexDssTkRgGNqs...DxptfEs==</SAMLMetadataDocument>
</GetSAMLProviderResult>
<ResponseMetadata>
  <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</GetSAMLProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetServerCertificate

Retrieves information about the specified server certificate stored in IAM.

For more information about working with server certificates, see Working with Server Certificates in the *IAM User Guide*. This topic includes a list of AWS services that can use the server certificates that you manage with IAM.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ServerCertificateName

The name of the server certificate you want to retrieve information about.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

ServerCertificate

A structure containing details about the server certificate.

Type: ServerCertificate (p. 480) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetServerCertificate.

Sample Request

```
https://iam.amazonaws.com/?Action=GetServerCertificate
&ServerCertificateName=ProdServerCert
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetServerCertificateResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<GetServerCertificateResult>
  <ServerCertificate>
    <ServerCertificateMetadata>
      <ServerCertificateName>ProdServerCert</ServerCertificateName>
      <Path>/company/servercerts/</Path>
      <Arn>arn:aws:iam::123456789012:server-certificate/company/servercerts/
ProdServerCert</Arn>
      <UploadDate>2010-05-08T01:02:03.004Z</UploadDate>
      <ServerCertificateId>ASCACKCEVSQ6C2EXAMPLE</ServerCertificateId>
      <Expiration>2012-05-08T01:02:03.004Z</Expiration>
    </ServerCertificateMetadata>
    <CertificateBody>
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxND10c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
    </CertificateBody>
  </ServerCertificate>
</GetServerCertificateResult>
<ResponseMetadata>
  <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
</ResponseMetadata>
</GetServerCertificateResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetServiceLastAccessedDetails

Retrieves a service last accessed report that was created using the `GenerateServiceLastAccessedDetails` operation. You can use the `JobId` parameter in `GetServiceLastAccessedDetails` to retrieve the status of your report job. When the report is complete, you can retrieve the generated report. The report includes a list of AWS services that the resource (user, group, role, or managed policy) can access.

> **Note**
> Service last accessed data does not use other policy types when determining whether a resource could access a service. These other policy types include resource-based policies, access control lists, AWS Organizations policies, IAM permissions boundaries, and AWS STS assume role policies. It only applies permissions policy logic. For more about the evaluation of policy types, see Evaluating Policies in the *IAM User Guide*.

For each service that the resource could access using permissions policies, the operation returns details about the most recent access attempt. If there was no attempt, the service is listed without details about the most recent attempt to access the service. If the operation fails, the `GetServiceLastAccessedDetails` operation returns the reason that it failed.

The `GetServiceLastAccessedDetails` operation returns a list of services. This list includes the number of entities that have attempted to access the service and the date and time of the last attempt. It also returns the ARN of the following entity, depending on the resource ARN that you used to generate the report:

- **User** – Returns the user ARN that you used to generate the report
- **Group** – Returns the ARN of the group member (user) that last attempted to access the service
- **Role** – Returns the role ARN that you used to generate the report
- **Policy** – Returns the ARN of the user or role that last used the policy to attempt to access the service

By default, the list is sorted by service namespace.

If you specified `ACTION_LEVEL` granularity when you generated the report, this operation returns service and action last accessed data. This includes the most recent access attempt for each tracked action within a service. Otherwise, this operation returns only service data.

For more information about service and action last accessed data, see Reducing Permissions Using Service Last Accessed Data in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

JobId

The ID of the request generated by the GenerateServiceLastAccessedDetails (p. 138) operation. The `JobId` returned by `GenerateServiceLastAccessedDetail` must be used by the same role within a session, or by the same user when used to call `GetServiceLastAccessedDetail`.

Type: String

Length Constraints: Fixed length of 36.

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

Error

An object that contains details about the reason the operation failed.

Type: ErrorDetails (p. 436) object

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

JobCompletionDate

The date and time, in ISO 8601 date-time format, when the generated report job was completed or failed.

This field is null if the job is still in progress, as indicated by a job status value of `IN_PROGRESS`.

Type: Timestamp

JobCreationDate

The date and time, in ISO 8601 date-time format, when the report job was created.

Type: Timestamp

JobStatus

The status of the job.

Type: String

Valid Values: `IN_PROGRESS | COMPLETED | FAILED`

JobType

The type of job. Service jobs return information about when each service was last accessed. Action jobs also include information about when tracked actions within the service were last accessed.

Type: String

Valid Values: `SERVICE_LEVEL | ACTION_LEVEL`

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

ServicesLastAccessed.member.N

A `ServiceLastAccessed` object that contains details about the most recent attempt to access the service.

Type: Array of ServiceLastAccessed (p. 483) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

This example illustrates one usage of GetServiceLastAccessedDetails.

Sample Request

```
https://iam.amazonaws.com/?Action=GetServiceLastAccessedDetails
&JobId=examplef-1305-c245-eba4-71fe298bcda7
```

```
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<IsTruncated>false</IsTruncated>
<JobCompletionDate>2018-10-24T19:47:35.241Z</JobCompletionDate>
<JobCreationDate>2018-10-24T19:47:31.466Z</JobCreationDate>
<JobStatus>COMPLETED</JobStatus>
<ServicesLastAccessed>
    <member>
        <ServiceName>AWS Identity and Access Management</ServiceName>
        <ServiceNamespace>iam</ServiceNamespace>
        <TotalAuthenticatedEntities>0</TotalAuthenticatedEntities>
    </member>
    <member>
        <LastAuthenticated>2018-10-24T19:11:00Z</LastAuthenticated>
        <LastAuthenticatedEntity>arn:aws:iam::123456789012:user/AWSExampleUser01</
LastAuthenticatedEntity>
        <LastAuthenticatedRegion>us-east-1</LastAuthenticatedRegion>
        <ServiceName>Amazon Simple Storage Service</ServiceName>
        <ServiceNamespace>s3</ServiceNamespace>
        <TotalAuthenticatedEntities>3</TotalAuthenticatedEntities>
        <TrackedActionsLastAccessed>
            <member>
                <ActionName>CreateBucket</ActionName>
                <LastAccessedEntity>arn:aws:iam::123456789012:user/AWSExampleUser01</
LastAccessedEntity>
                <LastAccessedRegion>us-east-1</LastAccessedRegion>
                <LastAccessedTime>2018-10-24T19:11:00Z</LastAccessedTime>
            </member>
            <member>
                <ActionName>PutBucketAcl</ActionName>
                <LastAccessedEntity></LastAccessedEntity>
                <LastAccessedRegion></LastAccessedRegion>
                <LastAccessedTime></LastAccessedTime>
            </member>
            <member>
                <ActionName>ListBucket</ActionName>
                <LastAccessedEntity>arn:aws:iam::123456789012:user/AWSExampleUser01</
LastAccessedEntity>
                <LastAccessedRegion>us-east-1</LastAccessedRegion>
                <LastAccessedTime>2018-10-24T19:10:53Z</LastAccessedTime>
            </member>
        </TrackedActionsLastAccessed>
    </member>
</ServicesLastAccessed>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

GetServiceLastAccessedDetailsWithEntities

After you generate a group or policy report using the `GenerateServiceLastAccessedDetails` operation, you can use the `JobId` parameter in `GetServiceLastAccessedDetailsWithEntities`. This operation retrieves the status of your report job and a list of entities that could have used group or policy permissions to access the specified service.

- **Group** – For a group report, this operation returns a list of users in the group that could have used the group's policies in an attempt to access the service.
- **Policy** – For a policy report, this operation returns a list of entities (users or roles) that could have used the policy in an attempt to access the service.

You can also use this operation for user or role reports to retrieve details about those entities.

If the operation fails, the `GetServiceLastAccessedDetailsWithEntities` operation returns the reason that it failed.

By default, the list of associated entities is sorted by date, with the most recent access listed first.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

JobId

The ID of the request generated by the `GenerateServiceLastAccessedDetails` operation.

Type: String

Length Constraints: Fixed length of 36.

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

ServiceNamespace

The service namespace for an AWS service. Provide the service namespace to learn when the IAM entity last attempted to access the specified service.

To learn the service namespace for a service, go to Actions, Resources, and Condition Keys for AWS Services in the *IAM User Guide*. Choose the name of the service to view details for that service. In the first paragraph, find the service prefix. For example, `(service prefix: a4b)`. For more information about service namespaces, see AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w-]*`

Required: Yes

Response Elements

The following elements are returned by the service.

EntityDetailsList.member.N

An `EntityDetailsList` object that contains details about when an IAM entity (user or role) used group or policy permissions in an attempt to access the specified AWS service.

Type: Array of EntityDetails (p. 433) objects

Error

An object that contains details about the reason the operation failed.

Type: ErrorDetails (p. 436) object

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

JobCompletionDate

The date and time, in ISO 8601 date-time format, when the generated report job was completed or failed.

This field is null if the job is still in progress, as indicated by a job status value of `IN_PROGRESS`.

Type: Timestamp

JobCreationDate

The date and time, in ISO 8601 date-time format, when the report job was created.

Type: Timestamp

JobStatus

The status of the job.

Type: String

Valid Values: `IN_PROGRESS | COMPLETED | FAILED`

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

This example illustrates one usage of GetServiceLastAccessedDetailsWithEntities.

Sample Request

```
https://iam.amazonaws.com/?Action=GetServiceLastAccessedDetailsWithEntities
&JobId=examplef-1305-c245-eba4-71fe298bcda7
&ServiceNamespace=iam
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<EntityDetailsList>
    <member>
        <EntityInfo>
            <Arn>arn:aws:iam::123456789012:user/AWSExampleUser01</Arn>
            <Id>AIDAEX2EXAMPLEB6IGCDC</Id>
            <Name>AWSExampleUser01</Name>
            <Path>/</Path>
```

```
            <Type>USER</Type>
        </EntityInfo>
        <LastAuthenticated>2018-10-24T19:10:00Z</LastAuthenticated>
    </member>
    <member>
        <EntityInfo>
            <Arn>arn:aws:iam::072398337363:role/AWSExampleRole01</Arn>
            <Id>AROAEAW2EXAMPLENXSIU4</Id>
            <Name>AWSExampleRole01</Name>
            <Path>/</Path>
            <Type>ROLE</Type>
        </EntityInfo>
    </member>
</EntityDetailsList>
<IsTruncated>false</IsTruncated>
<JobCompletionDate>2018-10-24T19:47:35.241Z</JobCompletionDate>
<JobCreationDate>2018-10-24T19:47:31.466Z</JobCreationDate>
<JobStatus>COMPLETED</JobStatus>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetServiceLinkedRoleDeletionStatus

Retrieves the status of your service-linked role deletion. After you use the DeleteServiceLinkedRole (p. 104) API operation to submit a service-linked role for deletion, you can use the `DeletionTaskId` parameter in `GetServiceLinkedRoleDeletionStatus` to check the status of the deletion. If the deletion fails, this operation returns the reason that it failed, if that information is returned by the service.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

DeletionTaskId

The deletion task identifier. This identifier is returned by the DeleteServiceLinkedRole (p. 104) operation in the format `task/aws-service-role/<service-principal-name>/<role-name>/<task-uuid>`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1000.

Required: Yes

Response Elements

The following elements are returned by the service.

Reason

An object that contains details about the reason the deletion failed.

Type: DeletionTaskFailureReasonType (p. 432) object

Status

The status of the deletion.

Type: String

Valid Values: `SUCCEEDED | IN_PROGRESS | FAILED | NOT_STARTED`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

The following example shows how to retrieve the status of the `DeletionTaskId` service-lined role deletion.

Sample Request

```
https://iam.amazonaws.com/?Action=GetServiceLinkedRoleDeletionStatus
&DeletionTaskId=task%2Faws-service-role%2Flex.amazonaws.com%2AWSServiceRoleForLexBots
%2Fec720f7a-c0ba-4838-be33-f72e1873dd52
&Version=2010-05-08
```

Example

The following example shows the status of the successful `DeletionTaskId` service-lined role deletion.

Sample Response

```
<GetServiceLinkedRoleDeletionStatusResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetServiceLinkedRoleDeletionStatusResult>
    <Status>SUCCEEDED</Status>
  </GetServiceLinkedRoleDeletionStatusResult>
  <ResponseMetadata>
    <RequestId>aa9259f4-8297-11e7-9f8f-8b008627ec76</RequestId>
  </ResponseMetadata>
</GetServiceLinkedRoleDeletionStatusResponse>
```

Example

The following example shows the status of the failed `DeletionTaskId` service-lined role deletion.

Sample Response

```
<GetServiceLinkedRoleDeletionStatusResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <GetServiceLinkedRoleDeletionStatusResult>
    <Status>FAILED</Status>
  </GetServiceLinkedRoleDeletionStatusResult>
  <DeletionTaskFailureReasonType>
    <Reason>role is being used</Reason>
    <RoleUsageList>
      <RoleUsageType>
        <Region>us-east-1</Region>
        <Resources>
          <Resource>arn1<Resource>
          <Resource>arn2<Resource>
```

```
        </Resources>
      </RoleUsageType>
      <RoleUsageType>
        <Region>us-west-2</Region>
        <Resources>
          <Resource>arn3<Resource>
          <Resource>arn4<Resource>
        </Resources>
      </RoleUsageType>
    </RoleUsageList>
  </DeletionTaskFailureReasonType>
  <ResponseMetadata>
    <RequestId>aa9259f4-8297-11e7-9f8f-8b008627ec76</RequestId>
  </ResponseMetadata>
</GetServiceLinkedRoleDeletionStatusResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetSSHPublicKey

Retrieves the specified SSH public key, including metadata about the key.

The SSH public key retrieved by this operation is used only for authenticating the associated IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Encoding

Specifies the public key encoding format to use in the response. To retrieve the public key in ssh-rsa format, use `SSH`. To retrieve the public key in PEM format, use `PEM`.

Type: String

Valid Values: `SSH | PEM`

Required: Yes

SSHPublicKeyId

The unique identifier for the SSH public key.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the IAM user associated with the SSH public key.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

SSHPublicKey

A structure containing details about the SSH public key.

Type: SSHPublicKey (p. 491) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

UnrecognizedPublicKeyEncoding

The request was rejected because the public key encoding format is unsupported or unrecognized.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of GetSSHPublicKey.

Sample Request

```
https://iam.amazonaws.com/?Action=GetSSHPublicKey
&Encoding=PEM
&SSHPublicKeyId=APKAEIVFHP46CEXAMPLE
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetSSHPublicKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetSSHPublicKeyResult>
    <SSHPublicKey>
      <UploadDate>2015-06-05T20:56:46Z</UploadDate>
      <Fingerprint>7a:1d:ea:9e:b0:80:ac:f8:ec:d8:dc:e6:a7:2c:fc:51</Fingerprint>
      <UserName>Jane</UserName>
      <SSHPublicKeyId>APKAEIVFHP46CEXAMPLE</SSHPublicKeyId>
      <Status>Active</Status>
      <SSHPublicKeyBody>
        -----BEGIN PUBLIC KEY-----
        MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsu+WpO9hhmqGTctHI1BE
        SJ/pq4GtAt9JJpIsDnjeB+mLbwnVJLFaaYzzoZuPOVhUc7yHMWjBLmfSEgJKfAH3
        n8m8R9D3UFoRC0rtKR2jJwAwFO3Tp9wgnqzvPtLMnG7uBEuD/nHStanrd6bbBv83
        kDSy5jiuc4yEWtTAEtyp8C8BxFTxHuCQ/sX4IbjtJ8M1IKZ3hjcJO5u6ooWCxZzQ
        hXXlPDniK/RZnO+YOaJR5umaAv23HAB7qx5H3A6WpyUyzXy0eTo9eAmUrET+JDXZ
        vqHufiDzO/MOCfb+KV1OJos2AxNtRuIFA1cTq7NF+upTIoV+gK1YJhCvjSuRkIJ/
        cwIDAQAB
```

```
        -----END PUBLIC KEY-----
      </SSHPublicKeyBody>
    </SSHPublicKey>
  </GetSSHPublicKeyResult>
  <ResponseMetadata>
    <RequestId>4817ee13-f36d-11e4-97db-33c4eEXAMPLE</RequestId>
  </ResponseMetadata>
</GetSSHPublicKeyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetUser

Retrieves information about the specified IAM user, including the user's creation date, path, unique ID, and ARN.

If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID used to sign the request to this API.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

UserName

The name of the user to get information about.

This parameter is optional. If it is not included, it defaults to the user making the request. This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _ +=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following element is returned by the service.

User

A structure containing details about the IAM user.

Important
Due to a service issue, password last used data does not include password use from May 3, 2018 22:50 PDT to May 23, 2018 14:08 PDT. This affects last sign-in dates shown in the IAM console and password last used dates in the IAM credential report, and returned by this GetUser API. If users signed in during the affected time, the password last used date that is returned is the date the user last signed in before May 3, 2018. For users that signed in after May 23, 2018 14:08 PDT, the returned password last used date is accurate.
You can use password last used information to identify unused credentials for deletion. For example, you might delete users who did not sign in to AWS in the last 90 days. In cases like this, we recommend that you adjust your evaluation window to include dates after May 23, 2018. Alternatively, if your users use access keys to access AWS programmatically you can refer to access key last used information because it is accurate for all dates.

Type: User (p. 499) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetUser.

Sample Request

```
https://iam.amazonaws.com/?Action=GetUser
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<GetUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <GetUserResult>
    <User>
      <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
      <Path>/division_abc/subdivision_xyz/</Path>
      <UserName>Bob</UserName>
      <Arn>arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/Bob</Arn>
      <CreateDate>2013-10-02T17:01:44Z</CreateDate>
      <PasswordLastUsed>2014-10-10T14:37:51Z</PasswordLastUsed>
    </User>
  </GetUserResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</GetUserResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

GetUserPolicy

Retrieves the specified inline policy document that is embedded in the specified IAM user.

> **Note**
> Policies returned by this API are URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

An IAM user can also have managed policies attached to it. To retrieve a managed policy document that is attached to a user, use GetPolicy (p. 182) to determine the policy's default version. Then use GetPolicyVersion (p. 185) to retrieve the policy document.

For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyName

The name of the policy document to get.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

UserName

The name of the user who the policy is associated with.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

PolicyDocument

The policy document.

IAM stores policies in JSON format. However, resources that were created using AWS CloudFormation templates can be formatted in YAML. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

PolicyName

The name of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

UserName

The user the policy is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of GetUserPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=GetUserPolicy
&UserName=Bob
&PolicyName=AllAccessPolicy
&AUTHPARAMS
```

Sample Response

```
<GetUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <GetUserPolicyResult>
    <UserName>Bob</UserName>
    <PolicyName>AllAccessPolicy</PolicyName>
    <PolicyDocument>
    {"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":"*","Resource":"*"}]}
    </PolicyDocument>
 </GetUserPolicyResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</GetUserPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAccessKeys

Returns information about the access key IDs associated with the specified IAM user. If there is none, the operation returns an empty list.

Although each user is limited to a small number of keys, you can still paginate the results using the `MaxItems` and `Marker` parameters.

If the `UserName` field is not specified, the user name is determined implicitly based on the AWS access key ID used to sign the request. This operation works for access keys under the AWS account. Consequently, you can use this operation to manage AWS account root user credentials even if the AWS account has no associated users.

Note
To ensure the security of your AWS account, the secret access key is accessible only during key and user creation.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the user.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following elements are returned by the service.

AccessKeyMetadata.member.N

A list of objects containing metadata about the access keys.

Type: Array of AccessKeyMetadata (p. 427) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListAccessKeys.

Sample Request

```
https://iam.amazonaws.com/?Action=ListAccessKeys
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAccessKeysResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListAccessKeysResult>
    <UserName>Bob</UserName>
    <AccessKeyMetadata>
       <member>
          <UserName>Bob</UserName>
          <AccessKeyId>AKIA1234567890EXAMPLE</AccessKeyId>
          <Status>Active</Status>
    <CreateDate>2016-12-03T18:53:41Z</CreateDate>
       </member>
       <member>
          <UserName>Susan</UserName>
          <AccessKeyId>AKIA2345678901EXAMPLE</AccessKeyId>
          <Status>Inactive</Status>
    <CreateDate>2017-03-25T20:38:14Z</CreateDate>
       </member>
    </AccessKeyMetadata>
    <IsTruncated>false</IsTruncated>
  </ListAccessKeysResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListAccessKeysResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAccountAliases

Lists the account alias associated with the AWS account (Note: you can have only one). For information about using an AWS account alias, see Using an Alias for Your AWS Account ID in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

AccountAliases.member.N

A list of aliases associated with the account. AWS supports only one alias per account.

Type: Array of strings

Length Constraints: Minimum length of 3. Maximum length of 63.

Pattern: `^[a-z0-9](([a-z0-9]|-(?!-))*[a-z0-9])?$`

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items.

Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListAccountAliases.

Sample Request

```
https://iam.amazonaws.com/?Action=ListAccountAliases
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAccountAliasesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListAccountAliasesResult>
  <IsTruncated>false</IsTruncated>
  <AccountAliases>
    <member>example-corporation</member>
  </AccountAliases>
</ListAccountAliasesResult>
<ResponseMetadata>
  <RequestId>c5a076e9-f1b0-11df-8fbe-45274EXAMPLE</RequestId>
</ResponseMetadata>
</ListAccountAliasesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAttachedGroupPolicies

Lists all managed policies that are attached to the specified IAM group.

An IAM group can also have inline policies embedded with it. To list the inline policies for a group, use the ListGroupPolicies (p. 242) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. You can use the `PathPrefix` parameter to limit the list of policies to only those matching the specified path prefix. If there are no policies attached to the specified group (or none that match the specified path prefix), the operation returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name (friendly name, not ARN) of the group to list attached policies for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all policies.

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

Response Elements

The following elements are returned by the service.

AttachedPolicies.member.N

A list of the attached policies.

Type: Array of AttachedPolicy (p. 430) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListAttachedGroupPolicies.

Sample Request

```
https://iam.amazonaws.com/?Action=ListAttachedGroupPolicies
&GroupName=ReadOnlyUsers
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAttachedGroupPoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListAttachedGroupPoliciesResult>
    <AttachedPolicies>
      <member>
        <PolicyName>ReadOnlyAccess</PolicyName>
        <PolicyArn>arn:aws:iam::aws:policy/ReadOnlyAccess</PolicyArn>
      </member>
    </AttachedPolicies>
    <IsTruncated>false</IsTruncated>
  </ListAttachedGroupPoliciesResult>
  <ResponseMetadata>
    <RequestId>710f2d3f-3df1-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListAttachedGroupPoliciesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

ListAttachedRolePolicies

Lists all managed policies that are attached to the specified IAM role.

An IAM role can also have inline policies embedded with it. To list the inline policies for a role, use the ListRolePolicies (p. 273) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. You can use the `PathPrefix` parameter to limit the list of policies to only those matching the specified path prefix. If there are no policies attached to the specified role (or none that match the specified path prefix), the operation returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all policies.

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

RoleName

The name (friendly name, not ARN) of the role to list attached policies for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

AttachedPolicies.member.N

A list of the attached policies.

Type: Array of AttachedPolicy (p. 430) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListAttachedRolePolicies.

Sample Request

```
https://iam.amazonaws.com/?Action=ListAttachedRolePolicies
&RoleName=ReadOnlyRole
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAttachedRolePoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListAttachedRolePoliciesResult>
    <AttachedPolicies>
      <member>
        <PolicyName>ReadOnlyAccess</PolicyName>
        <PolicyArn>arn:aws:iam::aws:policy/ReadOnlyAccess</PolicyArn>
      </member>
    </AttachedPolicies>
    <IsTruncated>false</IsTruncated>
  </ListAttachedRolePoliciesResult>
  <ResponseMetadata>
    <RequestId>9a3b490d-3ea5-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListAttachedRolePoliciesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

ListAttachedUserPolicies

Lists all managed policies that are attached to the specified IAM user.

An IAM user can also have inline policies embedded with it. To list the inline policies for a user, use the ListUserPolicies (p. 296) API. For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. You can use the `PathPrefix` parameter to limit the list of policies to only those matching the specified path prefix. If there are no policies attached to the specified group (or none that match the specified path prefix), the operation returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all policies.

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

UserName

The name (friendly name, not ARN) of the user to list attached policies for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

AttachedPolicies.member.N

A list of the attached policies.

Type: Array of AttachedPolicy (p. 430) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListAttachedUserPolicies.

Sample Request

```
https://iam.amazonaws.com/?Action=ListAttachedUserPolicies
&UserName=Alice
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListAttachedUserPoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListAttachedUserPoliciesResult>
    <AttachedPolicies>
      <member>
        <PolicyName>AdministratorAccess</PolicyName>
        <PolicyArn>arn:aws:iam::aws:policy/AdministratorAccess</PolicyArn>
      </member>
    </AttachedPolicies>
    <IsTruncated>false</IsTruncated>
  </ListAttachedUserPoliciesResult>
  <ResponseMetadata>
    <RequestId>75980e78-3ea6-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListAttachedUserPoliciesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

ListEntitiesForPolicy

Lists all IAM users, groups, and roles that the specified managed policy is attached to.

You can use the optional `EntityFilter` parameter to limit the results to a particular type of entity (users, groups, or roles). For example, to list only the roles that are attached to the specified policy, set `EntityFilter` to `Role`.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

EntityFilter

The entity type to use for filtering the results.

For example, when `EntityFilter` is `Role`, only the roles that are attached to the specified policy are returned. This parameter is optional. If it is not included, all attached entities (users, groups, and roles) are returned. The argument for this parameter must be one of the valid values listed below.

Type: String

Valid Values: `User | Role | Group | LocalManagedPolicy | AWSManagedPolicy`

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all entities.

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy for which you want the versions.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

PolicyUsageFilter

The policy usage method to use for filtering the results.

To list only permissions policies, set `PolicyUsageFilter` to `PermissionsPolicy`. To list only the policies used to set permissions boundaries, set the value to `PermissionsBoundary`.

This parameter is optional. If it is not included, all policies are returned.

Type: String

Valid Values: `PermissionsPolicy | PermissionsBoundary`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

PolicyGroups.member.N

A list of IAM groups that the policy is attached to.

Type: Array of PolicyGroup (p. 463) objects

PolicyRoles.member.N

A list of IAM roles that the policy is attached to.

Type: Array of PolicyRole (p. 464) objects

PolicyUsers.member.N

A list of IAM users that the policy is attached to.

Type: Array of PolicyUser (p. 465) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListEntitiesForPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=ListEntitiesForPolicy
&PolicyArn=arn:aws:iam::123456789012:policy/EC2-Devs
&Version=2010-05-08
```

```
&AUTHPARAMS
```

Sample Response

```
<ListEntitiesForPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListEntitiesForPolicyResult>
    <PolicyRoles>
      <member>
        <RoleName>DevRole</RoleName>
      </member>
    </PolicyRoles>
    <PolicyGroups>
      <member>
        <GroupName>Dev</GroupName>
      </member>
    </PolicyGroups>
    <IsTruncated>false</IsTruncated>
    <PolicyUsers>
      <member>
        <UserName>Alice</UserName>
      </member>
      <member>
        <UserName>Bob</UserName>
      </member>
    </PolicyUsers>
  </ListEntitiesForPolicyResult>
  <ResponseMetadata>
    <RequestId>eb358e22-9d1f-11e4-93eb-190ecEXAMPLE</RequestId>
  </ResponseMetadata>
</ListEntitiesForPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListGroupPolicies

Lists the names of the inline policies that are embedded in the specified IAM group.

An IAM group can also have managed policies attached to it. To list the managed policies that are attached to a group, use ListAttachedGroupPolicies (p. 226). For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. If there are no inline policies embedded with the specified group, the operation returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name of the group to list policies for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

PolicyNames.member.N

A list of policy names.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListGroupPolicies.

Sample Request

```
https://iam.amazonaws.com/?Action=ListGroupPolicies
&GroupName=Admins
&AUTHPARAMS
```

Sample Response

```
<ListGroupPoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ListGroupPoliciesResult>
    <PolicyNames>
       <member>AdminRoot</member>
       <member>KeyPolicy</member>
    </PolicyNames>
    <IsTruncated>false</IsTruncated>
 </ListGroupPoliciesResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ListGroupPoliciesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListGroups

Lists the IAM groups that have the specified path prefix.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example, the prefix `/division_abc/subdivision_xyz/` gets all groups whose path starts with `/division_abc/subdivision_xyz/`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all groups. This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

Groups.member.N

A list of groups.

Type: Array of Group (p. 440) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListGroups.

Sample Request

```
https://iam.amazonaws.com/?Action=ListGroups
&PathPrefix=/division_abc/subdivision_xyz/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListGroupsResponse>
  <ListGroupsResult>
    <Groups>
       <member>
```

```
            <Path>/division_abc/subdivision_xyz/</Path>
            <GroupName>Admins</GroupName>
            <GroupId>AGPACKCEVSQ6C2EXAMPLE</GroupId>
            <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
         </member>
         <member>
            <Path>/division_abc/subdivision_xyz/product_1234/engineering/
            </Path>
            <GroupName>Test</GroupName>
            <GroupId>AGP2MAB8DPLSRHEXAMPLE</GroupId>
            <Arn>arn:aws:iam::123456789012:group
            /division_abc/subdivision_xyz/product_1234/engineering/Test</Arn>
         </member>
         <member>
            <Path>/division_abc/subdivision_xyz/product_1234/</Path>
            <GroupName>Managers</GroupName>
            <GroupId>AGPIODR4TAW7CSEXAMPLE</GroupId>
            <Arn>arn:aws:iam::123456789012
            :group/division_abc/subdivision_xyz/product_1234/Managers</Arn>
         </member>
      </Groups>
      <IsTruncated>false</IsTruncated>
   </ListGroupsResult>
   <ResponseMetadata>
      <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
   </ResponseMetadata>
</ListGroupsResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListGroupsForUser

Lists the IAM groups that the specified IAM user belongs to.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the user to list groups for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

Groups.member.N

A list of groups.

Type: Array of Group (p. 440) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListGroupsForUser.

Sample Request

```
https://iam.amazonaws.com/?Action=ListGroupsForUser
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListGroupsForUserResponse>
  <ListGroupsForUserResult>
```

```
    <Groups>
       <member>
          <Path>/</Path>
          <GroupName>Admins</GroupName>
          <GroupId>AGPACKCEVSQ6C2EXAMPLE</GroupId>
          <Arn>arn:aws:iam::123456789012:group/Admins</Arn>
       </member>
    </Groups>
    <IsTruncated>false</IsTruncated>
  </ListGroupsForUserResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListGroupsForUserResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListInstanceProfiles

Lists the instance profiles that have the specified path prefix. If there are none, the operation returns an empty list. For more information about instance profiles, go to About Instance Profiles.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example, the prefix `/application_abc/component_xyz/` gets all instance profiles whose path starts with `/application_abc/component_xyz/`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all instance profiles. This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

InstanceProfiles.member.N

A list of instance profiles.

Type: Array of InstanceProfile (p. 444) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListInstanceProfiles.

Sample Request

```
https://iam.amazonaws.com/?Action=ListInstanceProfiles
&MaxItems=100
&PathPrefix=/application_abc/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListInstanceProfilesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
```

```
<ListInstanceProfilesResult>
  <IsTruncated>false</IsTruncated>
  <InstanceProfiles>
    <member>
      <InstanceProfileId>AIPA1234567890EXAMPLE</InstanceProfileId>
      <Roles>
        <member>
          <AssumeRolePolicyDocument>{  …  JSON POLICY DOCUMENT HERE … }</
AssumeRolePolicyDocument>
          <RoleId>AROA1234567890EXAMPLE</RoleId>
          <CreateDate>2016-04-27T21:18:27Z</CreateDate>
          <RoleName>ec2instancerole-MyADFSTestServer</RoleName>
          <Path>/</Path>,
          <Arn>arn:aws:iam::123456789012:role/ec2instancerole-MyADFSTestServer</Arn>
        </member>
      </Roles>
      <InstanceProfileName>Database</InstanceProfileName>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/component_xyz/
Database</Arn>
      <CreateDate>2012-05-09T16:27:03Z</CreateDate>
    </member>
    <member>
      <InstanceProfileId>AIPA2345678901EXAMPLE</InstanceProfileId>
      <Roles/>
      <InstanceProfileName>Webserver</InstanceProfileName>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/component_xyz/
Webserver</Arn>
      <CreateDate>2012-05-09T16:27:11Z</CreateDate>
    </member>
  </InstanceProfiles>
</ListInstanceProfilesResult>
<ResponseMetadata>
  <RequestId>fd74fa8d-99f3-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListInstanceProfilesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListInstanceProfilesForRole

Lists the instance profiles that have the specified associated IAM role. If there are none, the operation returns an empty list. For more information about instance profiles, go to About Instance Profiles.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

RoleName

The name of the role to list instance profiles for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

InstanceProfiles.member.N

A list of instance profiles.

Type: Array of InstanceProfile (p. 444) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListInstanceProfilesForRole.

Sample Request

```
https://iam.amazonaws.com/?Action=ListInstanceProfilesForRole
&MaxItems=100
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListInstanceProfilesForRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListInstanceProfilesForRoleResult>
  <IsTruncated>false</IsTruncated>
  <InstanceProfiles>
    <member>
      <Id>AIPACZLS2EYYXMEXAMPLE</Id>
      <Roles>
        <member>
          <Path>/application_abc/component_xyz/</Path>
          <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/S3Access</Arn>
          <RoleName>S3Access</RoleName>
          <AssumeRolePolicyDocument>
            {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
            "Principal":{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
          </AssumeRolePolicyDocument>
          <CreateDate>2012-05-09T15:45:35Z</CreateDate>
          <RoleId>AROACVSVTSZYK3EXAMPLE</RoleId>
        </member>
      </Roles>
      <InstanceProfileName>Webserver</InstanceProfileName>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:instance-profile/application_abc/component_xyz/
Webserver</Arn>
      <CreateDate>2012-05-09T16:27:11Z</CreateDate>
    </member>
  </InstanceProfiles>
</ListInstanceProfilesForRoleResult>
<ResponseMetadata>
  <RequestId>6a8c3992-99f4-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListInstanceProfilesForRoleResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListMFADevices

Lists the MFA devices for an IAM user. If the request includes a IAM user name, then this operation lists all the MFA devices associated with the specified user. If you do not specify a user name, IAM determines the user name implicitly based on the AWS access key ID signing the request for this API.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the user whose MFA devices you want to list.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

MFADevices.member.N

A list of MFA devices.

Type: Array of MFADevice (p. 451) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListMFADevices.

Sample Request

```
https://iam.amazonaws.com/?Action=ListMFADevices
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListMFADevicesResponse>
  <ListMFADevicesResult>
    <MFADevices>
       <member>
          <UserName>Bob</UserName>
          <SerialNumber>R1234</SerialNumber>
       </member>
    </MFADevices>
    <IsTruncated>false</IsTruncated>
  </ListMFADevicesResult>
  <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListMFADevicesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListOpenIDConnectProviders

Lists information about the IAM OpenID Connect (OIDC) provider resource objects defined in the AWS account.

Response Elements

The following element is returned by the service.

OpenIDConnectProviderList.member.N

The list of IAM OIDC provider resource objects defined in the AWS account.

Type: Array of OpenIDConnectProviderListEntry (p. 452) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListOpenIDConnectProviders.

Sample Request

```
https://iam.amazonaws.com/?Action=ListOpenIDConnectProviders
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListOpenIDConnectProvidersResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListOpenIDConnectProvidersResult>
    <OpenIDConnectProviderList>
      <member>
        <Arn>arn:aws:iam::123456789012:oidc-provider/server.example.com</Arn>
      </member>
      <member>
        <Arn>arn:aws:iam::123456789012:oidc-provider/server.example.org</Arn>
      </member>
    </OpenIDConnectProviderList>
  </ListOpenIDConnectProvidersResult>
  <ResponseMetadata>
    <RequestId>de2c0228-4f63-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</ListOpenIDConnectProvidersResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListPolicies

Lists all the managed policies that are available in your AWS account, including your own customer-defined managed policies and all AWS managed policies.

You can filter the list of policies that is returned using the optional `OnlyAttached`, `Scope`, and `PathPrefix` parameters. For example, to list only the customer managed policies in your AWS account, set `Scope` to `Local`. To list only AWS managed policies, set `Scope` to `AWS`.

You can paginate the results using the `MaxItems` and `Marker` parameters.

For more information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

OnlyAttached

A flag to filter the results to only the attached policies.

When `OnlyAttached` is `true`, the returned list contains only the policies that are attached to an IAM user, group, or role. When `OnlyAttached` is `false`, or when the parameter is not included, all policies are returned.

Type: Boolean

Required: No

PathPrefix

The path prefix for filtering the results. This parameter is optional. If it is not included, it defaults to a slash (/), listing all policies. This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

PolicyUsageFilter

The policy usage method to use for filtering the results.

To list only permissions policies, set `PolicyUsageFilter` to `PermissionsPolicy`. To list only the policies used to set permissions boundaries, set the value to `PermissionsBoundary`.

This parameter is optional. If it is not included, all policies are returned.

Type: String

Valid Values: `PermissionsPolicy | PermissionsBoundary`

Required: No

Scope

The scope to use for filtering the results.

To list only AWS managed policies, set `Scope` to `AWS`. To list only the customer managed policies in your AWS account, set `Scope` to `Local`.

This parameter is optional. If it is not included, or if it is set to `All`, all policies are returned.

Type: String

Valid Values: `All | AWS | Local`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Policies.member.N

A list of policies.

Type: Array of Policy (p. 457) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListPolicies.

Sample Request

```
https://iam.amazonaws.com/?Action=ListPolicies
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListPoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListPoliciesResult>
    <IsTruncated>true</IsTruncated>
    <Marker>EXAMPLEkakv9BCuUNFDtxWSyfzetYwEx2ADc8dnzfvERF5S6YMvXKx41t6gCl/eeaCX3Jo94/
bKqezEAg8TEVS
    99EKFLxm3jtbpl25FDWEXAMPLE
    </Marker>
    <Policies>
      <member>
        <PolicyName>ExamplePolicy</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
        <Path>/</Path>
        <Arn>arn:aws:iam::123456789012:policy/ExamplePolicy</Arn>
        <AttachmentCount>2</AttachmentCount>
        <CreateDate>2014-09-15T17:36:14Z</CreateDate>
        <UpdateDate>2014-09-15T20:31:47Z</UpdateDate>
      </member>
      <member>
        <PolicyName>PowerUserAccess</PolicyName>
```

```
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
        <Path>/</Path>
        <Arn>arn:aws:iam::aws:policy/PowerUserAccess</Arn>
        <AttachmentCount>0</AttachmentCount>
        <CreateDate>2014-08-21T20:25:01Z</CreateDate>
        <UpdateDate>2014-08-21T20:25:01Z</UpdateDate>
      </member>
      <member>
        <PolicyName>AdministratorAccess</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
        <Path>/</Path>
        <Arn>arn:aws:iam::aws:policy/AdministratorAccess</Arn>
        <AttachmentCount>1</AttachmentCount>
        <CreateDate>2014-08-21T20:11:25Z</CreateDate>
        <UpdateDate>2014-08-21T20:11:25Z</UpdateDate>
      </member>
      <member>
        <PolicyName>ReadOnlyAccess</PolicyName>
        <DefaultVersionId>v1</DefaultVersionId>
        <PolicyId>AGPACKCEVSQ6C2EXAMPLE</PolicyId>
        <Path>/</Path>
        <Arn>arn:aws:iam::aws:policy/ReadOnlyAccess</Arn>
        <AttachmentCount>6</AttachmentCount>
        <CreateDate>2014-08-21T20:31:44Z</CreateDate>
        <UpdateDate>2014-08-21T20:31:44Z</UpdateDate>
      </member>
    </Policies>
  </ListPoliciesResult>
  <ResponseMetadata>
    <RequestId>6207e832-3eb7-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListPoliciesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListPoliciesGrantingServiceAccess

Retrieves a list of policies that the IAM identity (user, group, or role) can use to access each specified service.

> **Note**
> This operation does not use other policy types when determining whether a resource could access a service. These other policy types include resource-based policies, access control lists, AWS Organizations policies, IAM permissions boundaries, and AWS STS assume role policies. It only applies permissions policy logic. For more about the evaluation of policy types, see Evaluating Policies in the *IAM User Guide*.

The list of policies returned by the operation depends on the ARN of the identity that you provide.

- **User** – The list of policies includes the managed and inline policies that are attached to the user directly. The list also includes any additional managed and inline policies that are attached to the group to which the user belongs.
- **Group** – The list of policies includes only the managed and inline policies that are attached to the group directly. Policies that are attached to the group's user are not included.
- **Role** – The list of policies includes only the managed and inline policies that are attached to the role.

For each managed policy, this operation returns the ARN and policy name. For each inline policy, it returns the policy name and the entity to which it is attached. Inline policies do not have an ARN. For more information about these policy types, see Managed Policies and Inline Policies in the *IAM User Guide*.

Policies that are attached to users and roles as permissions boundaries are not returned. To view which managed policy is currently used to set the permissions boundary for a user or role, use the GetUser (p. 214) or GetRole (p. 188) operations.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Arn

The ARN of the IAM identity (user, group, or role) whose policies you want to list.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

ServiceNamespaces.member.N

The service namespace for the AWS services whose policies you want to list.

To learn the service namespace for a service, go to Actions, Resources, and Condition Keys for AWS Services in the *IAM User Guide*. Choose the name of the service to view details for that service. In the first paragraph, find the service prefix. For example, `(service prefix: a4b)`. For more information about service namespaces, see AWS Service Namespaces in the *AWS General Reference*.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w-]*`

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

PoliciesGrantingServiceAccess.member.N

A `ListPoliciesGrantingServiceAccess` object that contains details about the permissions policies attached to the specified identity (user, group, or role).

Type: Array of ListPoliciesGrantingServiceAccessEntry (p. 446) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

This example illustrates one usage of ListPoliciesGrantingServiceAccess.

Sample Request

```
https://iam.amazonaws.com/?Action=ListPoliciesGrantingServiceAccess
&Arn=arn:aws:iam::123456789012:user/ExampleUser01
&ServiceNamespace.member.1=iam
&ServiceNamespace.member.2=ec2
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<IsTruncated>false</IsTruncated>
<PoliciesGrantingServiceAccess>
    <member>
        <Policies>
            <member>
                <PolicyArn>arn:aws:iam::123456789012:policy/ExampleIamPolicy</PolicyArn>
                <PolicyName>ExampleIamPolicy</PolicyName>
                <PolicyType>MANAGED</PolicyType>
            </member>
            <member>
                <EntityName>AWSExampleGroup1</EntityName>
                <EntityType>GROUP</EntityType>
                <PolicyName>policygen-AWSExampleGroup1-201810241414</PolicyName>
                <PolicyType>INLINE</PolicyType>
            </member>
        </Policies>
        <ServiceNamespace>iam</ServiceNamespace>
    </member>
    <member>
        <Policies>
            <member>
                <PolicyArn>arn:aws:iam::123456789012:policy/ExampleEc2Policy</PolicyArn>
                <PolicyName>ExampleEc2Policy</PolicyName>
                <PolicyType>MANAGED</PolicyType>
            </member>
        </Policies>
        <ServiceNamespace>ec2</ServiceNamespace>
    </member>
</PoliciesGrantingServiceAccess>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListPolicyVersions

Lists information about the versions of the specified managed policy, including the version that is currently set as the policy's default version.

For more information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy for which you want the versions.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Versions.member.N

A list of policy versions.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: Array of PolicyVersion (p. 466) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListPolicyVersions.

Sample Request

```
https://iam.amazonaws.com/?Action=ListPolicyVersions
```

```
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListPolicyVersionsResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListPolicyVersionsResult>
    <Versions>
      <member>
        <IsDefaultVersion>false</IsDefaultVersion>
        <VersionId>v3</VersionId>
        <CreateDate>2014-09-17T22:32:43Z</CreateDate>
      </member>
      <member>
        <IsDefaultVersion>true</IsDefaultVersion>
        <VersionId>v2</VersionId>
        <CreateDate>2014-09-15T20:31:47Z</CreateDate>
      </member>
      <member>
        <IsDefaultVersion>false</IsDefaultVersion>
        <VersionId>v1</VersionId>
        <CreateDate>2014-09-15T17:36:14Z</CreateDate>
      </member>
    </Versions>
    <IsTruncated>false</IsTruncated>
  </ListPolicyVersionsResult>
  <ResponseMetadata>
    <RequestId>a31d1a86-3eba-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</ListPolicyVersionsResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRolePolicies

Lists the names of the inline policies that are embedded in the specified IAM role.

An IAM role can also have managed policies attached to it. To list the managed policies that are attached to a role, use ListAttachedRolePolicies (p. 230). For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. If there are no inline policies embedded with the specified role, the operation returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

RoleName

The name of the role to list policies for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

PolicyNames.member.N

A list of policy names.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListRolePolicies.

Sample Request

```
https://iam.amazonaws.com/?Action=ListRolePolicies
&RoleName=S3Access
```

```
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListRolePoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListRolePoliciesResult>
  <PolicyNames>
    <member>CloudwatchPutMetricPolicy</member>
    <member>S3AccessPolicy</member>
  </PolicyNames>
  <IsTruncated>false</IsTruncated>
</ListRolePoliciesResult>
<ResponseMetadata>
  <RequestId>8c7e1816-99f0-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListRolePoliciesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRoles

Lists the IAM roles that have the specified path prefix. If there are none, the operation returns an empty list. For more information about roles, go to Working with Roles.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example, the prefix `/application_abc/component_xyz/` gets all roles whose path starts with `/application_abc/component_xyz/`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all roles. This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Roles.member.N

A list of roles.

Type: Array of Role (p. 471) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListRoles.

Sample Request

```
https://iam.amazonaws.com/?Action=ListRoles
&MaxItems=100
&PathPrefix=/application_abc/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListRolesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListRolesResult>
  <IsTruncated>false</IsTruncated>
```

```
  <Roles>
    <member>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/S3Access</Arn>
      <RoleName>S3Access</RoleName>
      <AssumeRolePolicyDocument>
        {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
        "Principal":{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
      </AssumeRolePolicyDocument>
      <CreateDate>2012-05-09T15:45:35Z</CreateDate>
      <RoleId>AROACVSVTSZYEXAMPLEYK</RoleId>
    </member>
    <member>
      <Path>/application_abc/component_xyz/</Path>
      <Arn>arn:aws:iam::123456789012:role/application_abc/component_xyz/SDBAccess</Arn>
      <RoleName>SDBAccess</RoleName>
      <AssumeRolePolicyDocument>
        {"Version":"2012-10-17","Statement":[{"Effect":"Allow",
        "Principal":{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
      </AssumeRolePolicyDocument>
      <CreateDate>2012-05-09T15:45:45Z</CreateDate>
      <RoleId>AROAC2ICXG32EXAMPLEWK</RoleId>
    </member>
  </Roles>
</ListRolesResult>
<ResponseMetadata>
  <RequestId>20f7279f-99ee-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListRolesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRoleTags

Lists the tags that are attached to the specified role. The returned list of tags is sorted by tag key. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

(Optional) Use this only when paginating results to indicate the maximum number of items that you want in the response. If additional items exist beyond the maximum that you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, it defaults to 100. Note that IAM might return fewer results, even when more results are available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

RoleName

The name of the IAM role for which you want to see the list of tags.

This parameter accepts (through its regex pattern) a string of characters that consist of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can use the `Marker` request parameter to make a subsequent pagination request that retrieves more items. Note that IAM might return fewer than the `MaxItems` number of results even when more results are available. Check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Tags.member.N

The list of tags currently that is attached to the role. Each tag consists of a key name and an associated value. If no tags are attached to the specified role, the response contains an empty list.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

The following example is formatted with line breaks for legibility.

The following example shows how to list the tags attached to a role named `taggedrole`.

Sample Request

```
POST / HTTP/1.1
Host: https://iam.amazonaws.com
Accept-Encoding: identity
User-Agent: aws-cli/1.11.143 Python/3.6.1 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.7.1
X-Amz-Date: 20170926T201509Z
```

```
Authorization: <auth details>
Content-Length: 58
Content-Type: application/x-www-form-urlencoded
Action=ListRoleTags&Version=2010-05-08&RoleName=taggedrole
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE
Content-Type: text/xml
Content-Length: 447
Date: Tue, 26 Sep 2017 20:15:09 GMT

<ListRoleTagsResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListRoleTagsResult>
    <IsTruncated>false</IsTruncated>
    <Tags>
      <member>
        <Key>Dept</Key>
        <Value>Accounting</Value>
      </member>
      <member>
        <Key>Cost Center</Key>
        <Value>12345</Value>
      </member>
    </Tags>
  </ListRoleTagsResult>
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</ListRoleTagsResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListSAMLProviders

Lists the SAML provider resource objects defined in IAM in the account.

Note
This operation requires Signature Version 4.

Response Elements

The following element is returned by the service.

SAMLProviderList.member.N

The list of SAML provider resource objects defined in IAM for this AWS account.

Type: Array of SAMLProviderListEntry (p. 479) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListSAMLProviders.

Sample Request

```
https://iam.amazonaws.com/?Action=ListSAMLProviders
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListSAMLProvidersResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListSAMLProvidersResult>
  <SAMLProviderList>
    <member>
      <Arn>arn:aws:iam::123456789012:saml-provider/MyUniversity</Arn>
      <ValidUntil>2032-05-09T16:27:11Z</ValidUntil>
      <CreateDate>2012-05-09T16:27:03Z</CreateDate>
    </member>
    <member>
      <Arn>arn:aws:iam::123456789012:saml-provider/MyUniversity</Arn>
      <ValidUntil>2015-03-11T13:11:02Z</ValidUntil>
      <CreateDate>2012-05-09T16:27:11Z</CreateDate>
    </member>
```

```
  </SAMLProviderList>
</ListSAMLProvidersResult>
<ResponseMetadata>
  <RequestId>fd74fa8d-99f3-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</ListSAMLProvidersResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListServerCertificates

Lists the server certificates stored in IAM that have the specified path prefix. If none exist, the operation returns an empty list.

You can paginate the results using the `MaxItems` and `Marker` parameters.

For more information about working with server certificates, see Working with Server Certificates in the *IAM User Guide*. This topic also includes a list of AWS services that can use the server certificates that you manage with IAM.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example: `/company/servercerts` would get all server certificates for which the path starts with `/company/servercerts`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all server certificates. This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

ServerCertificateMetadataList.member.N

A list of server certificates.

Type: Array of ServerCertificateMetadata (p. 481) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListServerCertificates.

Sample Request

```
https://iam.amazonaws.com/?Action=ListServerCertificates
&PathPrefix=/company/servercerts
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListServerCertificatesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListServerCertificatesResult>
  <IsTruncated>false</IsTruncated>
  <ServerCertificateMetadataList>
    <member>
      <ServerCertificateName>ProdServerCert</ServerCertificateName>
      <Path>/company/servercerts/</Path>
      <Arn>arn:aws:iam::123456789012:server-certificate/company/servercerts/
ProdServerCert</Arn>
      <UploadDate>2010-05-08T01:02:03.004Z</UploadDate>
      <ServerCertificateId>ASCACKCEVSQ6CEXAMPLE1</ServerCertificateId>
      <Expiration>2012-05-08T01:02:03.004Z</Expiration>
    </member>
    <member>
      <ServerCertificateName>BetaServerCert</ServerCertificateName>
      <Path>/company/servercerts/</Path>
      <Arn>arn:aws:iam::123456789012:server-certificate/company/servercerts/
BetaServerCert</Arn>
      <UploadDate>2010-05-08T02:03:01.004Z</UploadDate>
      <ServerCertificateId>ASCACKCEVSQ6CEXAMPLE2</ServerCertificateId>
      <Expiration>2012-05-08T02:03:01.004Z</Expiration>
    </member>
    <member>
      <ServerCertificateName>TestServerCert</ServerCertificateName>
      <Path>/company/servercerts/</Path>
      <Arn>arn:aws:iam::123456789012:server-certificate/company/servercerts/
TestServerCert</Arn>
      <UploadDate>2010-05-08T03:01:02.004Z</UploadDate>
      <ServerCertificateId>ASCACKCEVSQ6CEXAMPLE3</ServerCertificateId>
      <Expiration>2012-05-08T03:01:02.004Z</Expiration>
    </member>
  </ServerCertificateMetadataList>
</ListServerCertificatesResult>
<ResponseMetadata>
  <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
</ResponseMetadata>
</ListServerCertificatesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListServiceSpecificCredentials

Returns information about the service-specific credentials associated with the specified IAM user. If none exists, the operation returns an empty list. The service-specific credentials returned by this operation are used only for authenticating the IAM user to a specific service. For more information about using service-specific credentials to authenticate to an AWS service, see Set Up service-specific credentials in the AWS CodeCommit User Guide.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ServiceName

Filters the returned results to only those for the specified AWS service. If not specified, then AWS returns service-specific credentials for all services.

Type: String

Required: No

UserName

The name of the user whose service-specific credentials you want information about. If this value is not specified, then the operation assumes the user whose credentials are used to call the operation.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following element is returned by the service.

ServiceSpecificCredentials.member.N

A list of structures that each contain details about a service-specific credential.

Type: Array of ServiceSpecificCredentialMetadata (p. 487) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

NotSupportedService

The specified service does not support service-specific credentials.

HTTP Status Code: 404

Examples

Example

The following example shows how to get the list of all service-specific credentials for the IAM user named Anika.

Sample Request

```
https://iam.amazonaws.com/?Action=ListServiceSpecificCredentials
&UserName=anika
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListServiceSpecificCredentialsResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListServiceSpecificCredentialsResult>
    <ServiceSpecificCredentials>
      <member>
        <ServiceName>codecommit.amazonaws.com</ServiceName>
        <UserName>anika</UserName>
        <ServiceUserName>anika-at-123456789012</ServiceUserName>
        <ServiceSpecificCredentialId>ACCA12345ABCDEXAMPLE</ServiceSpecificCredentialId>
        <Status>Active</Status>
        <CreateDate>2016-11-01T17:44:54Z</CreateDate>
      </member>
      <member>
        <ServiceName>codecommit.amazonaws.com</ServiceName>
        <UserName>anika</UserName>
        <ServiceUserName>anika+1-at-123456789012</ServiceUserName>
        <ServiceSpecificCredentialId>ACCA67890FGHIEXAMPLE</ServiceSpecificCredentialId>
        <Status>Active</Status>
        <CreateDate>2016-11-01T18:22:26Z</CreateDate>
      </member>
    </ServiceSpecificCredentials>
  </ListServiceSpecificCredentialsResult>
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</ListServiceSpecificCredentialsResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListSigningCertificates

Returns information about the signing certificates associated with the specified IAM user. If none exists, the operation returns an empty list.

Although each user is limited to a small number of signing certificates, you can still paginate the results using the `MaxItems` and `Marker` parameters.

If the `UserName` field is not specified, the user name is determined implicitly based on the AWS access key ID used to sign the request for this API. This operation works for access keys under the AWS account. Consequently, you can use this operation to manage AWS account root user credentials even if the AWS account has no associated users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the IAM user whose signing certificates you want to examine.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following elements are returned by the service.

Certificates.member.N

A list of the user's signing certificate information.

Type: Array of SigningCertificate (p. 489) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListSigningCertificates.

Sample Request

```
https://iam.amazonaws.com/?Action=ListSigningCertificates
```

```
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListSigningCertificatesResponse>
  <ListSigningCertificatesResult>
    <UserName>Bob</UserName>
    <Certificates>
       <member>
          <UserName>Bob</UserName>
          <CertificateId>TA7SMEXAMPLEZ26OBPJE7EXAMPLE</CertificateId>
          <CertificateBody>
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
          </CertificateBody>
          <Status>Active</Status>
       </member>
    </Certificates>
    <IsTruncated>false</IsTruncated>
 </ListSigningCertificatesResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ListSigningCertificatesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListSSHPublicKeys

Returns information about the SSH public keys associated with the specified IAM user. If none exists, the operation returns an empty list.

The SSH public keys returned by this operation are used only for authenticating the IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Although each user is limited to a small number of keys, you can still paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the IAM user to list SSH public keys for. If none is specified, the `UserName` field is determined implicitly based on the AWS access key used to sign the request.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

SSHPublicKeys.member.N

A list of the SSH public keys assigned to IAM user.

Type: Array of SSHPublicKeyMetadata (p. 493) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

This example illustrates one usage of ListSSHPublicKeys.

Sample Request

```
https://iam.amazonaws.com/?Action=ListSSHPublicKeys
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListSSHPublicKeysResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ListSSHPublicKeysResult>
    <IsTruncated>false</IsTruncated>
    <SSHPublicKeys>
      <member>
        <UploadDate>2015-06-05T20:56:46Z</UploadDate>
        <UserName>Jane</UserName>
        <SSHPublicKeyId>APKAEIVFHP46CEXAMPLE</SSHPublicKeyId>
        <Status>Active</Status>
      </member>
    </SSHPublicKeys>
  </ListSSHPublicKeysResult>
  <ResponseMetadata>
    <RequestId>9f8e2d77-f36c-11e4-97db-33c4eEXAMPLE</RequestId>
  </ResponseMetadata>
</ListSSHPublicKeysResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListUserPolicies

Lists the names of the inline policies embedded in the specified IAM user.

An IAM user can also have managed policies attached to it. To list the managed policies that are attached to a user, use ListAttachedUserPolicies (p. 234). For more information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

You can paginate the results using the `MaxItems` and `Marker` parameters. If there are no inline policies embedded with the specified user, the operation returns an empty list.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the user to list policies for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

PolicyNames.member.N

A list of policy names.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListUserPolicies.

Sample Request

```
https://iam.amazonaws.com/?Action=ListUserPolicies
&UserName=Bob
```

```
&AUTHPARAMS
```

Sample Response

```
<ListUserPoliciesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ListUserPoliciesResult>
    <PolicyNames>
       <member>AllAccessPolicy</member>
       <member>KeyPolicy</member>
    </PolicyNames>
    <IsTruncated>false</IsTruncated>
 </ListUserPoliciesResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ListUserPoliciesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListUsers

Lists the IAM users that have the specified path prefix. If no path prefix is specified, the operation returns all users in the AWS account. If there are none, the operation returns an empty list.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PathPrefix

The path prefix for filtering the results. For example: `/division_abc/subdivision_xyz/`, which would get all user names whose path starts with `/division_abc/subdivision_xyz/`.

This parameter is optional. If it is not included, it defaults to a slash (/), listing all user names. This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `\u002F[\u0021-\u007F]*`

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Users.member.N

A list of users.

Type: Array of User (p. 499) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ListUsers.

Sample Request

```
https://iam.amazonaws.com/?Action=ListUsers
&PathPrefix=/division_abc/subdivision_xyz/product_1234/engineering/
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListUsersResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ListUsersResult>
    <Users>
       <member>
```

```
          <UserId>AID2MAB8DPLSRHEXAMPLE</UserId>
          <Path>/division_abc/subdivision_xyz/engineering/</Path>
          <UserName>Andrew</UserName>
          <Arn>arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/engineering/
Andrew</Arn>
          <CreateDate>2012-09-05T19:38:48Z</CreateDate>
          <PasswordLastUsed>2014-09-08T21:47:36Z</PasswordLastUsed>
       </member>
       <member>
          <UserId>AIDIODR4TAW7CSEXAMPLE</UserId>
          <Path>/division_abc/subdivision_xyz/engineering/</Path>
          <UserName>Jackie</UserName>
          <Arn>arn:aws:iam::123456789012:user/division_abc/subdivision_xyz/engineering/
Jackie</Arn>
          <CreateDate>2014-04-09T15:43:45Z</CreateDate>
          <PasswordLastUsed>2014-09-24T16:18:07Z</PasswordLastUsed>
       </member>
    </Users>
    <IsTruncated>false</IsTruncated>
 </ListUsersResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ListUsersResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListUserTags

Lists the tags that are attached to the specified user. The returned list of tags is sorted by tag key. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

(Optional) Use this only when paginating results to indicate the maximum number of items that you want in the response. If additional items exist beyond the maximum that you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, it defaults to 100. Note that IAM might return fewer results, even when more results are available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

UserName

The name of the IAM user whose tags you want to see.

This parameter accepts (through its regex pattern) a string of characters that consist of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can use the `Marker` request parameter to make a subsequent pagination request that retrieves more items. Note that IAM might return fewer than the `MaxItems` number of results even when more results are available. Check `IsTruncated` after every call to ensure that you receive all of your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Tags.member.N

The list of tags that are currently attached to the user. Each tag consists of a key name and an associated value. If no tags are attached to the specified user, the response contains an empty list.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

The following example is formatted with line breaks for legibility.

This example shows how to list the tags attached to a user whose IAM user name is `anika`.

Sample Request

```
POST / HTTP/1.1
Host: https://iam.amazonaws.com
Accept-Encoding: identity
User-Agent: aws-cli/1.11.143 Python/3.6.1 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.7.1
X-Amz-Date: 20170929T182447Z
```

```
Authorization: <auth details>
Content-Length: 55
Content-Type: application/x-www-form-urlencoded

Action=ListUserTags&Version=2010-05-08&UserName=anika
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE
Content-Type: text/xml
Content-Length: 484
Date: Fri, 29 Sep 2017 18:24:47 GMT

&ListUserTagsResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  &ListUserTagsResult>
    &IsTruncated>false&/IsTruncated>
    &Tags>
      &member>
        &Value>12345&/Value>
        &Key>Dept&/Key>
      &/member>
      &member>
        &Value>Accounting&/Value>
        &Key>Team&/Key>
      &/member>
    &/Tags>
  &/ListUserTagsResult>
  &ResponseMetadata>
    &RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE&/RequestId>
  &/ResponseMetadata>
&/ListUserTagsResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListVirtualMFADevices

Lists the virtual MFA devices defined in the AWS account by assignment status. If you do not specify an assignment status, the operation returns a list of all virtual MFA devices. Assignment status can be `Assigned`, `Unassigned`, or `Any`.

You can paginate the results using the `MaxItems` and `Marker` parameters.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AssignmentStatus

The status (`Unassigned` or `Assigned`) of the devices to list. If you do not specify an `AssignmentStatus`, the operation defaults to `Any`, which lists both assigned and unassigned virtual MFA devices.,

Type: String

Valid Values: `Assigned | Unassigned | Any`

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

Response Elements

The following elements are returned by the service.

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

VirtualMFADevices.member.N

The list of virtual MFA devices in the current account that match the `AssignmentStatus` value that was passed in the request.

Type: Array of VirtualMFADevice (p. 504) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

Examples

Example

This example illustrates one usage of ListVirtualMFADevices.

Sample Request

```
https://iam.amazonaws.com/?Action=ListVirtualMFADevices
&AssignmentStatus=Any
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ListVirtualMFADevicesResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ListVirtualMFADevicesResult>
  <IsTruncated>false</IsTruncated>
  <VirtualMFADevices>
    <member>
      <SerialNumber>
      arn:aws:iam::123456789012:mfa/MFAdeviceName
      </SerialNumber>
    </member>
    <member>
      <SerialNumber>
      arn:aws:iam::123456789012:mfa/RootMFAdeviceName
      </SerialNumber>
      <EnableDate>2011-10-20T20:49:03Z</EnableDate>
      <User>
```

```
        <UserId>123456789012</UserId>
        <Arn>arn:aws:iam::123456789012:root</Arn>
        <CreateDate>2009-10-13T22:00:36Z</CreateDate>
      </User>
    </member>
    <member>
      <SerialNumber>
      arn:aws:iam:::mfa/ExampleUserMFAdeviceName
      </SerialNumber>
      <EnableDate>2011-10-31T20:45:02Z</EnableDate>
      <User>
        <UserId>AIDEXAMPLE4EXAMPLEXYZ</UserId>
        <Path>/</Path>
        <UserName>ExampleUser</UserName>
        <Arn>arn:aws:iam::111122223333:user/ExampleUser</Arn>
        <CreateDate>2011-07-01T17:23:07Z</CreateDate>
      </User>
    </member>
  </VirtualMFADevices>
</ListVirtualMFADevicesResult>
<ResponseMetadata>
  <RequestId>b61ce1b1-0401-11e1-b2f8-2dEXAMPLEbfc</RequestId>
</ResponseMetadata>
</ListVirtualMFADevicesResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutGroupPolicy

Adds or updates an inline policy document that is embedded in the specified IAM group.

A user can also have managed policies attached to it. To attach a managed policy to a group, use AttachGroupPolicy (p. 13). To create a new managed policy, use CreatePolicy (p. 43). For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For information about limits on the number of inline policies that you can embed in a group, see Limitations on IAM Entities in the *IAM User Guide*.

Note
Because policy documents can be large, you should use POST rather than GET when calling `PutGroupPolicy`. For general information about using the Query API with IAM, go to Making Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name of the group to associate the policy with.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

PolicyDocument

The policy document.

You must provide policies in JSON format in IAM. However, for AWS CloudFormation templates formatted in YAML, you can provide the policy in JSON or YAML format. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PolicyName

The name of the policy document.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of PutGroupPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=PutGroupPolicy
&GroupName=Admins
```

```
&PolicyName=AdminRoot
&PolicyDocument={"Version":"2012-10-17","Statement":
{"Effect":"Allow","Action":"*","Resource":"*"}}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<PutGroupPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</PutGroupPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutRolePermissionsBoundary

Adds or updates the policy that is specified as the IAM role's permissions boundary. You can use an AWS managed policy or a customer managed policy to set the boundary for a role. Use the boundary to control the maximum permissions that the role can have. Setting a permissions boundary is an advanced feature that can affect the permissions for the role.

You cannot set the boundary for a service-linked role.

> **Important**
> Policies used as permissions boundaries do not provide permissions. You must also attach a permissions policy to the role. To learn how the effective permissions for a role are evaluated, see IAM JSON Policy Evaluation Logic in the IAM User Guide.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PermissionsBoundary

The ARN of the policy that is used to set the permissions boundary for the role.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

RoleName

The name (friendly name, not ARN) of the IAM role for which you want to set the permissions boundary.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PolicyNotAttachable

The request failed because AWS service role policies can only be attached to the service-linked role for that service.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutRolePolicy

Adds or updates an inline policy document that is embedded in the specified IAM role.

When you embed an inline policy in a role, the inline policy is used as part of the role's access (permissions) policy. The role's trust policy is created at the same time as the role, using CreateRole (p. 50). You can update a role's trust policy using UpdateAssumeRolePolicy (p. 376). For more information about IAM roles, go to Using Roles to Delegate Permissions and Federate Identities.

A role can also have a managed policy attached to it. To attach a managed policy to a role, use AttachRolePolicy (p. 16). To create a new managed policy, use CreatePolicy (p. 43). For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For information about limits on the number of inline policies that you can embed with a role, see Limitations on IAM Entities in the *IAM User Guide*.

Note
Because policy documents can be large, you should use POST rather than GET when calling `PutRolePolicy`. For general information about using the Query API with IAM, go to Making Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyDocument

The policy document.

You must provide policies in JSON format in IAM. However, for AWS CloudFormation templates formatted in YAML, you can provide the policy in JSON or YAML format. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PolicyName

The name of the policy document.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

RoleName

The name of the role to associate the policy with.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of PutRolePolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=PutRolePolicy
&RoleName=S3Access
&PolicyName=S3AccessPolicy
&PolicyDocument={"Version":"2012-10-17","Statement":
{"Effect":"Allow","Action":"s3:*","Resource":"*"}}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<PutRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</PutRolePolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutUserPermissionsBoundary

Adds or updates the policy that is specified as the IAM user's permissions boundary. You can use an AWS managed policy or a customer managed policy to set the boundary for a user. Use the boundary to control the maximum permissions that the user can have. Setting a permissions boundary is an advanced feature that can affect the permissions for the user.

> **Important**
> Policies that are used as permissions boundaries do not provide permissions. You must also attach a permissions policy to the user. To learn how the effective permissions for a user are evaluated, see IAM JSON Policy Evaluation Logic in the IAM User Guide.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PermissionsBoundary

The ARN of the policy that is used to set the permissions boundary for the user.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

UserName

The name (friendly name, not ARN) of the IAM user for which you want to set the permissions boundary.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PolicyNotAttachable

The request failed because AWS service role policies can only be attached to the service-linked role for that service.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutUserPolicy

Adds or updates an inline policy document that is embedded in the specified IAM user.

An IAM user can also have a managed policy attached to it. To attach a managed policy to a user, use AttachUserPolicy (p. 19). To create a new managed policy, use CreatePolicy (p. 43). For information about policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

For information about limits on the number of inline policies that you can embed in a user, see Limitations on IAM Entities in the *IAM User Guide*.

Note
Because policy documents can be large, you should use POST rather than GET when calling `PutUserPolicy`. For general information about using the Query API with IAM, go to Making Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyDocument

The policy document.

You must provide policies in JSON format in IAM. However, for AWS CloudFormation templates formatted in YAML, you can provide the policy in JSON or YAML format. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

PolicyName

The name of the policy document.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

UserName

The name of the user to associate the policy with.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of PutUserPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=PutUserPolicy
&UserName=Bob
```

```
&PolicyName=AllAccessPolicy
&PolicyDocument={"Version":"2012-10-17","Statement":
{"Effect":"Allow","Action":"*","Resource":"*"}}
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<PutUserPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</PutUserPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RemoveClientIDFromOpenIDConnectProvider

Removes the specified client ID (also known as audience) from the list of client IDs registered for the specified IAM OpenID Connect (OIDC) provider resource object.

This operation is idempotent; it does not fail or return an error if you try to remove a client ID that does not exist.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ClientID

The client ID (also known as audience) to remove from the IAM OIDC provider resource. For more information about client IDs, see CreateOpenIDConnectProvider (p. 39).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Required: Yes

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the IAM OIDC provider resource to remove the client ID from. You can get a list of OIDC provider ARNs by using the ListOpenIDConnectProviders (p. 260) operation.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of RemoveClientIDFromOpenIDConnectProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=RemoveClientIDFromOpenIDConnectProvider
&ClientID=my-application-ID
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<RemoveClientIDFromOpenIDConnectProviderResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>1a5214df-4f67-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</RemoveClientIDFromOpenIDConnectProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RemoveRoleFromInstanceProfile

Removes the specified IAM role from the specified EC2 instance profile.

> **Important**
> Make sure that you do not have any Amazon EC2 instances running with the role you are about to remove from the instance profile. Removing a role from an instance profile that is associated with a running instance might break any applications running on the instance.

For more information about IAM roles, go to Working with Roles. For more information about instance profiles, go to About Instance Profiles.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

InstanceProfileName

The name of the instance profile to update.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

RoleName

The name of the role to remove.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of RemoveRoleFromInstanceProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=RemoveRoleFromInstanceProfile
&InstanceProfileName=Webserver
&RoleName=S3Access
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<RemoveRoleFromInstanceProfileResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ResponseMetadata>
  <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</RemoveRoleFromInstanceProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

RemoveUserFromGroup

Removes the specified user from the specified group.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

The name of the group to update.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

UserName

The name of the user to remove.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of RemoveUserFromGroup.

Sample Request

```
https://iam.amazonaws.com/?Action=RemoveUserFromGroup
&GroupName=Managers
&UserName=Bob
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<RemoveUserFromGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</RemoveUserFromGroupResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ResetServiceSpecificCredential

Resets the password for a service-specific credential. The new password is AWS generated and cryptographically strong. It cannot be configured by the user. Resetting the password immediately invalidates the previous password associated with this user.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ServiceSpecificCredentialId

The unique identifier of the service-specific credential.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The name of the IAM user associated with the service-specific credential. If this value is not specified, then the operation assumes the user whose credentials are used to call the operation.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following element is returned by the service.

ServiceSpecificCredential

A structure with details about the updated service-specific credential, including the new password.

Important
This is the **only** time that you can access the password. You cannot recover the password later, but you can reset it again.

Type: ServiceSpecificCredential (p. 485) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

The following example shows how to request a new password for an existing service-specific credential that is associated with a specific IAM user.

Sample Request

```
https://iam.amazonaws.com/?Action=ResetServiceSpecificCredential
&UserName=Jane
&ServiceSpecificCredentialId=ACCA12345ABCDEXAMPLE
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ResetServiceSpecificCredentialResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResetServiceSpecificCredentialResult>
    <ServiceSpecificCredential>
      <CreateDate>2016-10-15T20:56:46.012Z</CreateDate>
      <ServiceName>codecommit.amazonaws.com</ServiceName>
      <ServiceUserName>Jane-123456789012</ServiceUserName>
      <ServicePassword>wJalrXUtnFEMI/K7MDENGPxRfiCYzEXAMPLE</ServicePassword>
      <ServiceSpecificCredentialId>ACCA12345ABCDEXAMPLE</ServiceSpecificCredentialId>
      <Status>Active</Status>
      <UserName>Jane</UserName>
    </ServiceSpecificCredential>
  </ResetServiceSpecificCredentialResult>
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</ResetServiceSpecificCredentialResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ResyncMFADevice

Synchronizes the specified MFA device with its IAM resource object on the AWS servers.

For more information about creating and working with virtual MFA devices, go to Using a Virtual MFA Device in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AuthenticationCode1

An authentication code emitted by the device.

The format for this parameter is a sequence of six digits.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `[\d]+`

Required: Yes

AuthenticationCode2

A subsequent authentication code emitted by the device.

The format for this parameter is a sequence of six digits.

Type: String

Length Constraints: Fixed length of 6.

Pattern: `[\d]+`

Required: Yes

SerialNumber

Serial number that uniquely identifies the MFA device.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 9. Maximum length of 256.

Pattern: `[\w+=/:,.@-]+`

Required: Yes

UserName

The name of the user whose MFA device you want to resynchronize.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidAuthenticationCode

The request was rejected because the authentication code was not recognized. The error message describes the specific error.

HTTP Status Code: 403

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of ResyncMFADevice.

Sample Request

```
https://iam.amazonaws.com/?Action=ResyncMFADevice
&UserName=Bob
&SerialNumber=R1234
&AuthenticationCode1=234567
&AuthenticationCode2=987654
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<ResyncMFADeviceResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
```

```
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</ResyncMFADeviceResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

SetDefaultPolicyVersion

Sets the specified version of the specified policy as the policy's default (operative) version.

This operation affects all users, groups, and roles that the policy is attached to. To list the users, groups, and roles that the policy is attached to, use the ListEntitiesForPolicy (p. 238) API.

For information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyArn

The Amazon Resource Name (ARN) of the IAM policy whose default version you want to set.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

VersionId

The version of the policy to set as the default (operative) version.

For more information about managed policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of SetDefaultPolicyVersion.

Sample Request

```
https://iam.amazonaws.com/?Action=SetDefaultPolicyVersion
&PolicyArn=arn:aws:iam::123456789012:policy/S3-read-only-example-bucket
&VersionId=v3
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SetDefaultPolicyVersionResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>35f241af-3ebc-11e4-9d0d-6f969EXAMPLE</RequestId>
  </ResponseMetadata>
</SetDefaultPolicyVersionResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

SetSecurityTokenServicePreferences

Sets the specified version of the global endpoint token as the token version used for the AWS account.

By default, AWS Security Token Service (STS) is available as a global service, and all STS requests go to a single endpoint at `https://sts.amazonaws.com`. AWS recommends using Regional STS endpoints to reduce latency, build in redundancy, and increase session token availability. For information about Regional endpoints for STS, see AWS Regions and Endpoints in the *AWS General Reference*.

If you make an STS call to the global endpoint, the resulting session tokens might be valid in some Regions but not others. It depends on the version that is set in this operation. Version 1 tokens are valid only in AWS Regions that are available by default. These tokens do not work in manually enabled Regions, such as Asia Pacific (Hong Kong). Version 2 tokens are valid in all Regions. However, version 2 tokens are longer and might affect systems where you temporarily store tokens. For information, see Activating and Deactivating STS in an AWS Region in the *IAM User Guide*.

To view the current session token version, see the `GlobalEndpointTokenVersion` entry in the response of the GetAccountSummary (p. 152) operation.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GlobalEndpointTokenVersion

The version of the global endpoint token. Version 1 tokens are valid only in AWS Regions that are available by default. These tokens do not work in manually enabled Regions, such as Asia Pacific (Hong Kong). Version 2 tokens are valid in all Regions. However, version 2 tokens are longer and might affect systems where you temporarily store tokens.

For information, see Activating and Deactivating STS in an AWS Region in the *IAM User Guide*.

Type: String

Valid Values: `v1Token | v2Token`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of SetSecurityTokenServicePreferences.

Sample Request

```
https://iam.amazonaws.com/?Action=SetSecurityTokenServicePreferences
&GlobalEndpointTokenVersion=v2token
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SetSecurityTokenServicePreferences xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>31a241af-1ebc-12b4-9d0d-8f876EXAMPLE</RequestId>
  </ResponseMetadata>
</SetSecurityTokenServicePreferences>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

SimulateCustomPolicy

Simulate how a set of IAM policies and optionally a resource-based policy works with a list of API operations and AWS resources to determine the policies' effective permissions. The policies are provided as strings.

The simulation does not perform the API operations; it only checks the authorization to determine if the simulated policies allow or deny the operations.

If you want to simulate existing policies that are attached to an IAM user, group, or role, use SimulatePrincipalPolicy (p. 346) instead.

Context keys are variables that are maintained by AWS and its services and which provide details about the context of an API query request. You can use the `Condition` element of an IAM policy to evaluate context keys. To get the list of context keys that the policies require for correct simulation, use GetContextKeysForCustomPolicy (p. 156).

If the output is long, you can use `MaxItems` and `Marker` parameters to paginate the results.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ActionNames.member.N

A list of names of API operations to evaluate in the simulation. Each operation is evaluated against each resource. Each operation must include the service identifier, such as `iam:CreateUser`. This operation does not support using wildcards (*) in an action name.

Type: Array of strings

Length Constraints: Minimum length of 3. Maximum length of 128.

Required: Yes

CallerArn

The ARN of the IAM user that you want to use as the simulated caller of the API operations. `CallerArn` is required if you include a `ResourcePolicy` so that the policy's `Principal` element has a value to use in evaluating the policy.

You can specify only the ARN of an IAM user. You cannot specify the ARN of an assumed role, federated user, or a service principal.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ContextEntries.member.N

A list of context keys and corresponding values for the simulation to use. Whenever a context key is evaluated in one of the simulated IAM permissions policies, the corresponding value is supplied.

Type: Array of ContextEntry (p. 431) objects

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PermissionsBoundaryPolicyInputList.member.N

The IAM permissions boundary policy to simulate. The permissions boundary sets the maximum permissions that an IAM entity can have. You can input only one permissions boundary when you pass a policy to this operation. For more information about permissions boundaries, see Permissions Boundaries for IAM Entities in the *IAM User Guide*. The policy input is specified as a string that contains the complete, valid JSON text of a permissions boundary policy.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

PolicyInputList.member.N

A list of policy documents to include in the simulation. Each document is specified as a string containing the complete, valid JSON text of an IAM policy. Do not include any resource-based policies in this parameter. Any resource-based policy must be submitted with the `ResourcePolicy` parameter. The policies cannot be "scope-down" policies, such as you could include in a call to

GetFederationToken or one of the AssumeRole API operations. In other words, do not use policies designed to restrict what a user can do while using the temporary credentials.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

ResourceArns.member.N

A list of ARNs of AWS resources to include in the simulation. If this parameter is not provided, then the value defaults to `*` (all resources). Each API in the `ActionNames` parameter is evaluated for each resource in this list. The simulation determines the access result (allowed or denied) of each combination and reports it in the response.

The simulation does not automatically retrieve policies for the specified resources. If you want to include a resource policy in the simulation, then you must include the policy as a string in the `ResourcePolicy` parameter.

If you include a `ResourcePolicy`, then it must be applicable to all of the resources included in the simulation or you receive an invalid input error.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ResourceHandlingOption

Specifies the type of simulation to run. Different API operations that support resource-based policies require different combinations of resources. By specifying the type of simulation to run, you enable the policy simulator to enforce the presence of the required resources to ensure reliable simulation results. If your simulation does not match one of the following scenarios, then you can omit this parameter. The following list shows each of the supported scenario values and the resources that you must define to run the simulation.

Each of the EC2 scenarios requires that you specify instance, image, and security-group resources. If your scenario includes an EBS volume, then you must specify that volume as a resource. If the EC2 scenario includes VPC, then you must supply the network-interface resource. If it includes an IP subnet, then you must specify the subnet resource. For more information on the EC2 scenario options, see Supported Platforms in the *Amazon EC2 User Guide*.

- **EC2-Classic-InstanceStore**

  instance, image, security-group
- **EC2-Classic-EBS**

instance, image, security-group, volume

- **EC2-VPC-InstanceStore**

  instance, image, security-group, network-interface
- **EC2-VPC-InstanceStore-Subnet**

  instance, image, security-group, network-interface, subnet
- **EC2-VPC-EBS**

  instance, image, security-group, network-interface, volume
- **EC2-VPC-EBS-Subnet**

  instance, image, security-group, network-interface, subnet, volume

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Required: No

ResourceOwner

An ARN representing the AWS account ID that specifies the owner of any simulated resource that does not identify its owner in the resource ARN. Examples of resource ARNs include an S3 bucket or object. If `ResourceOwner` is specified, it is also used as the account owner of any `ResourcePolicy` included in the simulation. If the `ResourceOwner` parameter is not specified, then the owner of the resources and the resource policy defaults to the account of the identity provided in `CallerArn`. This parameter is required only if you specify a resource-based policy and account that owns the resource is different from the account that owns the simulated calling user `CallerArn`.

The ARN for an account uses the following syntax: `arn:aws:iam::`*`AWS-account-ID`*`:root`. For example, to represent the account with the 112233445566 ID, use the following ARN: `arn:aws:iam::112233445566-ID:root`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ResourcePolicy

A resource-based policy to include in the simulation provided as a string. Each resource in the simulation is treated as if it had this policy attached. You can include only one resource-based policy in a simulation.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

Response Elements

The following elements are returned by the service.

EvaluationResults.member.N

The results of the simulation.

Type: Array of EvaluationResult (p. 437) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

PolicyEvaluation

The request failed because a provided policy could not be successfully evaluated. An additional detailed message indicates the source of the failure.

HTTP Status Code: 500

Examples

Example: Using Context Keys in a Policy Simulation

This example specifies a policy by string and supplies a `ContextEntry` to use for the context key that the policy references. Note that all parameters are shown in unencoded form here for clarity but must be URL encoded to be included as a part of a real HTML request. The results show that the policy allows `s3:ListBucket` access to the S3 bucket named `teambucket`.

Sample Request

```
https://iam.amazonaws.com/Action=SimulateCustomPolicy
&ActionNames.member.1=s3:ListBucket
&ResourceArns.member.1=arn:aws:s3:::teambucket
&ContextEntries.member.1.ContextKeyName=aws:MultiFactorAuthPresent
&ContextEntries.member.1.ContextKeyType=boolean
&ContextEntries.member.1.ContextKeyValues.member.1=true
&PermissionsBoundaryPolicyInputList.member.1='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Deny",
    "Action":{"iam:GetRole","iam:CreateRole","iam:DeleteRole"},
    "Resource":{"*"}
    }
}'
&PolicyInputList.member.1='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Action":"s3:ListBucket",
    "Resource":"arn:aws:s3:::teambucket",
    "Condition":{
      "Bool":{"aws:MultiFactorAuthPresent":"true"}
    }
  }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SimulateCustomPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <SimulateCustomPolicyResult>
    <IsTruncated>false</IsTruncated>
    <EvaluationResults>
      <member>
        <MatchedStatements>
          <member>
            <SourcePolicyId>PolicyInputList.1</SourcePolicyId>
            <EndPosition>
              <Column>4</Column>
              <Line>11</Line>
            </EndPosition>
            <StartPosition>
              <Column>16</Column>
              <Line>4</Line>
            </StartPosition>
          </member>
        </MatchedStatements>
        <MissingContextValues/>
        <EvalResourceName>arn:aws:s3:::teambucket</EvalResourceName>
        <EvalDecision>allowed</EvalDecision>
        <EvalActionName>s3:ListBucket</EvalActionName>
      </member>
    </EvaluationResults>
  </SimulateCustomPolicyResult>
  <ResponseMetadata>
    <RequestId>1cdb5b0a-4c15-11e5-b121-bd8c7EXAMPLE</RequestId>
  </ResponseMetadata>
</SimulateCustomPolicyResponse>
```

Example: Same-Account Simulation

This example specifies an identity-based policy and a permissions boundary for the user Mateo. Both policies allow IAM actions only. However, a resource-based policy permits Mateo to perform the actions `s3:Put*` or `s3:List*` on the Production bucket. As a result, the simulation allows the action. Note that for same-account simulations where a resource ARN is specified, the `EvalDecisionDetails` parameter is returned, but the response is empty.

Sample Request

```
https://iam.amazonaws.com/Action=SimulateCustomPolicy
&ActionNames.member.1=s3:PutObject
&CallerArn:arn:aws:iam::111122223333:user/mateo
&ResourceArns.member.1=arn:aws:s3:::production/Test
&ResourceOwner=arn:aws:iam::111122223333:root
&PermissionsBoundaryPolicyInputList.member.1='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Action":{"iam:*"},
    "Resource":{"*"}
 }
}'
&PolicyInputList.member.1='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Action":{"iam:*"},
    "Resource":{"*"}
 }
}'
&ResourcePolicy='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Principal":{"AWS":"arn:aws:iam::111122223333:user/mateo"}
    "Action":{"s3:List*","s3:Put*"},
    "Resource":{"arn:aws:s3:::production/*"}
 }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SimulateCustomPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
    <SimulateCustomPolicyResult>
        <IsTruncated>false</IsTruncated>
        <EvaluationResults>
            <member>
                <EvalDecisionDetails/>
                <PermissionsBoundaryDecisionDetail>
                    <AllowedByPermissionsBoundary>false</AllowedByPermissionsBoundary>
                </PermissionsBoundaryDecisionDetail>
                <MatchedStatements>
                    <member>
                        <SourcePolicyId>ResourcePolicy</SourcePolicyId>
                        <EndPosition>
                            <Column>259</Column>
                            <Line>1</Line>
                        </EndPosition>
                        <SourcePolicyType>Resource Policy</SourcePolicyType>
```

```
                        <StartPosition>
                            <Column>68</Column>
                            <Line>1</Line>
                        </StartPosition>
                    </member>
                </MatchedStatements>
                <MissingContextValues/>
                <EvalResourceName>arn:aws:s3:::production/Test</EvalResourceName>
                <EvalDecision>allowed</EvalDecision>
                <EvalActionName>s3:PutObject</EvalActionName>
                <ResourceSpecificResults>
                    <member>
                        <PermissionsBoundaryDecisionDetail>
                            <AllowedByPermissionsBoundary>false</
AllowedByPermissionsBoundary>
                        </PermissionsBoundaryDecisionDetail>
                        <MatchedStatements>
                            <member>
                                <SourcePolicyId>ResourcePolicy</SourcePolicyId>
                                <EndPosition>
                                    <Column>259</Column>
                                    <Line>1</Line>
                                </EndPosition>
                                <SourcePolicyType>Resource Policy</SourcePolicyType>
                                <StartPosition>
                                    <Column>68</Column>
                                    <Line>1</Line>
                                </StartPosition>
                            </member>
                        </MatchedStatements>
                        <EvalResourceDecision>allowed</EvalResourceDecision>
                        <MissingContextValues/>
                        <EvalResourceName>arn:aws:s3:::production/Test</EvalResourceName>
                    </member>
                </ResourceSpecificResults>
            </member>
        </EvaluationResults>
    </SimulateCustomPolicyResult>
    <ResponseMetadata>
        <RequestId>7b2092ca-5d35-499d-bc6d-e9b49EXAMPLE</RequestId>
    </ResponseMetadata>
</SimulateCustomPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

SimulatePrincipalPolicy

Simulate how a set of IAM policies attached to an IAM entity works with a list of API operations and AWS resources to determine the policies' effective permissions. The entity can be an IAM user, group, or role. If you specify a user, then the simulation also includes all of the policies that are attached to groups that the user belongs to.

You can optionally include a list of one or more additional policies specified as strings to include in the simulation. If you want to simulate only policies specified as strings, use SimulateCustomPolicy (p. 338) instead.

You can also optionally include one resource-based policy to be evaluated with each of the resources included in the simulation.

The simulation does not perform the API operations; it only checks the authorization to determine if the simulated policies allow or deny the operations.

Note: This API discloses information about the permissions granted to other users. If you do not want users to see other user's permissions, then consider allowing them to use SimulateCustomPolicy (p. 338) instead.

Context keys are variables maintained by AWS and its services that provide details about the context of an API query request. You can use the `Condition` element of an IAM policy to evaluate context keys. To get the list of context keys that the policies require for correct simulation, use GetContextKeysForPrincipalPolicy (p. 159).

If the output is long, you can use the `MaxItems` and `Marker` parameters to paginate the results.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ActionNames.member.N

A list of names of API operations to evaluate in the simulation. Each operation is evaluated for each resource. Each operation must include the service identifier, such as `iam:CreateUser`.

Type: Array of strings

Length Constraints: Minimum length of 3. Maximum length of 128.

Required: Yes

CallerArn

The ARN of the IAM user that you want to specify as the simulated caller of the API operations. If you do not specify a `CallerArn`, it defaults to the ARN of the user that you specify in `PolicySourceArn`, if you specified a user. If you include both a `PolicySourceArn` (for example, `arn:aws:iam::123456789012:user/David`) and a `CallerArn` (for example, `arn:aws:iam::123456789012:user/Bob`), the result is that you simulate calling the API operations as Bob, as if Bob had David's policies.

You can specify only the ARN of an IAM user. You cannot specify the ARN of an assumed role, federated user, or a service principal.

`CallerArn` is required if you include a `ResourcePolicy` and the `PolicySourceArn` is not the ARN for an IAM user. This is required so that the resource-based policy's `Principal` element has a value to use in evaluating the policy.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ContextEntries.member.N

A list of context keys and corresponding values for the simulation to use. Whenever a context key is evaluated in one of the simulated IAM permissions policies, the corresponding value is supplied.

Type: Array of ContextEntry (p. 431) objects

Required: No

Marker

Use this parameter only when paginating results and only after you receive a response indicating that the results are truncated. Set it to the value of the `Marker` element in the response that you received to indicate where the next call should start.

Type: String

Length Constraints: Minimum length of 1.

Pattern: `[\u0020-\u00FF]+`

Required: No

MaxItems

Use this only when paginating results to indicate the maximum number of items you want in the response. If additional items exist beyond the maximum you specify, the `IsTruncated` response element is `true`.

If you do not include this parameter, the number of items defaults to 100. Note that IAM might return fewer results, even when there are more results available. In that case, the `IsTruncated` response element returns `true`, and `Marker` contains a value to include in the subsequent call that tells the service where to continue from.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1000.

Required: No

PermissionsBoundaryPolicyInputList.member.N

The IAM permissions boundary policy to simulate. The permissions boundary sets the maximum permissions that the entity can have. You can input only one permissions boundary when you pass a policy to this operation. An IAM entity can only have one permissions boundary in effect at a time. For example, if a permissions boundary is attached to an entity and you pass in a different permissions boundary policy using this parameter, then the new permissions boundary policy is used for the simulation. For more information about permissions boundaries, see Permissions Boundaries for IAM Entities in the *IAM User Guide*. The policy input is specified as a string containing the complete, valid JSON text of a permissions boundary policy.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range

- The printable characters in the Basic Latin and Latin-1 Supplement character set (through \u00FF)
- The special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D)

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: [\u0009\u000A\u000D\u0020-\u00FF]+

Required: No

PolicyInputList.member.N

An optional list of additional policy documents to include in the simulation. Each document is specified as a string containing the complete, valid JSON text of an IAM policy.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (\u0020) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through \u00FF)
- The special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D)

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: [\u0009\u000A\u000D\u0020-\u00FF]+

Required: No

PolicySourceArn

The Amazon Resource Name (ARN) of a user, group, or role whose policies you want to include in the simulation. If you specify a user, group, or role, the simulation includes all policies that are associated with that entity. If you specify a user, the simulation also includes all policies that are attached to any groups the user belongs to.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

ResourceArns.member.N

A list of ARNs of AWS resources to include in the simulation. If this parameter is not provided, then the value defaults to * (all resources). Each API in the ActionNames parameter is evaluated for each resource in this list. The simulation determines the access result (allowed or denied) of each combination and reports it in the response.

The simulation does not automatically retrieve policies for the specified resources. If you want to include a resource policy in the simulation, then you must include the policy as a string in the ResourcePolicy parameter.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ResourceHandlingOption

Specifies the type of simulation to run. Different API operations that support resource-based policies require different combinations of resources. By specifying the type of simulation to run, you enable the policy simulator to enforce the presence of the required resources to ensure reliable simulation results. If your simulation does not match one of the following scenarios, then you can omit this parameter. The following list shows each of the supported scenario values and the resources that you must define to run the simulation.

Each of the EC2 scenarios requires that you specify instance, image, and security group resources. If your scenario includes an EBS volume, then you must specify that volume as a resource. If the EC2 scenario includes VPC, then you must supply the network interface resource. If it includes an IP subnet, then you must specify the subnet resource. For more information on the EC2 scenario options, see Supported Platforms in the *Amazon EC2 User Guide*.

- **EC2-Classic-InstanceStore**

  instance, image, security group
- **EC2-Classic-EBS**

  instance, image, security group, volume
- **EC2-VPC-InstanceStore**

  instance, image, security group, network interface
- **EC2-VPC-InstanceStore-Subnet**

  instance, image, security group, network interface, subnet
- **EC2-VPC-EBS**

  instance, image, security group, network interface, volume
- **EC2-VPC-EBS-Subnet**

  instance, image, security group, network interface, subnet, volume

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Required: No

ResourceOwner

An AWS account ID that specifies the owner of any simulated resource that does not identify its owner in the resource ARN. Examples of resource ARNs include an S3 bucket or object. If `ResourceOwner` is specified, it is also used as the account owner of any `ResourcePolicy` included in the simulation. If the `ResourceOwner` parameter is not specified, then the owner of the resources and the resource policy defaults to the account of the identity provided in `CallerArn`. This parameter is required only if you specify a resource-based policy and account that owns the resource is different from the account that owns the simulated calling user `CallerArn`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

ResourcePolicy

A resource-based policy to include in the simulation provided as a string. Each resource in the simulation is treated as if it had this policy attached. You can include only one resource-based policy in a simulation.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

Response Elements

The following elements are returned by the service.

EvaluationResults.member.N

The results of the simulation.

Type: Array of EvaluationResult (p. 437) objects

IsTruncated

A flag that indicates whether there are more items to return. If your results were truncated, you can make a subsequent pagination request using the `Marker` request parameter to retrieve more items. Note that IAM might return fewer than the `MaxItems` number of results even when there are more results available. We recommend that you check `IsTruncated` after every call to ensure that you receive all your results.

Type: Boolean

Marker

When `IsTruncated` is `true`, this element is present and contains the value to use for the `Marker` parameter in a subsequent pagination request.

Type: String

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PolicyEvaluation

The request failed because a provided policy could not be successfully evaluated. An additional detailed message indicates the source of the failure.

HTTP Status Code: 500

Examples

Example: Simulating a Policy

This example simulates calling the Amazon S3 API operations GetObject, PutObject, and DeleteObject for a specific S3 bucket. The simulation includes all policies that are attached to the user Jill. In this example, the user Jill has only the managed policy "AmazonS3ReadOnlyAccess" attached. Note that all parameters are shown in unencoded form here for clarity but must be URL encoded to be included as a part of a real HTML request. In the results, the simulation shows that Jill can add new files to the bucket because of the additional policy specified as a string parameter. In addition, she can read from the bucket because of the managed policy attached to the user. However, she cannot delete anything from the S3 bucket because of the default `implicitDeny`.

Sample Request

```
https://iam.amazonaws.com/Action=SimulatePrincipalPolicy
&ActionNames.member.1=s3:PutObject
&ActionNames.member.2=s3:GetObject
&ActionNames.member.3=s3:DeleteObject
&ResourceArns.member.1="arn:aws:s3:::my-test-bucket"
&PolicySourceArn=arn:aws:iam:::user/Jill
&PolicyInputList.member.1='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Action":"s3:PutObject",
    "Resource":"arn:aws:s3:::my-test-bucket"
  }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SimulatePrincipalPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <SimulatePrincipalPolicyResult>
    <IsTruncated>false</IsTruncated>
    <EvaluationResults>
      <member>
        <MatchedStatements>
          <member>
            <SourcePolicyId>PolicyInputList.1</SourcePolicyId>
            <EndPosition>
```

```
              <Column>4</Column>
              <Line>7</Line>
            </EndPosition>
            <StartPosition>
              <Column>16</Column>
              <Line>3</Line>
            </StartPosition>
          </member>
        </MatchedStatements>
        <MissingContextValues/>
        <EvalResourceName>arn:aws:s3:::my-test-bucket</EvalResourceName>
        <EvalDecision>allowed</EvalDecision>
        <EvalActionName>s3:PutObject</EvalActionName>
      </member>
      <member>
        <MatchedStatements>
          <member>
            <SourcePolicyId>AmazonS3ReadOnlyAccess</SourcePolicyId>
            <EndPosition>
              <Column>6</Column>
              <Line>11</Line>
            </EndPosition>
            <StartPosition>
              <Column>17</Column>
              <Line>3</Line>
            </StartPosition>
          </member>
        </MatchedStatements>
        <MissingContextValues/>
        <EvalResourceName>arn:aws:s3:::my-test-bucket</EvalResourceName>
        <EvalDecision>allowed</EvalDecision>
        <EvalActionName>s3:GetObject</EvalActionName>
      </member>
      <member>
        <MatchedStatements/>
        <MissingContextValues/>
        <EvalResourceName>arn:aws:s3:::my-test-bucket</EvalResourceName>
        <EvalDecision>implicitDeny</EvalDecision>
        <EvalActionName>s3:DeleteObject</EvalActionName>
      </member>
    </EvaluationResults>
  </SimulatePrincipalPolicyResult>
  <ResponseMetadata>
    <RequestId>004d7059-4c14-11e5-b121-bd8c7EXAMPLE</RequestId>
  </ResponseMetadata>
</SimulatePrincipalPolicyResponse>
```

Example: Same-Account Simulation

This example evaluates policies in the same account only. The simulated user Mateo has an identity-based policy attached that allows the `iam:GetRole` action. The permissions boundary policy specified in the simulation allows all IAM and S3 actions. Note that for same-account simulations where a resource ARN is specified, the `EvalDecisionDetails` parameter is returned, but the response is empty.

Sample Request

```
https://iam.amazonaws.com/Action=SimulatePrincipalPolicy
&ActionNames.member.1=iam:GetRole
&ResourceArns.member.1="arn:aws:iam::111122223333:role/pol-sim-test"
&PolicySourceArn=arn:aws:iam::111122223333:user/mateo
&PermissionsBoundaryPolicyInputList.member.1='{
```

```
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Action":{"iam:*","s3:*"},
    "Resource":{"*"}
  }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<SimulatePrincipalPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
    <SimulatePrincipalPolicyResult>
        <IsTruncated>false</IsTruncated>
        <EvaluationResults>
            <member>
                <EvalDecisionDetails/>
                <PermissionsBoundaryDecisionDetail>
                    <AllowedByPermissionsBoundary>true</AllowedByPermissionsBoundary>
                </PermissionsBoundaryDecisionDetail>
                <MatchedStatements>
                    <member>
                        <SourcePolicyId>user_admin_AdminUser</SourcePolicyId>
                        <EndPosition>
                            <Column>84</Column>
                            <Line>1</Line>
                        </EndPosition>
                        <SourcePolicyType>IAM Policy</SourcePolicyType>
                        <StartPosition>
                            <Column>38</Column>
                            <Line>1</Line>
                        </StartPosition>
                    </member>
                </MatchedStatements>
                <MissingContextValues/>
                <EvalResourceName>arn:aws:iam::111122223333:role/pol-sim-test</
EvalResourceName>
                <EvalDecision>allowed</EvalDecision>
                <EvalActionName>iam:GetRole</EvalActionName>
                <ResourceSpecificResults>
                    <member>
                        <PermissionsBoundaryDecisionDetail>
                            <AllowedByPermissionsBoundary>true</
AllowedByPermissionsBoundary>
                        </PermissionsBoundaryDecisionDetail>
                        <MatchedStatements>
                            <member>
                                <SourcePolicyId>user_admin_AdminUser</SourcePolicyId>
                                <EndPosition>
                                    <Column>84</Column>
                                    <Line>1</Line>
                                </EndPosition>
                                <SourcePolicyType>IAM Policy</SourcePolicyType>
                                <StartPosition>
                                    <Column>38</Column>
                                    <Line>1</Line>
                                </StartPosition>
                            </member>
                        </MatchedStatements>
                        <EvalResourceDecision>allowed</EvalResourceDecision>
                        <MissingContextValues/>
                        <EvalResourceName>arn:aws:iam::111122223333:role/pol-sim-test</
EvalResourceName>
```

```
                    </member>
                </ResourceSpecificResults>
            </member>
        </EvaluationResults>
    </SimulatePrincipalPolicyResult>
    <ResponseMetadata>
        <RequestId>896e97bd-ff20-47d0-9f91-5d696EXAMPLE</RequestId>
    </ResponseMetadata>
</SimulatePrincipalPolicyResponse>
```

Example: Cross-Account Simulation

This example is for a simulation that evaluates policies in two accounts. The resource-based policy allows the `s3:PutObject` action for the user Arnav on Mary's bucket in Account 2. However, the overall result of the simulation for the action is implicitly denied. Arnav's identity-based policy in Account 1 does not allow the action. Additionally, the permissions boundary set for Arnav in Account 1 does not allow S3 actions. The results of each of the policy types included in the simulation is returned in the `EvalDecisionDetails` parameter.

Sample Request

```
https://iam.amazonaws.com/Action=SimulatePrincipalPolicy
&ActionNames.member.1=s3:PutObject
&ResourceArns.member.1="arn:aws:s3:::mary/Test"
&ResourceOwner=arn:aws:iam::123456789012:root
&PolicySourceArn=arn:aws:iam::444455556666:user/arnav
&PermissionsBoundaryPolicyInputList.member.1='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Action":{"iam:*"},
    "Resource":{"*"}
 }
}'
&ResourcePolicy='{
  "Version":"2012-10-17",
  "Statement":{
    "Effect":"Allow",
    "Principal":{"AWS":"arn:aws:iam::444455556666:user/arnav"}
    "Action":{"s3:List*","s3:Put*"},
    "Resource":{"arn:aws:s3:::mary/*"}
 }
}'
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
SimulatePrincipalPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
    <SimulatePrincipalPolicyResult>
        <IsTruncated>false</IsTruncated>
        <EvaluationResults>
            <member>
                <EvalDecisionDetails>
                    <entry>
                        <key>IAM Policy</key>
                        <value>implicitDeny</value>
                    </entry>
                    <entry>
                        <key>Resource Policy</key>
                        <value>allowed</value>
```

```
                    </entry>
                    <entry>
                        <key>Permissions Boundary Policy</key>
                        <value>implicitDeny</value>
                    </entry>
                </EvalDecisionDetails>
                <PermissionsBoundaryDecisionDetail>
                    <AllowedByPermissionsBoundary>false</AllowedByPermissionsBoundary>
                </PermissionsBoundaryDecisionDetail>
                <MatchedStatements/>
                <MissingContextValues/>
                <EvalResourceName>arn:aws:s3:::mary/Test</EvalResourceName>
                <EvalDecision>implicitDeny</EvalDecision>
                <EvalActionName>s3:PutObject</EvalActionName>
                <ResourceSpecificResults>
                    <member>
                        <EvalDecisionDetails>
                            <entry>
                                <key>Permissions Boundary Policy</key>
                                <value>implicitDeny</value>
                            </entry>
                            <entry>
                                <key>IAM Policy</key>
                                <value>implicitDeny</value>
                            </entry>
                            <entry>
                                <key>Resource Policy</key>
                                <value>allowed</value>
                            </entry>
                        </EvalDecisionDetails>
                        <PermissionsBoundaryDecisionDetail>
                            <AllowedByPermissionsBoundary>false</
AllowedByPermissionsBoundary>
                        </PermissionsBoundaryDecisionDetail>
                        <MatchedStatements>
                            <member>
                                <SourcePolicyId>ResourcePolicy</SourcePolicyId>
                                <EndPosition>
                                    <Column>259</Column>
                                    <Line>1</Line>
                                </EndPosition>
                                <SourcePolicyType>Resource Policy</SourcePolicyType>
                                <StartPosition>
                                    <Column>68</Column>
                                    <Line>1</Line>
                                </StartPosition>
                            </member>
                        </MatchedStatements>
                        <EvalResourceDecision>implicitDeny</EvalResourceDecision>
                        <MissingContextValues/>
                        <EvalResourceName>arn:aws:s3:::mary/Test</EvalResourceName>
                    </member>
                </ResourceSpecificResults>
            </member>
        </EvaluationResults>
    </SimulatePrincipalPolicyResult>
    <ResponseMetadata>
        <RequestId>3ebb073c-781a-437e-81a9-2a88eEXAMPLE</RequestId>
    </ResponseMetadata>
</SimulatePrincipalPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagRole

Adds one or more tags to an IAM role. The role can be a regular role or a service-linked role. If a tag with the same key name already exists, then that tag is overwritten with the new value.

A tag consists of a key name and an associated value. By assigning tags to your resources, you can do the following:

- **Administrative grouping and discovery** - Attach tags to resources to aid in organization and search. For example, you could search for all resources with the key name *Project* and the value *MyImportantProject*. Or search for all resources with the key name *Cost Center* and the value *41200*.
- **Access control** - Reference tags in IAM user-based and resource-based policies. You can use tags to restrict access to only an IAM user or role that has a specified tag attached. You can also restrict access to only those resources that have a certain tag attached. For examples of policies that show how to use tags to control access, see Control Access Using IAM Tags in the *IAM User Guide*.
- **Cost allocation** - Use tags to help track which individuals and teams are using which AWS resources.

Note

- Make sure that you have no invalid tags and that you do not exceed the allowed number of tags per role. In either case, the entire request fails and *no* tags are added to the role.
- AWS always interprets the tag `Value` as a single string. If you need to store an array, you can store comma-separated values in the string. However, you must interpret the value in your code.

For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

RoleName

The name of the role that you want to add tags to.

This parameter accepts (through its regex pattern) a string of characters that consist of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Tags.member.N

The list of tags that you want to attach to the role. Each tag consists of a key name and an associated value. You can specify this with a JSON string.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

The following example is formatted with line breaks for legibility.

The following example shows how to add tags to an existing role.

Sample Request

```
POST / HTTP/1.1
Host: https://iam.amazonaws.com
Accept-Encoding: identity
User-Agent: aws-cli/1.11.143 Python/3.6.1 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.7.1
X-Amz-Date: 20170929T180252Z
Authorization: <auth details>
Content-Length: 97
Content-Type: application/x-www-form-urlencoded
```

```
Action=TagRole&Version=2010-05-08&RoleName=taggedrole
       &Tags.member.1.Key=Dept&Tags.member.1.Value=Accounting
       &Tags.member.2.Key=Cost Center&Tags.member.2.Value=12345
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE
Content-Type: text/xml
Content-Length: 194
Date: Fri, 29 Sep 2017 18:02:51 GMT

<TagRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</TagRoleResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagUser

Adds one or more tags to an IAM user. If a tag with the same key name already exists, then that tag is overwritten with the new value.

A tag consists of a key name and an associated value. By assigning tags to your resources, you can do the following:

- **Administrative grouping and discovery** - Attach tags to resources to aid in organization and search. For example, you could search for all resources with the key name *Project* and the value *MyImportantProject*. Or search for all resources with the key name *Cost Center* and the value *41200*.
- **Access control** - Reference tags in IAM user-based and resource-based policies. You can use tags to restrict access to only an IAM requesting user or to a role that has a specified tag attached. You can also restrict access to only those resources that have a certain tag attached. For examples of policies that show how to use tags to control access, see Control Access Using IAM Tags in the *IAM User Guide*.
- **Cost allocation** - Use tags to help track which individuals and teams are using which AWS resources.

Note

- Make sure that you have no invalid tags and that you do not exceed the allowed number of tags per role. In either case, the entire request fails and *no* tags are added to the role.
- AWS always interprets the tag `Value` as a single string. If you need to store an array, you can store comma-separated values in the string. However, you must interpret the value in your code.

For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Tags.member.N

The list of tags that you want to attach to the user. Each tag consists of a key name and an associated value.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Required: Yes

UserName

The name of the user that you want to add tags to.

This parameter accepts (through its regex pattern) a string of characters that consist of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

The following example is formatted with line breaks for legibility.

The following example shows how to add tags to an existing user.

Sample Request

```
POST / HTTP/1.1
Host: https://iam.amazonaws.com
Accept-Encoding: identity
User-Agent: aws-cli/1.11.143 Python/3.6.1 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.7.1
X-Amz-Date: 20170929T181747Z
Authorization: <auth details>
Content-Length: 99
Content-Type: application/x-www-form-urlencoded
```

```
Action=TagUser&Version=2010-05-08&UserName=anika
              &Tags.member.1.Key=Dept&Tags.member.1.Value=Accounting
              &Tags.member.2.Key=Cost Center&Tags.member.2.Value=12345
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE
Content-Type: text/xml
Content-Length: 194
Date: Fri, 29 Sep 2017 18:17:47 GMT

<TagUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</TagUserResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UntagRole

Removes the specified tags from the role. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

RoleName

The name of the IAM role from which you want to remove tags.

This parameter accepts (through its regex pattern) a string of characters that consist of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

TagKeys.member.N

A list of key names as a simple array of strings. The tags with matching keys are removed from the specified role.

Type: Array of strings

Array Members: Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\p{L}\p{Z}\p{N}_.:/=+\-@]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

The following example is formatted with line breaks for legibility.

The following example shows how to remove a tag with the key `Dept` from a role named `taggedrole`.

Sample Request

```
POST / HTTP/1.1
Host: https://iam.amazonaws.com
Accept-Encoding: identity
User-Agent: aws-cli/1.11.143 Python/3.6.1 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.7.1
X-Amz-Date: 20170929T182851Z
Authorization: <auth details>
Content-Length: 78
Content-Type: application/x-www-form-urlencoded

Action=UntagRole&Version=2010-05-08&RoleName=taggedrole
       &TagKeys.member.1=Dept
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE
Content-Type: text/xml
Content-Length: 198
Date: Fri, 29 Sep 2017 18:28:50 GMT

<UntagRoleResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</UntagRoleResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

UntagUser

Removes the specified tags from the user. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

TagKeys.member.N

A list of key names as a simple array of strings. The tags with matching keys are removed from the specified user.

Type: Array of strings

Array Members: Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\p{L}\p{Z}\p{N}_.:/=+\-@]+`

Required: Yes

UserName

The name of the IAM user from which you want to remove tags.

This parameter accepts (through its regex pattern) a string of characters that consist of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: =,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

The following example is formatted with line breaks for legibility.

The following example shows how to remove tags that are attached to a user whose IAM user name is `anika`.

Sample Request

```
POST / HTTP/1.1
Host: https://iam.amazonaws.com
Accept-Encoding: identity
User-Agent: aws-cli/1.11.143 Python/3.6.1 Linux/3.2.45-0.6.wd.865.49.315.metal1.x86_64
 botocore/1.7.1
X-Amz-Date: 20170929T183048Z
Authorization: <auth details>
Content-Length: 74
Content-Type: application/x-www-form-urlencoded

Action=UntagUser&Version=2010-05-08&UserName=anika
       &TagKeys.member.1=Dept
```

Sample Response

```
HTTP/1.1 200 OK
x-amzn-RequestId: EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE
Content-Type: text/xml
Content-Length: 198
Date: Fri, 29 Sep 2017 18:30:47 GMT

<UntagUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</UntagUserResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateAccessKey

Changes the status of the specified access key from Active to Inactive, or vice versa. This operation can be used to disable a user's key as part of a key rotation workflow.

If the `UserName` is not specified, the user name is determined implicitly based on the AWS access key ID used to sign the request. This operation works for access keys under the AWS account. Consequently, you can use this operation to manage AWS account root user credentials even if the AWS account has no associated users.

For information about rotating keys, see Managing Keys and Certificates in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AccessKeyId

The access key ID of the secret access key you want to update.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status you want to assign to the secret access key. `Active` means that the key can be used for API calls to AWS, while `Inactive` means that the key cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the user whose key you want to update.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateAccessKey.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateAccessKey
&UserName=Bob
&AccessKeyId=AKIAIOSFODNN7EXAMPLE
&Status=Inactive
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateAccessKeyResponse>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateAccessKeyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateAccountPasswordPolicy

Updates the password policy settings for the AWS account.

Note

- This operation does not support partial updates. No parameters are required, but if you do not specify a parameter, that parameter's value reverts to its default value. See the **Request Parameters** section for each parameter's default value. Also note that some parameters do not allow the default parameter to be explicitly set. Instead, to invoke the default value, do not include that parameter when you invoke the operation.

For more information about using a password policy, see Managing an IAM Password Policy in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

AllowUsersToChangePassword

Allows all IAM users in your account to use the AWS Management Console to change their own passwords. For more information, see Letting IAM Users Change Their Own Passwords in the *IAM User Guide*.

If you do not specify a value for this parameter, then the operation uses the default value of `false`. The result is that IAM users in the account do not automatically have permissions to change their own password.

Type: Boolean

Required: No

HardExpiry

Prevents IAM users from setting a new password after their password has expired. The IAM user cannot be accessed until an administrator resets the password.

If you do not specify a value for this parameter, then the operation uses the default value of `false`. The result is that IAM users can change their passwords after they expire and continue to sign in as the user.

Type: Boolean

Required: No

MaxPasswordAge

The number of days that an IAM user password is valid.

If you do not specify a value for this parameter, then the operation uses the default value of `0`. The result is that IAM user passwords never expire.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1095.

Required: No

MinimumPasswordLength

The minimum number of characters allowed in an IAM user password.

If you do not specify a value for this parameter, then the operation uses the default value of `6`.

Type: Integer

Valid Range: Minimum value of 6. Maximum value of 128.

Required: No

PasswordReusePrevention

Specifies the number of previous passwords that IAM users are prevented from reusing.

If you do not specify a value for this parameter, then the operation uses the default value of `0`. The result is that IAM users are not prevented from reusing previous passwords.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 24.

Required: No

RequireLowercaseCharacters

Specifies whether IAM user passwords must contain at least one lowercase character from the ISO basic Latin alphabet (a to z).

If you do not specify a value for this parameter, then the operation uses the default value of `false`. The result is that passwords do not require at least one lowercase character.

Type: Boolean

Required: No

RequireNumbers

Specifies whether IAM user passwords must contain at least one numeric character (0 to 9).

If you do not specify a value for this parameter, then the operation uses the default value of `false`. The result is that passwords do not require at least one numeric character.

Type: Boolean

Required: No

RequireSymbols

Specifies whether IAM user passwords must contain at least one of the following non-alphanumeric characters:

! @ # $ % ^ & * ( ) _ + - = [ ] { } | '

If you do not specify a value for this parameter, then the operation uses the default value of `false`. The result is that passwords do not require at least one symbol character.

Type: Boolean

Required: No

RequireUppercaseCharacters

Specifies whether IAM user passwords must contain at least one uppercase character from the ISO basic Latin alphabet (A to Z).

If you do not specify a value for this parameter, then the operation uses the default value of `false`. The result is that passwords do not require at least one uppercase character.

Type: Boolean

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateAccountPasswordPolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateAccountPasswordPolicy
&AllowUsersToChangePassword=true
&HardExpiry=false
&MaxPasswordAge=90
&MinimumPasswordLength=12
&PasswordReusePrevention=12
&RequireLowercaseCharacters=true
&RequireNumbers=true
&RequireSymbols=true
&RequireUppercaseCharacters=true
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateAccountPasswordPolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateAccountPasswordPolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateAssumeRolePolicy

Updates the policy that grants an IAM entity permission to assume a role. This is typically referred to as the "role trust policy". For more information about roles, go to Using Roles to Delegate Permissions and Federate Identities.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

PolicyDocument

The policy that grants an entity permission to assume the role.

You must provide policies in JSON format in IAM. However, for AWS CloudFormation templates formatted in YAML, you can provide the policy in JSON or YAML format. AWS CloudFormation always converts a YAML policy to JSON format before submitting it to IAM.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

RoleName

The name of the role to update with the new policy.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedPolicyDocument

The request was rejected because the policy document was malformed. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of UpdateAssumeRolePolicy.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateAssumeRolePolicy
&PolicyDocument={"Version":"2012-10-17","Statement":[{"Effect":"Allow",
"Principal":{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
&RoleName=S3AccessForEC2Instances
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateAssumeRolePolicyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ResponseMetadata>
  <RequestId>309c1671-99ed-11e1-a4c3-270EXAMPLE04</RequestId>
</ResponseMetadata>
</UpdateAssumeRolePolicyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateGroup

Updates the name and/or the path of the specified IAM group.

Important
You should understand the implications of changing a group's path or name. For more information, see Renaming Users and Groups in the *IAM User Guide*.

Note
The person making the request (the principal), must have permission to change the role group with the old name and the new name. For example, to change the group named `Managers` to `MGRs`, the principal must have a policy that allows them to update both groups. If the principal has permission to update the `Managers` group, but not the `MGRs` group, then the update fails. For more information about permissions, see Access Management.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

GroupName

Name of the IAM group to update. If you're changing the name of the group, this is the original name.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

NewGroupName

New name for the IAM group. Only include this if changing the group's name.

IAM user, group, role, and policy names must be unique within the account. Names are not distinguished by case. For example, you cannot create resources named both "MyResource" and "myresource".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

NewPath

New path for the IAM group. Only include this if changing the group's path.

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateGroup.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateGroup
&GroupName=Test
&NewGroupName=Test_1
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateGroupResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
```

```
</UpdateGroupResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateLoginProfile

Changes the password for the specified IAM user.

IAM users can change their own passwords by calling ChangePassword (p. 22). For more information about modifying passwords, see Managing Passwords in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Password

The new password for the specified IAM user.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

However, the format can be further restricted by the account administrator by setting a password policy on the AWS account. For more information, see UpdateAccountPasswordPolicy (p. 372).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

PasswordResetRequired

Allows this new password to be used only once by requiring the specified IAM user to set a new password on next sign-in.

Type: Boolean

Required: No

UserName

The name of the user whose password you want to update.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

PasswordPolicyViolation

The request was rejected because the provided password did not meet the requirements imposed by the account password policy.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateLoginProfile.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateLoginProfile
&UserName=Bob
&Password=^L[p*#Z*8o)K
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateLoginProfileResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
```

```
</UpdateLoginProfileResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateOpenIDConnectProviderThumbprint

Replaces the existing list of server certificate thumbprints associated with an OpenID Connect (OIDC) provider resource object with a new list of thumbprints.

The list that you pass with this operation completely replaces the existing list of thumbprints. (The lists are not merged.)

Typically, you need to update a thumbprint only when the identity provider's certificate changes, which occurs rarely. However, if the provider's certificate *does* change, any attempt to assume an IAM role that specifies the OIDC provider as a principal fails until the certificate thumbprint is updated.

> **Note**
> Trust for the OIDC provider is derived from the provider's certificate and is validated by the thumbprint. Therefore, it is best to limit access to the `UpdateOpenIDConnectProviderThumbprint` operation to highly privileged users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

OpenIDConnectProviderArn

The Amazon Resource Name (ARN) of the IAM OIDC provider resource object for which you want to update the thumbprint. You can get a list of OIDC provider ARNs by using the ListOpenIDConnectProviders (p. 260) operation.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

ThumbprintList.member.N

A list of certificate thumbprints that are associated with the specified IAM OpenID Connect provider. For more information, see CreateOpenIDConnectProvider (p. 39).

Type: Array of strings

Length Constraints: Fixed length of 40.

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateOpenIDConnectProviderThumbprint.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateOpenIDConnectProviderThumbprint
&ThumbprintList.list.1=c3768084dfb3d2b68b7897bf5f565da8eEXAMPLE
&OpenIDConnectProviderArn=arn:aws:iam::123456789012:oidc-provider/server.example.com
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateOpenIDConnectProviderThumbprintResponse xmlns="https://iam.amazonaws.com/
doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>29b6031c-4f66-11e4-aefa-bfd6aEXAMPLE</RequestId>
  </ResponseMetadata>
</UpdateOpenIDConnectProviderThumbprintResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateRole

Updates the description or maximum session duration setting of a role.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Description

The new description that you want to apply to the specified role.

Type: String

Length Constraints: Maximum length of 1000.

Pattern: `[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}]*`

Required: No

MaxSessionDuration

The maximum session duration (in seconds) that you want to set for the specified role. If you do not specify a value for this setting, the default maximum of one hour is applied. This setting can have a value from 1 hour to 12 hours.

Anyone who assumes the role from the AWS CLI or API can use the `DurationSeconds` API parameter or the `duration-seconds` CLI parameter to request a longer session. The `MaxSessionDuration` setting determines the maximum duration that can be requested using the `DurationSeconds` parameter. If users don't specify a value for the `DurationSeconds` parameter, their security credentials are valid for one hour by default. This applies when you use the `AssumeRole*` API operations or the `assume-role*` CLI operations but does not apply when you use those operations to create a console URL. For more information, see Using IAM Roles in the *IAM User Guide*.

Type: Integer

Valid Range: Minimum value of 3600. Maximum value of 43200.

Required: No

RoleName

The name of the role that you want to modify.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateRoleDescription

Use UpdateRole (p. 387) instead.

Modifies only the description of a role. This operation performs the same function as the `Description` parameter in the `UpdateRole` operation.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

Description

The new description that you want to apply to the specified role.

Type: String

Length Constraints: Maximum length of 1000.

Pattern: `[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}]*`

Required: Yes

RoleName

The name of the role that you want to modify.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

Role

A structure that contains details about the modified role.

Type: Role (p. 471) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

UnmodifiableEntity

The request was rejected because only the service that depends on the service-linked role can modify or delete the role on your behalf. The error message includes the name of the service that depends on this service-linked role. You must request the change through that service.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateSAMLProvider

Updates the metadata document for an existing SAML provider resource object.

Note
This operation requires Signature Version 4.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

SAMLMetadataDocument

An XML document generated by an identity provider (IdP) that supports SAML 2.0. The document includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that are received from the IdP. You must generate the metadata document using the identity management software that is used as your organization's IdP.

Type: String

Length Constraints: Minimum length of 1000. Maximum length of 10000000.

Required: Yes

SAMLProviderArn

The Amazon Resource Name (ARN) of the SAML provider to update.

For more information about ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Response Elements

The following element is returned by the service.

SAMLProviderArn

The Amazon Resource Name (ARN) of the SAML provider that was updated.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

InvalidInput

The request was rejected because an invalid or out-of-range value was supplied for an input parameter.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateSAMLProvider.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateSAMLProvider
&Name=arn:aws:iam::123456789012:saml-provider/MyUniversity
&SAMLMetadataDocument=VGhpcyBpcyB3aGVyZSB5b3UgcHV0IHRoZSBTQU1MIHByb3ZpZGVyIG1ldGFkYXRhIGRvY3VtZW50
LCBCYXNlNjQtZW5jb2RlZCBpbnRvIGEgYmlnIHN0cmluZy4=
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateSAMLProviderResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<UpdateSAMLProviderResult>
  <SAMLProviderArn>arn:aws:iam::123456789012:saml-provider/MyUniversity</SAMLProviderArn>
</UpdateSAMLProviderResult>
<ResponseMetadata>
  <RequestId>29f47818-99f5-11e1-a4c3-27EXAMPLE804</RequestId>
</ResponseMetadata>
</UpdateSAMLProviderResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateServerCertificate

Updates the name and/or the path of the specified server certificate stored in IAM.

For more information about working with server certificates, see Working with Server Certificates in the *IAM User Guide*. This topic also includes a list of AWS services that can use the server certificates that you manage with IAM.

Important
You should understand the implications of changing a server certificate's path or name. For more information, see Renaming a Server Certificate in the *IAM User Guide*.

Note
The person making the request (the principal), must have permission to change the server certificate with the old name and the new name. For example, to change the certificate named `ProductionCert` to `ProdCert`, the principal must have a policy that allows them to update both certificates. If the principal has permission to update the `ProductionCert` group, but not the `ProdCert` certificate, then the update fails. For more information about permissions, see Access Management in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

NewPath

The new path for the server certificate. Include this only if you are updating the server certificate's path.

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

NewServerCertificateName

The new name for the server certificate. Include this only if you are updating the server certificate's name. The name of the certificate cannot contain any spaces.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

ServerCertificateName

The name of the server certificate that you want to update.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateServerCertificate.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateServerCertificate
&ServerCertificateName=OldProdServerCertName
&NewServerCertificateName=NewProdServerCertName
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateServerCertificateResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<ResponseMetadata>
  <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
</ResponseMetadata>
</UpdateServerCertificateResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateServiceSpecificCredential

Sets the status of a service-specific credential to `Active` or `Inactive`. Service-specific credentials that are inactive cannot be used for authentication to the service. This operation can be used to disable a user's service-specific credential as part of a credential rotation work flow.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

ServiceSpecificCredentialId

The unique identifier of the service-specific credential.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status to be assigned to the service-specific credential.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user associated with the service-specific credential. If you do not specify this value, then the operation assumes the user whose credentials are used to call the operation.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

The following example shows how to set the state to "Active" for a service-specific credential associated with the specified IAM user.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateServiceSpecificCredential
&ServiceSpecificCredentialId=ACCA12345ABCDEXAMPLE
&UserName=Anika
&Status=Active
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateServiceSpecificCredentialResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
  </ResponseMetadata>
</UpdateServiceSpecificCredentialResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateSigningCertificate

Changes the status of the specified user signing certificate from active to disabled, or vice versa. This operation can be used to disable an IAM user's signing certificate as part of a certificate rotation work flow.

If the `UserName` field is not specified, the user name is determined implicitly based on the AWS access key ID used to sign the request. This operation works for access keys under the AWS account. Consequently, you can use this operation to manage AWS account root user credentials even if the AWS account has no associated users.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

CertificateId

The ID of the signing certificate you want to update.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status you want to assign to the certificate. `Active` means that the certificate can be used for API calls to AWS `Inactive` means that the certificate cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user the signing certificate belongs to.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateSigningCertificate.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateSigningCertificate
&UserName=Bob
&CertificateId=TA7SMP42TDN5Z26OBPJE7EXAMPLE
&Status=Inactive
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateSigningCertificateResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <ResponseMetadata>
    <RequestId>EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateSigningCertificateResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

UpdateSSHPublicKey

Sets the status of an IAM user's SSH public key to active or inactive. SSH public keys that are inactive cannot be used for authentication. This operation can be used to disable a user's SSH public key as part of a key rotation work flow.

The SSH public key affected by this operation is used only for authenticating the associated IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

SSHPublicKeyId

The unique identifier for the SSH public key.

This parameter allows (through its regex pattern) a string of characters that can consist of any upper or lowercased letter or digit.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status to assign to the SSH public key. `Active` means that the key can be used for authentication with an AWS CodeCommit repository. `Inactive` means that the key cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user associated with the SSH public key.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

Examples

Example

This example illustrates one usage of UpdateSSHPublicKey.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateSSHPublicKey
&SSHPublicKeyId=APKAEIVFHP46CEXAMPLE
&Status=Inactive
&UserName=Jane
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateSSHPublicKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <ResponseMetadata>
    <RequestId>d3d9215c-f36b-11e4-97ab-c53b2EXAMPLE</RequestId>
  </ResponseMetadata>
</UpdateSSHPublicKeyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateUser

Updates the name and/or the path of the specified IAM user.

Important
You should understand the implications of changing an IAM user's path or name. For more information, see Renaming an IAM User and Renaming an IAM Group in the *IAM User Guide*.

Note
To change a user name, the requester must have appropriate permissions on both the source object and the target object. For example, to change Bob to Robert, the entity making the request must have permission on Bob and Robert, or must have permission on all (*). For more information about permissions, see Permissions and Policies.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

NewPath

New path for the IAM user. Include this parameter only if you're changing the user's path.

This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (`\u0021`) through the DEL character (`\u007F`), including most punctuation characters, digits, and upper and lowercased letters.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

NewUserName

New name for the user. Include this parameter only if you're changing the user's name.

IAM user, group, role, and policy names must be unique within the account. Names are not distinguished by case. For example, you cannot create resources named both "MyResource" and "myresource".

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

UserName

Name of the user to update. If you're changing the name of the user, this is the original user name.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

ConcurrentModification

The request was rejected because multiple requests to change this object were submitted simultaneously. Wait a few minutes and submit your request again.

HTTP Status Code: 409

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

EntityTemporarilyUnmodifiable

The request was rejected because it referenced an entity that is temporarily unmodifiable, such as a user name that was deleted and then recreated. The error indicates that the request is likely to succeed if you try again after waiting several minutes. The error message describes the entity.

HTTP Status Code: 409

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UpdateUser.

Sample Request

```
https://iam.amazonaws.com/?Action=UpdateUser
```

```
&UserName=Bob
&NewUserName=Robert
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UpdateUserResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
 <UpdateUserResult>
 <User>
    <Path>/division_abc/subdivision_xyz/</Path>
    <UserName>Robert</UserName>
    <UserId>AIDACKCEVSQ6C2EXAMPLE</UserId>
    <Arn>arn:aws::123456789012:user/division_abc/subdivision_xyz/Robert
    </Arn>
 </User>
 </UpdateUserResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
</UpdateUserResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UploadServerCertificate

Uploads a server certificate entity for the AWS account. The server certificate entity includes a public key certificate, a private key, and an optional certificate chain, which should all be PEM-encoded.

We recommend that you use AWS Certificate Manager to provision, manage, and deploy your server certificates. With ACM you can request a certificate, deploy it to AWS resources, and let ACM handle certificate renewals for you. Certificates provided by ACM are free. For more information about using ACM, see the AWS Certificate Manager User Guide.

For more information about working with server certificates, see Working with Server Certificates in the *IAM User Guide*. This topic includes a list of AWS services that can use the server certificates that you manage with IAM.

For information about the number of server certificates you can upload, see Limitations on IAM Entities and Objects in the *IAM User Guide*.

Note
Because the body of the public key certificate, private key, and the certificate chain can be large, you should use POST rather than GET when calling `UploadServerCertificate`. For information about setting up signatures and authorization through the API, go to Signing AWS API Requests in the *AWS General Reference*. For general information about using the Query API with IAM, go to Calling the API by Making HTTP Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

CertificateBody

The contents of the public key certificate in PEM-encoded format.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

CertificateChain

The contents of the certificate chain. This is typically a concatenation of the PEM-encoded public key certificates of the chain.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range

- The printable characters in the Basic Latin and Latin-1 Supplement character set (through \u00FF)
- The special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Pattern: [\u0009\u000A\u000D\u0020-\u00FF]+

Required: No

Path

The path for the server certificate. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

This parameter is optional. If it is not included, it defaults to a slash (/). This parameter allows (through its regex pattern) a string of characters consisting of either a forward slash (/) by itself or a string that must begin and end with forward slashes. In addition, it can contain any ASCII character from the ! (\u0021) through the DEL character (\u007F), including most punctuation characters, digits, and upper and lowercased letters.

> **Note**
> If you are uploading a server certificate specifically for use with Amazon CloudFront distributions, you must specify a path using the path parameter. The path must begin with /cloudfront and must include a trailing slash (for example, /cloudfront/test/).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: (\u002F)|(\u002F[\u0021-\u007F]+\u002F)

Required: No

PrivateKey

The contents of the private key in PEM-encoded format.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (\u0020) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through \u00FF)
- The special characters tab (\u0009), line feed (\u000A), and carriage return (\u000D)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: [\u0009\u000A\u000D\u0020-\u00FF]+

Required: Yes

ServerCertificateName

The name for the server certificate. Do not include the path in this value. The name of the certificate cannot contain any spaces.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

ServerCertificateMetadata

The meta information of the uploaded server certificate without its certificate body, certificate chain, and private key.

Type: ServerCertificateMetadata (p. 481) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

KeyPairMismatch

The request was rejected because the public key certificate and the private key do not match.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedCertificate

The request was rejected because the certificate was malformed or expired. The error message describes the specific error.

HTTP Status Code: 400

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UploadServerCertificate.

Sample Request

```
https://iam.amazonaws.com/?Action=UploadServerCertificate
&ServerCertificateName=ProdServerCert
&Path=/company/servercerts/
&CertificateBody=
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
&PrivateKey=
-----BEGIN DSA PRIVATE KEY-----
MIIBugIBTTKBgQD33xToSXPJ6hr37L3+KNi3/7DgywlBcvlFPPSHIw3ORuO/22mT
8Cy5fT89WwNvZ3BPKWU6OZ38TQv3eWjNc/3U3+oqVNG2poX5nCPOtO1b96HYX2mR
3FTdH6FRKbQEhpDzZ6tRrjTHjMX6sT3JRWkBd2c4bGu+HUHO1H7QvrCTeQIVTKMs
TCKCyrLiGhUWuUGNJUMU6y6zToGTHl84Tz7TPwDGDXuy/Dk5s4jTVr+xibROC/gS
Qrs4Dzz3T1ze6lvU8S1KT9UsOB5FUJNTTPCPey+Lo4mmK6b23XdTyCIT8e2fsm2j
jHHC1pIPiTkdLS3j6ZYjF8LY6TENFng+LDY/xwPOl7TJVoD3J/WXC2J9CEYq9o34
kq6WWn3CgYTuo54nXUgnoCb3xdG8COFrg+oTbIkHTSzs3w5o/GGgKK7TDF3UlJjq
vHNyJQ6kWBrQRR1Xp5KYQ4c/Dm5kef+62mH53HpcCELguWVcffuVQpmq3EWL9Zp9
jobTJQ2VHjb5IVxiO6HRSd27di3njyrzUuJCyHSDTqwLJmTThpd6OTIUTL3Tc4m2
62TITdw53KWJEXAMPLE=
-----END DSA PRIVATE KEY-----
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UploadServerCertificateResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
<UploadServerCertificateResult>
  <ServerCertificateMetadata>
    <ServerCertificateName>ProdServerCert</ServerCertificateName>
    <Path>/company/servercerts/</Path>
    <Arn>arn:aws:iam::123456789012:server-certificate/company/servercerts/ProdServerCert</
Arn>
    <UploadDate>2010-05-08T01:02:03.004Z</UploadDate>
    <ServerCertificateId>ASCACKCEVSQ6C2EXAMPLE</ServerCertificateId>
    <Expiration>2012-05-08T01:02:03.004Z</Expiration>
  </ServerCertificateMetadata>
</UploadServerCertificateResult>
<ResponseMetadata>
  <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
</ResponseMetadata>
```

```
</UploadServerCertificateResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UploadSigningCertificate

Uploads an X.509 signing certificate and associates it with the specified IAM user. Some AWS services use X.509 signing certificates to validate requests that are signed with a corresponding private key. When you upload the certificate, its default status is `Active`.

If the `UserName` is not specified, the IAM user name is determined implicitly based on the AWS access key ID used to sign the request. This operation works for access keys under the AWS account. Consequently, you can use this operation to manage AWS account root user credentials even if the AWS account has no associated users.

Note
Because the body of an X.509 certificate can be large, you should use POST rather than GET when calling `UploadSigningCertificate`. For information about setting up signatures and authorization through the API, go to Signing AWS API Requests in the *AWS General Reference*. For general information about using the Query API with IAM, go to Making Query Requests in the *IAM User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

CertificateBody

The contents of the signing certificate.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

UserName

The name of the user the signing certificate is for.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Response Elements

The following element is returned by the service.

Certificate

Information about the certificate.

Type: SigningCertificate (p. 489) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

DuplicateCertificate

The request was rejected because the same certificate is associated with an IAM user in the account.

HTTP Status Code: 409

EntityAlreadyExists

The request was rejected because it attempted to create a resource that already exists.

HTTP Status Code: 409

InvalidCertificate

The request was rejected because the certificate is invalid.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

MalformedCertificate

The request was rejected because the certificate was malformed or expired. The error message describes the specific error.

HTTP Status Code: 400

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

ServiceFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

Examples

Example

This example illustrates one usage of UploadSigningCertificate.

Sample Request

```
https://iam.amazonaws.com/?Action=UploadSigningCertificate
&UserName=Bob
&CertificateBody=
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
&Version=2010-05-08
&AUTHPARAMS
```

Sample Response

```
<UploadSigningCertificateResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <UploadSigningCertificateResult>
    <Certificate>
      <UserName>Bob</UserName>
      <CertificateId>TA7SMP42TDN5Z26OBPJE7EXAMPLE</CertificateId>
      <CertificateBody>
-----BEGIN CERTIFICATE-----
MIICdzCCAeCgAwIBAgIGANc+Ha2wMA0GCSqGSIb3DQEBBQUAMFMxCzAJBgNVBAYT
AlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMQwwCgYDVQQLEwNBV1MxITAfBgNVBAMT
GEFXUyBMaW1pdGVkLUFzc3VyYW5jZSBDQTAeFw0wOTAyMDQxNzE5MjdaFw0xMDAy
MDQxNzE5MjdaMFIxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBbWF6b24uY29tMRcw
FQYDVQQLEw5BV1MtRGV2ZWxvcGVyczEVMBMGA1UEAxMMNTdxNDl0c3ZwYjRtMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpB/vsOwmT/O0td1RqzKjttSBaPjbr
dqwNe9BrOyB08fw2+Ch5oonZYXfGUrT6mkYXH5fQot9HvASrzAKHO596FdJA6DmL
ywdWe1Oggk7zFSXO1Xv+3vPrJtaYxYo3eRIp7w80PMkiOv6M0XK8ubcTouODeJbf
suDqcLnLDxwsvwIDAQABo1cwVTAOBgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAww
CgYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQULGNaBphBumaKbDRK
CAi0mH8B3mowDQYJKoZIhvcNAQEFBQADgYEAuKxhkXaCLGcqDuweKtO/AEw9ZePH
wr0XqsaIK2HZboqruebXEGsojK4Ks0WzwgrEynuHJwTn760xe39rSqXWIOGrOBaX
wFpWHVjTFMKk+tSDG1lssLHyYWWdFFU4AnejRGORJYNaRHgVTKjHphc5jEhHm0BX
AEaHzTpmEXAMPLE=
-----END CERTIFICATE-----
      </CertificateBody>
      <Status>Active</Status>
    </Certificate>
 </UploadSigningCertificateResult>
 <ResponseMetadata>
    <RequestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</RequestId>
 </ResponseMetadata>
```

```
</UploadSigningCertificateResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UploadSSHPublicKey

Uploads an SSH public key and associates it with the specified IAM user.

The SSH public key uploaded by this operation can be used only for authenticating the associated IAM user to an AWS CodeCommit repository. For more information about using SSH keys to authenticate to an AWS CodeCommit repository, see Set up AWS CodeCommit for SSH Connections in the *AWS CodeCommit User Guide*.

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 506).

SSHPublicKeyBody

The SSH public key. The public key must be encoded in ssh-rsa format or PEM format. The minimum bit-length of the public key is 2048 bits. For example, you can generate a 2048-bit key, and the resulting PEM file is 1679 bytes long.

The regex pattern used to validate this parameter is a string of characters consisting of the following:

- Any printable ASCII character ranging from the space character (`\u0020`) through the end of the ASCII character range
- The printable characters in the Basic Latin and Latin-1 Supplement character set (through `\u00FF`)
- The special characters tab (`\u0009`), line feed (`\u000A`), and carriage return (`\u000D`)

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

UserName

The name of the IAM user to associate the SSH public key with.

This parameter allows (through its regex pattern) a string of characters consisting of upper and lowercase alphanumeric characters with no spaces. You can also include any of the following characters: _+=,.@-

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Response Elements

The following element is returned by the service.

SSHPublicKey

Contains information about the SSH public key.

Type: SSHPublicKey (p. 491) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 508).

DuplicateSSHPublicKey

The request was rejected because the SSH public key is already associated with the specified IAM user.

HTTP Status Code: 400

InvalidPublicKey

The request was rejected because the public key is malformed or otherwise invalid.

HTTP Status Code: 400

LimitExceeded

The request was rejected because it attempted to create resources beyond the current AWS account limits. The error message describes the limit exceeded.

HTTP Status Code: 409

NoSuchEntity

The request was rejected because it referenced a resource entity that does not exist. The error message describes the resource.

HTTP Status Code: 404

UnrecognizedPublicKeyEncoding

The request was rejected because the public key encoding format is unsupported or unrecognized.

HTTP Status Code: 400

Examples

Example

This example illustrates one usage of UploadSSHPublicKey.

Sample Request

```
https://iam.amazonaws.com/?Action=UploadSSHPublicKey
&SSHPublicKeyBody=ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCy75ak72GGaoZNy0cjUERIn
+mrga0C30kmkiwOeN4H6YtvCdUksVppjPOhm485WFRzvIcxaMEuZ9ISAkp8AfefybxH0PdQWhELSu0p
HaMnADAU7dOn3CCerO8+0sycbu4ES4P+cdK1qet3ptsG/zeQNLLmOK5zjIRa1MAS3KnwLwHEVPEe4JD
+xfghuO0nwzUgpneGNwk7m7qihYLFnNCFdeU8OeIr9Fmc75g5olHm6ZoC/bccAHurHkfcDpanJTLNfL
R5Oj14CZSsRP4kNdm+oe5+IPM78w4J9v4pXU4mizYDE21G4gUDVxOrs0X66lMihX6ArVgmEK+NK5GQg
n9z jane@example.com
&UserName=Jane
&Version=2010-05-08
```

```
&AUTHPARAMS
```

Sample Response

```
<UploadSSHPublicKeyResponse xmlns="https://iam.amazonaws.com/doc/2010-05-08/">
  <UploadSSHPublicKeyResult>
    <PublicKey>
      <UploadDate>2015-06-05T20:56:46.012Z</UploadDate>
      <Fingerprint>7a:1d:ea:9e:b0:80:ac:f8:ec:d8:dc:e6:a7:2c:fc:51</Fingerprint>
      <UserName>Jane</UserName>
      <SSHPublicKeyId>APKAEIVFHP46CEXAMPLE</SSHPublicKeyId>
      <Status>Active</Status>
      <SSHPublicKeyBody>
        ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCy75ak72GGaoZNy0cjUERIn+mrga0C30k
        mkiwOeN4H6YtvCdUksVppjPOhm485WFRzvIcxaMEuZ9ISAkp8AfefybxH0PdQWhELSu0pHa
        MnADAU7dOn3CCerO8+0sycbu4ES4P+cdK1qet3ptsG/zeQNLLmOK5zjIRa1MAS3KnwLwHEV
        PEe4JD+xfghuO0nwzUgpneGNwk7m7qihYLFnNCFdeU8OeIr9Fmc75g5olHm6ZoC/bccAHur
        HkfcDpanJTLNfLR5Oj14CZSsRP4kNdm+oe5+IPM78w4J9v4pXU4mizYDE21G4gUDVxOrs0X
        66lMihX6ArVgmEK+NK5GQgn9z jane@example.com
      </SSHPublicKeyBody>
    </PublicKey>
  </UploadSSHPublicKeyResult>
  <ResponseMetadata>
    <RequestId>3da97a2f-f369-11e4-97ab-c53b2EXAMPLE</RequestId>
  </ResponseMetadata>
</UploadSSHPublicKeyResponse>
```

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The AWS Identity and Access Management API contains several data types that various actions use. This section describes each data type in detail.

> **Note**
> The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

AccessDetail

An object that contains details about when a principal in the reported AWS Organizations entity last attempted to access an AWS service. A principal can be an IAM user, an IAM role, or the AWS account root user within the reported Organizations entity.

This data type is a response element in the GetOrganizationsAccessReport (p. 178) operation.

Contents

EntityPath

The path of the Organizations entity (root, organizational unit, or account) from which an authenticated principal last attempted to access the service. AWS does not report unauthenticated requests.

This field is null if no principals (IAM users, IAM roles, or root users) in the reported Organizations entity attempted to access the service within the reporting period.

Type: String

Length Constraints: Minimum length of 19. Maximum length of 427.

Pattern: `^o-[0-9a-z]{10,32}\/r-[0-9a-z]{4,32}[0-9a-z-\/]*`

Required: No

LastAuthenticatedTime

The date and time, in ISO 8601 date-time format, when an authenticated principal most recently attempted to access the service. AWS does not report unauthenticated requests.

This field is null if no principals in the reported Organizations entity attempted to access the service within the reporting period.

Type: Timestamp

Required: No

Region

The Region where the last service access attempt occurred.

This field is null if no principals in the reported Organizations entity attempted to access the service within the reporting period.

Type: String

Required: No

ServiceName

The name of the service in which access was attempted.

Type: String

Required: Yes

ServiceNamespace

The namespace of the service in which access was attempted.

To learn the service namespace of a service, go to Actions, Resources, and Condition Keys for AWS Services in the *IAM User Guide*. Choose the name of the service to view details for that service. In the first paragraph, find the service prefix. For example, `(service prefix: a4b)`. For more information about service namespaces, see AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w-]*`

Required: Yes

TotalAuthenticatedEntities

The number of accounts with authenticated principals (root users, IAM users, and IAM roles) that attempted to access the service in the reporting period.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AccessKey

Contains information about an AWS access key.

This data type is used as a response element in the CreateAccessKey (p. 25) and ListAccessKeys (p. 220) operations.

Note
The `SecretAccessKey` value is returned only in response to CreateAccessKey (p. 25). You can get a secret access key only when you first create an access key; you cannot recover the secret access key later. If you lose a secret access key, you must create a new access key.

Contents

AccessKeyId

The ID for this access key.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

CreateDate

The date when the access key was created.

Type: Timestamp

Required: No

SecretAccessKey

The secret key used to sign requests.

Type: String

Required: Yes

Status

The status of the access key. `Active` means that the key is valid for API calls, while `Inactive` means it is not.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user that the access key is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AccessKeyLastUsed

Contains information about the last time an AWS access key was used since IAM began tracking this information on April 22, 2015.

This data type is used as a response element in the GetAccessKeyLastUsed (p. 141) operation.

Contents

LastUsedDate

The date and time, in ISO 8601 date-time format, when the access key was most recently used. This field is null in the following situations:

- The user does not have an access key.
- An access key exists but has not been used since IAM began tracking this information.
- There is no sign-in data associated with the user.

Type: Timestamp

Required: Yes

Region

The AWS Region where this access key was most recently used. The value for this field is "N/A" in the following situations:

- The user does not have an access key.
- An access key exists but has not been used since IAM began tracking this information.
- There is no sign-in data associated with the user.

For more information about AWS Regions, see Regions and Endpoints in the Amazon Web Services General Reference.

Type: String

Required: Yes

ServiceName

The name of the AWS service with which this access key was most recently used. The value of this field is "N/A" in the following situations:

- The user does not have an access key.
- An access key exists but has not been used since IAM started tracking this information.
- There is no sign-in data associated with the user.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWS SDK for Ruby V3

AccessKeyMetadata

Contains information about an AWS access key, without its secret key.

This data type is used as a response element in the ListAccessKeys (p. 220) operation.

Contents

AccessKeyId

The ID for this access key.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

CreateDate

The date when the access key was created.

Type: Timestamp

Required: No

Status

The status of the access key. `Active` means that the key is valid for API calls; `Inactive` means it is not.

Type: String

Valid Values: `Active | Inactive`

Required: No

UserName

The name of the IAM user that the key is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AttachedPermissionsBoundary

Contains information about an attached permissions boundary.

An attached permissions boundary is a managed policy that has been attached to a user or role to set the permissions boundary.

For more information about permissions boundaries, see Permissions Boundaries for IAM Identities in the *IAM User Guide*.

Contents

PermissionsBoundaryArn

The ARN of the policy used to set the permissions boundary for the user or role.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

PermissionsBoundaryType

The permissions boundary usage type that indicates what type of IAM resource is used as the permissions boundary for an entity. This data type can only have a value of `Policy`.

Type: String

Valid Values: `PermissionsBoundaryPolicy`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AttachedPolicy

Contains information about an attached policy.

An attached policy is a managed policy that has been attached to a user, group, or role. This data type is used as a response element in the ListAttachedGroupPolicies (p. 226), ListAttachedRolePolicies (p. 230), ListAttachedUserPolicies (p. 234), and GetAccountAuthorizationDetails (p. 143) operations.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Contents

PolicyArn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

PolicyName

The friendly name of the attached policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ContextEntry

Contains information about a condition context key. It includes the name of the key and specifies the value (or values, if the context key supports multiple values) to use in the simulation. This information is used when evaluating the `Condition` elements of the input policies.

This data type is used as an input parameter to SimulateCustomPolicy (p. 338) and SimulatePrincipalPolicy (p. 346).

Contents

ContextKeyName

The full name of a condition context key, including the service prefix. For example, `aws:SourceIp` or `s3:VersionId`.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 256.

Required: No

ContextKeyType

The data type of the value (or values) specified in the `ContextKeyValues` parameter.

Type: String

Valid Values: `string | stringList | numeric | numericList | boolean | booleanList | ip | ipList | binary | binaryList | date | dateList`

Required: No

ContextKeyValues.member.N

The value (or values, if the condition context key supports multiple values) to provide to the simulation when the key is referenced by a `Condition` element in an input policy.

Type: Array of strings

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DeletionTaskFailureReasonType

The reason that the service-linked role deletion failed.

This data type is used as a response element in the GetServiceLinkedRoleDeletionStatus (p. 208) operation.

Contents

Reason

A short description of the reason that the service-linked role deletion failed.

Type: String

Length Constraints: Maximum length of 1000.

Required: No

RoleUsageList.member.N

A list of objects that contains details about the service-linked role deletion failure, if that information is returned by the service. If the service-linked role has active sessions or if any resources that were used by the role have not been deleted from the linked service, the role can't be deleted. This parameter includes a list of the resources that are associated with the role and the Region in which the resources are being used.

Type: Array of RoleUsageType (p. 478) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EntityDetails

An object that contains details about when the IAM entities (users or roles) were last used in an attempt to access the specified AWS service.

This data type is a response element in the GetServiceLastAccessedDetailsWithEntities (p. 204) operation.

Contents

EntityInfo

The `EntityInfo` object that contains details about the entity (user or role).

Type: EntityInfo (p. 434) object

Required: Yes

LastAuthenticated

The date and time, in ISO 8601 date-time format, when the authenticated entity last attempted to access AWS. AWS does not report unauthenticated requests.

This field is null if no IAM entities attempted to access the service within the reporting period.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EntityInfo

Contains details about the specified entity (user or role).

This data type is an element of the EntityDetails (p. 433) object.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Id

The identifier of the entity (user or role).

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Name

The name of the entity (user or role).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Path

The path to the entity (user or role). For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

Type

The type of entity (user or role).

Type: String

Valid Values: `USER | ROLE | GROUP`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ErrorDetails

Contains information about the reason that the operation failed.

This data type is used as a response element in the GetOrganizationsAccessReport (p. 178), GetServiceLastAccessedDetails (p. 199), and GetServiceLastAccessedDetailsWithEntities (p. 204) operations.

Contents

Code

The error code associated with the operation failure.

Type: String

Required: Yes

Message

Detailed information about the reason that the operation failed.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EvaluationResult

Contains the results of a simulation.

This data type is used by the return parameter of `SimulateCustomPolicy (p. 338)` and `SimulatePrincipalPolicy (p. 346)` .

Contents

EvalActionName

The name of the API operation tested on the indicated resource.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 128.

Required: Yes

EvalDecision

The result of the simulation.

Type: String

Valid Values: `allowed | explicitDeny | implicitDeny`

Required: Yes

EvalDecisionDetails , EvalDecisionDetails.entry.N.key (key), EvalDecisionDetails.entry.N.value (value)

Additional details about the results of the cross-account evaluation decision. This parameter is populated for only cross-account simulations. It contains a brief summary of how each policy type contributes to the final evaluation decision.

If the simulation evaluates policies within the same account and includes a resource ARN, then the parameter is present but the response is empty. If the simulation evaluates policies within the same account and specifies all resources (*), then the parameter is not returned.

When you make a cross-account request, AWS evaluates the request in the trusting account and the trusted account. The request is allowed only if both evaluations return `true`. For more information about how policies are evaluated, see Evaluating Policies Within a Single Account.

If an AWS Organizations SCP included in the evaluation denies access, the simulation ends. In this case, policy evaluation does not proceed any further and this parameter is not returned.

Type: String to string map

Key Length Constraints: Minimum length of 3. Maximum length of 256.

Valid Values: `allowed | explicitDeny | implicitDeny`

Required: No

EvalResourceName

The ARN of the resource that the indicated API operation was tested on.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: No

MatchedStatements.member.N

A list of the statements in the input policies that determine the result for this scenario. Remember that even if multiple statements allow the operation on the resource, if only one statement denies that operation, then the explicit deny overrides any allow. In addition, the deny statement is the only entry included in the result.

Type: Array of Statement (p. 495) objects

Required: No

MissingContextValues.member.N

A list of context keys that are required by the included input policies but that were not provided by one of the input parameters. This list is used when the resource in a simulation is "*", either explicitly, or when the `ResourceArns` parameter blank. If you include a list of resources, then any missing context values are instead included under the `ResourceSpecificResults` section. To discover the context keys used by a set of policies, you can call GetContextKeysForCustomPolicy (p. 156) or GetContextKeysForPrincipalPolicy (p. 159).

Type: Array of strings

Length Constraints: Minimum length of 5. Maximum length of 256.

Required: No

OrganizationsDecisionDetail

A structure that details how Organizations and its service control policies affect the results of the simulation. Only applies if the simulated user's account is part of an organization.

Type: OrganizationsDecisionDetail (p. 453) object

Required: No

PermissionsBoundaryDecisionDetail

Contains information about the effect that a permissions boundary has on a policy simulation when the boundary is applied to an IAM entity.

Type: PermissionsBoundaryDecisionDetail (p. 456) object

Required: No

ResourceSpecificResults.member.N

The individual results of the simulation of the API operation specified in EvalActionName on each resource.

Type: Array of ResourceSpecificResult (p. 469) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWS SDK for Ruby V3

Group

Contains information about an IAM group entity.

This data type is used as a response element in the following operations:

- CreateGroup (p. 30)
- GetGroup (p. 164)
- ListGroups (p. 245)

Contents

Arn

The Amazon Resource Name (ARN) specifying the group. For more information about ARNs and how to use them in policies, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

CreateDate

The date and time, in ISO 8601 date-time format, when the group was created.

Type: Timestamp

Required: Yes

GroupId

The stable and unique string identifying the group. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

GroupName

The friendly name that identifies the group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Path

The path to the group. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

GroupDetail

Contains information about an IAM group, including all of the group's policies.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 143) operation.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AttachedManagedPolicies.member.N

A list of the managed policies attached to the group.

Type: Array of AttachedPolicy (p. 430) objects

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the group was created.

Type: Timestamp

Required: No

GroupId

The stable and unique string identifying the group. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

GroupName

The friendly name that identifies the group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

GroupPolicyList.member.N

A list of the inline policies embedded in the group.

Type: Array of PolicyDetail (p. 460) objects

Required: No

Path

The path to the group. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

InstanceProfile

Contains information about an instance profile.

This data type is used as a response element in the following operations:

- CreateInstanceProfile (p. 33)
- GetInstanceProfile (p. 170)
- ListInstanceProfiles (p. 251)
- ListInstanceProfilesForRole (p. 254)

Contents

Arn

The Amazon Resource Name (ARN) specifying the instance profile. For more information about ARNs and how to use them in policies, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

CreateDate

The date when the instance profile was created.

Type: Timestamp

Required: Yes

InstanceProfileId

The stable and unique string identifying the instance profile. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

InstanceProfileName

The name identifying the instance profile.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

Path

The path to the instance profile. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

Roles.member.N

The role associated with the instance profile.

Type: Array of Role (p. 471) objects

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ListPoliciesGrantingServiceAccessEntry

Contains details about the permissions policies that are attached to the specified identity (user, group, or role).

This data type is used as a response element in the ListPoliciesGrantingServiceAccess (p. 266) operation.

Contents

Policies.member.N

The `PoliciesGrantingServiceAccess` object that contains details about the policy.

Type: Array of PolicyGrantingServiceAccess (p. 461) objects

Required: No

ServiceNamespace

The namespace of the service that was accessed.

To learn the service namespace of a service, go to Actions, Resources, and Condition Keys for AWS Services in the *IAM User Guide*. Choose the name of the service to view details for that service. In the first paragraph, find the service prefix. For example, `(service prefix: a4b)`. For more information about service namespaces, see AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w-]*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LoginProfile

Contains the user name and password create date for a user.

This data type is used as a response element in the CreateLoginProfile (p. 36) and GetLoginProfile (p. 173) operations.

Contents

CreateDate

The date when the password for the user was created.

Type: Timestamp

Required: Yes

PasswordResetRequired

Specifies whether the user is required to set a new password on next sign-in.

Type: Boolean

Required: No

UserName

The name of the user, which can be used for signing in to the AWS Management Console.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ManagedPolicyDetail

Contains information about a managed policy, including the policy's ARN, versions, and the number of principal entities (users, groups, and roles) that the policy is attached to.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 143) operation.

For more information about managed policies, see Managed Policies and Inline Policies in the *IAM User Guide*.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AttachmentCount

The number of principal entities (users, groups, and roles) that the policy is attached to.

Type: Integer

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the policy was created.

Type: Timestamp

Required: No

DefaultVersionId

The identifier for the version of the policy that is set as the default (operative) version.

For more information about policy versions, see Versioning for Managed Policies in the *IAM User Guide*.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: No

Description

A friendly description of the policy.

Type: String

Length Constraints: Maximum length of 1000.

Required: No

IsAttachable

Specifies whether the policy can be attached to an IAM user, group, or role.

Type: Boolean

Required: No

Path

The path to the policy.

For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

PermissionsBoundaryUsageCount

The number of entities (users and roles) for which the policy is used as the permissions boundary.

For more information about permissions boundaries, see Permissions Boundaries for IAM Identities in the *IAM User Guide*.

Type: Integer

Required: No

PolicyId

The stable and unique string identifying the policy.

For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

PolicyName

The friendly name (not ARN) identifying the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

PolicyVersionList.member.N

A list containing information about the versions of the policy.

Type: Array of PolicyVersion (p. 466) objects

Required: No

UpdateDate

The date and time, in ISO 8601 date-time format, when the policy was last updated.

When a policy has only one version, this field contains the date and time when the policy was created. When a policy has more than one version, this field contains the date and time when the most recent policy version was created.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MFADevice

Contains information about an MFA device.

This data type is used as a response element in the ListMFADevices (p. 257) operation.

Contents

EnableDate

The date when the MFA device was enabled for the user.

Type: Timestamp

Required: Yes

SerialNumber

The serial number that uniquely identifies the MFA device. For virtual MFA devices, the serial number is the device ARN.

Type: String

Length Constraints: Minimum length of 9. Maximum length of 256.

Pattern: `[\w+=/:,.@-]+`

Required: Yes

UserName

The user with whom the MFA device is associated.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OpenIDConnectProviderListEntry

Contains the Amazon Resource Name (ARN) for an IAM OpenID Connect provider.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OrganizationsDecisionDetail

Contains information about the effect that Organizations has on a policy simulation.

Contents

AllowedByOrganizations

Specifies whether the simulated operation is allowed by the Organizations service control policies that impact the simulated user's account.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PasswordPolicy

Contains information about the account password policy.

This data type is used as a response element in the GetAccountPasswordPolicy (p. 150) operation.

Contents

AllowUsersToChangePassword

Specifies whether IAM users are allowed to change their own password.

Type: Boolean

Required: No

ExpirePasswords

Indicates whether passwords in the account expire. Returns true if `MaxPasswordAge` contains a value greater than 0. Returns false if MaxPasswordAge is 0 or not present.

Type: Boolean

Required: No

HardExpiry

Specifies whether IAM users are prevented from setting a new password after their password has expired.

Type: Boolean

Required: No

MaxPasswordAge

The number of days that an IAM user password is valid.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 1095.

Required: No

MinimumPasswordLength

Minimum length to require for IAM user passwords.

Type: Integer

Valid Range: Minimum value of 6. Maximum value of 128.

Required: No

PasswordReusePrevention

Specifies the number of previous passwords that IAM users are prevented from reusing.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 24.

Required: No

RequireLowercaseCharacters

Specifies whether IAM user passwords must contain at least one lowercase character (a to z).

Type: Boolean

Required: No

RequireNumbers

Specifies whether IAM user passwords must contain at least one numeric character (0 to 9).

Type: Boolean

Required: No

RequireSymbols

Specifies whether IAM user passwords must contain at least one of the following symbols:

! @ # $ % ^ & * ( ) _ + - = [ ] { } | '

Type: Boolean

Required: No

RequireUppercaseCharacters

Specifies whether IAM user passwords must contain at least one uppercase character (A to Z).

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PermissionsBoundaryDecisionDetail

Contains information about the effect that a permissions boundary has on a policy simulation when the boundary is applied to an IAM entity.

Contents

AllowedByPermissionsBoundary

Specifies whether an action is allowed by a permissions boundary that is applied to an IAM entity (user or role). A value of `true` means that the permissions boundary does not deny the action. This means that the policy includes an `Allow` statement that matches the request. In this case, if an identity-based policy also allows the action, the request is allowed. A value of `false` means that either the requested action is not allowed (implicitly denied) or that the action is explicitly denied by the permissions boundary. In both of these cases, the action is not allowed, regardless of the identity-based policy.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Policy

Contains information about a managed policy.

This data type is used as a response element in the CreatePolicy (p. 43), GetPolicy (p. 182), and ListPolicies (p. 262) operations.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AttachmentCount

The number of entities (users, groups, and roles) that the policy is attached to.

Type: Integer

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the policy was created.

Type: Timestamp

Required: No

DefaultVersionId

The identifier for the version of the policy that is set as the default version.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: No

Description

A friendly description of the policy.

This element is included in the response to the GetPolicy (p. 182) operation. It is not included in the response to the ListPolicies (p. 262) operation.

Type: String

Length Constraints: Maximum length of 1000.

Required: No

IsAttachable

Specifies whether the policy can be attached to an IAM user, group, or role.

Type: Boolean

Required: No

Path

The path to the policy.

For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `((/[A-Za-z0-9\.,\+@=_-]+)*)/`

Required: No

PermissionsBoundaryUsageCount

The number of entities (users and roles) for which the policy is used to set the permissions boundary.

For more information about permissions boundaries, see Permissions Boundaries for IAM Identities in the *IAM User Guide*.

Type: Integer

Required: No

PolicyId

The stable and unique string identifying the policy.

For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

PolicyName

The friendly name (not ARN) identifying the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

UpdateDate

The date and time, in ISO 8601 date-time format, when the policy was last updated.

When a policy has only one version, this field contains the date and time when the policy was created. When a policy has more than one version, this field contains the date and time when the most recent policy version was created.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyDetail

Contains information about an IAM policy, including the policy document.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 143) operation.

Contents

PolicyDocument

The policy document.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

PolicyName

The name of the policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyGrantingServiceAccess

Contains details about the permissions policies that are attached to the specified identity (user, group, or role).

This data type is an element of the ListPoliciesGrantingServiceAccessEntry (p. 446) object.

Contents

EntityName

The name of the entity (user or role) to which the inline policy is attached.

This field is null for managed policies. For more information about these policy types, see Managed Policies and Inline Policies in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

EntityType

The type of entity (user or role) that used the policy to access the service to which the inline policy is attached.

This field is null for managed policies. For more information about these policy types, see Managed Policies and Inline Policies in the *IAM User Guide*.

Type: String

Valid Values: `USER | ROLE | GROUP`

Required: No

PolicyArn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

PolicyName

The policy name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

PolicyType

The policy type. For more information about these policy types, see Managed Policies and Inline Policies in the *IAM User Guide*.

Type: String

Valid Values: `INLINE | MANAGED`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyGroup

Contains information about a group that a managed policy is attached to.

This data type is used as a response element in the ListEntitiesForPolicy (p. 238) operation.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Contents

GroupId

The stable and unique string identifying the group. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

GroupName

The name (friendly name, not ARN) identifying the group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyRole

Contains information about a role that a managed policy is attached to.

This data type is used as a response element in the ListEntitiesForPolicy (p. 238) operation.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Contents

RoleId

The stable and unique string identifying the role. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

RoleName

The name (friendly name, not ARN) identifying the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyUser

Contains information about a user that a managed policy is attached to.

This data type is used as a response element in the ListEntitiesForPolicy (p. 238) operation.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Contents

UserId

The stable and unique string identifying the user. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

UserName

The name (friendly name, not ARN) identifying the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyVersion

Contains information about a version of a managed policy.

This data type is used as a response element in the CreatePolicyVersion (p. 47), GetPolicyVersion (p. 185), ListPolicyVersions (p. 270), and GetAccountAuthorizationDetails (p. 143) operations.

For more information about managed policies, refer to Managed Policies and Inline Policies in the *IAM User Guide*.

Contents

CreateDate

The date and time, in ISO 8601 date-time format, when the policy version was created.

Type: Timestamp

Required: No

Document

The policy document.

The policy document is returned in the response to the GetPolicyVersion (p. 185) and GetAccountAuthorizationDetails (p. 143) operations. It is not returned in the response to the CreatePolicyVersion (p. 47) or ListPolicyVersions (p. 270) operations.

The policy document returned in this structure is URL-encoded compliant with RFC 3986. You can use a URL decoding method to convert the policy back to plain JSON text. For example, if you use Java, you can use the `decode` method of the `java.net.URLDecoder` utility class in the Java SDK. Other languages and SDKs provide similar functionality.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

IsDefaultVersion

Specifies whether the policy version is set as the policy's default version.

Type: Boolean

Required: No

VersionId

The identifier for the policy version.

Policy version identifiers always begin with `v` (always lowercase). When a policy is created, the first policy version is `v1`.

Type: String

Pattern: `v[1-9][0-9]*(\.[A-Za-z0-9-]*)?`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Position

Contains the row and column of a location of a `Statement` element in a policy document.

This data type is used as a member of the `Statement (p. 495)` type.

Contents

Column

The column in the line containing the specified position in the document.

Type: Integer

Required: No

Line

The line containing the specified position in the document.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceSpecificResult

Contains the result of the simulation of a single API operation call on a single resource.

This data type is used by a member of the EvaluationResult (p. 437) data type.

Contents

EvalDecisionDetails , EvalDecisionDetails.entry.N.key (key), EvalDecisionDetails.entry.N.value (value)

Additional details about the results of the evaluation decision on a single resource. This parameter is returned only for cross-account simulations. This parameter explains how each policy type contributes to the resource-specific evaluation decision.

Type: String to string map

Key Length Constraints: Minimum length of 3. Maximum length of 256.

Valid Values: `allowed | explicitDeny | implicitDeny`

Required: No

EvalResourceDecision

The result of the simulation of the simulated API operation on the resource specified in `EvalResourceName`.

Type: String

Valid Values: `allowed | explicitDeny | implicitDeny`

Required: Yes

EvalResourceName

The name of the simulated resource, in Amazon Resource Name (ARN) format.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Required: Yes

MatchedStatements.member.N

A list of the statements in the input policies that determine the result for this part of the simulation. Remember that even if multiple statements allow the operation on the resource, if *any* statement denies that operation, then the explicit deny overrides any allow. In addition, the deny statement is the only entry included in the result.

Type: Array of Statement (p. 495) objects

Required: No

MissingContextValues.member.N

A list of context keys that are required by the included input policies but that were not provided by one of the input parameters. This list is used when a list of ARNs is included in the `ResourceArns` parameter instead of "*". If you do not specify individual resources, by setting `ResourceArns` to "*" or by not including the `ResourceArns` parameter, then any missing context values are instead included under the `EvaluationResults` section. To discover the

context keys used by a set of policies, you can call GetContextKeysForCustomPolicy (p. 156) or GetContextKeysForPrincipalPolicy (p. 159).

Type: Array of strings

Length Constraints: Minimum length of 5. Maximum length of 256.

Required: No

PermissionsBoundaryDecisionDetail

Contains information about the effect that a permissions boundary has on a policy simulation when that boundary is applied to an IAM entity.

Type: PermissionsBoundaryDecisionDetail (p. 456) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Role

Contains information about an IAM role. This structure is returned as a response element in several API operations that interact with roles.

Contents

Arn

The Amazon Resource Name (ARN) specifying the role. For more information about ARNs and how to use them in policies, see IAM Identifiers in the *IAM User Guide* guide.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

AssumeRolePolicyDocument

The policy that grants an entity permission to assume the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the role was created.

Type: Timestamp

Required: Yes

Description

A description of the role that you provide.

Type: String

Length Constraints: Maximum length of 1000.

Pattern: `[\p{L}\p{M}\p{Z}\p{S}\p{N}\p{P}]*`

Required: No

MaxSessionDuration

The maximum session duration (in seconds) for the specified role. Anyone who uses the AWS CLI, or API to assume the role can specify the duration using the optional `DurationSeconds` API parameter or `duration-seconds` CLI parameter.

Type: Integer

Valid Range: Minimum value of 3600. Maximum value of 43200.

Required: No

Path

The path to the role. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

PermissionsBoundary

The ARN of the policy used to set the permissions boundary for the role.

For more information about permissions boundaries, see Permissions Boundaries for IAM Identities in the *IAM User Guide*.

Type: AttachedPermissionsBoundary (p. 429) object

Required: No

RoleId

The stable and unique string identifying the role. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

RoleLastUsed

Contains information about the last time that an IAM role was used. This includes the date and time and the Region in which the role was last used. Activity is only reported for the trailing 400 days. This period can be shorter if your Region began supporting these features within the last year. The role might have been used more than 400 days ago. For more information, see Regions Where Data Is Tracked in the *IAM User Guide*.

Type: RoleLastUsed (p. 477) object

Required: No

RoleName

The friendly name that identifies the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

Tags.member.N

A list of tags that are attached to the specified role. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RoleDetail

Contains information about an IAM role, including all of the role's policies.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 143) operation.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AssumeRolePolicyDocument

The trust policy that grants permission to assume the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 131072.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

AttachedManagedPolicies.member.N

A list of managed policies attached to the role. These policies are the role's access (permissions) policies.

Type: Array of AttachedPolicy (p. 430) objects

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the role was created.

Type: Timestamp

Required: No

InstanceProfileList.member.N

A list of instance profiles that contain this role.

Type: Array of InstanceProfile (p. 444) objects

Required: No

Path

The path to the role. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

PermissionsBoundary

The ARN of the policy used to set the permissions boundary for the role.

For more information about permissions boundaries, see Permissions Boundaries for IAM Identities in the *IAM User Guide*.

Type: AttachedPermissionsBoundary (p. 429) object

Required: No

RoleId

The stable and unique string identifying the role. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

RoleLastUsed

Contains information about the last time that an IAM role was used. This includes the date and time and the Region in which the role was last used. Activity is only reported for the trailing 400 days. This period can be shorter if your Region began supporting these features within the last year. The role might have been used more than 400 days ago. For more information, see Regions Where Data Is Tracked in the *IAM User Guide*.

Type: RoleLastUsed (p. 477) object

Required: No

RoleName

The friendly name that identifies the role.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

RolePolicyList.member.N

A list of inline policies embedded in the role. These policies are the role's access (permissions) policies.

Type: Array of PolicyDetail (p. 460) objects

Required: No

Tags.member.N

A list of tags that are attached to the specified role. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RoleLastUsed

Contains information about the last time that an IAM role was used. This includes the date and time and the Region in which the role was last used. Activity is only reported for the trailing 400 days. This period can be shorter if your Region began supporting these features within the last year. The role might have been used more than 400 days ago. For more information, see Regions Where Data Is Tracked in the *IAM User Guide*.

This data type is returned as a response element in the GetRole (p. 188) and GetAccountAuthorizationDetails (p. 143) operations.

Contents

LastUsedDate

The date and time, in ISO 8601 date-time format that the role was last used.

This field is null if the role has not been used within the IAM tracking period. For more information about the tracking period, see Regions Where Data Is Tracked in the *IAM User Guide*.

Type: Timestamp

Required: No

Region

The name of the AWS Region in which the role was last used.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RoleUsageType

An object that contains details about how a service-linked role is used, if that information is returned by the service.

This data type is used as a response element in the GetServiceLinkedRoleDeletionStatus (p. 208) operation.

Contents

Region

The name of the Region where the service-linked role is being used.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 100.

Required: No

Resources.member.N

The name of the resource that is using the service-linked role.

Type: Array of strings

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SAMLProviderListEntry

Contains the list of SAML providers for this account.

Contents

Arn

The Amazon Resource Name (ARN) of the SAML provider.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

CreateDate

The date and time when the SAML provider was created.

Type: Timestamp

Required: No

ValidUntil

The expiration date and time for the SAML provider.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServerCertificate

Contains information about a server certificate.

This data type is used as a response element in the GetServerCertificate (p. 196) operation.

Contents

CertificateBody

The contents of the public key certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

CertificateChain

The contents of the public key certificate chain.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2097152.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: No

ServerCertificateMetadata

The meta information of the server certificate, such as its name, path, ID, and ARN.

Type: ServerCertificateMetadata (p. 481) object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServerCertificateMetadata

Contains information about a server certificate without its certificate body, certificate chain, and private key.

This data type is used as a response element in the UploadServerCertificate (p. 407) and ListServerCertificates (p. 284) operations.

Contents

Arn

The Amazon Resource Name (ARN) specifying the server certificate. For more information about ARNs and how to use them in policies, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

Expiration

The date on which the certificate is set to expire.

Type: Timestamp

Required: No

Path

The path to the server certificate. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

ServerCertificateId

The stable and unique string identifying the server certificate. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

ServerCertificateName

The name that identifies the server certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: Yes

UploadDate

The date when the server certificate was uploaded.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServiceLastAccessed

Contains details about the most recent attempt to access the service.

This data type is used as a response element in the GetServiceLastAccessedDetails (p. 199) operation.

Contents

LastAuthenticated

The date and time, in ISO 8601 date-time format, when an authenticated entity most recently attempted to access the service. AWS does not report unauthenticated requests.

This field is null if no IAM entities attempted to access the service within the reporting period.

Type: Timestamp

Required: No

LastAuthenticatedEntity

The ARN of the authenticated entity (user or role) that last attempted to access the service. AWS does not report unauthenticated requests.

This field is null if no IAM entities attempted to access the service within the reporting period.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

LastAuthenticatedRegion

The Region from which the authenticated entity (user or role) last attempted to access the service. AWS does not report unauthenticated requests.

This field is null if no IAM entities attempted to access the service within the reporting period.

Type: String

Required: No

ServiceName

The name of the service in which access was attempted.

Type: String

Required: Yes

ServiceNamespace

The namespace of the service in which access was attempted.

To learn the service namespace of a service, go to Actions, Resources, and Condition Keys for AWS Services in the *IAM User Guide*. Choose the name of the service to view details for that service. In the first paragraph, find the service prefix. For example, `(service prefix: a4b)`. For more information about service namespaces, see AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w-]*`

Required: Yes

TotalAuthenticatedEntities

The total number of authenticated principals (root user, IAM users, or IAM roles) that have attempted to access the service.

This field is null if no principals attempted to access the service within the reporting period.

Type: Integer

Required: No

TrackedActionsLastAccessed.member.N

An object that contains details about the most recent attempt to access a tracked action within the service.

This field is null if there no tracked actions or if the principal did not use the tracked actions within the reporting period. This field is also null if the report was generated at the service level and not the action level. For more information, see the `Granularity` field in GenerateServiceLastAccessedDetails (p. 138).

Type: Array of TrackedActionLastAccessed (p. 497) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServiceSpecificCredential

Contains the details of a service-specific credential.

Contents

CreateDate

The date and time, in ISO 8601 date-time format, when the service-specific credential were created.

Type: Timestamp

Required: Yes

ServiceName

The name of the service associated with the service-specific credential.

Type: String

Required: Yes

ServicePassword

The generated password for the service-specific credential.

Type: String

Required: Yes

ServiceSpecificCredentialId

The unique identifier for the service-specific credential.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

ServiceUserName

The generated user name for the service-specific credential. This value is generated by combining the IAM user's name combined with the ID number of the AWS account, as in `jane-at-123456789012`, for example. This value cannot be configured by the user.

Type: String

Length Constraints: Minimum length of 17. Maximum length of 200.

Pattern: `[\w+=,.@-]+`

Required: Yes

Status

The status of the service-specific credential. `Active` means that the key is valid for API calls, while `Inactive` means it is not.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user associated with the service-specific credential.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ServiceSpecificCredentialMetadata

Contains additional details about a service-specific credential.

Contents

CreateDate

The date and time, in ISO 8601 date-time format, when the service-specific credential were created.

Type: Timestamp

Required: Yes

ServiceName

The name of the service associated with the service-specific credential.

Type: String

Required: Yes

ServiceSpecificCredentialId

The unique identifier for the service-specific credential.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

ServiceUserName

The generated user name for the service-specific credential.

Type: String

Length Constraints: Minimum length of 17. Maximum length of 200.

Pattern: `[\w+=,.@-]+`

Required: Yes

Status

The status of the service-specific credential. `Active` means that the key is valid for API calls, while `Inactive` means it is not.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UserName

The name of the IAM user associated with the service-specific credential.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SigningCertificate

Contains information about an X.509 signing certificate.

This data type is used as a response element in the UploadSigningCertificate (p. 412) and ListSigningCertificates (p. 290) operations.

Contents

CertificateBody

The contents of the signing certificate.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

CertificateId

The ID for the signing certificate.

Type: String

Length Constraints: Minimum length of 24. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status of the signing certificate. `Active` means that the key is valid for API calls, while `Inactive` means it is not.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UploadDate

The date when the signing certificate was uploaded.

Type: Timestamp

Required: No

UserName

The name of the user the signing certificate is associated with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SSHPublicKey

Contains information about an SSH public key.

This data type is used as a response element in the GetSSHPublicKey (p. 211) and UploadSSHPublicKey (p. 416) operations.

Contents

Fingerprint

The MD5 message digest of the SSH public key.

Type: String

Length Constraints: Fixed length of 48.

Pattern: `[:\w]+`

Required: Yes

SSHPublicKeyBody

The SSH public key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16384.

Pattern: `[\u0009\u000A\u000D\u0020-\u00FF]+`

Required: Yes

SSHPublicKeyId

The unique identifier for the SSH public key.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status of the SSH public key. `Active` means that the key can be used for authentication with an AWS CodeCommit repository. `Inactive` means that the key cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UploadDate

The date and time, in ISO 8601 date-time format, when the SSH public key was uploaded.

Type: Timestamp

Required: No

UserName

The name of the IAM user associated with the SSH public key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SSHPublicKeyMetadata

Contains information about an SSH public key, without the key's body or fingerprint.

This data type is used as a response element in the ListSSHPublicKeys (p. 293) operation.

Contents

SSHPublicKeyId

The unique identifier for the SSH public key.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

Status

The status of the SSH public key. `Active` means that the key can be used for authentication with an AWS CodeCommit repository. `Inactive` means that the key cannot be used.

Type: String

Valid Values: `Active | Inactive`

Required: Yes

UploadDate

The date and time, in ISO 8601 date-time format, when the SSH public key was uploaded.

Type: Timestamp

Required: Yes

UserName

The name of the IAM user associated with the SSH public key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Statement

Contains a reference to a `Statement` element in a policy document that determines the result of the simulation.

This data type is used by the `MatchedStatements` member of the `EvaluationResult (p. 437)` type.

Contents

EndPosition

The row and column of the end of a `Statement` in an IAM policy.

Type: Position (p. 468) object

Required: No

SourcePolicyId

The identifier of the policy that was provided as an input.

Type: String

Required: No

SourcePolicyType

The type of the policy.

Type: String

Valid Values: `user | group | role | aws-managed | user-managed | resource | none`

Required: No

StartPosition

The row and column of the beginning of the `Statement` in an IAM policy.

Type: Position (p. 468) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

A structure that represents user-provided metadata that can be associated with a resource such as an IAM user or role. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Contents

Key

The key name that can be used to look up or retrieve the associated value. For example, `Department` or `Cost Center` are common choices.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\p{L}\p{Z}\p{N}_.:/=+\-@]+`

Required: Yes

Value

The value associated with this tag. For example, tags with a key name of `Department` could have values such as `Human Resources`, `Accounting`, and `Support`. Tags with a key name of `Cost Center` might have values that consist of the number associated with the different cost centers in your company. Typically, many resources have tags with the same key name but with different values.

> **Note**
> AWS always interprets the tag `Value` as a single string. If you need to store an array, you can store comma-separated values in the string. However, you must interpret the value in your code.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[\p{L}\p{Z}\p{N}_.:/=+\-@]*`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TrackedActionLastAccessed

Contains details about the most recent attempt to access an action within the service.

This data type is used as a response element in the GetServiceLastAccessedDetails (p. 199) operation.

Contents

ActionName

The name of the tracked action to which access was attempted. Tracked actions are actions that report activity to IAM.

Type: String

Required: No

LastAccessedEntity

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

LastAccessedRegion

The Region from which the authenticated entity (user or role) last attempted to access the tracked action. AWS does not report unauthenticated requests.

This field is null if no IAM entities attempted to access the service within the reporting period.

Type: String

Required: No

LastAccessedTime

The date and time, in ISO 8601 date-time format, when an authenticated entity most recently attempted to access the tracked service. AWS does not report unauthenticated requests.

This field is null if no IAM entities attempted to access the service within the reporting period.

Type: Timestamp

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWS SDK for Ruby V3

User

Contains information about an IAM user entity.

This data type is used as a response element in the following operations:

- CreateUser (p. 63)
- GetUser (p. 214)
- ListUsers (p. 299)

Contents

Arn

The Amazon Resource Name (ARN) that identifies the user. For more information about ARNs and how to use ARNs in policies, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: Yes

CreateDate

The date and time, in ISO 8601 date-time format, when the user was created.

Type: Timestamp

Required: Yes

PasswordLastUsed

The date and time, in ISO 8601 date-time format, when the user's password was last used to sign in to an AWS website. For a list of AWS websites that capture a user's last sign-in time, see the Credential Reports topic in the *IAM User Guide*. If a password is used more than once in a five-minute span, only the first use is returned in this field. If the field is null (no value), then it indicates that they never signed in with a password. This can be because:

- The user never had a password.
- A password exists but has not been used since IAM started tracking this information on October 20, 2014.

A null value does not mean that the user *never* had a password. Also, if the user does not currently have a password but had one in the past, then this field contains the date and time the most recent password was used.

This value is returned only in the GetUser (p. 214) and ListUsers (p. 299) operations.

Type: Timestamp

Required: No

Path

The path to the user. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: Yes

PermissionsBoundary

The ARN of the policy used to set the permissions boundary for the user.

For more information about permissions boundaries, see Permissions Boundaries for IAM Identities in the *IAM User Guide*.

Type: AttachedPermissionsBoundary (p. 429) object

Required: No

Tags.member.N

A list of tags that are associated with the specified user. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Required: No

UserId

The stable and unique string identifying the user. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: Yes

UserName

The friendly name identifying the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

UserDetail

Contains information about an IAM user, including all the user's policies and all the IAM groups the user is in.

This data type is used as a response element in the GetAccountAuthorizationDetails (p. 143) operation.

Contents

Arn

The Amazon Resource Name (ARN). ARNs are unique identifiers for AWS resources.

For more information about ARNs, go to Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

Type: String

Length Constraints: Minimum length of 20. Maximum length of 2048.

Required: No

AttachedManagedPolicies.member.N

A list of the managed policies attached to the user.

Type: Array of AttachedPolicy (p. 430) objects

Required: No

CreateDate

The date and time, in ISO 8601 date-time format, when the user was created.

Type: Timestamp

Required: No

GroupList.member.N

A list of IAM groups that the user is in.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `[\w+=,.@-]+`

Required: No

Path

The path to the user. For more information about paths, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `(\u002F)|(\u002F[\u0021-\u007F]+\u002F)`

Required: No

PermissionsBoundary

The ARN of the policy used to set the permissions boundary for the user.

For more information about permissions boundaries, see Permissions Boundaries for IAM Identities in the *IAM User Guide*.

Type: AttachedPermissionsBoundary (p. 429) object

Required: No

Tags.member.N

A list of tags that are associated with the specified user. For more information about tagging, see Tagging IAM Identities in the *IAM User Guide*.

Type: Array of Tag (p. 496) objects

Array Members: Maximum number of 50 items.

Required: No

UserId

The stable and unique string identifying the user. For more information about IDs, see IAM Identifiers in the *IAM User Guide*.

Type: String

Length Constraints: Minimum length of 16. Maximum length of 128.

Pattern: `[\w]+`

Required: No

UserName

The friendly name identifying the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[\w+=,.@-]+`

Required: No

UserPolicyList.member.N

A list of the inline policies embedded in the user.

Type: Array of PolicyDetail (p. 460) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWS SDK for Ruby V3

VirtualMFADevice

Contains information about a virtual MFA device.

Contents

Base32StringSeed

The base32 seed defined as specified in RFC3548. The `Base32StringSeed` is base64-encoded.

Type: Base64-encoded binary data object

Required: No

EnableDate

The date and time on which the virtual MFA device was enabled.

Type: Timestamp

Required: No

QRCodePNG

A QR code PNG image that encodes `otpauth://totp/$virtualMFADeviceName@$AccountName?secret=$Base32String` where `$virtualMFADeviceName` is one of the create call arguments. `AccountName` is the user name if set (otherwise, the account ID otherwise), and `Base32String` is the seed in base32 format. The `Base32String` value is base64-encoded.

Type: Base64-encoded binary data object

Required: No

SerialNumber

The serial number associated with `VirtualMFADevice`.

Type: String

Length Constraints: Minimum length of 9. Maximum length of 256.

Pattern: `[\w+=/:,.@-]+`

Required: Yes

User

The IAM user associated with this virtual MFA device.

Type: User (p. 499) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2

- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is

not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS Security Token Service, go to AWS Services That Work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400