API Reference

AWS Private CA Connector for Active Directory

API Version 2018-05-10

AWS Private CA Connector for Active Directory: API Reference

Table of Contents

Welcome

AWS Private CA Connector for Active Directory creates a connector between AWS Private CA and Active Directory (AD) that enables you to provision security certificates for AD signed by a private CA that you own. For more information, see AWS Private CA Connector for Active Directory.

This document was last published on January 27, 2026.

Actions

The following actions are supported:

- CreateConnector
- CreateDirectoryRegistration
- CreateServicePrincipalName
- CreateTemplate
- CreateTemplateGroupAccessControlEntry
- DeleteConnector
- DeleteDirectoryRegistration
- DeleteServicePrincipalName
- DeleteTemplate
- DeleteTemplateGroupAccessControlEntry
- GetConnector
- GetDirectoryRegistration
- GetServicePrincipalName
- GetTemplate
- GetTemplateGroupAccessControlEntry
- ListConnectors
- ListDirectoryRegistrations
- ListServicePrincipalNames
- ListTagsForResource
- ListTemplateGroupAccessControlEntries
- ListTemplates
- TagResource
- UntagResource
- UpdateTemplate
- UpdateTemplateGroupAccessControlEntry

CreateConnector

Creates a connector between AWS Private CA and an Active Directory. You must specify the private CA, directory ID, and security groups.

Request Syntax

```
POST /connectors HTTP/1.1
Content-type: application/json

{
   "CertificateAuthorityArn": "string",
   "ClientToken": "string",
   "DirectoryId": "string",
   "Tags": {
      "string" : "string"
   },
   "VpcInformation": {
      "IpAddressType": "string",
      "SecurityGroupIds": [ "string" ]
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the certificate authority being used.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:acm-pca:[\w-]+:[0-9]+:certificate-authority\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

ClientToken

Idempotency token.

Type: String

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

Pattern: `[!-~]+`

Required: No

DirectoryId

The identifier of the Active Directory.

Type: String

Pattern: `d-[0-9a-f]{10}`

Required: Yes

Tags

Metadata assigned to a connector consisting of a key-value pair.

Type: String to string map

Required: No

VpcInformation

Information about your VPC and security groups used with the connector.

Type: VpcInformation object

Required: Yes

Response Syntax

```
HTTP/1.1 202
```

```
Content-type: application/json

{
   "ConnectorArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response.

The following data is returned in JSON format by the service.

ConnectorArn

If successful, the Amazon Resource Name (ARN) of the connector for Active Directory.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ServiceQuotaExceededException

Request would cause a service quota to be exceeded.

QuotaCode

The code associated with the service quota.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

ServiceCode

Identifies the originating service.

HTTP Status Code: 402

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateDirectoryRegistration

Creates a directory registration that authorizes communication between AWS Private CA and an Active Directory

Request Syntax

```
POST /directoryRegistrations HTTP/1.1
Content-type: application/json

{
   "ClientToken": "string",
   "DirectoryId": "string",
   "Tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

ClientToken

Idempotency token.

Type: String

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

Pattern: `[!-~]+`

Required: No

DirectoryId

The identifier of the Active Directory.

Type: String

Pattern: `d-[0-9a-f]{10}`

Required: Yes

Tags

Metadata assigned to a directory registration consisting of a key-value pair.

Type: String to string map

Required: No

Response Syntax

```
HTTP/1.1 202
Content-type: application/json

{
   "DirectoryRegistrationArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response.

The following data is returned in JSON format by the service.

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

CreateServicePrincipalName

Creates a service principal name (SPN) for the service account in Active Directory. Kerberos authentication uses SPNs to associate a service instance with a service sign-in account.

Request Syntax

```
POST /directoryRegistrations/DirectoryRegistrationArn/
servicePrincipalNames/ConnectorArn HTTP/1.1
Content-type: application/json

{
   "ClientToken": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

ClientToken

Idempotency token.

Type: String

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

Pattern: `[!-~]+`

Required: No

Response Syntax

```
HTTP/1.1 202
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateTemplate

Creates an Active Directory compatible certificate template. The connectors issues certificates using these templates based on the requester’s Active Directory group membership.

Request Syntax

```
POST /templates HTTP/1.1
Content-type: application/json

{
   "ClientToken": "string",
   "ConnectorArn": "string",
   "Definition": { ... },
   "Name": "string",
   "Tags": {
      "string" : "string"
   }
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

ClientToken

Idempotency token.

Type: String

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

Pattern: `[!-~]+`

Required: No

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Definition

Template configuration to define the information included in certificates. Define certificate validity and renewal periods, certificate request handling and enrollment options, key usage extensions, application policies, and cryptography settings.

Type: TemplateDefinition object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

Name

Name of the template. The template name must be unique.

Type: String

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

Pattern: `(?!^\s+$)((?![\x5c'\x2b,;<=>#\x22])([\x20-\x7E]))+`

Required: Yes

Tags

Metadata assigned to a template consisting of a key-value pair.

Type: String to string map

Required: No

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "TemplateArn": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TemplateArn

If successful, the Amazon Resource Name (ARN) of the template.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ServiceQuotaExceededException

Request would cause a service quota to be exceeded.

QuotaCode

The code associated with the service quota.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

ServiceCode

Identifies the originating service.

HTTP Status Code: 402

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateTemplateGroupAccessControlEntry

Create a group access control entry. Allow or deny Active Directory groups from enrolling and/or autoenrolling with the template based on the group security identifiers (SIDs).

Request Syntax

```
POST /templates/TemplateArn/accessControlEntries HTTP/1.1
Content-type: application/json

{
   "AccessRights": {
      "AutoEnroll": "string",
      "Enroll": "string"
   },
   "ClientToken": "string",
   "GroupDisplayName": "string",
   "GroupSecurityIdentifier": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

AccessRights

Allow or deny permissions for an Active Directory group to enroll or autoenroll certificates for a template.

Type: AccessRights object

Required: Yes

ClientToken

Idempotency token.

Type: String

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

Pattern: `[!-~]+`

Required: No

GroupDisplayName

Name of the Active Directory group. This name does not need to match the group name in Active Directory.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[\x20-\x7E]+`

Required: Yes

GroupSecurityIdentifier

Security identifier (SID) of the group object from Active Directory. The SID starts with "S-".

Type: String

Length Constraints: Minimum length of 7. Maximum length of 256.

Pattern: `S-[0-9]-([0-9]+-){1,14}[0-9]+`

Required: Yes

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ServiceQuotaExceededException

Request would cause a service quota to be exceeded.

QuotaCode

The code associated with the service quota.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

ServiceCode

Identifies the originating service.

HTTP Status Code: 402

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteConnector

Deletes a connector for Active Directory. You must provide the Amazon Resource Name (ARN) of the connector that you want to delete. You can find the ARN by calling the https://docs.aws.amazon.com/pca-connector-ad/latest/APIReference/API_ListConnectors action. Deleting a connector does not deregister your directory with AWS Private CA. You can deregister your directory by calling the https://docs.aws.amazon.com/pca-connector-ad/latest/APIReference/API_DeleteDirectoryRegistration action.

Request Syntax

```
DELETE /connectors/ConnectorArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 202
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteDirectoryRegistration

Deletes a directory registration. Deleting a directory registration deauthorizes AWS Private CA with the directory.

Request Syntax

```
DELETE /directoryRegistrations/DirectoryRegistrationArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 202
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteServicePrincipalName

Deletes the service principal name (SPN) used by a connector to authenticate with your Active Directory.

Request Syntax

```
DELETE /directoryRegistrations/DirectoryRegistrationArn/
servicePrincipalNames/ConnectorArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 202
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

DeleteTemplate

Deletes a template. Certificates issued using the template are still valid until they are revoked or expired.

Request Syntax

```
DELETE /templates/TemplateArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 202
```

Response Elements

If the action is successful, the service sends back an HTTP 202 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

DeleteTemplateGroupAccessControlEntry

Deletes a group access control entry.

Request Syntax

```
DELETE /templates/TemplateArn/accessControlEntries/GroupSecurityIdentifier HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

GroupSecurityIdentifier

Security identifier (SID) of the group object from Active Directory. The SID starts with "S-".

Length Constraints: Minimum length of 7. Maximum length of 256.

Pattern: `S-[0-9]-([0-9]+-){1,14}[0-9]+`

Required: Yes

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetConnector

Lists information about your connector. You specify the connector on input by its ARN (Amazon Resource Name).

Request Syntax

```
GET /connectors/ConnectorArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Connector": {
      "Arn": "string",
      "CertificateAuthorityArn": "string",
      "CertificateEnrollmentPolicyServerEndpoint": "string",
      "CreatedAt": number,
      "DirectoryId": "string",
      "Status": "string",
      "StatusReason": "string",
      "UpdatedAt": number,
      "VpcInformation": {
         "IpAddressType": "string",
         "SecurityGroupIds": [ "string" ]
      }
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Connector

A structure that contains information about your connector.

Type: Connector object

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetDirectoryRegistration

A structure that contains information about your directory registration.

Request Syntax

```
GET /directoryRegistrations/DirectoryRegistrationArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "DirectoryRegistration": {
      "Arn": "string",
      "CreatedAt": number,
      "DirectoryId": "string",
      "Status": "string",
      "StatusReason": "string",
      "UpdatedAt": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

DirectoryRegistration

The directory registration represents the authorization of the connector service with a directory.

Type: DirectoryRegistration object

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetServicePrincipalName

Lists the service principal name that the connector uses to authenticate with Active Directory.

Request Syntax

```
GET /directoryRegistrations/DirectoryRegistrationArn/servicePrincipalNames/ConnectorArn
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ServicePrincipalName": { 
      "ConnectorArn": "string",
      "CreatedAt": number,
      "DirectoryRegistrationArn": "string",
      "Status": "string",
      "StatusReason": "string",
      "UpdatedAt": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

ServicePrincipalName

The service principal name that the connector uses to authenticate with Active Directory.

Type: ServicePrincipalName object

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetTemplate

Retrieves a certificate template that the connector uses to issue certificates from a private CA.

Request Syntax

```
GET /templates/TemplateArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Template": {
      "Arn": "string",
      "ConnectorArn": "string",
      "CreatedAt": number,
      "Definition": { ... },
      "Name": "string",
      "ObjectIdentifier": "string",
      "PolicySchema": number,
      "Revision": {
         "MajorRevision": number,
         "MinorRevision": number
      },
      "Status": "string",
      "UpdatedAt": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Template

A certificate template that the connector uses to issue certificates from a private CA.

Type: Template object

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetTemplateGroupAccessControlEntry

Retrieves the group access control entries for a template.

Request Syntax

```
GET /templates/TemplateArn/accessControlEntries/GroupSecurityIdentifier HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

GroupSecurityIdentifier

Security identifier (SID) of the group object from Active Directory. The SID starts with "S-".

Length Constraints: Minimum length of 7. Maximum length of 256.

Pattern: `S-[0-9]-([0-9]+-){1,14}[0-9]+`

Required: Yes

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "AccessControlEntry": {
      "AccessRights": {
         "AutoEnroll": "string",
         "Enroll": "string"
      },
      "CreatedAt": number,
      "GroupDisplayName": "string",
      "GroupSecurityIdentifier": "string",
      "TemplateArn": "string",
      "UpdatedAt": number
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AccessControlEntry

An access control entry allows or denies an Active Directory group from enrolling and/or autoenrolling with a template.

Type: AccessControlEntry object

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListConnectors

Lists the connectors that you created by using the https://docs.aws.amazon.com/pca-connector-ad/latest/APIReference/API_CreateConnector action.

Request Syntax

```
GET /connectors?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

Use this parameter when paginating results to specify the maximum number of items to return in the response on each page. If additional items exist beyond the number you specify, the `NextToken` element is sent in the response. Use this `NextToken` value in a subsequent request to retrieve additional items.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "Connectors": [
      {
         "Arn": "string",
         "CertificateAuthorityArn": "string",
         "CertificateEnrollmentPolicyServerEndpoint": "string",
         "CreatedAt": number,
         "DirectoryId": "string",
         "Status": "string",
         "StatusReason": "string",
         "UpdatedAt": number,
         "VpcInformation": {
            "IpAddressType": "string",
            "SecurityGroupIds": [ "string" ]
         }
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Connectors

Summary information about each connector you have created.

Type: Array of ConnectorSummary objects

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the NextToken parameter from the response you just received.

Type: String

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListDirectoryRegistrations

Lists the directory registrations that you created by using the https://docs.aws.amazon.com/pca-connector-ad/latest/APIReference/API_CreateDirectoryRegistration action.

Request Syntax

```
GET /directoryRegistrations?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

Use this parameter when paginating results to specify the maximum number of items to return in the response on each page. If additional items exist beyond the number you specify, the `NextToken` element is sent in the response. Use this `NextToken` value in a subsequent request to retrieve additional items.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "DirectoryRegistrations": [
      {
         "Arn": "string",
         "CreatedAt": number,
         "DirectoryId": "string",
         "Status": "string",
         "StatusReason": "string",
         "UpdatedAt": number
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

DirectoryRegistrations

Summary information about each directory registration you have created.

Type: Array of DirectoryRegistrationSummary objects

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

Type: String

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListServicePrincipalNames

Lists the service principal names that the connector uses to authenticate with Active Directory.

Request Syntax

```
GET /directoryRegistrations/DirectoryRegistrationArn/servicePrincipalNames?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: Yes

MaxResults

Use this parameter when paginating results to specify the maximum number of items to return in the response on each page. If additional items exist beyond the number you specify, the `NextToken` element is sent in the response. Use this `NextToken` value in a subsequent request to retrieve additional items.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ServicePrincipalNames": [
      {
         "ConnectorArn": "string",
         "CreatedAt": number,
         "DirectoryRegistrationArn": "string",
         "Status": "string",
         "StatusReason": "string",
         "UpdatedAt": number
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

Type: String

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

ServicePrincipalNames

The service principal name, if any, that the connector uses to authenticate with Active Directory.

Type: Array of ServicePrincipalNameSummary objects

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsForResource

Lists the tags, if any, that are associated with your resource.

Request Syntax

```
GET /tags/ResourceArn HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) that was returned when you created the resource.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Tags

The tags, if any, that are associated with your resource.

Type: String to string map

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTemplateGroupAccessControlEntries

Lists group access control entries you created.

Request Syntax

```
GET /templates/TemplateArn/accessControlEntries?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

MaxResults

Use this parameter when paginating results to specify the maximum number of items to return in the response on each page. If additional items exist beyond the number you specify, the `NextToken` element is sent in the response. Use this `NextToken` value in a subsequent request to retrieve additional items.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "AccessControlEntries": [
      {
         "AccessRights": {
            "AutoEnroll": "string",
            "Enroll": "string"
         },
         "CreatedAt": number,
         "GroupDisplayName": "string",
         "GroupSecurityIdentifier": "string",
         "TemplateArn": "string",
         "UpdatedAt": number
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

AccessControlEntries

An access control entry grants or denies permission to an Active Directory group to enroll certificates for a template.

Type: Array of AccessControlEntrySummary objects

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

Type: String

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTemplates

Lists the templates, if any, that are associated with a connector.

Request Syntax

```
GET /templates?ConnectorArn=ConnectorArn&MaxResults=MaxResults&NextToken=NextToken
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

MaxResults

Use this parameter when paginating results to specify the maximum number of items to return in the response on each page. If additional items exist beyond the number you specify, the `NextToken` element is sent in the response. Use this `NextToken` value in a subsequent request to retrieve additional items.

Valid Range: Minimum value of 1. Maximum value of 1000.

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Templates": [
      {
         "Arn": "string",
         "ConnectorArn": "string",
         "CreatedAt": number,
         "Definition": { ... },
         "Name": "string",
         "ObjectIdentifier": "string",
         "PolicySchema": number,
         "Revision": {
            "MajorRevision": number,
            "MinorRevision": number
         },
         "Status": "string",
         "UpdatedAt": number
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken

Use this parameter when paginating results in a subsequent request after you receive a response with truncated results. Set it to the value of the `NextToken` parameter from the response you just received.

Type: String

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

Pattern: `(?:[A-Za-z0-9_-]{4})*(?:[A-Za-z0-9_-]{2}==|[A-Za-z0-9_-]{3}=)?`

Templates

Custom configuration templates used when issuing a certificate.

Type: Array of TemplateSummary objects

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

TagResource

Adds one or more tags to your resource.

Request Syntax

```
POST /tags/ResourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": { 
      "string" : "string" 
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) that was returned when you created the resource.

Required: Yes

Request Body

The request accepts the following data in JSON format.

Tags

Metadata assigned to a directory registration consisting of a key-value pair.

Type: String to string map

Required: Yes

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UntagResource

Removes one or more tags from your resource.

Request Syntax

```
DELETE /tags/ResourceArn?tagKeys=TagKeys HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

ResourceArn

The Amazon Resource Name (ARN) that was returned when you created the resource.

Required: Yes

TagKeys

Specifies a list of tag keys that you want to remove from the specified resources.

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 204
```

Response Elements

If the action is successful, the service sends back an HTTP 204 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateTemplate

Update template configuration to define the information included in certificates.

Request Syntax

```
PATCH /templates/TemplateArn HTTP/1.1
Content-type: application/json

{
   "Definition": { ... },
   "ReenrollAllCertificateHolders": boolean
}
```

URI Request Parameters

The request uses the following URI parameters.

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

Definition

Template configuration to define the information included in certificates. Define certificate validity and renewal periods, certificate request handling and enrollment options, key usage extensions, application policies, and cryptography settings.

Type: TemplateDefinition object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

ReenrollAllCertificateHolders

This setting allows the major version of a template to be increased automatically. All members of Active Directory groups that are allowed to enroll with a template will receive a new certificate issued using that template.

Type: Boolean

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateTemplateGroupAccessControlEntry

Update a group access control entry you created using CreateTemplateGroupAccessControlEntry.

Request Syntax

```
PATCH /templates/TemplateArn/accessControlEntries/GroupSecurityIdentifier HTTP/1.1
Content-type: application/json

{
   "AccessRights": {
      "AutoEnroll": "string",
      "Enroll": "string"
   },
   "GroupDisplayName": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

GroupSecurityIdentifier

Security identifier (SID) of the group object from Active Directory. The SID starts with "S-".

Length Constraints: Minimum length of 7. Maximum length of 256.

Pattern: `S-[0-9]-([0-9]+-){1,14}[0-9]+`

Required: Yes

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

AccessRights

Allow or deny permissions for an Active Directory group to enroll or autoenroll certificates for a template.

Type: AccessRights object

Required: No

GroupDisplayName

Name of the Active Directory group. This name does not need to match the group name in Active Directory.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[\x20-\x7E]+`

Required: No

Response Syntax

```
HTTP/1.1 200
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

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

AccessDeniedException

You can receive this error if you attempt to create a resource share when you don't have the required permissions. This can be caused by insufficient permissions in policies attached to your

AWS Identity and Access Management (IAM) principal. It can also happen because of restrictions in place from an AWS Organizations service control policy (SCP) that affects your AWS account.

HTTP Status Code: 403

ConflictException

This request cannot be completed for one of the following reasons because the requested resource was being concurrently modified by another request.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 409

InternalServerException

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

HTTP Status Code: 500

ResourceNotFoundException

The operation tried to access a nonexistent resource. The resource might not be specified correctly, or its status might not be ACTIVE.

ResourceId

The identifier of the AWS resource.

ResourceType

The resource type, which can be one of `Connector`, `Template`, `TemplateGroupAccessControlEntry`, `ServicePrincipalName`, or `DirectoryRegistration`.

HTTP Status Code: 404

ThrottlingException

The limit on the number of requests per second was exceeded.

QuotaCode

The code associated with the quota.

ServiceCode

Identifies the originating service.

HTTP Status Code: 429

ValidationException

An input validation error occurred. For example, invalid characters in a template name, or if a pagination token is invalid.

Reason

The reason for the validation error. This won't be return for every validation exception.

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 V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The PcaConnectorAd 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:

- AccessControlEntry
- AccessControlEntrySummary
- AccessRights
- ApplicationPolicies
- ApplicationPolicy
- CertificateValidity
- Connector
- ConnectorSummary
- DirectoryRegistration
- DirectoryRegistrationSummary
- EnrollmentFlagsV2
- EnrollmentFlagsV3
- EnrollmentFlagsV4
- ExtensionsV2
- ExtensionsV3
- ExtensionsV4
- GeneralFlagsV2
- GeneralFlagsV3
- GeneralFlagsV4
- KeyUsage

- KeyUsageFlags
- KeyUsageProperty
- KeyUsagePropertyFlags
- PrivateKeyAttributesV2
- PrivateKeyAttributesV3
- PrivateKeyAttributesV4
- PrivateKeyFlagsV2
- PrivateKeyFlagsV3
- PrivateKeyFlagsV4
- ServicePrincipalName
- ServicePrincipalNameSummary
- SubjectNameFlagsV2
- SubjectNameFlagsV3
- SubjectNameFlagsV4
- Template
- TemplateDefinition
- TemplateRevision
- TemplateSummary
- TemplateV2
- TemplateV3
- TemplateV4
- ValidityPeriod
- VpcInformation

AccessControlEntry

An access control entry allows or denies Active Directory groups based on their security identifiers (SIDs) from enrolling and/or autoenrolling with the template.

Contents

AccessRights

Permissions to allow or deny an Active Directory group to enroll or autoenroll certificates issued against a template.

Type: AccessRights object

Required: No

CreatedAt

The date and time that the Access Control Entry was created.

Type: Timestamp

Required: No

GroupDisplayName

Name of the Active Directory group. This name does not need to match the group name in Active Directory.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[\x20-\x7E]+`

Required: No

GroupSecurityIdentifier

Security identifier (SID) of the group object from Active Directory. The SID starts with "S-".

Type: String

Length Constraints: Minimum length of 7. Maximum length of 256.

Pattern: `S-[0-9]-([0-9]+-){1,14}[0-9]+`

Required: No

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

UpdatedAt

The date and time that the Access Control Entry was updated.

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 Java V2
- AWS SDK for Ruby V3

AccessControlEntrySummary

Summary of group access control entries that allow or deny Active Directory groups based on their security identifiers (SIDs) from enrolling and/or autofenrolling with the template.

Contents

AccessRights

Allow or deny an Active Directory group from enrolling and autoenrolling certificates issued against a template.

Type: AccessRights object

Required: No

CreatedAt

The date and time that the Access Control Entry was created.

Type: Timestamp

Required: No

GroupDisplayName

Name of the Active Directory group. This name does not need to match the group name in Active Directory.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[\x20-\x7E]+`

Required: No

GroupSecurityIdentifier

Security identifier (SID) of the group object from Active Directory. The SID starts with "S-".

Type: String

Length Constraints: Minimum length of 7. Maximum length of 256.

Pattern: `S-[0-9]-([0-9]+-){1,14}[0-9]+`

Required: No

TemplateArn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

UpdatedAt

The date and time that the Access Control Entry was updated.

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 Java V2
- AWS SDK for Ruby V3

AccessRights

Allow or deny permissions for an Active Directory group to enroll or autoenroll certificates for a template.

Contents

AutoEnroll

Allow or deny an Active Directory group from autoenrolling certificates issued against a template. The Active Directory group must be allowed to enroll to allow autoenrollment

Type: String

Valid Values: `ALLOW | DENY`

Required: No

Enroll

Allow or deny an Active Directory group from enrolling certificates issued against a template.

Type: String

Valid Values: `ALLOW | DENY`

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 Java V2
- AWS SDK for Ruby V3

ApplicationPolicies

Application policies describe what the certificate can be used for.

Contents

Policies

Application policies describe what the certificate can be used for.

Type: Array of ApplicationPolicy objects

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Required: Yes

Critical

Marks the application policy extension as critical.

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 Java V2
- AWS SDK for Ruby V3

ApplicationPolicy

Application policies describe what the certificate can be used for.

Contents

Important

This data type is a UNION, so only one of the following members can be specified when used or returned.

PolicyObjectIdentifier

The object identifier (OID) of an application policy.

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))(\.([0-9]+)){0,126}`

Required: No

PolicyType

The type of application policy

Type: String

Valid Values: `ALL_APPLICATION_POLICIES | ANY_PURPOSE | ATTESTATION_IDENTITY_KEY_CERTIFICATE | CERTIFICATE_REQUEST_AGENT | CLIENT_AUTHENTICATION | CODE_SIGNING | CTL_USAGE | DIGITAL_RIGHTS | DIRECTORY_SERVICE_EMAIL_REPLICATION | DISALLOWED_LIST | DNS_SERVER_TRUST | DOCUMENT_ENCRYPTION | DOCUMENT_SIGNING | DYNAMIC_CODE_GENERATOR | EARLY_LAUNCH_ANTIMALWARE_DRIVER | EMBEDDED_WINDOWS_SYSTEM_COMPONENT_VERIFICATION | ENCLAVE | ENCRYPTING_FILE_SYSTEM | ENDORSEMENT_KEY_CERTIFICATE | FILE_RECOVERY | HAL_EXTENSION | IP_SECURITY_END_SYSTEM | IP_SECURITY_IKE_INTERMEDIATE | IP_SECURITY_TUNNEL_TERMINATION | IP_SECURITY_USER |`

`ISOLATED_USER_MODE | KDC_AUTHENTICATION | KERNEL_MODE_CODE_SIGNING | KEY_PACK_LICENSES | KEY_RECOVERY | KEY_RECOVERY_AGENT | LICENSE_SERVER_VERIFICATION | LIFETIME_SIGNING | MICROSOFT_PUBLISHER | MICROSOFT_TIME_STAMPING | MICROSOFT_TRUST_LIST_SIGNING | OCSP_SIGNING | OEM_WINDOWS_SYSTEM_COMPONENT_VERIFICATION | PLATFORM_CERTIFICATE | PREVIEW_BUILD_SIGNING | PRIVATE_KEY_ARCHIVAL | PROTECTED_PROCESS_LIGHT_VERIFICATION | PROTECTED_PROCESS_VERIFICATION | QUALIFIED_SUBORDINATION | REVOKED_LIST_SIGNER | ROOT_PROGRAM_AUTO_UPDATE_CA_REVOCATION | ROOT_PROGRAM_AUTO_UPDATE_END_REVOCATION | ROOT_PROGRAM_NO_OSCP_FAILOVER_TO_CRL | ROOT_LIST_SIGNER | SECURE_EMAIL | SERVER_AUTHENTICATION | SMART_CARD_LOGIN | SPC_ENCRYPTED_DIGEST_RETRY_COUNT | SPC_RELAXED_PE_MARKER_CHECK | TIME_STAMPING | WINDOWS_HARDWARE_DRIVER_ATTESTED_VERIFICATION | WINDOWS_HARDWARE_DRIVER_EXTENDED_VERIFICATION | WINDOWS_HARDWARE_DRIVER_VERIFICATION | WINDOWS_HELLO_RECOVERY_KEY_ENCRYPTION | WINDOWS_KITS_COMPONENT | WINDOWS_RT_VERIFICATION | WINDOWS_SOFTWARE_EXTENSION_VERIFICATION | WINDOWS_STORE | WINDOWS_SYSTEM_COMPONENT_VERIFICATION | WINDOWS_TCB_COMPONENT | WINDOWS_THIRD_PARTY_APPLICATION_COMPONENT | WINDOWS_UPDATE`

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 Java V2
- AWS SDK for Ruby V3

CertificateValidity

Information describing the end of the validity period of the certificate. This parameter sets the “Not After” date for the certificate. Certificate validity is the period of time during which a certificate is valid. Validity can be expressed as an explicit date and time when the certificate expires, or as a span of time after issuance, stated in days, months, or years. For more information, see Validity in RFC 5280. This value is unaffected when ValidityNotBefore is also specified. For example, if Validity is set to 20 days in the future, the certificate will expire 20 days from issuance time regardless of the ValidityNotBefore value.

Contents

RenewalPeriod

Renewal period is the period of time before certificate expiration when a new certificate will be requested.

Type: ValidityPeriod object

Required: Yes

ValidityPeriod

Information describing the end of the validity period of the certificate. This parameter sets the “Not After” date for the certificate. Certificate validity is the period of time during which a certificate is valid. Validity can be expressed as an explicit date and time when the certificate expires, or as a span of time after issuance, stated in days, months, or years. For more information, see Validity in RFC 5280. This value is unaffected when ValidityNotBefore is also specified. For example, if Validity is set to 20 days in the future, the certificate will expire 20 days from issuance time regardless of the ValidityNotBefore value.

Type: ValidityPeriod 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 Java V2
- AWS SDK for Ruby V3

Connector

AWS Private CA Connector for Active Directory is a service that links your Active Directory with AWS Private CA. The connector brokers the exchange of certificates from AWS Private CA to domain-joined users and machines managed with Active Directory.

Contents

Arn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the certificate authority being used.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:acm-pca:[\w-]+:[0-9]+:certificate-authority\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CertificateEnrollmentPolicyServerEndpoint

Certificate enrollment endpoint for Active Directory domain-joined objects reach out to when requesting certificates.

Type: String

Required: No

CreatedAt

The date and time that the connector was created.

Type: Timestamp

Required: No

DirectoryId

The identifier of the Active Directory.

Type: String

Pattern: `d-[0-9a-f]{10}`

Required: No

Status

Status of the connector. Status can be creating, active, deleting, or failed.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED`

Required: No

StatusReason

Additional information about the connector status if the status is failed.

Type: String

Valid Values: `CA_CERTIFICATE_REGISTRATION_FAILED | DIRECTORY_ACCESS_DENIED | INTERNAL_FAILURE | INSUFFICIENT_FREE_ADDRESSES | INVALID_SUBNET_IP_PROTOCOL | PRIVATECA_ACCESS_DENIED | PRIVATECA_RESOURCE_NOT_FOUND | SECURITY_GROUP_NOT_IN_VPC | VPC_ACCESS_DENIED | VPC_ENDPOINT_LIMIT_EXCEEDED | VPC_RESOURCE_NOT_FOUND`

Required: No

UpdatedAt

The date and time that the connector was updated.

Type: Timestamp

Required: No

VpcInformation

Information of the VPC and security group(s) used with the connector.

Type: VpcInformation 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 Java V2
- AWS SDK for Ruby V3

ConnectorSummary

Summary description of the AWS Private CA AD connectors belonging to an AWS account.

Contents

Arn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CertificateAuthorityArn

The Amazon Resource Name (ARN) of the certificate authority being used.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:acm-pca:[\w-]+:[0-9]+:certificate-authority\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CertificateEnrollmentPolicyServerEndpoint

Certificate enrollment endpoint for Active Directory domain-joined objects to request certificates.

Type: String

Required: No

CreatedAt

The date and time that the connector was created.

Type: Timestamp

Required: No

DirectoryId

The identifier of the Active Directory.

Type: String

Pattern: `d-[0-9a-f]{10}`

Required: No

Status

Status of the connector. Status can be creating, active, deleting, or failed.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED`

Required: No

StatusReason

Additional information about the connector status if the status is failed.

Type: String

Valid Values: `CA_CERTIFICATE_REGISTRATION_FAILED | DIRECTORY_ACCESS_DENIED | INTERNAL_FAILURE | INSUFFICIENT_FREE_ADDRESSES | INVALID_SUBNET_IP_PROTOCOL | PRIVATECA_ACCESS_DENIED | PRIVATECA_RESOURCE_NOT_FOUND | SECURITY_GROUP_NOT_IN_VPC | VPC_ACCESS_DENIED | VPC_ENDPOINT_LIMIT_EXCEEDED | VPC_RESOURCE_NOT_FOUND`

Required: No

UpdatedAt

The date and time that the connector was updated.

Type: Timestamp

Required: No

VpcInformation

Information of the VPC and security group(s) used with the connector.

Type: VpcInformation 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 Java V2
- AWS SDK for Ruby V3

DirectoryRegistration

The directory registration represents the authorization of the connector service with a directory.

Contents

Arn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: No

CreatedAt

The date and time that the directory registration was created.

Type: Timestamp

Required: No

DirectoryId

The identifier of the Active Directory.

Type: String

Pattern: `d-[0-9a-f]{10}`

Required: No

Status

Status of the directory registration.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED`

Required: No

StatusReason

Additional information about the directory registration status if the status is failed.

Type: String

Valid Values: `DIRECTORY_ACCESS_DENIED | DIRECTORY_RESOURCE_NOT_FOUND | DIRECTORY_NOT_ACTIVE | DIRECTORY_NOT_REACHABLE | DIRECTORY_TYPE_NOT_SUPPORTED | INTERNAL_FAILURE`

Required: No

UpdatedAt

The date and time that the directory registration was updated.

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 Java V2
- AWS SDK for Ruby V3

DirectoryRegistrationSummary

The directory registration represents the authorization of the connector service with the Active Directory.

Contents

Arn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: No

CreatedAt

The date and time that the directory registration was created.

Type: Timestamp

Required: No

DirectoryId

The identifier of the Active Directory.

Type: String

Pattern: `d-[0-9a-f]{10}`

Required: No

Status

Status of the directory registration.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED`

Required: No

StatusReason

Additional information about the directory registration status if the status is failed.

Type: String

Valid Values: `DIRECTORY_ACCESS_DENIED | DIRECTORY_RESOURCE_NOT_FOUND | DIRECTORY_NOT_ACTIVE | DIRECTORY_NOT_REACHABLE | DIRECTORY_TYPE_NOT_SUPPORTED | INTERNAL_FAILURE`

Required: No

UpdatedAt

The date and time that the directory registration was updated.

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 Java V2
- AWS SDK for Ruby V3

EnrollmentFlagsV2

Template configurations for v2 template schema.

Contents

EnableKeyReuseOnNtTokenKeysetStorageFull

Allow renewal using the same key.

Type: Boolean

Required: No

IncludeSymmetricAlgorithms

Include symmetric algorithms allowed by the subject.

Type: Boolean

Required: No

NoSecurityExtension

This flag instructs the CA to not include the security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2), as specified in [MS-WCCE] sections 2.2.2.7.7.4 and 3.2.2.6.2.1.4.5.9, in the issued certificate. This addresses a Windows Kerberos elevation-of-privilege vulnerability.

Type: Boolean

Required: No

RemoveInvalidCertificateFromPersonalStore

Delete expired or revoked certificates instead of archiving them.

Type: Boolean

Required: No

UserInteractionRequired

Require user interaction when the subject is enrolled and the private key associated with the certificate is used.

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 Java V2
- AWS SDK for Ruby V3

EnrollmentFlagsV3

Template configurations for v3 template schema.

Contents

EnableKeyReuseOnNtTokenKeysetStorageFull

Allow renewal using the same key.

Type: Boolean

Required: No

IncludeSymmetricAlgorithms

Include symmetric algorithms allowed by the subject.

Type: Boolean

Required: No

NoSecurityExtension

This flag instructs the CA to not include the security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2), as specified in [MS-WCCE] sections 2.2.2.7.7.4 and 3.2.2.6.2.1.4.5.9, in the issued certificate. This addresses a Windows Kerberos elevation-of-privilege vulnerability.

Type: Boolean

Required: No

RemoveInvalidCertificateFromPersonalStore

Delete expired or revoked certificates instead of archiving them.

Type: Boolean

Required: No

UserInteractionRequired

Require user interaction when the subject is enrolled and the private key associated with the certificate is used.

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 Java V2
- AWS SDK for Ruby V3

EnrollmentFlagsV4

Template configurations for v4 template schema.

Contents

EnableKeyReuseOnNtTokenKeysetStorageFull

Allow renewal using the same key.

Type: Boolean

Required: No

IncludeSymmetricAlgorithms

Include symmetric algorithms allowed by the subject.

Type: Boolean

Required: No

NoSecurityExtension

This flag instructs the CA to not include the security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2), as specified in [MS-WCCE] sections 2.2.2.7.7.4 and 3.2.2.6.2.1.4.5.9, in the issued certificate. This addresses a Windows Kerberos elevation-of-privilege vulnerability.

Type: Boolean

Required: No

RemoveInvalidCertificateFromPersonalStore

Delete expired or revoked certificates instead of archiving them.

Type: Boolean

Required: No

UserInteractionRequired

Require user interaction when the subject is enrolled and the private key associated with the certificate is used.

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 Java V2
- AWS SDK for Ruby V3

ExtensionsV2

Certificate extensions for v2 template schema

Contents

KeyUsage

The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate.

Type: KeyUsage object

Required: Yes

ApplicationPolicies

Application policies specify what the certificate is used for and its purpose.

Type: ApplicationPolicies 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 Java V2
- AWS SDK for Ruby V3

ExtensionsV3

Certificate extensions for v3 template schema

Contents

KeyUsage

The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate.

Type: KeyUsage object

Required: Yes

ApplicationPolicies

Application policies specify what the certificate is used for and its purpose.

Type: ApplicationPolicies 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 Java V2
- AWS SDK for Ruby V3

ExtensionsV4

Certificate extensions for v4 template schema

Contents

KeyUsage

The key usage extension defines the purpose (e.g., encipherment, signature) of the key contained in the certificate.

Type: KeyUsage object

Required: Yes

ApplicationPolicies

Application policies specify what the certificate is used for and its purpose.

Type: ApplicationPolicies 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 Java V2
- AWS SDK for Ruby V3

GeneralFlagsV2

General flags for v2 template schema that defines if the template is for a machine or a user and if the template can be issued using autoenrollment.

Contents

AutoEnrollment

Allows certificate issuance using autoenrollment. Set to TRUE to allow autoenrollment.

Type: Boolean

Required: No

MachineType

Defines if the template is for machines or users. Set to TRUE if the template is for machines. Set to FALSE if the template is for users.

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 Java V2
- AWS SDK for Ruby V3

GeneralFlagsV3

General flags for v3 template schema that defines if the template is for a machine or a user and if the template can be issued using autoenrollment.

Contents

AutoEnrollment

Allows certificate issuance using autoenrollment. Set to TRUE to allow autoenrollment.

Type: Boolean

Required: No

MachineType

Defines if the template is for machines or users. Set to TRUE if the template is for machines. Set to FALSE if the template is for users

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 Java V2
- AWS SDK for Ruby V3

GeneralFlagsV4

General flags for v4 template schema that defines if the template is for a machine or a user and if the template can be issued using autoenrollment.

Contents

AutoEnrollment

Allows certificate issuance using autoenrollment. Set to TRUE to allow autoenrollment.

Type: Boolean

Required: No

MachineType

Defines if the template is for machines or users. Set to TRUE if the template is for machines. Set to FALSE if the template is for users

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 Java V2
- AWS SDK for Ruby V3

KeyUsage

The key usage extension defines the purpose (e.g., encipherment, signature) of the key contained in the certificate.

Contents

UsageFlags

The key usage flags represent the purpose (e.g., encipherment, signature) of the key contained in the certificate.

Type: KeyUsageFlags object

Required: Yes

Critical

Sets the key usage extension to critical.

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 Java V2
- AWS SDK for Ruby V3

KeyUsageFlags

The key usage flags represent the purpose (e.g., encipherment, signature) of the key contained in the certificate.

Contents

DataEncipherment

DataEncipherment is asserted when the subject public key is used for directly enciphering raw user data without the use of an intermediate symmetric cipher.

Type: Boolean

Required: No

DigitalSignature

The digitalSignature is asserted when the subject public key is used for verifying digital signatures.

Type: Boolean

Required: No

KeyAgreement

KeyAgreement is asserted when the subject public key is used for key agreement.

Type: Boolean

Required: No

KeyEncipherment

KeyEncipherment is asserted when the subject public key is used for enciphering private or secret keys, i.e., for key transport.

Type: Boolean

Required: No

NonRepudiation

NonRepudiation is asserted when the subject public key is used to verify digital signatures.

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 Java V2
- AWS SDK for Ruby V3

KeyUsageProperty

The key usage property defines the purpose of the private key contained in the certificate. You can specify specific purposes using property flags or all by using property type ALL.

Contents

> ⚠ **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

PropertyFlags

You can specify key usage for encryption, key agreement, and signature. You can use property flags or property type but not both.

Type: KeyUsagePropertyFlags object

Required: No

PropertyType

You can specify all key usages using property type ALL. You can use property type or property flags but not both.

Type: String

Valid Values: ALL

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 Java V2

- AWS SDK for Ruby V3

KeyUsagePropertyFlags

Specifies key usage.

Contents

Decrypt

Allows key for encryption and decryption.

Type: Boolean

Required: No

KeyAgreement

Allows key exchange without encryption.

Type: Boolean

Required: No

Sign

Allow key use for digital signature.

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 Java V2
- AWS SDK for Ruby V3

PrivateKeyAttributesV2

Defines the attributes of the private key.

Contents

KeySpec

Defines the purpose of the private key. Set it to "KEY_EXCHANGE" or "SIGNATURE" value.

Type: String

Valid Values: `KEY_EXCHANGE | SIGNATURE`

Required: Yes

MinimalKeyLength

Set the minimum key length of the private key.

Type: Integer

Valid Range: Minimum value of 1.

Required: Yes

CryptoProviders

Defines the cryptographic providers used to generate the private key.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 100.

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 Java V2
- AWS SDK for Ruby V3

PrivateKeyAttributesV3

Defines the attributes of the private key.

Contents

Algorithm

Defines the algorithm used to generate the private key.

Type: String

Valid Values: `RSA | ECDH_P256 | ECDH_P384 | ECDH_P521`

Required: Yes

KeySpec

Defines the purpose of the private key. Set it to "KEY_EXCHANGE" or "SIGNATURE" value.

Type: String

Valid Values: `KEY_EXCHANGE | SIGNATURE`

Required: Yes

KeyUsageProperty

The key usage property defines the purpose of the private key contained in the certificate. You can specify specific purposes using property flags or all by using property type ALL.

Type: KeyUsageProperty object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: Yes

MinimalKeyLength

Set the minimum key length of the private key.

Type: Integer

Valid Range: Minimum value of 1.

Required: Yes

CryptoProviders

Defines the cryptographic providers used to generate the private key.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 100.

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 Java V2
- AWS SDK for Ruby V3

PrivateKeyAttributesV4

Defines the attributes of the private key.

Contents

KeySpec

Defines the purpose of the private key. Set it to "KEY_EXCHANGE" or "SIGNATURE" value.

Type: String

Valid Values: `KEY_EXCHANGE | SIGNATURE`

Required: Yes

MinimalKeyLength

Set the minimum key length of the private key.

Type: Integer

Valid Range: Minimum value of 1.

Required: Yes

Algorithm

Defines the algorithm used to generate the private key.

Type: String

Valid Values: `RSA | ECDH_P256 | ECDH_P384 | ECDH_P521`

Required: No

CryptoProviders

Defines the cryptographic providers used to generate the private key.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Length Constraints: Minimum length of 1. Maximum length of 100.

Required: No

KeyUsageProperty

The key usage property defines the purpose of the private key contained in the certificate. You can specify specific purposes using property flags or all by using property type ALL.

Type: KeyUsageProperty object

Note: This object is a Union. Only one member of this object can be specified or returned.

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 Java V2
- AWS SDK for Ruby V3

PrivateKeyFlagsV2

Private key flags for v2 templates specify the client compatibility, if the private key can be exported, and if user input is required when using a private key.

Contents

ClientVersion

Defines the minimum client compatibility.

Type: String

Valid Values: `WINDOWS_SERVER_2003 | WINDOWS_SERVER_2008 | WINDOWS_SERVER_2008_R2 | WINDOWS_SERVER_2012 | WINDOWS_SERVER_2012_R2 | WINDOWS_SERVER_2016`

Required: Yes

ExportableKey

Allows the private key to be exported.

Type: Boolean

Required: No

StrongKeyProtectionRequired

Require user input when using the private key for enrollment.

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 Java V2

- AWS SDK for Ruby V3

PrivateKeyFlagsV3

Private key flags for v3 templates specify the client compatibility, if the private key can be exported, if user input is required when using a private key, and if an alternate signature algorithm should be used.

Contents

ClientVersion

Defines the minimum client compatibility.

Type: String

Valid Values: `WINDOWS_SERVER_2008 | WINDOWS_SERVER_2008_R2 | WINDOWS_SERVER_2012 | WINDOWS_SERVER_2012_R2 | WINDOWS_SERVER_2016`

Required: Yes

ExportableKey

Allows the private key to be exported.

Type: Boolean

Required: No

RequireAlternateSignatureAlgorithm

Reguires the PKCS #1 v2.1 signature format for certificates. You should verify that your CA, objects, and applications can accept this signature format.

Type: Boolean

Required: No

StrongKeyProtectionRequired

Requirer user input when using the private key for enrollment.

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 Java V2
- AWS SDK for Ruby V3

PrivateKeyFlagsV4

Private key flags for v4 templates specify the client compatibility, if the private key can be exported, if user input is required when using a private key, if an alternate signature algorithm should be used, and if certificates are renewed using the same private key.

Contents

ClientVersion

Defines the minimum client compatibility.

Type: String

Valid Values: `WINDOWS_SERVER_2012 | WINDOWS_SERVER_2012_R2 | WINDOWS_SERVER_2016`

Required: Yes

ExportableKey

Allows the private key to be exported.

Type: Boolean

Required: No

RequireAlternateSignatureAlgorithm

Requires the PKCS #1 v2.1 signature format for certificates. You should verify that your CA, objects, and applications can accept this signature format.

Type: Boolean

Required: No

RequireSameKeyRenewal

Renew certificate using the same private key.

Type: Boolean

Required: No

StrongKeyProtectionRequired

Require user input when using the private key for enrollment.

Type: Boolean

Required: No

UseLegacyProvider

Specifies the cryptographic service provider category used to generate private keys. Set to TRUE to use Legacy Cryptographic Service Providers and FALSE to use Key Storage Providers.

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 Java V2
- AWS SDK for Ruby V3

ServicePrincipalName

The service principal name that the connector uses to authenticate with Active Directory.

Contents

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.html.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the service principal name was created.

Type: Timestamp

Required: No

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: No

Status

The status of a service principal name.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED`

Required: No

StatusReason

Additional information for the status of a service principal name if the status is failed.

Type: String

Valid Values: `DIRECTORY_ACCESS_DENIED | DIRECTORY_NOT_ACTIVE | DIRECTORY_NOT_REACHABLE | DIRECTORY_RESOURCE_NOT_FOUND | SPN_EXISTS_ON_DIFFERENT_AD_OBJECT | SPN_LIMIT_EXCEEDED | INTERNAL_FAILURE`

Required: No

UpdatedAt

The date and time that the service principal name was updated.

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 Java V2
- AWS SDK for Ruby V3

ServicePrincipalNameSummary

The service principal name that the connector uses to authenticate with Active Directory.

Contents

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the service principal name was created.

Type: Timestamp

Required: No

DirectoryRegistrationArn

The Amazon Resource Name (ARN) that was returned when you called CreateDirectoryRegistration.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:directory-registration\/d-[0-9a-f]{10}`

Required: No

Status

The status of a service principal name.

Type: String

Valid Values: `CREATING | ACTIVE | DELETING | FAILED`

Required: No

StatusReason

Additional information for the status of a service principal name if the status is failed.

Type: String

Valid Values: `DIRECTORY_ACCESS_DENIED | DIRECTORY_NOT_ACTIVE | DIRECTORY_NOT_REACHABLE | DIRECTORY_RESOURCE_NOT_FOUND | SPN_EXISTS_ON_DIFFERENT_AD_OBJECT | SPN_LIMIT_EXCEEDED | INTERNAL_FAILURE`

Required: No

UpdatedAt

Time when the service principal name was updated.

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 Java V2
- AWS SDK for Ruby V3

SubjectNameFlagsV2

Information to include in the subject name and alternate subject name of the certificate. The subject name can be common name, directory path, DNS as common name, or left blank. You can optionally include email to the subject name for user templates. If you leave the subject name blank then you must set a subject alternate name. The subject alternate name (SAN) can include globally unique identifier (GUID), DNS, domain DNS, email, service principal name (SPN), and user principal name (UPN). You can leave the SAN blank. If you leave the SAN blank, then you must set a subject name.

Contents

RequireCommonName

Include the common name in the subject name.

Type: Boolean

Required: No

RequireDirectoryPath

Include the directory path in the subject name.

Type: Boolean

Required: No

RequireDnsAsCn

Include the DNS as common name in the subject name.

Type: Boolean

Required: No

RequireEmail

Include the subject's email in the subject name.

Type: Boolean

Required: No

SanRequireDirectoryGuid

Include the globally unique identifier (GUID) in the subject alternate name.

Type: Boolean

Required: No

SanRequireDns

Include the DNS in the subject alternate name.

Type: Boolean

Required: No

SanRequireDomainDns

Include the domain DNS in the subject alternate name.

Type: Boolean

Required: No

SanRequireEmail

Include the subject's email in the subject alternate name.

Type: Boolean

Required: No

SanRequireSpn

Include the service principal name (SPN) in the subject alternate name.

Type: Boolean

Required: No

SanRequireUpn

Include the user principal name (UPN) in the subject alternate name.

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 Java V2
- AWS SDK for Ruby V3

SubjectNameFlagsV3

Information to include in the subject name and alternate subject name of the certificate. The subject name can be common name, directory path, DNS as common name, or left blank. You can optionally include email to the subject name for user templates. If you leave the subject name blank then you must set a subject alternate name. The subject alternate name (SAN) can include globally unique identifier (GUID), DNS, domain DNS, email, service principal name (SPN), and user principal name (UPN). You can leave the SAN blank. If you leave the SAN blank, then you must set a subject name.

Contents

RequireCommonName

Include the common name in the subject name.

Type: Boolean

Required: No

RequireDirectoryPath

Include the directory path in the subject name.

Type: Boolean

Required: No

RequireDnsAsCn

Include the DNS as common name in the subject name.

Type: Boolean

Required: No

RequireEmail

Include the subject's email in the subject name.

Type: Boolean

Required: No

SanRequireDirectoryGuid

Include the globally unique identifier (GUID) in the subject alternate name.

Type: Boolean

Required: No

SanRequireDns

Include the DNS in the subject alternate name.

Type: Boolean

Required: No

SanRequireDomainDns

Include the domain DNS in the subject alternate name.

Type: Boolean

Required: No

SanRequireEmail

Include the subject's email in the subject alternate name.

Type: Boolean

Required: No

SanRequireSpn

Include the service principal name (SPN) in the subject alternate name.

Type: Boolean

Required: No

SanRequireUpn

Include the user principal name (UPN) in the subject alternate name.

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 Java V2
- AWS SDK for Ruby V3

SubjectNameFlagsV4

Information to include in the subject name and alternate subject name of the certificate. The subject name can be common name, directory path, DNS as common name, or left blank. You can optionally include email to the subject name for user templates. If you leave the subject name blank then you must set a subject alternate name. The subject alternate name (SAN) can include globally unique identifier (GUID), DNS, domain DNS, email, service principal name (SPN), and user principal name (UPN). You can leave the SAN blank. If you leave the SAN blank, then you must set a subject name.

Contents

RequireCommonName

Include the common name in the subject name.

Type: Boolean

Required: No

RequireDirectoryPath

Include the directory path in the subject name.

Type: Boolean

Required: No

RequireDnsAsCn

Include the DNS as common name in the subject name.

Type: Boolean

Required: No

RequireEmail

Include the subject's email in the subject name.

Type: Boolean

Required: No

SanRequireDirectoryGuid

Include the globally unique identifier (GUID) in the subject alternate name.

Type: Boolean

Required: No

SanRequireDns

Include the DNS in the subject alternate name.

Type: Boolean

Required: No

SanRequireDomainDns

Include the domain DNS in the subject alternate name.

Type: Boolean

Required: No

SanRequireEmail

Include the subject's email in the subject alternate name.

Type: Boolean

Required: No

SanRequireSpn

Include the service principal name (SPN) in the subject alternate name.

Type: Boolean

Required: No

SanRequireUpn

Include the user principal name (UPN) in the subject alternate name.

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 Java V2
- AWS SDK for Ruby V3

Template

An Active Directory compatible certificate template. Connectors issue certificates against these templates based on the requestor's Active Directory group membership.

Contents

Arn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the template was created.

Type: Timestamp

Required: No

Definition

Template configuration to define the information included in certificates. Define certificate validity and renewal periods, certificate request handling and enrollment options, key usage extensions, application policies, and cryptography settings.

Type: TemplateDefinition object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

Name

Name of the templates. Template names must be unique.

Type: String

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

Pattern: `(?!^\s+$)((?![\x5c'\x2b,;<=>#\x22])([\x20-\x7E]))+`

Required: No

ObjectIdentifier

Object identifier of a template.

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))(\.([0-9]+)){0,126}`

Required: No

PolicySchema

The template schema version. Template schema versions can be v2, v3, or v4. The template configuration options change based on the template schema version.

Type: Integer

Required: No

Revision

The version of the template. Template updates will increment the minor revision. Re-enrolling all certificate holders will increment the major revision.

Type: TemplateRevision object

Required: No

Status

Status of the template. Status can be creating, active, deleting, or failed.

Type: String

Valid Values: `ACTIVE | DELETING`

Required: No

UpdatedAt

The date and time that the template was updated.

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 Java V2
- AWS SDK for Ruby V3

TemplateDefinition

Template configuration to define the information included in certificates. Define certificate validity and renewal periods, certificate request handling and enrollment options, key usage extensions, application policies, and cryptography settings.

Contents

> ⚠ **Important**
>
> This data type is a UNION, so only one of the following members can be specified when used or returned.

TemplateV2

Template configuration to define the information included in certificates. Define certificate validity and renewal periods, certificate request handling and enrollment options, key usage extensions, application policies, and cryptography settings.

Type: TemplateV2 object

Required: No

TemplateV3

Template configuration to define the information included in certificates. Define certificate validity and renewal periods, certificate request handling and enrollment options, key usage extensions, application policies, and cryptography settings.

Type: TemplateV3 object

Required: No

TemplateV4

Template configuration to define the information included in certificates. Define certificate validity and renewal periods, certificate request handling and enrollment options, key usage extensions, application policies, and cryptography settings.

Type: TemplateV4 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 Java V2
- AWS SDK for Ruby V3

TemplateRevision

The revision version of the template. Template updates will increment the minor revision. Re-enrolling all certificate holders will increment the major revision.

Contents

MajorRevision

The revision version of the template. Re-enrolling all certificate holders will increment the major revision.

Type: Integer

Required: Yes

MinorRevision

The revision version of the template. Re-enrolling all certificate holders will increment the major revision.

Type: Integer

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 Java V2
- AWS SDK for Ruby V3

TemplateSummary

An Active Directory compatible certificate template. Connectors issue certificates against these templates based on the requestor's Active Directory group membership.

Contents

Arn

The Amazon Resource Name (ARN) that was returned when you called CreateTemplate.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}\/template\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

ConnectorArn

The Amazon Resource Name (ARN) that was returned when you called CreateConnector.

Type: String

Length Constraints: Minimum length of 5. Maximum length of 200.

Pattern: `arn:[\w-]+:pca-connector-ad:[\w-]+:[0-9]+:connector\/[0-9a-f]{8}(-[0-9a-f]{4}){3}-[0-9a-f]{12}`

Required: No

CreatedAt

The date and time that the template was created.

Type: Timestamp

Required: No

Definition

Template configuration to define the information included in certificates. Define certificate validity and renewal periods, certificate request handling and enrollment options, key usage extensions, application policies, and cryptography settings.

Type: TemplateDefinition object

Note: This object is a Union. Only one member of this object can be specified or returned.

Required: No

Name

Name of the template. The template name must be unique.

Type: String

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

Pattern: `(?!^\s+$)((?![\x5c'\x2b,;<=>#\x22])([\x20-\x7E]))+`

Required: No

ObjectIdentifier

Object identifier of a template.

Type: String

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

Pattern: `([0-2])\.([0-9]|([0-3][0-9]))(\.([0-9]+)){0,126}`

Required: No

PolicySchema

The template schema version. Template schema versions can be v2, v3, or v4. The template configuration options change based on the template schema version.

Type: Integer

Required: No

Revision

The revision version of the template. Template updates will increment the minor revision. Re-enrolling all certificate holders will increment the major revision.

Type: TemplateRevision object

Required: No

Status

Status of the template. Status can be creating, active, deleting, or failed.

Type: String

Valid Values: `ACTIVE | DELETING`

Required: No

UpdatedAt

The date and time that the template was updated.

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 Java V2
- AWS SDK for Ruby V3

TemplateV2

v2 template schema that uses Legacy Cryptographic Providers.

Contents

CertificateValidity

Certificate validity describes the validity and renewal periods of a certificate.

Type: CertificateValidity object

Required: Yes

EnrollmentFlags

Enrollment flags describe the enrollment settings for certificates such as using the existing private key and deleting expired or revoked certificates.

Type: EnrollmentFlagsV2 object

Required: Yes

Extensions

Extensions describe the key usage extensions and application policies for a template.

Type: ExtensionsV2 object

Required: Yes

GeneralFlags

General flags describe whether the template is used for computers or users and if the template can be used with autoenrollment.

Type: GeneralFlagsV2 object

Required: Yes

PrivateKeyAttributes

Private key attributes allow you to specify the minimal key length, key spec, and cryptographic providers for the private key of a certificate for v2 templates. V2 templates allow you to use Legacy Cryptographic Service Providers.

Type: PrivateKeyAttributesV2 object

Required: Yes

PrivateKeyFlags

Private key flags for v2 templates specify the client compatibility, if the private key can be exported, and if user input is required when using a private key.

Type: PrivateKeyFlagsV2 object

Required: Yes

SubjectNameFlags

Subject name flags describe the subject name and subject alternate name that is included in a certificate.

Type: SubjectNameFlagsV2 object

Required: Yes

SupersededTemplates

List of templates in Active Directory that are superseded by this template.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

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

Pattern: `(?!^\s+$)((?![\x5c'\x2b,;<=>#\x22])([\x20-\x7E]))+`

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 Java V2

- AWS SDK for Ruby V3

TemplateV3

v3 template schema that uses Key Storage Providers.

Contents

CertificateValidity

Certificate validity describes the validity and renewal periods of a certificate.

Type: CertificateValidity object

Required: Yes

EnrollmentFlags

Enrollment flags describe the enrollment settings for certificates such as using the existing private key and deleting expired or revoked certificates.

Type: EnrollmentFlagsV3 object

Required: Yes

Extensions

Extensions describe the key usage extensions and application policies for a template.

Type: ExtensionsV3 object

Required: Yes

GeneralFlags

General flags describe whether the template is used for computers or users and if the template can be used with autoenrollment.

Type: GeneralFlagsV3 object

Required: Yes

HashAlgorithm

Specifies the hash algorithm used to hash the private key.

Type: String

Valid Values: `SHA256 | SHA384 | SHA512`

Required: Yes

PrivateKeyAttributes

Private key attributes allow you to specify the algorithm, minimal key length, key spec, key usage, and cryptographic providers for the private key of a certificate for v3 templates. V3 templates allow you to use Key Storage Providers.

Type: PrivateKeyAttributesV3 object

Required: Yes

PrivateKeyFlags

Private key flags for v3 templates specify the client compatibility, if the private key can be exported, if user input is required when using a private key, and if an alternate signature algorithm should be used.

Type: PrivateKeyFlagsV3 object

Required: Yes

SubjectNameFlags

Subject name flags describe the subject name and subject alternate name that is included in a certificate.

Type: SubjectNameFlagsV3 object

Required: Yes

SupersededTemplates

List of templates in Active Directory that are superseded by this template.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

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

Pattern: `(?!^\s+$)((?![\x5c'\x2b,;<=>#\x22])([\x20-\x7E]))+`

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 Java V2
- AWS SDK for Ruby V3

TemplateV4

v4 template schema that can use either Legacy Cryptographic Providers or Key Storage Providers.

Contents

CertificateValidity

Certificate validity describes the validity and renewal periods of a certificate.

Type: CertificateValidity object

Required: Yes

EnrollmentFlags

Enrollment flags describe the enrollment settings for certificates using the existing private key and deleting expired or revoked certificates.

Type: EnrollmentFlagsV4 object

Required: Yes

Extensions

Extensions describe the key usage extensions and application policies for a template.

Type: ExtensionsV4 object

Required: Yes

GeneralFlags

General flags describe whether the template is used for computers or users and if the template can be used with autoenrollment.

Type: GeneralFlagsV4 object

Required: Yes

PrivateKeyAttributes

Private key attributes allow you to specify the minimal key length, key spec, key usage, and cryptographic providers for the private key of a certificate for v4 templates. V4 templates allow you to use either Key Storage Providers or Legacy Cryptographic Service Providers. You specify the cryptography provider category in private key flags.

Type: PrivateKeyAttributesV4 object

Required: Yes

PrivateKeyFlags

Private key flags for v4 templates specify the client compatibility, if the private key can be exported, if user input is required when using a private key, if an alternate signature algorithm should be used, and if certificates are renewed using the same private key.

Type: PrivateKeyFlagsV4 object

Required: Yes

SubjectNameFlags

Subject name flags describe the subject name and subject alternate name that is included in a certificate.

Type: SubjectNameFlagsV4 object

Required: Yes

HashAlgorithm

Specifies the hash algorithm used to hash the private key. Hash algorithm can only be specified when using Key Storage Providers.

Type: String

Valid Values: SHA256 | SHA384 | SHA512

Required: No

SupersededTemplates

List of templates in Active Directory that are superseded by this template.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

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

Pattern: `(?!^\s+$)((?![\x5c'\x2b,;<=>#\x22])([\x20-\x7E]))+`

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 Java V2
- AWS SDK for Ruby V3

ValidityPeriod

Information describing the end of the validity period of the certificate. This parameter sets the “Not After” date for the certificate. Certificate validity is the period of time during which a certificate is valid. Validity can be expressed as an explicit date and time when the certificate expires, or as a span of time after issuance, stated in hours, days, months, or years. For more information, see Validity in RFC 5280. This value is unaffected when ValidityNotBefore is also specified. For example, if Validity is set to 20 days in the future, the certificate will expire 20 days from issuance time regardless of the ValidityNotBefore value.

Contents

Period

The numeric value for the validity period.

Type: Long

Valid Range: Minimum value of 1. Maximum value of 8766000.

Required: Yes

PeriodType

The unit of time. You can select hours, days, weeks, months, and years.

Type: String

Valid Values: `HOURS | DAYS | WEEKS | MONTHS | YEARS`

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 Java V2
- AWS SDK for Ruby V3

VpcInformation

Information about your VPC and security groups used with the connector.

Contents

SecurityGroupIds

The security groups used with the connector. You can use a maximum of 4 security groups with a connector.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 4 items.

Length Constraints: Minimum length of 11. Maximum length of 20.

Pattern: `(?:sg-[0-9a-f]{8}|sg-[0-9a-f]{17})`

Required: Yes

IpAddressType

The VPC IP address type.

Type: String

Valid Values: `IPV4 | DUALSTACK`

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 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 Signing AWS API requests in the *IAM User Guide*.

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 Create a signed AWS API request in the *IAM User Guide*.

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 Elements of an AWS API request signature in the *IAM User Guide*.

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 STS, see AWS services that work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, 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 Create a signed AWS API request in the *IAM User Guide*.

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: 403

ExpiredTokenException

The security token included in the request is expired

HTTP Status Code: 403

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 403

InternalFailure

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

HTTP Status Code: 500

MalformedHttpRequestException

Problems with the request at the HTTP level, e.g. we can't decompress the body according to the decompression algorithm specified by the content-encoding.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 401

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestAbortedException

Convenient exception that can be used when a request is aborted before a reply is sent back (e.g. client closed connection).

HTTP Status Code: 400

RequestEntityTooLargeException

Problems with the request at the HTTP level. The request entity is too large.

HTTP Status Code: 413

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

RequestTimeoutException

Problems with the request at the HTTP level. Reading the Request timed out.

HTTP Status Code: 408

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

UnrecognizedClientException

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

UnknownOperationException

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 404

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400