AWS Shield Advanced

AWS Shield Advanced API Reference

API Version 2016-06-02

AWS Shield Advanced: AWS Shield Advanced API Reference

Table of Contents

Welcome

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

This document was last published on November 19, 2018.

Actions

The following actions are supported:

AssociateDRTLogBucket

Authorizes the DDoS Response team (DRT) to access the specified Amazon S3 bucket containing your flow logs. You can associate up to 10 Amazon S3 buckets with your subscription.

To use the services of the DRT and make an `AssociateDRTLogBucket` request, you must be subscribed to the Business Support plan or the Enterprise Support plan.

Request Syntax

```
{
   "LogBucket": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

LogBucket (p. 3)

The Amazon S3 bucket that contains your flow logs.

Type: String

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

Pattern: `^([a-z]|(\d(?!\d{0,2}\.\d{1,3}\.\d{1,3}\.\d{1,3})))([a-z\d]|(\.(?!(\.|-)))|(-(?!\.))){1,61}[a-z\d]$`

Required: Yes

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 (p. 61).

AccessDeniedForDependencyException

In order to grant the necessary access to the DDoS Response Team, the user submitting `AssociateDRTRole` must have the `iam:PassRole` permission. This error indicates the user did not have the appropriate permissions. For more information, see Granting a User Permissions to Pass a Role to an AWS Service.

HTTP Status Code: 400

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidOperationException

Exception that indicates that the operation would not cause any change to occur.

HTTP Status Code: 400

InvalidParameterException

Exception that indicates that the parameters passed to the API are invalid.

HTTP Status Code: 400

LimitsExceededException

Exception that indicates that the operation would exceed a limit.

`Type` is the type of limit that would be exceeded.

`Limit` is the threshold that would be exceeded.

HTTP Status Code: 400

NoAssociatedRoleException

The ARN of the role that you specifed does not exist.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the protection state has been modified by another client. You can retry the request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

AssociateDRTRole

Authorizes the DDoS Response team (DRT), using the specified role, to access your AWS account to assist with DDoS attack mitigation during potential attacks. This enables the DRT to inspect your AWS WAF configuration and create or update AWS WAF rules and web ACLs.

You can associate only one `RoleArn` with your subscription. If you submit an `AssociateDRTRole` request for an account that already has an associated role, the new `RoleArn` will replace the existing `RoleArn`.

Prior to making the `AssociateDRTRole` request, you must attach the AWSShieldDRTAccessPolicy managed policy to the role you will specify in the request. For more information see Attaching and Detaching IAM Policies. The role must also trust the service principal `drt.shield.amazonaws.com`. For more information, see IAM JSON Policy Elements: Principal.

The DRT will have access only to your AWS WAF and Shield resources. By submitting this request, you authorize the DRT to inspect your AWS WAF and Shield configuration and create and update AWS WAF rules and web ACLs on your behalf. The DRT takes these actions only if explicitly authorized by you.

You must have the `iam:PassRole` permission to make an `AssociateDRTRole` request. For more information, see Granting a User Permissions to Pass a Role to an AWS Service.

To use the services of the DRT and make an `AssociateDRTRole` request, you must be subscribed to the Business Support plan or the Enterprise Support plan.

Request Syntax

```
{
   "RoleArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

RoleArn (p. 5)

The Amazon Resource Name (ARN) of the role the DRT will use to access your AWS account.

Prior to making the `AssociateDRTRole` request, you must attach the AWSShieldDRTAccessPolicy managed policy to this role. For more information see Attaching and Detaching IAM Policies.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `^arn:aws:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Required: Yes

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 (p. 61).

AccessDeniedForDependencyException

In order to grant the necessary access to the DDoS Response Team, the user submitting `AssociateDRTRole` must have the `iam:PassRole` permission. This error indicates the user did not have the appropriate permissions. For more information, see Granting a User Permissions to Pass a Role to an AWS Service.

HTTP Status Code: 400

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidOperationException

Exception that indicates that the operation would not cause any change to occur.

HTTP Status Code: 400

InvalidParameterException

Exception that indicates that the parameters passed to the API are invalid.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the protection state has been modified by another client. You can retry the request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

CreateProtection

Enables AWS Shield Advanced for a specific AWS resource. The resource can be an Amazon CloudFront distribution, Elastic Load Balancing load balancer, Elastic IP Address, or an Amazon Route 53 hosted zone.

You can add protection to only a single resource with each CreateProtection request. If you want to add protection to multiple resources at once, use the AWS WAF console. For more information see Getting Started with AWS Shield Advanced and Add AWS Shield Advanced Protection to more AWS Resources.

Request Syntax

```
{
   "Name": "string",
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

Name (p. 7)

Friendly name for the `Protection` you are creating.

Type: String

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

Pattern: `[ a-zA-Z0-9_\\.\\-]*`

Required: Yes

ResourceArn (p. 7)

The ARN (Amazon Resource Name) of the resource to be protected.

The ARN should be in one of the following formats:

- For an Application Load Balancer: `arn:aws:elasticloadbalancing:`*region*`:`*account-id*`:loadbalancer/app/`*load-balancer-name*`/`*load-balancer-id*
- For an Elastic Load Balancer (Classic Load Balancer): `arn:aws:elasticloadbalancing:`*region*`:`*account-id*`:loadbalancer/`*load-balancer-name*
- For AWS CloudFront distribution: `arn:aws:cloudfront::`*account-id*`:distribution/`*distribution-id*
- For Amazon Route 53: `arn:aws:route53:::hostedzone/`*hosted-zone-id*
- For an Elastic IP address: `arn:aws:ec2:`*region*`:`*account-id*`:eip-allocation/`*allocation-id*

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `^arn:aws.*`

Required: Yes

Response Syntax

```
{
   "ProtectionId": "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.

ProtectionId (p. 8)

The unique identifier (ID) for the Protection (p. 51) object that is created.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 36.

Pattern: `[a-zA-Z0-9\\-]*`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidOperationException

Exception that indicates that the operation would not cause any change to occur.

HTTP Status Code: 400

InvalidResourceException

Exception that indicates that the resource is invalid. You might not have access to the resource, or the resource might not exist.

HTTP Status Code: 400

LimitsExceededException

Exception that indicates that the operation would exceed a limit.

`Type` is the type of limit that would be exceeded.

`Limit` is the threshold that would be exceeded.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the protection state has been modified by another client. You can retry the request.

HTTP Status Code: 400

ResourceAlreadyExistsException

Exception indicating the specified resource already exists.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

CreateSubscription

Activates AWS Shield Advanced for an account.

As part of this request you can specify `EmergencySettings` that automaticaly grant the DDoS response team (DRT) needed permissions to assist you during a suspected DDoS attack. For more information see Authorize the DDoS Response Team to Create Rules and Web ACLs on Your Behalf.

When you initally create a subscription, your subscription is set to be automatically renewed at the end of the existing subscription period. You can change this by submitting an `UpdateSubscription` request.

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 (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

ResourceAlreadyExistsException

Exception indicating the specified resource already exists.

HTTP Status Code: 400

See Also

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

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

DeleteProtection

Deletes an AWS Shield Advanced Protection (p. 51).

Request Syntax

```
{
   "ProtectionId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

ProtectionId (p. 11)

The unique identifier (ID) for the Protection (p. 51) object to be deleted.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 36.

Pattern: `[a-zA-Z0-9\\-]*`

Required: Yes

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 (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

OptimisticLockException

Exception that indicates that the protection state has been modified by another client. You can retry the request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

DeleteSubscription

This action has been deprecated.

Removes AWS Shield Advanced from an account. AWS Shield Advanced requires a 1-year subscription commitment. You cannot delete a subscription prior to the completion of that commitment.

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 (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

LockedSubscriptionException

You are trying to update a subscription that has not yet completed the 1-year commitment. You can change the `AutoRenew` parameter during the last 30 days of your subscription. This exception indicates that you are attempting to change `AutoRenew` prior to that period.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

DescribeAttack

Describes the details of a DDoS attack.

Request Syntax

```
{
   "AttackId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

AttackId (p. 14)

The unique identifier (ID) for the attack that to be described.

Type: String

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

Pattern: `[a-zA-Z0-9\\-]*`

Required: Yes

Response Syntax

```
{
   "Attack": {
      "AttackCounters": [
         {
            "Average": number,
            "Max": number,
            "N": number,
            "Name": "string",
            "Sum": number,
            "Unit": "string"
         }
      ],
      "AttackId": "string",
      "AttackProperties": [
         {
            "AttackLayer": "string",
            "AttackPropertyIdentifier": "string",
            "TopContributors": [
               {
                  "Name": "string",
                  "Value": number
               }
            ],
            "Total": number,
            "Unit": "string"
         }
      ],
```

```
      "EndTime": number,
      "Mitigations": [
         {
            "MitigationName": "string"
         }
      ],
      "ResourceArn": "string",
      "StartTime": number,
      "SubResources": [
         {
            "AttackVectors": [
               {
                  "VectorCounters": [
                     {
                        "Average": number,
                        "Max": number,
                        "N": number,
                        "Name": "string",
                        "Sum": number,
                        "Unit": "string"
                     }
                  ],
                  "VectorType": "string"
               }
            ],
            "Counters": [
               {
                  "Average": number,
                  "Max": number,
                  "N": number,
                  "Name": "string",
                  "Sum": number,
                  "Unit": "string"
               }
            ],
            "Id": "string",
            "Type": "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.

Attack (p. 14)

The attack that is described.

Type: AttackDetail (p. 41) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

AccessDeniedException

Exception that indicates the specified `AttackId` does not exist, or the requester does not have the appropriate permissions to access the `AttackId`.

HTTP Status Code: 400

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

See Also

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

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

DescribeDRTAccess

Returns the current role and list of Amazon S3 log buckets used by the DDoS Response team (DRT) to access your AWS account while assisting with attack mitigation.

Response Syntax

```
{
   "LogBucketList": [ "string" ],
   "RoleArn": "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.

LogBucketList (p. 17)

The list of Amazon S3 buckets accessed by the DRT.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 10 items.

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

Pattern: `^([a-z]|(\d(?!\d{0,2}\.\d{1,3}\.\d{1,3}\.\d{1,3})))([a-z\d]|(\.(?!(\.|-)))|(-(?!\.))){1,61}[a-z\d]$`

RoleArn (p. 17)

The Amazon Resource Name (ARN) of the role the DRT used to access your AWS account.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `^arn:aws:iam::\d{12}:role/?[a-zA-Z_0-9+=,.@\-_/]+`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

DescribeEmergencyContactSettings

Lists the email addresses that the DRT can use to contact you during a suspected attack.

Response Syntax

```
{
   "EmergencyContactList": [
      {
         "EmailAddress": "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.

EmergencyContactList (p. 19)

A list of email addresses that the DRT can use to contact you during a suspected attack.

Type: Array of EmergencyContact (p. 48) objects

Array Members: Minimum number of 0 items. Maximum number of 10 items.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

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

DescribeProtection

Lists the details of a Protection (p. 51) object.

Request Syntax

```
{
   "ProtectionId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

ProtectionId (p. 21)

The unique identifier (ID) for the Protection (p. 51) object that is described.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 36.

Pattern: `[a-zA-Z0-9\\-]*`

Required: Yes

Response Syntax

```
{
   "Protection": {
      "Id": "string",
      "Name": "string",
      "ResourceArn": "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.

Protection (p. 21)

The Protection (p. 51) object that is described.

Type: Protection (p. 51) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

DescribeSubscription

Provides details about the AWS Shield Advanced subscription for an account.

Response Syntax

```
{
   "Subscription": {
      "AutoRenew": "string",
      "EndTime": number,
      "Limits": [
         {
            "Max": number,
            "Type": "string"
         }
      ],
      "StartTime": number,
      "TimeCommitmentInSeconds": 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.

Subscription (p. 23)

The AWS Shield Advanced subscription details for an account.

Type: Subscription (p. 53) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface

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

DisassociateDRTLogBucket

Removes the DDoS Response team's (DRT) access to the specified Amazon S3 bucket containing your flow logs.

To make a `DisassociateDRTLogBucket` request, you must be subscribed to the Business Support plan or the Enterprise Support plan. However, if you are not subscribed to one of these support plans, but had been previously and had granted the DRT access to your account, you can submit a `DisassociateDRTLogBucket` request to remove this access.

Request Syntax

```
{
   "LogBucket": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

LogBucket (p. 25)

The Amazon S3 bucket that contains your flow logs.

Type: String

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

Pattern: `^([a-z]|(\d(?!\d{0,2}\.\d{1,3}\.\d{1,3}\.\d{1,3})))([a-z\d]|(\.(?!(\.|-)))|(-(?!\.))){1,61}[a-z\d]$`

Required: Yes

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 (p. 61).

AccessDeniedForDependencyException

In order to grant the necessary access to the DDoS Response Team, the user submitting `AssociateDRTRole` must have the `iam:PassRole` permission. This error indicates the user did not have the appropriate permissions. For more information, see Granting a User Permissions to Pass a Role to an AWS Service.

HTTP Status Code: 400

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidOperationException

Exception that indicates that the operation would not cause any change to occur.

HTTP Status Code: 400

NoAssociatedRoleException

The ARN of the role that you specifed does not exist.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the protection state has been modified by another client. You can retry the request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

DisassociateDRTRole

Removes the DDoS Response team's (DRT) access to your AWS account.

To make a `DisassociateDRTRole` request, you must be subscribed to the Business Support plan or the Enterprise Support plan. However, if you are not subscribed to one of these support plans, but had been previously and had granted the DRT access to your account, you can submit a `DisassociateDRTRole` request to remove this access.

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 (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidOperationException

Exception that indicates that the operation would not cause any change to occur.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the protection state has been modified by another client. You can retry the request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

GetSubscriptionState

Returns the `SubscriptionState`, either `Active` or `Inactive`.

Response Syntax

```
{
   "SubscriptionState": "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.

SubscriptionState (p. 29)

The status of the subscription.

Type: String

Valid Values: `ACTIVE | INACTIVE`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

See Also

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

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

ListAttacks

Returns all ongoing DDoS attacks or all DDoS attacks during a specified time period.

Request Syntax

```
{
   "EndTime": {
      "FromInclusive": number,
      "ToExclusive": number
   },
   "MaxResults": number,
   "NextToken": "string",
   "ResourceArns": [ "string" ],
   "StartTime": {
      "FromInclusive": number,
      "ToExclusive": number
   }
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

EndTime (p. 30)

The end of the time period for the attacks. This is a `timestamp` type. The sample request above indicates a `number` type because the default used by WAF is Unix time in seconds. However any valid timestamp format is allowed.

Type: TimeRange (p. 58) object

Required: No

MaxResults (p. 30)

The maximum number of AttackSummary (p. 45) objects to be returned. If this is left blank, the first 20 results will be returned.

This is a maximum value; it is possible that AWS WAF will return the results in smaller batches. That is, the number of AttackSummary (p. 45) objects returned could be less than `MaxResults`, even if there are still more AttackSummary (p. 45) objects yet to return. If there are more AttackSummary (p. 45) objects to return, AWS WAF will always also return a `NextToken`.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 10000.

Required: No

NextToken (p. 30)

The `ListAttacksRequest.NextMarker` value from a previous call to `ListAttacksRequest`. Pass null if this is the first call.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^.*$`

Required: No

ResourceArns (p. 30)

The ARN (Amazon Resource Name) of the resource that was attacked. If this is left blank, all applicable resources for this account will be included.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `^arn:aws.*`

Required: No

StartTime (p. 30)

The start of the time period for the attacks. This is a `timestamp` type. The sample request above indicates a `number` type because the default used by WAF is Unix time in seconds. However any valid timestamp format is allowed.

Type: TimeRange (p. 58) object

Required: No

Response Syntax

```
{
   "AttackSummaries": [
      {
         "AttackId": "string",
         "AttackVectors": [
            {
               "VectorType": "string"
            }
         ],
         "EndTime": number,
         "ResourceArn": "string",
         "StartTime": 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.

AttackSummaries (p. 31)

The attack information for the specified time range.

Type: Array of AttackSummary (p. 45) objects

NextToken (p. 31)

The token returned by a previous call to indicate that there is more data available. If not null, more results are available. Pass this value for the `NextMarker` parameter in a subsequent call to `ListAttacks` to retrieve the next set of items.

AWS WAF might return the list of AttackSummary (p. 45) objects in batches smaller than the number specified by MaxResults. If there are more AttackSummary (p. 45) objects to return, AWS WAF will always also return a `NextToken`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^.*$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidOperationException

Exception that indicates that the operation would not cause any change to occur.

HTTP Status Code: 400

InvalidParameterException

Exception that indicates that the parameters passed to the API are invalid.

HTTP Status Code: 400

See Also

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

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

ListProtections

Lists all Protection (p. 51) objects for the account.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

MaxResults (p. 33)

The maximum number of Protection (p. 51) objects to be returned. If this is left blank the first 20 results will be returned.

This is a maximum value; it is possible that AWS WAF will return the results in smaller batches. That is, the number of Protection (p. 51) objects returned could be less than `MaxResults`, even if there are still more Protection (p. 51) objects yet to return. If there are more Protection (p. 51) objects to return, AWS WAF will always also return a `NextToken`.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 10000.

Required: No

NextToken (p. 33)

The `ListProtectionsRequest.NextToken` value from a previous call to `ListProtections`. Pass null if this is the first call.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^.*$`

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "Protections": [
      {
         "Id": "string",
         "Name": "string",
         "ResourceArn": "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.

NextToken (p. 33)

If you specify a value for `MaxResults` and you have more Protections than the value of MaxResults, AWS Shield Advanced returns a NextToken value in the response that allows you to list another group of Protections. For the second and subsequent ListProtections requests, specify the value of NextToken from the previous response to get information about another batch of Protections.

AWS WAF might return the list of Protection (p. 51) objects in batches smaller than the number specified by MaxResults. If there are more Protection (p. 51) objects to return, AWS WAF will always also return a `NextToken`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^.*$`

Protections (p. 33)

The array of enabled Protection (p. 51) objects.

Type: Array of Protection (p. 51) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidPaginationTokenException

Exception that indicates that the NextToken specified in the request is invalid. Submit the request using the NextToken value that was returned in the response.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

UpdateEmergencyContactSettings

Updates the details of the list of email addresses that the DRT can use to contact you during a suspected attack.

Request Syntax

```
{
   "EmergencyContactList": [
      {
         "EmailAddress": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

EmergencyContactList (p. 36)

A list of email addresses that the DRT can use to contact you during a suspected attack.

Type: Array of EmergencyContact (p. 48) objects

Array Members: Minimum number of 0 items. Maximum number of 10 items.

Required: No

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 (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidParameterException

Exception that indicates that the parameters passed to the API are invalid.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the protection state has been modified by another client. You can retry the request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

UpdateSubscription

Updates the details of an existing subscription. Only enter values for parameters you want to change. Empty parameters are not updated.

Request Syntax

```
{
   "AutoRenew": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 59).

The request accepts the following data in JSON format.

AutoRenew (p. 38)

When you initally create a subscription, `AutoRenew` is set to `ENABLED`. If `ENABLED`, the subscription will be automatically renewed at the end of the existing subscription period. You can change this by submitting an `UpdateSubscription` request. If the `UpdateSubscription` request does not included a value for `AutoRenew`, the existing value for `AutoRenew` remains unchanged.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

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 (p. 61).

InternalErrorException

Exception that indicates that a problem occurred with the service infrastructure. You can retry the request.

HTTP Status Code: 500

InvalidParameterException

Exception that indicates that the parameters passed to the API are invalid.

HTTP Status Code: 400

LockedSubscriptionException

You are trying to update a subscription that has not yet completed the 1-year commitment. You can change the `AutoRenew` parameter during the last 30 days of your subscription. This exception indicates that you are attempting to change `AutoRenew` prior to that period.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the protection state has been modified by another client. You can retry the request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist.

HTTP Status Code: 400

See Also

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

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

Data Types

The AWS Shield 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:

AttackDetail

The details of a DDoS attack.

Contents

AttackCounters

List of counters that describe the attack for the specified time period.

Type: Array of SummarizedCounter (p. 56) objects

Required: No

AttackId

The unique identifier (ID) of the attack.

Type: String

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

Pattern: `[a-zA-Z0-9\\-]*`

Required: No

AttackProperties

The array of AttackProperty (p. 43) objects.

Type: Array of AttackProperty (p. 43) objects

Required: No

EndTime

The time the attack ended, in Unix time in seconds. For more information see timestamp.

Type: Timestamp

Required: No

Mitigations

List of mitigation actions taken for the attack.

Type: Array of Mitigation (p. 50) objects

Required: No

ResourceArn

The ARN (Amazon Resource Name) of the resource that was attacked.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `^arn:aws.*`

Required: No

StartTime

The time the attack started, in Unix time in seconds. For more information see timestamp.

Type: Timestamp

Required: No

SubResources

If applicable, additional detail about the resource being attacked, for example, IP address or URL.

Type: Array of SubResourceSummary (p. 52) objects

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

AttackProperty

Details of the described attack.

Contents

AttackLayer

The type of DDoS event that was observed. `NETWORK` indicates layer 3 and layer 4 events and `APPLICATION` indicates layer 7 events.

Type: String

Valid Values: `NETWORK | APPLICATION`

Required: No

AttackPropertyIdentifier

Defines the DDoS attack property information that is provided.

Type: String

Valid Values: `DESTINATION_URL | REFERRER | SOURCE_ASN | SOURCE_COUNTRY | SOURCE_IP_ADDRESS | SOURCE_USER_AGENT`

Required: No

TopContributors

The array of Contributor (p. 47) objects that includes the top five contributors to an attack.

Type: Array of Contributor (p. 47) objects

Required: No

Total

The total contributions made to this attack by all contributors, not just the five listed in the `TopContributors` list.

Type: Long

Required: No

Unit

The unit of the `Value` of the contributions.

Type: String

Valid Values: `BITS | BYTES | PACKETS | REQUESTS`

Required: No

See Also

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

- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

AttackSummary

Summarizes all DDoS attacks for a specified time period.

Contents

AttackId

The unique identifier (ID) of the attack.

Type: String

Required: No

AttackVectors

The list of attacks for a specified time period.

Type: Array of AttackVectorDescription (p. 46) objects

Required: No

EndTime

The end time of the attack, in Unix time in seconds. For more information see timestamp.

Type: Timestamp

Required: No

ResourceArn

The ARN (Amazon Resource Name) of the resource that was attacked.

Type: String

Required: No

StartTime

The start time of the attack, in Unix time in seconds. For more information see timestamp.

Type: Timestamp

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

AttackVectorDescription

Describes the attack.

Contents

VectorType

The attack type. Valid values:

- UDP_TRAFFIC
- UDP_FRAGMENT
- GENERIC_UDP_REFLECTION
- DNS_REFLECTION
- NTP_REFLECTION
- CHARGEN_REFLECTION
- SSDP_REFLECTION
- PORT_MAPPER
- RIP_REFLECTION
- SNMP_REFLECTION
- MSSQL_REFLECTION
- NET_BIOS_REFLECTION
- SYN_FLOOD
- ACK_FLOOD
- REQUEST_FLOOD

Type: String

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Contributor

A contributor to the attack and their contribution.

Contents

Name

The name of the contributor. This is dependent on the `AttackPropertyIdentifier`. For example, if the `AttackPropertyIdentifier` is `SOURCE_COUNTRY`, the `Name` could be `United States`.

Type: String

Required: No

Value

The contribution of this contributor expressed in Protection (p. 51) units. For example `10,000`.

Type: Long

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

EmergencyContact

Contact information that the DRT can use to contact you during a suspected attack.

Contents

EmailAddress

An email address that the DRT can use to contact you during a suspected attack.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 150.

Pattern: `^\S+@\S+\.\S+$`

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Limit

Specifies how many protections of a given type you can create.

Contents

Max

The maximum number of protections that can be created for the specified `Type`.

Type: Long

Required: No

Type

The type of protection.

Type: String

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Mitigation

The mitigation applied to a DDoS attack.

Contents

MitigationName

The name of the mitigation taken for this attack.

Type: String

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Protection

An object that represents a resource that is under DDoS protection.

Contents

Id

The unique identifier (ID) of the protection.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 36.

Pattern: `[a-zA-Z0-9\\-]*`

Required: No

Name

The friendly name of the protection. For example, `My CloudFront distributions`.

Type: String

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

Pattern: `[ a-zA-Z0-9_\\.\\-]*`

Required: No

ResourceArn

The ARN (Amazon Resource Name) of the AWS resource that is protected.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `^arn:aws.*`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

SubResourceSummary

The attack information for the specified SubResource.

Contents

AttackVectors

The list of attack types and associated counters.

Type: Array of SummarizedAttackVector (p. 55) objects

Required: No

Counters

The counters that describe the details of the attack.

Type: Array of SummarizedCounter (p. 56) objects

Required: No

Id

The unique identifier (ID) of the `SubResource`.

Type: String

Required: No

Type

The `SubResource` type.

Type: String

Valid Values: `IP | URL`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Subscription

Information about the AWS Shield Advanced subscription for an account.

Contents

AutoRenew

If `ENABLED`, the subscription will be automatically renewed at the end of the existing subscription period.

When you initally create a subscription, `AutoRenew` is set to `ENABLED`. You can change this by submitting an `UpdateSubscription` request. If the `UpdateSubscription` request does not included a value for `AutoRenew`, the existing value for `AutoRenew` remains unchanged.

Type: String

Valid Values: `ENABLED | DISABLED`

Required: No

EndTime

The date and time your subscription will end.

Type: Timestamp

Required: No

Limits

Specifies how many protections of a given type you can create.

Type: Array of Limit (p. 49) objects

Required: No

StartTime

The start time of the subscription, in Unix time in seconds. For more information see timestamp.

Type: Timestamp

Required: No

TimeCommitmentInSeconds

The length, in seconds, of the AWS Shield Advanced subscription for the account.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

SummarizedAttackVector

A summary of information about the attack.

Contents

VectorCounters

The list of counters that describe the details of the attack.

Type: Array of SummarizedCounter (p. 56) objects

Required: No

VectorType

The attack type, for example, SNMP reflection or SYN flood.

Type: String

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

SummarizedCounter

The counter that describes a DDoS attack.

Contents

Average

The average value of the counter for a specified time period.

Type: Double

Required: No

Max

The maximum value of the counter for a specified time period.

Type: Double

Required: No

N

The number of counters for a specified time period.

Type: Integer

Required: No

Name

The counter name.

Type: String

Required: No

Sum

The total of counter values for a specified time period.

Type: Double

Required: No

Unit

The unit of the counters.

Type: String

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java

- AWS SDK for Ruby V2

TimeRange

The time range.

Contents

FromInclusive

The start time, in Unix time in seconds. For more information see timestamp.

Type: Timestamp

Required: No

ToExclusive

The end time, in Unix time in seconds. For more information see timestamp.

Type: Timestamp

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is

not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS Security Token Service, go to AWS Services That Work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

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

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400