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 1
Actions 2
CreateProtection 3
Request Syntax 3
Request Parameters 3
Response Syntax 3
Response Elements 3
Errors 4
See Also 4
CreateSubscription 6
Response Elements 6
Errors 6
See Also 6
DeleteProtection 7
Request Syntax 7
Request Parameters 7
Response Elements 7
Errors 7
See Also 8
DeleteSubscription 9
Response Elements 9
Errors 9
See Also 9
DescribeAttack 10
Request Syntax 10
Request Parameters 10
Response Syntax 10
Response Elements 11
Errors 11
See Also 11
DescribeProtection 13
Request Syntax 13
Request Parameters 13
Response Syntax 13
Response Elements 13
Errors 13
See Also 14
DescribeSubscription 15
Response Syntax 15
Response Elements 15
Errors 15
See Also 15
ListAttacks 17
Request Syntax 17
Request Parameters 17
Response Syntax 18
Response Elements 18
Errors 19
See Also 19
ListProtections 20
Request Syntax 20
Request Parameters 20
Response Syntax 20
Response Elements 20

Errors 21
See Also 21
Data Types 22
AttackDetail 23
Contents 23
See Also 24
AttackSummary 25
Contents 25
See Also 25
AttackVectorDescription 26
Contents 26
See Also 26
Mitigation 27
Contents 27
See Also 27
Protection 28
Contents 28
See Also 28
SubResourceSummary 29
Contents 29
See Also 29
Subscription 30
Contents 30
See Also 30
SummarizedAttackVector 31
Contents 31
See Also 31
SummarizedCounter 32
Contents 32
See Also 32
TimeRange 34
Contents 34
See Also 34
Common Parameters 35
Common Errors 37

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 July 20, 2017.

Actions

The following actions are supported:

- CreateProtection (p. 3)
- CreateSubscription (p. 6)
- DeleteProtection (p. 7)
- DeleteSubscription (p. 9)
- DescribeAttack (p. 10)
- DescribeProtection (p. 13)
- DescribeSubscription (p. 15)
- ListAttacks (p. 17)
- ListProtections (p. 20)

CreateProtection

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

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 35).

The request accepts the following data in JSON format.

Name (p. 3)

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. 3)

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

Type: String

Length Constraints: Minimum length of 1.

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. 3)

The unique identifier (ID) for the Protection (p. 28) 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. 37).

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.

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.

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. 37).

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. 28).

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 35).

The request accepts the following data in JSON format.

ProtectionId (p. 7)

The unique identifier (ID) for the Protection (p. 28) 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. 37).

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

Removes AWS Shield Advanced from an account.

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. 37).

InternalErrorException

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

HTTP Status Code: 500

LockedSubscriptionException

Exception that indicates that the subscription 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

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. 35).

The request accepts the following data in JSON format.

AttackId (p. 10)

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",
      "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. 10)

The attack that is described.

Type: AttackDetail (p. 23) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 37).

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

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. 28) object.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 35).

The request accepts the following data in JSON format.

ProtectionId (p. 13)

The unique identifier (ID) for the Protection (p. 28) 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. 13)

The Protection (p. 28) object that is described.

Type: Protection (p. 28) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 37).

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": {
      "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. 15)

The AWS Shield Advanced subscription details for an account.

Type: Subscription (p. 30) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 37).

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

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. 35).

The request accepts the following data in JSON format.

EndTime (p. 17)

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. 34) object

Required: No

MaxResults (p. 17)

The maximum number of AttackSummary (p. 25) objects to be returned. If this is left blank, the first 20 results will be returned.

Type: Integer

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

Required: No

NextToken (p. 17)

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.

Required: No

ResourceArns (p. 17)

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.

Required: No

StartTime (p. 17)

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. 34) 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. 18)

The attack information for the specified time range.

Type: Array of AttackSummary (p. 25) objects

NextToken (p. 18)

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.

Type: String

Length Constraints: Minimum length of 1.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 37).

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. 28) 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. 35).

The request accepts the following data in JSON format.

MaxResults (p. 20)

The maximum number of Protection (p. 28) objects to be returned. If this is left blank the first 20 results will be returned.

Type: Integer

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

Required: No

NextToken (p. 20)

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.

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. 20)

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.

Type: String

Length Constraints: Minimum length of 1.

Protections (p. 20)

The array of enabled Protection (p. 28) objects.

Type: Array of Protection (p. 28) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 37).

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

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 (p. 23)
- AttackSummary (p. 25)
- AttackVectorDescription (p. 26)
- Mitigation (p. 27)
- Protection (p. 28)
- SubResourceSummary (p. 29)
- Subscription (p. 30)
- SummarizedAttackVector (p. 31)
- SummarizedCounter (p. 32)
- TimeRange (p. 34)

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. 32) 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

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. 27) objects

Required: No

ResourceArn

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

Type: String

Length Constraints: Minimum length of 1.

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. 29) 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

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. 26) 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

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.

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. 31) objects

Required: No

Counters

The counters that describe the details of the attack.

Type: Array of SummarizedCounter (p. 32) 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

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. 32) 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