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 October 6, 2021.

Actions

The following actions are supported:

- AssociateDRTLogBucket (p. 3)
- AssociateDRTRole (p. 5)
- AssociateHealthCheck (p. 8)
- AssociateProactiveEngagementDetails (p. 10)
- CreateProtection (p. 12)
- CreateProtectionGroup (p. 15)
- CreateSubscription (p. 18)
- DeleteProtection (p. 19)
- DeleteProtectionGroup (p. 21)
- DeleteSubscription (p. 23)
- DescribeAttack (p. 24)
- DescribeAttackStatistics (p. 27)
- DescribeDRTAccess (p. 29)
- DescribeEmergencyContactSettings (p. 31)
- DescribeProtection (p. 33)
- DescribeProtectionGroup (p. 35)
- DescribeSubscription (p. 37)
- DisableProactiveEngagement (p. 39)
- DisassociateDRTLogBucket (p. 41)
- DisassociateDRTRole (p. 43)
- DisassociateHealthCheck (p. 45)
- EnableProactiveEngagement (p. 47)
- GetSubscriptionState (p. 49)
- ListAttacks (p. 50)
- ListProtectionGroups (p. 53)
- ListProtections (p. 56)
- ListResourcesInProtectionGroup (p. 59)
- ListTagsForResource (p. 62)
- TagResource (p. 64)
- UntagResource (p. 66)
- UpdateEmergencyContactSettings (p. 68)
- UpdateProtectionGroup (p. 70)
- UpdateSubscription (p. 73)

AssociateDRTLogBucket

Authorizes the Shield Response Team (SRT) to access the specified Amazon S3 bucket containing log data such as Application Load Balancer access logs, CloudFront logs, or logs from third party sources. You can associate up to 10 Amazon S3 buckets with your subscription.

To use the services of the SRT 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. 107).

The request accepts the following data in JSON format.

LogBucket (p. 3)

The Amazon S3 bucket that contains the logs that you want to share.

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. 109).

AccessDeniedForDependencyException

In order to grant the necessary access to the Shield Response Team (SRT) the user submitting the request 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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

LimitsExceededException

Exception that indicates that the operation would exceed a limit.

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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

AssociateDRTRole

Authorizes the Shield Response Team (SRT) using the specified role, to access your AWS account to assist with DDoS attack mitigation during potential attacks. This enables the SRT 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 SRT will have access only to your AWS WAF and Shield resources. By submitting this request, you authorize the SRT to inspect your AWS WAF and Shield configuration and create and update AWS WAF rules and web ACLs on your behalf. The SRT 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 SRT 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. 107).

The request accepts the following data in JSON format.

RoleArn (p. 5)

The Amazon Resource Name (ARN) of the role the SRT 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. 109).

AccessDeniedForDependencyException

In order to grant the necessary access to the Shield Response Team (SRT) the user submitting the request 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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

- AWS SDK for Ruby V3

AssociateHealthCheck

Adds health-based detection to the Shield Advanced protection for a resource. Shield Advanced health-based detection uses the health of your AWS resource to improve responsiveness and accuracy in attack detection and mitigation.

You define the health check in Route 53 and then associate it with your Shield Advanced protection. For more information, see Shield Advanced Health-Based Detection in the *AWS WAF Developer Guide*.

Request Syntax

```
{
   "HealthCheckArn": "string",
   "ProtectionId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

HealthCheckArn (p. 8)

The Amazon Resource Name (ARN) of the health check to associate with the protection.

Type: String

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

Pattern: `^arn:aws:route53:::healthcheck/\S{36}$`

Required: Yes

ProtectionId (p. 8)

The unique identifier (ID) for the Protection (p. 89) object to add the health check association to.

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. 109).

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. If available, this exception includes details in additional properties.

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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

AssociateProactiveEngagementDetails

Initializes proactive engagement and sets the list of contacts for the Shield Response Team (SRT) to use. You must provide at least one phone number in the emergency contact list.

After you have initialized proactive engagement using this call, to disable or enable proactive engagement, use the calls `DisableProactiveEngagement` and `EnableProactiveEngagement`.

> **Note**
> This call defines the list of email addresses and phone numbers that the SRT can use to contact you for escalations to the SRT and to initiate proactive customer support.
> The contacts that you provide in the request replace any contacts that were already defined. If you already have contacts defined and want to use them, retrieve the list using `DescribeEmergencyContactSettings` and then provide it to this call.

Request Syntax

```
{
   "EmergencyContactList": [
      {
         "ContactNotes": "string",
         "EmailAddress": "string",
         "PhoneNumber": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

EmergencyContactList (p. 10)

A list of email addresses and phone numbers that the Shield Response Team (SRT) can use to contact you for escalations to the SRT and to initiate proactive customer support.

To enable proactive engagement, the contact list must include at least one phone number.

> **Note**
> The contacts that you provide here replace any contacts that were already defined. If you already have contacts defined and want to use them, retrieve the list using `DescribeEmergencyContactSettings` and then provide it here.

Type: Array of EmergencyContact (p. 86) objects

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

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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

CreateProtection

Enables AWS Shield Advanced for a specific AWS resource. The resource can be an Amazon CloudFront distribution, Elastic Load Balancing load balancer, AWS Global Accelerator accelerator, 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",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

Name (p. 12)

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. 12)

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 an Amazon CloudFront distribution: `arn:aws:cloudfront::`*`account-id`*`:distribution/`*`distribution-id`*
- For an AWS Global Accelerator accelerator: `arn:aws:globalaccelerator::`*`account-id`*`:accelerator/`*`accelerator-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

Tags (p. 12)

One or more tag key-value pairs for the Protection (p. 89) object that is created.

Type: Array of Tag (p. 104) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

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. 13)

The unique identifier (ID) for the Protection (p. 89) 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. 109).

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. If available, this exception includes details in additional properties.

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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceAlreadyExistsException

Exception indicating the specified resource already exists. If available, this exception includes details in additional properties.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

CreateProtectionGroup

Creates a grouping of protected resources so they can be handled as a collective. This resource grouping improves the accuracy of detection and reduces false positives.

Request Syntax

```
{
   "Aggregation": "string",
   "Members": [ "string" ],
   "Pattern": "string",
   "ProtectionGroupId": "string",
   "ResourceType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

Aggregation (p. 15)

Defines how AWS Shield combines resource data for the group in order to detect, mitigate, and report events.

- Sum - Use the total traffic across the group. This is a good choice for most cases. Examples include Elastic IP addresses for EC2 instances that scale manually or automatically.
- Mean - Use the average of the traffic across the group. This is a good choice for resources that share traffic uniformly. Examples include accelerators and load balancers.
- Max - Use the highest traffic from each resource. This is useful for resources that don't share traffic and for resources that share that traffic in a non-uniform way. Examples include Amazon CloudFront and origin resources for CloudFront distributions.

Type: String

Valid Values: `SUM | MEAN | MAX`

Required: Yes

Members (p. 15)

The Amazon Resource Names (ARNs) of the resources to include in the protection group. You must set this when you set `Pattern` to `ARBITRARY` and you must not set it for any other `Pattern` setting.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 10000 items.

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

Pattern: `^arn:aws.*`

Required: No

Pattern (p. 15)

The criteria to use to choose the protected resources for inclusion in the group. You can include all resources that have protections, provide a list of resource Amazon Resource Names (ARNs), or include all resources of a specified resource type.

Type: String

Valid Values: `ALL | ARBITRARY | BY_RESOURCE_TYPE`

Required: Yes

ProtectionGroupId (p. 15)

The name of the protection group. You use this to identify the protection group in lists and to manage the protection group, for example to update, delete, or describe it.

Type: String

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

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

Required: Yes

ResourceType (p. 15)

The resource type to include in the protection group. All protected resources of this type are included in the protection group. Newly protected resources of this type are automatically added to the group. You must set this when you set `Pattern` to `BY_RESOURCE_TYPE` and you must not set it for any other `Pattern` setting.

Type: String

Valid Values: `CLOUDFRONT_DISTRIBUTION | ROUTE_53_HOSTED_ZONE | ELASTIC_IP_ALLOCATION | CLASSIC_LOAD_BALANCER | APPLICATION_LOAD_BALANCER | GLOBAL_ACCELERATOR`

Required: No

Tags (p. 15)

One or more tag key-value pairs for the protection group.

Type: Array of Tag (p. 104) objects

Array Members: Minimum number of 0 items. Maximum number of 200 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. 109).

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. If available, this exception includes details in additional properties.

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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceAlreadyExistsException

Exception indicating the specified resource already exists. If available, this exception includes details in additional properties.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

CreateSubscription

Activates AWS Shield Advanced for an account.

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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

DeleteProtection

Deletes an AWS Shield Advanced Protection (p. 89).

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

ProtectionId (p. 19)

The unique identifier (ID) for the Protection (p. 89) 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. 109).

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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

DeleteProtectionGroup

Removes the specified protection group.

Request Syntax

```
{
   "ProtectionGroupId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

ProtectionGroupId (p. 21)

The name of the protection group. You use this to identify the protection group in lists and to manage the protection group, for example to update, delete, or describe it.

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. 109).

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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

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. 107).

The request accepts the following data in JSON format.

AttackId (p. 24)

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. 24)

The attack that is described.

Type: AttackDetail (p. 76) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

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

DescribeAttackStatistics

Provides information about the number and type of attacks AWS Shield has detected in the last year for all resources that belong to your account, regardless of whether you've defined Shield protections for them. This operation is available to Shield customers as well as to Shield Advanced customers.

The operation returns data for the time range of midnight UTC, one year ago, to midnight UTC, today. For example, if the current time is `2020-10-26 15:39:32 PDT`, equal to `2020-10-26 22:39:32 UTC`, then the time range for the attack data returned is from `2019-10-26 00:00:00 UTC` to `2020-10-26 00:00:00 UTC`.

The time range indicates the period covered by the attack statistics data items.

Response Syntax

```
{
   "DataItems": [
      {
         "AttackCount": number,
         "AttackVolume": {
            "BitsPerSecond": {
               "Max": number
            },
            "PacketsPerSecond": {
               "Max": number
            },
            "RequestsPerSecond": {
               "Max": number
            }
         }
      }
   ],
   "TimeRange": {
      "FromInclusive": number,
      "ToExclusive": 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.

DataItems (p. 27)

The data that describes the attacks detected during the time period.

Type: Array of AttackStatisticsDataItem (p. 80) objects

TimeRange (p. 27)

The time range.

Type: TimeRange (p. 105) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

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

DescribeDRTAccess

Returns the current role and list of Amazon S3 log buckets used by the Shield Response Team (SRT) 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. 29)

The list of Amazon S3 buckets accessed by the SRT.

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. 29)

The Amazon Resource Name (ARN) of the role the SRT 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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

DescribeEmergencyContactSettings

A list of email addresses and phone numbers that the Shield Response Team (SRT) can use to contact you if you have proactive engagement enabled, for escalations to the SRT and to initiate proactive customer support.

Response Syntax

```
{
   "EmergencyContactList": [
      {
         "ContactNotes": "string",
         "EmailAddress": "string",
         "PhoneNumber": "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. 31)

A list of email addresses and phone numbers that the Shield Response Team (SRT) can use to contact you if you have proactive engagement enabled, for escalations to the SRT and to initiate proactive customer support.

Type: Array of EmergencyContact (p. 86) 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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

DescribeProtection

Lists the details of a Protection (p. 89) object.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

ProtectionId (p. 33)

The unique identifier (ID) for the Protection (p. 89) object that is described. When submitting the `DescribeProtection` request you must provide either the `ResourceArn` or the `ProtectionID`, but not both.

Type: String

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

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

Required: No

ResourceArn (p. 33)

The ARN (Amazon Resource Name) of the AWS resource for the Protection (p. 89) object that is described. When submitting the `DescribeProtection` request you must provide either the `ResourceArn` or the `ProtectionID`, but not both.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

Response Syntax

```
{
   "Protection": {
      "HealthCheckIds": [ "string" ],
      "Id": "string",
      "Name": "string",
      "ProtectionArn": "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. 33)

The Protection (p. 89) object that is described.

Type: Protection (p. 89) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

DescribeProtectionGroup

Returns the specification for the specified protection group.

Request Syntax

```
{
   "ProtectionGroupId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

ProtectionGroupId (p. 35)

The name of the protection group. You use this to identify the protection group in lists and to manage the protection group, for example to update, delete, or describe it.

Type: String

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

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

Required: Yes

Response Syntax

```
{
   "ProtectionGroup": {
      "Aggregation": "string",
      "Members": [ "string" ],
      "Pattern": "string",
      "ProtectionGroupArn": "string",
      "ProtectionGroupId": "string",
      "ResourceType": "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.

ProtectionGroup (p. 35)

A grouping of protected resources that you and AWS Shield Advanced can monitor as a collective. This resource grouping improves the accuracy of detection and reduces false positives.

Type: ProtectionGroup (p. 91) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

DescribeSubscription

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

Response Syntax

```
{
   "Subscription": {
      "AutoRenew": "string",
      "EndTime": number,
      "Limits": [
         {
            "Max": number,
            "Type": "string"
         }
      ],
      "ProactiveEngagementStatus": "string",
      "StartTime": number,
      "SubscriptionArn": "string",
      "SubscriptionLimits": {
         "ProtectionGroupLimits": {
            "MaxProtectionGroups": number,
            "PatternTypeLimits": {
               "ArbitraryPatternLimits": {
                  "MaxMembers": number
               }
            }
         },
         "ProtectionLimits": {
            "ProtectedResourceTypeLimits": [
               {
                  "Max": number,
                  "Type": "string"
               }
            ]
         }
      },
      "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. 37)

The AWS Shield Advanced subscription details for an account.

Type: Subscription (p. 98) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

DisableProactiveEngagement

Removes authorization from the Shield Response Team (SRT) to notify contacts about escalations to the SRT and to initiate proactive customer support.

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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

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

DisassociateDRTLogBucket

Removes the Shield Response Team's (SRT) access to the specified Amazon S3 bucket containing the logs that you shared previously.

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 SRT 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. 107).

The request accepts the following data in JSON format.

LogBucket (p. 41)

The Amazon S3 bucket that contains the logs that you want to share.

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. 109).

AccessDeniedForDependencyException

In order to grant the necessary access to the Shield Response Team (SRT) the user submitting the request 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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

DisassociateDRTRole

Removes the Shield Response Team's (SRT) 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 SRT 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. 109).

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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

- AWS SDK for Ruby V3

DisassociateHealthCheck

Removes health-based detection from the Shield Advanced protection for a resource. Shield Advanced health-based detection uses the health of your AWS resource to improve responsiveness and accuracy in attack detection and mitigation.

You define the health check in Route 53 and then associate or disassociate it with your Shield Advanced protection. For more information, see Shield Advanced Health-Based Detection in the *AWS WAF Developer Guide*.

Request Syntax

```
{
   "HealthCheckArn": "string",
   "ProtectionId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

HealthCheckArn (p. 45)

The Amazon Resource Name (ARN) of the health check that is associated with the protection.

Type: String

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

Pattern: `^arn:aws:route53:::healthcheck/\S{36}$`

Required: Yes

ProtectionId (p. 45)

The unique identifier (ID) for the Protection (p. 89) object to remove the health check association from.

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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

EnableProactiveEngagement

Authorizes the Shield Response Team (SRT) to use email and phone to notify contacts about escalations to the SRT and to initiate proactive customer support.

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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

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

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. 49)

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. 109).

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

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. 107).

The request accepts the following data in JSON format.

EndTime (p. 50)

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 AWS WAF is Unix time in seconds. However any valid timestamp format is allowed.

Type: TimeRange (p. 105) object

Required: No

MaxResults (p. 50)

The maximum number of AttackSummary (p. 81) objects to return. If you leave this blank, Shield Advanced returns the first 20 results.

This is a maximum value. Shield Advanced might return the results in smaller batches. That is, the number of objects returned could be less than `MaxResults`, even if there are still more objects yet to return. If there are more objects to return, Shield Advanced returns a value in `NextToken` that you can use in your next request, to get the next batch of objects.

Type: Integer

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

Required: No

NextToken (p. 50)

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. 50)

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. 50)

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 AWS WAF is Unix time in seconds. However any valid timestamp format is allowed.

Type: TimeRange (p. 105) 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. 51)

The attack information for the specified time range.

Type: Array of AttackSummary (p. 81) objects

NextToken (p. 51)

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.

Shield Advanced might return the list of AttackSummary (p. 81) objects in batches smaller than the number specified by MaxResults. If there are more attack summary objects to return, Shield Advanced 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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

ListProtectionGroups

Retrieves the ProtectionGroup (p. 91) 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. 107).

The request accepts the following data in JSON format.

MaxResults (p. 53)

The maximum number of ProtectionGroup (p. 91) objects to return. If you leave this blank, Shield Advanced returns the first 20 results.

This is a maximum value. Shield Advanced might return the results in smaller batches. That is, the number of objects returned could be less than `MaxResults`, even if there are still more objects yet to return. If there are more objects to return, Shield Advanced returns a value in `NextToken` that you can use in your next request, to get the next batch of objects.

Type: Integer

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

Required: No

NextToken (p. 53)

The next token value from a previous call to `ListProtectionGroups`. 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",
   "ProtectionGroups": [
      {
         "Aggregation": "string",
         "Members": [ "string" ],
         "Pattern": "string",
         "ProtectionGroupArn": "string",
         "ProtectionGroupId": "string",
         "ResourceType": "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. 53)

> If you specify a value for `MaxResults` and you have more protection groups than the value of MaxResults, AWS Shield Advanced returns this token that you can use in your next request, to get the next batch of objects.
>
> Type: String
>
> Length Constraints: Minimum length of 1. Maximum length of 4096.
>
> Pattern: `^.*$`

ProtectionGroups (p. 53)

> Type: Array of ProtectionGroup (p. 91) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

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. If available, this exception includes details in additional properties.
>
> HTTP Status Code: 400

See Also

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

- AWS Command Line Interface

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

ListProtections

Lists all Protection (p. 89) 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. 107).

The request accepts the following data in JSON format.

MaxResults (p. 56)

The maximum number of Protection (p. 89) objects to return. If you leave this blank, Shield Advanced returns the first 20 results.

This is a maximum value. Shield Advanced might return the results in smaller batches. That is, the number of objects returned could be less than `MaxResults`, even if there are still more objects yet to return. If there are more objects to return, Shield Advanced returns a value in `NextToken` that you can use in your next request, to get the next batch of objects.

Type: Integer

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

Required: No

NextToken (p. 56)

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": [
      {
         "HealthCheckIds": [ "string" ],
         "Id": "string",
         "Name": "string",
         "ProtectionArn": "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. 56)

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.

Shield Advanced might return the list of Protection (p. 89) objects in batches smaller than the number specified by MaxResults. If there are more Protection (p. 89) objects to return, Shield Advanced will always also return a `NextToken`.

Type: String

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

Pattern: `^.*$`

Protections (p. 56)

The array of enabled Protection (p. 89) objects.

Type: Array of Protection (p. 89) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

ListResourcesInProtectionGroup

Retrieves the resources that are included in the protection group.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

MaxResults (p. 59)

The maximum number of resource ARN objects to return. If you leave this blank, Shield Advanced returns the first 20 results.

This is a maximum value. Shield Advanced might return the results in smaller batches. That is, the number of objects returned could be less than `MaxResults`, even if there are still more objects yet to return. If there are more objects to return, Shield Advanced returns a value in `NextToken` that you can use in your next request, to get the next batch of objects.

Type: Integer

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

Required: No

NextToken (p. 59)

The next token value from a previous call to `ListResourcesInProtectionGroup`. Pass null if this is the first call.

Type: String

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

Pattern: `^.*$`

Required: No

ProtectionGroupId (p. 59)

The name of the protection group. You use this to identify the protection group in lists and to manage the protection group, for example to update, delete, or describe it.

Type: String

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

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

Required: Yes

Response Syntax

```
{
   "NextToken": "string",
   "ResourceArns": [ "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. 60)

If you specify a value for `MaxResults` and you have more resources in the protection group than the value of MaxResults, AWS Shield Advanced returns this token that you can use in your next request, to get the next batch of objects.

Type: String

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

Pattern: `^.*$`

ResourceArns (p. 60)

The Amazon Resource Names (ARNs) of the resources that are included in the protection group.

Type: Array of strings

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

Pattern: `^arn:aws.*`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

ListTagsForResource

Gets information about AWS tags for a specified Amazon Resource Name (ARN) in AWS Shield.

Request Syntax

```
{
   "ResourceARN": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

ResourceARN (p. 62)

The Amazon Resource Name (ARN) of the resource to get tags for.

Type: String

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

Pattern: `^arn:aws.*`

Required: Yes

Response Syntax

```
{
   "Tags": [ 
      { 
         "Key": "string",
         "Value": "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 (p. 62)

A list of tag key and value pairs associated with the specified resource.

Type: Array of Tag (p. 104) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 109).

InternalErrorException

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

HTTP Status Code: 500

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

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

TagResource

Adds or updates tags for a resource in AWS Shield.

Request Syntax

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

ResourceARN (p. 64)

The Amazon Resource Name (ARN) of the resource that you want to add or update tags for.

Type: String

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

Pattern: `^arn:aws.*`

Required: Yes

Tags (p. 64)

The tags that you want to modify or add to the resource.

Type: Array of Tag (p. 104) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

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. 109).

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. If available, this exception includes details in additional properties.

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

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

UntagResource

Removes tags from a resource in AWS Shield.

Request Syntax

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

ResourceARN (p. 66)

The Amazon Resource Name (ARN) of the resource that you want to remove tags from.

Type: String

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

Pattern: `^arn:aws.*`

Required: Yes

TagKeys (p. 66)

The tag key for each tag that you want to remove from the resource.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 200 items.

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

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. 109).

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. If available, this exception includes details in additional properties.

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

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

UpdateEmergencyContactSettings

Updates the details of the list of email addresses and phone numbers that the Shield Response Team (SRT) can use to contact you if you have proactive engagement enabled, for escalations to the SRT and to initiate proactive customer support.

Request Syntax

```
{
   "EmergencyContactList": [
      {
         "ContactNotes": "string",
         "EmailAddress": "string",
         "PhoneNumber": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

EmergencyContactList (p. 68)

A list of email addresses and phone numbers that the Shield Response Team (SRT) can use to contact you if you have proactive engagement enabled, for escalations to the SRT and to initiate proactive customer support.

If you have proactive engagement enabled, the contact list must include at least one phone number.

Type: Array of EmergencyContact (p. 86) 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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

UpdateProtectionGroup

Updates an existing protection group. A protection group is a grouping of protected resources so they can be handled as a collective. This resource grouping improves the accuracy of detection and reduces false positives.

Request Syntax

```
{
   "Aggregation": "string",
   "Members": [ "string" ],
   "Pattern": "string",
   "ProtectionGroupId": "string",
   "ResourceType": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 107).

The request accepts the following data in JSON format.

Aggregation (p. 70)

Defines how AWS Shield combines resource data for the group in order to detect, mitigate, and report events.

- Sum - Use the total traffic across the group. This is a good choice for most cases. Examples include Elastic IP addresses for EC2 instances that scale manually or automatically.
- Mean - Use the average of the traffic across the group. This is a good choice for resources that share traffic uniformly. Examples include accelerators and load balancers.
- Max - Use the highest traffic from each resource. This is useful for resources that don't share traffic and for resources that share that traffic in a non-uniform way. Examples include Amazon CloudFront distributions and origin resources for CloudFront distributions.

Type: String

Valid Values: `SUM | MEAN | MAX`

Required: Yes

Members (p. 70)

The Amazon Resource Names (ARNs) of the resources to include in the protection group. You must set this when you set `Pattern` to `ARBITRARY` and you must not set it for any other `Pattern` setting.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 10000 items.

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

Pattern: `^arn:aws.*`

Required: No

Pattern (p. 70)

The criteria to use to choose the protected resources for inclusion in the group. You can include all resources that have protections, provide a list of resource Amazon Resource Names (ARNs), or include all resources of a specified resource type.

Type: String

Valid Values: `ALL | ARBITRARY | BY_RESOURCE_TYPE`

Required: Yes

ProtectionGroupId (p. 70)

The name of the protection group. You use this to identify the protection group in lists and to manage the protection group, for example to update, delete, or describe it.

Type: String

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

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

Required: Yes

ResourceType (p. 70)

The resource type to include in the protection group. All protected resources of this type are included in the protection group. You must set this when you set `Pattern` to `BY_RESOURCE_TYPE` and you must not set it for any other `Pattern` setting.

Type: String

Valid Values: `CLOUDFRONT_DISTRIBUTION | ROUTE_53_HOSTED_ZONE | ELASTIC_IP_ALLOCATION | CLASSIC_LOAD_BALANCER | APPLICATION_LOAD_BALANCER | GLOBAL_ACCELERATOR`

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. 109).

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. If available, this exception includes details in additional properties.

HTTP Status Code: 400

OptimisticLockException

Exception that indicates that the resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

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. 107).

The request accepts the following data in JSON format.

AutoRenew (p. 73)

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. 109).

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. If available, this exception includes details in additional properties.

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 resource state has been modified by another client. Retrieve the resource and then retry your request.

HTTP Status Code: 400

ResourceNotFoundException

Exception indicating the specified resource does not exist. If available, this exception includes details in additional properties.

HTTP Status Code: 400

See Also

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

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

Data Types

The AWS Shield Advanced 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. 102) 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 objects that provide details of the AWS Shield event.

For infrastructure layer events (L3 and L4 events) after January 25, 2021, you can view metrics for top contributors in Amazon CloudWatch metrics. For more information, see AWS Shield metrics and alarms in the *AWS WAF Developer Guide*.

Type: Array of AttackProperty (p. 78) 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. 88) 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. 97) objects

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AttackProperty

Details of a AWS Shield event. This is provided as part of an AttackDetail (p. 76).

Contents

AttackLayer

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

For infrastructure layer events (L3 and L4 events) after January 25, 2021, you can view metrics for top contributors in Amazon CloudWatch metrics. For more information, see AWS Shield metrics and alarms in the *AWS WAF Developer Guide*.

Type: String

Valid Values: `NETWORK | APPLICATION`

Required: No

AttackPropertyIdentifier

Defines the AWS Shield event property information that is provided. The `WORDPRESS_PINGBACK_REFLECTOR` and `WORDPRESS_PINGBACK_SOURCE` values are valid only for WordPress reflective pingback events.

Type: String

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

Required: No

TopContributors

Contributor objects for the top five contributors to a Shield event.

Type: Array of Contributor (p. 85) objects

Required: No

Total

The total contributions made to this Shield event by all contributors.

Type: Long

Required: No

Unit

The unit used for the `Contributor` `Value` property.

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 V2
- AWS SDK for Ruby V3

AttackStatisticsDataItem

A single attack statistics data record. This is returned by DescribeAttackStatistics (p. 27) along with a time range indicating the time period that the attack statistics apply to.

Contents

AttackCount

The number of attacks detected during the time period. This is always present, but might be zero.

Type: Long

Required: Yes

AttackVolume

Information about the volume of attacks during the time period. If the accompanying `AttackCount` is zero, this setting might be empty.

Type: AttackVolume (p. 83) object

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

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. 82) 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 V2
- AWS SDK for Ruby V3

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
- HTTP_REFLECTION
- UDS_REFLECTION
- MEMCACHED_REFLECTION

Type: String

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AttackVolume

Information about the volume of attacks during the time period, included in an AttackStatisticsDataItem (p. 80). If the accompanying `AttackCount` in the statistics object is zero, this setting might be empty.

Contents

BitsPerSecond

A statistics object that uses bits per second as the unit. This is included for network level attacks.

Type: AttackVolumeStatistics (p. 84) object

Required: No

PacketsPerSecond

A statistics object that uses packets per second as the unit. This is included for network level attacks.

Type: AttackVolumeStatistics (p. 84) object

Required: No

RequestsPerSecond

A statistics object that uses requests per second as the unit. This is included for application level attacks, and is only available for accounts that are subscribed to Shield Advanced.

Type: AttackVolumeStatistics (p. 84) object

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AttackVolumeStatistics

Statistics objects for the various data types in AttackVolume (p. 83).

Contents

Max

The maximum attack volume observed for the given unit.

Type: Double

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

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. 89) 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 V2
- AWS SDK for Ruby V3

EmergencyContact

Contact information that the SRT can use to contact you if you have proactive engagement enabled, for escalations to the SRT and to initiate proactive customer support.

Contents

ContactNotes

Additional notes regarding the contact.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^[\w\s\.\-,:/()+@]*$`

Required: No

EmailAddress

The email address for the contact.

Type: String

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

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

Required: Yes

PhoneNumber

The phone number for the contact.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 16.

Pattern: `^\+[1-9]\d{1,14}$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

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 V2
- AWS SDK for Ruby V3

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 V2
- AWS SDK for Ruby V3

Protection

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

Contents

HealthCheckIds

The unique identifier (ID) for the Route 53 health check that's associated with the protection.

Type: Array of strings

Required: No

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 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

ProtectionArn

The ARN (Amazon Resource Name) of the protection.

Type: String

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

Pattern: `^arn:aws.*`

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 V2
- AWS SDK for Ruby V3

ProtectionGroup

A grouping of protected resources that you and AWS Shield Advanced can monitor as a collective. This resource grouping improves the accuracy of detection and reduces false positives.

Contents

Aggregation

Defines how AWS Shield combines resource data for the group in order to detect, mitigate, and report events.

- Sum - Use the total traffic across the group. This is a good choice for most cases. Examples include Elastic IP addresses for EC2 instances that scale manually or automatically.
- Mean - Use the average of the traffic across the group. This is a good choice for resources that share traffic uniformly. Examples include accelerators and load balancers.
- Max - Use the highest traffic from each resource. This is useful for resources that don't share traffic and for resources that share that traffic in a non-uniform way. Examples include Amazon CloudFront distributions and origin resources for CloudFront distributions.

Type: String

Valid Values: `SUM | MEAN | MAX`

Required: Yes

Members

The Amazon Resource Names (ARNs) of the resources to include in the protection group. You must set this when you set `Pattern` to `ARBITRARY` and you must not set it for any other `Pattern` setting.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 10000 items.

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

Pattern: `^arn:aws.*`

Required: Yes

Pattern

The criteria to use to choose the protected resources for inclusion in the group. You can include all resources that have protections, provide a list of resource Amazon Resource Names (ARNs), or include all resources of a specified resource type.

Type: String

Valid Values: `ALL | ARBITRARY | BY_RESOURCE_TYPE`

Required: Yes

ProtectionGroupArn

The ARN (Amazon Resource Name) of the protection group.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

ProtectionGroupId

The name of the protection group. You use this to identify the protection group in lists and to manage the protection group, for example to update, delete, or describe it.

Type: String

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

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

Required: Yes

ResourceType

The resource type to include in the protection group. All protected resources of this type are included in the protection group. You must set this when you set `Pattern` to `BY_RESOURCE_TYPE` and you must not set it for any other `Pattern` setting.

Type: String

Valid Values: `CLOUDFRONT_DISTRIBUTION | ROUTE_53_HOSTED_ZONE | ELASTIC_IP_ALLOCATION | CLASSIC_LOAD_BALANCER | APPLICATION_LOAD_BALANCER | GLOBAL_ACCELERATOR`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectionGroupArbitraryPatternLimits

Limits settings on protection groups with arbitrary pattern type.

Contents

MaxMembers

The maximum number of resources you can specify for a single arbitrary pattern in a protection group.

Type: Long

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectionGroupLimits

Limits settings on protection groups for your subscription.

Contents

MaxProtectionGroups

The maximum number of protection groups that you can have at one time.

Type: Long

Required: Yes

PatternTypeLimits

Limits settings by pattern type in the protection groups for your subscription.

Type: ProtectionGroupPatternTypeLimits (p. 95) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectionGroupPatternTypeLimits

Limits settings by pattern type in the protection groups for your subscription.

Contents

ArbitraryPatternLimits

Limits settings on protection groups with arbitrary pattern type.

Type: ProtectionGroupArbitraryPatternLimits (p. 93) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtectionLimits

Limits settings on protections for your subscription.

Contents

ProtectedResourceTypeLimits

The maximum number of resource types that you can specify in a protection.

Type: Array of Limit (p. 87) objects

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SubResourceSummary

The attack information for the specified SubResource.

Contents

AttackVectors

The list of attack types and associated counters.

Type: Array of SummarizedAttackVector (p. 101) objects

Required: No

Counters

The counters that describe the details of the attack.

Type: Array of SummarizedCounter (p. 102) 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 V2
- AWS SDK for Ruby V3

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. 87) objects

Required: No

ProactiveEngagementStatus

If `ENABLED`, the Shield Response Team (SRT) will use email and phone to notify contacts about escalations to the SRT and to initiate proactive customer support.

If `PENDING`, you have requested proactive engagement and the request is pending. The status changes to `ENABLED` when your request is fully processed.

If `DISABLED`, the SRT will not proactively notify contacts about escalations or to initiate proactive customer support.

Type: String

Valid Values: `ENABLED | DISABLED | PENDING`

Required: No

StartTime

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

Type: Timestamp

Required: No

SubscriptionArn

The ARN (Amazon Resource Name) of the subscription.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

SubscriptionLimits

Limits settings for your subscription.

Type: SubscriptionLimits (p. 100) object

Required: Yes

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 V2
- AWS SDK for Ruby V3

SubscriptionLimits

Limits settings for your subscription.

Contents

ProtectionGroupLimits

Limits settings on protection groups for your subscription.

Type: ProtectionGroupLimits (p. 94) object

Required: Yes

ProtectionLimits

Limits settings on protections for your subscription.

Type: ProtectionLimits (p. 96) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

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. 102) 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 V2
- AWS SDK for Ruby V3

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 V2

- AWS SDK for Ruby V3

Tag

A tag associated with an AWS resource. Tags are key:value pairs that you can use to categorize and manage your resources, for purposes like billing or other management. Typically, the tag key represents a category, such as "environment", and the tag value represents a specific value within that category, such as "test," "development," or "production". Or you might set the tag key to "customer" and the value to the customer name or ID. You can specify one or more tags to add to each AWS resource, up to 50 tags for a resource.

Contents

Key

Part of the key:value pair that defines a tag. You can use a tag key to describe a category of information, such as "customer." Tag keys are case-sensitive.

Type: String

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

Required: No

Value

Part of the key:value pair that defines a tag. You can use a tag value to describe a specific value within a category, such as "companyA" or "companyB." Tag values are case-sensitive.

Type: String

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

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

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 V2
- AWS SDK for Ruby V3

ValidationExceptionField

Provides information about a particular parameter passed inside a request that resulted in an exception.

Contents

message

The message describing why the parameter failed validation.

Type: String

Required: Yes

name

The name of the parameter that failed validation.

Type: String

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

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

Action

The action to be performed.

Type: string

Required: Yes

Version

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

Type: string

Required: Yes

X-Amz-Algorithm

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

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

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

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

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

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

Type: string

Required: Conditional

X-Amz-Date

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

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

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

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

Type: string

Required: Conditional

X-Amz-Signature

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

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

Type: string

Required: Conditional

X-Amz-SignedHeaders

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

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

Type: string

Required: Conditional

Common Errors

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

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

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

HTTP Status Code: 500

InvalidAction

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

HTTP Status Code: 400

InvalidClientTokenId

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

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

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

HTTP Status Code: 400

InvalidQueryParameter

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

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

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

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

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

HTTP Status Code: 403

RequestExpired

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

HTTP Status Code: 400

ServiceUnavailable

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

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

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

HTTP Status Code: 400